RUBEN-SANCHEZ-MARIN-TSP.docx

INFORME DE ORIGINALIDAD

12%	11%	2%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	1%
2	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	<1%
3	repositorio.ug.edu.ec Fuente de Internet	<1%
4	www.coursehero.com Fuente de Internet	<1%
5	www.slideshare.net Fuente de Internet	<1%
6	openaccess.uoc.edu Fuente de Internet	<1%
7	repositorio.untels.edu.pe Fuente de Internet	<1%
8	repositorio.uncp.edu.pe Fuente de Internet	<1%
9	riunet.upv.es Fuente de Internet	

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA UNTELS

(Art. 45º de la ley Nº 30220 – Ley)

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (https://repositorio.untels.edu.pe), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10° del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

TIPO DE TRABAJO DE INVESTIGACIÓN

1). TESIS ( ) 2). TRABAJO DE SUFICIENCIA PROFESIONAL (x)

DATOS PERSONALES

Apellidos y Nombres: RUBEN VICTOR SANCHEZ MARIN
D.N.I.: 72875684
Otro Documento:
Nacionalidad: PERUANA
Teléfono: 933107914
e-mail: 2012200140@untels.edu.pe

DATOS ACADÉMICOS

Pregrado

Facultad: FACULTAD DE INGENERÍA Y GESTIÓN
Programa Académico: TRABAJO DE SUFICIENCIA PROFESIONAL
Título Profesional otorgado: INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

Postgrado

Universidad de Procedencia:
País:
Grado Académico otorgado:

Datos de trabajo de investigación

Título: "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD PARA LA DETECCIÓN DE AMENAZAS EN UNA ENTIDAD PÚBLICA DEL SECTOR SALUD"
Fecha de Sustentación: 14 DE DICIEMBRE DEL 2024
Calificación: APROBADO POR UNANIMIDAD
Año de Publicación: 2025

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo _____ No autorizo __X__

2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO ABIERTO 12.1(*)	**info:eu-repo/semantics/openAccess** (Para documentos en acceso abierto)	( )

3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva N° 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO RESTRINGIDO	**info:eu-repo/semantics/restrictedAccess** (Para documentos restringidos)	(x)
	info:eu-repo/semantics/embargoedAccess (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo)	( )
	info:eu-repo/semantics/closedAccess (para documentos confidenciales)	( )

(*) http://renati.sunedu.gob.pe

UNTELS | UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

Rellene la siguiente información si su trabajo de investigación es de acceso restringido:

Atribuciones de acceso restringido:
info:eu-repo/semantics/restrictedAccess

Motivos de la elección del acceso restringido:
El motivo de la restricción se debe a que hay datos de la empresa confidenciales o datos que no deben ser públicos.

SANCHEZ MARIN RUBEN VICTOR
APELLIDOS Y NOMBRES

72875684
DNI

Firma y huella:

Lima, 28 de enero del 20 25

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENERÍA ELECTRÓNICA Y TELECOMUNICACIONES

“IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD PARA LA DETECCIÓN DE AMENAZAS EN UNA ENTIDAD PÚBLICA DEL SECTOR SALUD”

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

SANCHEZ MARIN, RUBEN VICTOR
ORCID: 0009-0006-4829-1662

ASESOR
CAMPOS AGUADO, FREDY
ORCID: 0000-0003-3419-925X

Villa El Salvador
2024

UNIVERSIDAD NACIONAL
TECNOLÓGICA DE LIMA SUR

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

En Villa El Salvador, siendo las 12:00 horas del día 14 de diciembre del año 2024, reunidos en las instalaciones de la UNTELS, los miembros del Jurado Evaluador, integrado por:

PRESIDENTE: **Dr. Santiago Linder Rubiños Jimenez** ORCID N° 0000-0003-0095-6988 Colegiatura N°112655

SECRETARIO: **Mg. José Ambrosio Machuca Mines** ORCID N° 0000-0002-7069-7654 Colegiatura N°158894

VOCAL : **Mg. Pablo Andrés Villegas Chunga** ORCID N° 0009-0004-1623-7173 Colegiatura N°199274

Nombrados por Resolución de Decanato N° 232-2024, de fecha 12 de diciembre 2024, quienes dan inicio a la Sesión Pública de Sustentación del Trabajo de Suficiencia Profesional.

Acto seguido, el aspirante al Título Profesional de **Ingeniero Electrónico y Telecomunicaciones**
Don (ña): **RUBEN VICTOR SANCHEZ MARIN** identificado(a) con D.N.I. N° 72875684; procedió con la Sustentación del Trabajo de Suficiencia Profesional Titulado: **IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD PARA LA DETECCIÓN DE AMENAZAS EN UNA ENTIDAD PÚBLICA DEL SECTOR SALUD**

Autorizado mediante Resolución de Decanato N° 237-2024, de fecha 12 de diciembre de 2024, de conformidad con las disposiciones del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional vigente, sustentó y absolvió las interrogantes que le formularon los señores miembros del Jurado Evaluador.
Concluida la Sustentación se procedió a la evaluación y calificación correspondiente, de acuerdo al **Art. 57°** del Reglamento General para optar el Título Profesional.

CALIFICACIÓN		CONDICIÓN	EQUIVALENCIA
NÚMERO	LETRAS		
16	DIECISEIS	APROBADO POR UNANIMIDAD	BUENO

Siendo las 12:30 HS del día 14 de diciembre del 2024, se dio por concluido el acto de sustentación, firmando el jurado evaluador el Acta de Sustentación y con firma del sustentante en señal de conformidad.

Dr. Santiago Linder Rubiños Jimenez
PRESIDENTE

Mg. José Ambrosio Machuca Mines
SECRETARIO

Mg. Pablo Andrés Villegas Chunga
VOCAL

RUBEN VICTOR SANCHEZ MARIN
SUSTENTANTE

Nota: Artículo 50°. - Para el inicio y desarrollo de la sustentación se requiere la presencia física y permanente de los integrantes del jurado. De faltar algún miembro del jurado, la sustentación procederá con los dos integrantes presentes.
En caso de ausencia del presidente del jurado, ésta será asumida por el jurado de mayor categoría y antigüedad. En caso de ausencia de dos (02) integrantes del jurado, se suspenderá el acto de sustentación, pudiendo reprogramarse dentro de los cinco (05) días hábiles siguientes, sin perjuicio de aplicar el artículo 62° del presente Reglamento.

DEDICATORIA

Dedico este trabajo a mi madre Yolanda Marin por ayudarme y brindarme su apoyo en todo el periodo universitario a mi hermano Giampiere que con su apoyo incondicional supo guiarme en toda la etapa universitaria.

AGRADECIMIENTOS

Agradezco a los docentes de mi casa de estudios UNTELS por las enseñanzas adquiridas a lo largo de mi formación universitaria.

.

ÍNDICE

ÍNDICE iv
ÍNDIDE DE TABLAS vi
ÍNDIDE DE FIGURAS vii
RESUMEN ix
INTRODUCCIÓN x
CAPÍTULO I ASPECTOS GENERALES 12
1.1. Contexto 12
1.2. Delimitación del Proyecto 13
1.2.1. Temporal 13
1.2.2. Espacial 13
1.3. Objetivos 13
1.3.1. Objetivo general 13
1.3.2. Objetivos específicos 13
CAPÍTULO II MARCO TEÓRICO 14
2.1. Antecedentes 14
2.1.1. Antecedentes Nacionales 14
2.1.2 Antecedentes Internacionales 17
2.2. Bases teóricas 18
2.2.1. Centro de Operaciones de Seguridad (SOC) 18
2.2.2. Gestión de información y eventos de seguridad 22
2.2.3. Plataformas de monitoreo 26
2.2.4. Tecnología de gestión de eventos e información de seguridad –SIEM 28
2.2.5. Estándares y normas de seguridad 31
2.2.6. Principios básicos de la seguridad informática 35
2.3. Definición de términos básicos 36
CAPÍTULO III DESARROLLO DEL TRABAJO PROFESIONAL 38
3.1. Determinación y análisis del problema 38
3.2. Modelo de solución propuesto: 41
3.3. Resultados 55
CONCLUSIONES 64
RECOMENDACIONES 65

REFERENCIAS BIBLIOGRÁFICAS 66
ANEXOS 71

ÍNDIDE DE TABLAS

Tabla 1 *Característica recomendadas según el hardware* 45
Tabla 2 *Cumplimiento de pruebas realizadas* 54
Tabla 3 *Eventos del syslog monitoreados por el SIEM en 2024* 60

ÍNDIDE DE FIGURAS

Figura 1 Esquema de funcionamiento de un SOC 22
Figura 2 Comparación entre un IDS e IPS 30
Figura 3 Estructura General del estándar ISO / IEC 27032..... 32
Figura 4 Comparativa entre el NIS CSF y las buenas prácticas COBIT 5..... 33
Figura 5 Estructura del marco NIST v 1.1. 34
Figura 6 Denuncias de ciberseguridad ante la PNP 39
Figura 7 Etapas de implementación de proyecto..... 41
Figura 8 Dispositivos de seguridad utilizando protocolo SNMP..... 42
Figura 9 Monitoreo mediante plataforma Opmanger 43
Figura 10 Configuración en el portal de monitoreo Opmanger 43
Figura 11 Transferencia de transmisión y recepción en la interface ethernet1-1-WAN..... 44
Figura 12 Descarga del software LOG360 45
Figura 13. Descarga del software LOG360 46
Figura 14 Perfil de servidor Syslog..... 47
Figura 15 Interfaz de Configuración de Perfiles de Reenvío de Logs..... 47
Figura 16 Reglas de política de seguridad 48
Figura 17 Topología de sincronización del equipo firewall al servidor SIEM 48
Figura 18 Licencia del SIEM Log360..... 49
Figura 19 Descripción de accesos y roles al SIEM Log360..... 49
Figura 20 Configuración de correos para el envío de notificaciones y alertas..... 50
Figura 21 Configuración de notificaciones del SIEM Log360 51
Figura 22 Alertas registradas del SIEM Log360 51
Figura 23 Configuración de parámetros en el SIEM Log360 52
Figura 24 Configuración de Perfil de Alerta en Log360 para Notificaciones de Ataques..... 53
Figura 25 Comprobación de conectividad mediante comando ping 56
Figura 26 Monitorización del tiempo de actividad y carga del sistema 56
Figura 27 Promedio de uso del CPU durante noviembre del 2024..... 57
Figura 28 Promedio de uso del RAM durante noviembre del 2024 58
Figura 29 Uso de disco en la unidad D..... 59
Figura 30 Detalles de la licencia de ManageEngine EventLog Analyzer 59

Figura 31 Registro de tráfico Syslog en el firewall 60
Figura 32 Tablero de monitoreo Log360 61
Figura 33 Alertas reportadas en la entidad de salud 62
Figura 34 Alertas generada por Palo Alto 63

RESUMEN

En la actualidad las instituciones del estado han incrementado la previsión ante cualquier incidente de ciberseguridad debido al incremento de los ataques en tal sentido existe el Decreto Supremo N° 132-2018-PCM - Estrategia Nacional de Ciberseguridad publicado por la PCM (Presidencia de consejo de ministros) que establece los criterios de seguridad digital en el ámbito nacional (PCM 2018). Esta investigación se enfoca en la puesta en marcha de un SIEM (Security information and event management) en la empresa Smart Global SAC para monitorear la infraestructura de tecnología información de una entidad pública del Perú en rubro de salud.

La empresa realizaba la monitorización de los equipos de infraestructura de sus clientes con una plataforma en base a los protocolos SNMP (Simple Network Management Protocol) y Netflow, los cuales presentaban limitaciones para describir los eventos ocurridos en la infraestructura TI de la entidad por ello que se decidió implementar un SIEM para mejorar la monitorización en tiempo real y prever las respuestas ante cualquier incidente de ciberseguridad seguridad de la infraestructura. Para ello proyecto consistió en el levantamiento de información de infraestructura del cliente, preparación e implementación del sistema, activación de las reglas perimetrales y validaciones del sistema.

Los resultados de la implementación muestran que se mejoró en 60% la seguridad de la infraestructura de la entidad ya que observaban eventos en tiempo real para su posterior mitigación.

INTRODUCCIÓN

En la actualidad, debido a la creciente dependencia de sistemas tecnológicos y al manejo de grandes volúmenes de datos electrónicos sensibles, como los registros médicos y la información personal de los pacientes, la ciberseguridad en el sector salud ha evolucionado como una preocupación importante (Alanazi, 2023). Diversos estudios han señalado que los datos en el sector salud son altamente vulnerables a ciberataques debido a su naturaleza crítica, lo que transforma a este sector en el blanco de los ciberdelincuentes. En el informe de Cervera y Goussens (2024) se destaca un aumento drástico en los ataques cibernéticos, afectando al 90% de las instituciones de salud a nivel mundial, que sufrieron al menos una violación de datos.

A nivel global, los ciberataques generan violaciones de datos que cuestan en promedio $4 millones por incidente. En el sector salud, los ataques de ransomware representan el 54% de los incidentes de ciberseguridad, mientras que el 43% involucra el robo o violación de datos. De estos, el 46% tenía como objetivo acceder a datos de salud (López, 2024). Además, el mercado de la ciberseguridad en el ámbito de la salud está en crecimiento a causa del incremento de las infracciones de datos en el sector. El costo promedio de una infracción de datos en el ámbito de la salud fue de 9,23 millones de dólares en ese mismo año, según el informe Cost of a Data Breach, publicado por IBM en 2021 (Kriptos, 2024).

A nivel nacional, el Perú según el índice Global de Seguridad (GCI) de un total de 165 países ocupa la posición 86 y los sectores más afectados con un 62% son salud, gobierno y minera (Vargas, 2023). Además, una encuesta de EY Perú reveló que el 51% de las empresas experimentaron un incremento en ataques cibernéticos disruptivos desde 2020, lo que evidencia la falta de políticas adecuadas y de una gestión eficiente de riesgos cibernéticos (Mishima, 2021). La Defensoría del pueblo muestra un análisis sobre los ciberdelitos en el Perú donde indicó que según las entidades de investigación en 2021 se registraron 12,827 denuncias de ciberdelitos ante la Policía Nacional del Perú. Las regiones con mayor impacto de ciberdelitos fueron Callao con el 5.2%, Lima con el 53%, Arequipa con

el 5.7%, y La Libertad con el 5% según el informe generado el 2023 por La Defensoría del pueblo (Defensoría del Pueblo, 2023). Diversos factores contribuyen a agravar esta problemática. Uno de los factores es la obsoleta tecnología en entidades del sector salud, que aún dependen de sistemas informáticos desactualizados y sin actualizaciones de seguridad periódicas (Ruiz, 2023). El limitado conocimiento en ciberseguridad por parte del personal del sector salud representa un desafío crítico, ya que es necesario enfrentar amenazas más sofisticadas para proteger la privacidad de los pacientes y la integridad de la atención médica en un contexto digital requieren enfrentar amenazas más sofisticadas. La escasez de profesionales especializados en ciberseguridad dentro del sector salud agrava aún más la vulnerabilidad de las instituciones frente a estos riesgos (Gomero y Sánchez, 2024).

En el contexto de la entidad pública del sector salud en la que se realizó el proyecto, se ha evidenciado una creciente preocupación por los incidentes de ciberseguridad. Además, se identificaron múltiples vulnerabilidades en sus sistemas críticos, las cuales podrían comprometer la protección de los datos de los pacientes y afectar la operatividad del servicio en caso de un ataque, lo que hizo imperativa la implementación de una solución tecnológica especializada en detectar y realizar acciones preventivas. El proyecto buscó reducir los posibles impactos en la infraestructura de la entidad pública como una forma de reducir el tiempo de detección de amenazas, mitigar ataques de ciberdelincuentes por lo cual se realizó la implementación de un SIEM. Como primer paso se realizó las revisiones y el levantamiento de información de todos sus equipamientos, una auditoria de las configuraciones, posteriormente se sincronizó la herramienta SIEM con los dispositivos de seguridad del cliente (Smart Global, 2024).

El desarrollo del trabajo incluye los siguientes capítulos: En el capítulo I se realizó una descripción del contexto de la empresa, se realizó la delimitación del proyecto y se definieron los objetivos del trabajo, en el capítulo II se detalló los antecedentes nacionales e internacionales utilizados como base para este trabajo y se desarrolló las bases teóricas del trabajo y en el capítulo III se realizó el desarrollo del trabajo profesional donde se menciona la implementación del proyecto y los resultados obtenidos.

CAPÍTULO I
ASPECTOS GENERALES

1.1. Contexto

Smart Global SAC se enfoca tanto en brindar servicios de TI y Redes como en ofrecer soluciones a la medida de sus clientes. De este modo, se incluye en todas las fases de sus proyectos como diseño, provisión de soluciones, instalación, monitoreo, administración, operación y soporte. Su equipo de profesionales, altamente capacitados y certificados por sociedades internacionales más reconocidas en el ámbito de equipos y sistemas computacionales, es gran fortaleza porque garantiza un alto nivel de especialización técnica y el uso de ideas creativas en el mercado. Finalmente, cuentan con herramientas que permiten la atención eficiente y demostraciones en tiempo real, logrando así ofrecer un servicio rápido y efectivo (Smart Global, 2024).

La visión es ser reconocidos como una compañía líder en servicios y soluciones buscando la excelencia a través de la innovación, calidad y compromiso (Smart Global, 2024).

La misión Smart Global SAC es transformar las tecnologías de la información en un valor añadido para sus clientes. La empresa se enfoca en ofrecer soluciones tecnológicas innovadoras, eficientes y de calidad alta que resuelvan problemas y generen oportunidades de crecimiento y mejora para sus negocios (Smart Global, 2024).

1.2. Delimitación del Proyecto

1.2.1. Temporal

El proyecto tuvo una duración de 6 meses, iniciando el mes de marzo hasta agosto del año 2024.

1.2.2. Espacial

El proyecto se ejecutó en la empresa Smart Global SAC en el distrito de San Isidro Lima Perú donde se implementó el servidor en el centro de datos de acuerdo a las especificaciones técnicas del fabricante, posterior a ello se realizó la sincronización de los equipos del cliente con el sistema y finalmente la configuración en el SIEM para la monitorización de los equipos en tiempo real.

1.3. Objetivos

1.3.1. Objetivo general

Implementar un sistema de gestión de información y eventos de seguridad (SIEM) para la detección de amenazas e incidente de ciberseguridad para una entidad pública del sector salud.

1.3.2. Objetivos específicos

- Determinar la situación inicial de la infraestructura de la entidad pública y planificar las estrategias adecuadas para minimizar los riesgos informáticos.
- Implementar el sistema SIEM para la detección de amenazas e incidentes en tiempo real.
- Validar la implementación del SIEM para la detección de amenazas e incidentes de ciberseguridad en la infraestructura de la entidad pública del sector de salud.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes

A continuación, se presentan los trabajos previos tanto a nivel internacional e internacional que sustentan lo realizado en el presente trabajo:

2.1.1. Antecedentes Nacionales

Bayona y Palacios (2019) en su estudio sobre la implementación del software Log360 para cumplir 10 del estándar de seguridad de datos para la industria de tarjetas de pago cuyo objetivo fue implementar el software SIEM Log360 para que una entidad bancaria cumpliera con el requerimiento 10 del estándar PCI DSS, enfocándose en mejorar la seguridad y visibilidad de los eventos de la red. La metodología utilizada siguió una adaptación de la metodología PDCA, que incluyó cinco fases: recolección de información mediante un cuestionario, diagnóstico de brechas usando análisis GAP, planificación de la implementación con diagramas de Gantt y matrices RACI, implementación del software, y verificación del cumplimiento de las mejoras. Los resultados mostraron que, tras la implementación, el índice de cumplimiento del requisito 10 aumentó de 69.4% a un nivel significativamente mayor, logrando automatizar los procesos de auditoría de eventos y mejorar la habilidad de identificación de defectos e inconvenientes mediante tecnologías emergentes como inteligencia artificial. En términos de números, se auditó un total de 457 servidores, configurando eventos en tiempo real en 9 controladores de dominio y realizando copias de seguridad de eventos en repositorios centralizados. Asimismo, la automatización y la implementación de tecnologías de vanguardia son esenciales para optimizar la administración de la seguridad. Concluyeron que el banco cumplió eficazmente con el estándar PCI DSS, potenciando así su seguridad interna.

Bermudez (2024) en su “Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones” buscó evaluar el valor de la

ciberseguridad en las entidades. Según sus resultados, el mantenimiento de la integridad, privacidad y disponibilidad de los datos depende del seguimiento de los estándares de seguridad informática. Adoptar medidas de ciberseguridad también parece mejorar la respuesta a incidentes, agilizar la gestión de accesos, impulsar la funcionalidad y lograr así un 25% más de eficiencia operativa. Además, se ha decidido que la formación de los próximos profesionales de las Ciencias de la Información debe tener la ciberseguridad como capacidad fundamental. En conclusión, la protección de datos depende de estándares internacionales como ISO/IEC 27001, por lo que su implementación en las instituciones peruanas aumenta la esperanza en la digitalización.

Vasquez (2023) en su estudio “Implementación de servicio de centro de operaciones de ciberseguridad (CYBERSOC) con plataformas opensource a entidad financiera” pretendía establecer un centro de operaciones de ciberseguridad (CyberSOC) con plataformas de código abierto para prevenir, distinguir, evaluar, monitorizar y gestionar problemas de ciberseguridad. El planteamiento abordó el diseño de la construcción necesaria, el uso de plataformas para controlar las alarmas, el desarrollo de protocolos para la respuesta a incidentes, el análisis forense y la gestión de brechas. Los resultados revelaron que el servicio rectificó el 85% de los incidentes el mismo día en que las 1.200 alertas de seguridad fueron reconocidas y clasificadas como críticas o no. Además, se subrayó la posibilidad que esta opción ofrece a las instituciones financieras con recursos limitados, mejorando así su capacidad para supervisar y gestionar eventos. Se comprobó que el uso de CyberSOC con aplicaciones de acceso abierto ayuda a reducir eficazmente las vulnerabilidades de ciberseguridad, mejorando así la seguridad de la empresa.

Montalván (2020) en su estudio sobre “Actualización de los sistemas Firewall para mejorar la ciberseguridad en la Marina de Guerra del Perú” fortalecieron la ciberseguridad de la Marina de Guerra del Perú mediante la actualización de sus sistemas de cortafuegos, teniendo en cuenta las limitaciones

tecnológicas y los desafíos de seguridad a los que se encontraba la entidad. La metodología incluyó un análisis comparativo de los cortafuegos del mercado usando herramientas como benchmarking, evaluaciones de calidad y diagramas de flujo. Se eligió el firewall Checkpoint 5800 por su potencia, facilidad de uso y buen precio. Los hallazgos mostraron que el tiempo para aplicar las regulaciones de seguridad bajó de 45 minutos a segundos en normas básicas ya unos minutos en las más complejas. El nuevo sistema también permitió conectar hasta 300 usuarios vía VPN, superando ampliamente el límite anterior de 30 usuarios. Además, el nuevo firewall elevó el grado de seguridad al incorporar funciones avanzadas, como el monitoreo del tráfico cifrado SSL y la protección contra vulnerabilidades de día cero. Asimismo, los hallazgos más importantes revelaron que la implementación del firewall Checkpoint no solo mejoró la seguridad, sino que también incrementó la eficiencia operativa y redujo la carga de trabajo del personal técnico. Concluyendo que la necesidad de renovar regularmente las soluciones de ciberseguridad para enfrentar amenazas cada vez más sofisticadas, recomendando la elección de soluciones tecnológicas que equilibren funcionalidad y presupuesto.

Zegarra (2020) en su tesis “Desarrollo de un gestor de notificaciones multiagente para la reducción de los tiempos de diagnóstico y mitigación de fallos en redes IP” cuyo objetivo fue crear un sistema multiagente para el control de notificaciones en redes IP para reducir las fallas y mejorar los tiempos de diagnóstico. La metodología usada consistió en la puesta en marcha de un prototipo operativo basado en el método INGENIAS para el diseño y estudio de sistemas multiagente, empleando el desarrollo de agentes como herramientas proactivas para recolectar y procesar eventos en redes. Los hallazgos indicaron que el sistema propuesto redujo los tiempos de tratamiento y diagnóstico, logrando una disminución del 30% en el tiempo necesario para detectar fallos y del 40% en el tiempo para mitigar fallos en redes inestables. Estos sistemas mejoran la capacidad para responder a fallos en las redes, facilitando una gestión más eficiente y reduciendo la intervención humana. Concluyendo que implementar sistemas

multiagente es efectivo para administrar redes IP, ya que permite detectar errores de forma temprana y resolver problemas.

2.1.2 Antecedentes Internacionales

Manzoor et al. (2024) en su estudio sobre Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs, para medir su eficacia ante ataques cibernéticos y su cumplimiento con regulaciones en entornos de recursos limitados. Las soluciones evaluadas fueron Elastic Security, Wazuh, OSSIM y SIEMonster, probadas mediante simulaciones en redes empresariales de PYME. Se analizaron el procesamiento de eventos por segundo (EPS), la integridad de los registros y las reglas de clasificación. Wazuh destacó con un EPS promedio de 14,000 en pfSense y 10,000 en Snort, seguido de OSSIM y Elastic Security con unos 9,000, y SIEMonster con 7,600. Además, Wazuh obtuvo la mejor calificación en seguridad (47/50), consolidándose como la opción más adecuada para las PYME. Aunque las soluciones de código abierto son rentables y efectivas, requieren mejoras en escalabilidad y en la integración de inteligencia de amenazas avanzadas, por lo que Wazuh se recomienda para fortalecer la ciberseguridad sin sobrepasar las limitaciones presupuestarias.

Ariffin et al. (2022) En su investigación sobre Deployment of Honeypot and SIEM Tools for Cyber Security Education Model In UITM, cuyo objetivo fue proponer y desplegar un modelo de laboratorio de ciberseguridad equipado con herramientas SIEM y honeypot para enriquecer la educación y el progreso en ciberseguridad en la Universiti Teknologi MARA (UiTM). La metodología incluyó una revisión, diseño del modelo, implementación de honeypot y SIEM, pruebas funcionales y una encuesta a estudiantes y docentes. Los resultados mostraron que el honeypot atrajo múltiples intentos de hacking, capturando datos valiosos como IPs, nombres de usuario y contraseñas, mientras que el SIEM procesó y correlacionó datos de amenazas de ataques entrantes y salientes de manera efectiva. De los 50 encuestados, 27 respondieron, de los cuales el 92.6% eran estudiantes y el 59.35% eran de nivel universitario, con el 100% participando en materias de

ciberseguridad. El 90% de los encuestados afirmó que el laboratorio mejoró su experiencia de aprendizaje. La investigación concluye que el modelo de laboratorio es efectivo para la enseñanza de ciberseguridad y sugiere futuras expansiones con datos de otros dispositivos de seguridad como firewalls y servidores de correo electrónico.

Añazco (2021) en su tesis “Sistema de gestión de eventos e información de seguridad (SIEM) de la infraestructura tecnológica de la universidad internacional SEK” cuyo objetivo fue implementar un sistema de Gestión de Eventos e Información de Seguridad (SIEM) mediante la herramienta OSSIM AlienVault para optimizar la ciberseguridad en la infraestructura tecnológica de la Universidad Internacional SEK en Ecuador La metodología consistió en instalar un servidor Linux con OSSIM AlienVault, configurar la aplicación para monitorear incidentes de seguridad y crear scripts en SHELL para analizar datos de rendimiento y posibles amenazas. Los resultados mostraron que la calificación de seguridad de la universidad, evaluada con los 20 controles de CIS, fue baja, con un promedio de 1.34/5, lo cual refleja una implementación insuficiente en aspectos clave de seguridad informática. Aunque la implementación del SIEM es un avance importante, se necesita reforzar los requisitos internos y políticas de seguridad para mejorar su efectividad. Concluyeron que OSSIM AlienVault facilitó el monitoreo de la infraestructura tecnológica, pero también se identificaron carencias en la gestión de inventarios y procesos automatizados de seguridad.

2.2. Bases teóricas

La organización se da a la tarea de implementar un sistema de gestión de eventos e información de seguridad (SIEM) incluyendo los aspectos de ciberseguridad y consulta de eventos en tiempo real. Este sistema permite la supervisión de amenazas activas y mejora así la capacidad para detectar y responder a incidentes en la infraestructura.

2.2.1. Centro de Operaciones de Seguridad (SOC)

a) Definición

Un SOC se encarga de salvaguardar los datos de las entidades. Sus esfuerzos se centran en rastrear, evaluar y detener los peligros en línea que puedan comprometer a la empresa. Salvaguardan sitios web, servidores, bases de datos, aplicaciones, terminales y redes en uso mediante experiencia y soluciones tecnológicas (Oracle, 2020).

El SOC cumple como propósito que posibles incidentes sean identificados, analizados e informados del hecho. Dentro de los especialistas se pueden diferenciar según el nivel y las funciones, en las que se pueden incluir la ingeniería inversa del malware o el criptoanálisis, como se mencionó el centro de servicios de protección puede trabajar en conjunto con otros equipos, como, por ejemplo, el equipo de emergencia cibernética. Si bien implementar y mantener puede generar una inversión considerable, también se puede optar por un SOC externo mediante un proveedor gestionado de servicios (MSP) (Oracle, 2020).

b) Tipos de centros de operación

En la seguridad informática se presentan diversos tipos de centro de operación que pueden variar según su finalidad y los conocimientos para lograr el objetivo asignado, como por ejemplo, se presentan los Centro de Control de Red (NOC) que se enfocan en mantener la red y las comunicaciones funcionando óptimamente, es decir, su responsabilidad es vigilar y resolver posibles averías de tráfico de red, según convenga para que la conectividad y el acceso a internet sean lo más adecuado posible (López, 2021); adicionalmente los Centro de Operaciones de Emergencia (EOC) y los Centro de Operaciones de Amenazas (TOC) facilitan el estudio de nuevas vulnerabilidades y amenazas para una rápida y efectiva respuesta ante crisis. Según la organización, se puede distinguir tres tipos de SOC, como se detalla a continuación (Pérez, 2023):

Distribuido: Presente en aquellas organizaciones que presentan diversas sedes de trabajo, sin embargo, se emplea una única sede para el monitoreo y vigilancia de los servicios, o bien se contrate de los servicios de un proveedor al ser muy pequeña en tamaño.

Mixto: Tipo de organización que cuenta con un SOC, pero no cuenta con el personal especialista para los niveles necesarios, siendo la contratación del servicio de especialistas de más alto nivel para satisfacer las necesidades.

Físico: Presente en aquellos SOC que cuentan con los recursos y personal indispensables para un monitoreo y respuesta de 24x7 al contar con recursos suficientes.

c) Personal del SOC

El personal del centro de mando se puede dividir según el grado de formación y especialización, como se detalla a continuación (Pérez, 2023):

Nivel 1: Analistas que se encargan de monitorear las actividades y enviar las alertas de posibles anomalías en un escenario de incidente.

Nivel 2: Especialistas que cumplen la función de auditar un incidente para establecer los datos y servicios comprometidos en el incidente para dar una respuesta.

Nivel 3: Personal de mayor calificación y cumple como función resolver los incidentes y presentar planes de mejora para prevenir futuros incidentes.

Es necesario precisar que para el éxito de un SOC, se debe buscar la cohesión en el equipo de trabajo, sin importar el nivel del trabajador, pues la comunicación y el aprendizaje son factores importantes dentro de todo el equipo para el monitoreo, detección y mitigación en escenarios que afecten la actividad.

d) Funciones del SOC

El SOC cumple como función el monitoreo, respuesta a incidentes y entrega de analíticas, sin embargo, es necesario implementar controles avanzados para garantizar la adaptabilidad a los desafíos emergentes, como por ejemplo, las amenazas complejas y direccionales, por lo que es fundamental que se cumpla con funciones claves a partir de herramientas de análisis, detección y remediación robusta (Rico, 2021).

Automatización en detección y respuesta: Mediante el uso de herramientas de análisis de tráfico de detección y respuesta en el punto final y redes, se analiza los flujos de trabajo que puede servir para abarcar labores de investigación y detección ante incidentes, siendo fundamental en puntos finales de la red para garantizar el diagnóstico de amenazas de alto riesgo y tomar acciones oportunas. La automatización de esta actividad favorece en reducir la carga de trabajo y hacer una tarea más eficiente durante la detección.

Proactividad: El incremento de ataques debido a operaciones remotas, por lo que las solicitudes, conexiones y tráfico no se encuentran centralizadas, en ese sentido, se debe revisar distintos puntos para el análisis de vulnerabilidad de cada situación, pues desde equipos finales se pueden acceder a usuarios y redes.

Búsqueda de amenazas complejas: Actualmente, las amenazas se enfocan en atacar objetivos específicos para generar daños sustanciales, por lo que una de sus funciones es proveer la capacidad de monitoreo para impedir el ingreso de algún tipo de amenazas y, en caso haya ocurrido, mediante herramientas asegurar la erradicación total del código malicioso.

Fuente de conocimiento: La base funcional de un SOC es la inteligencia pues de este modo, permite nutrir de conocimiento a los integrantes del equipo para fomentar el conocimiento y una actualización constante en seguridad informática.

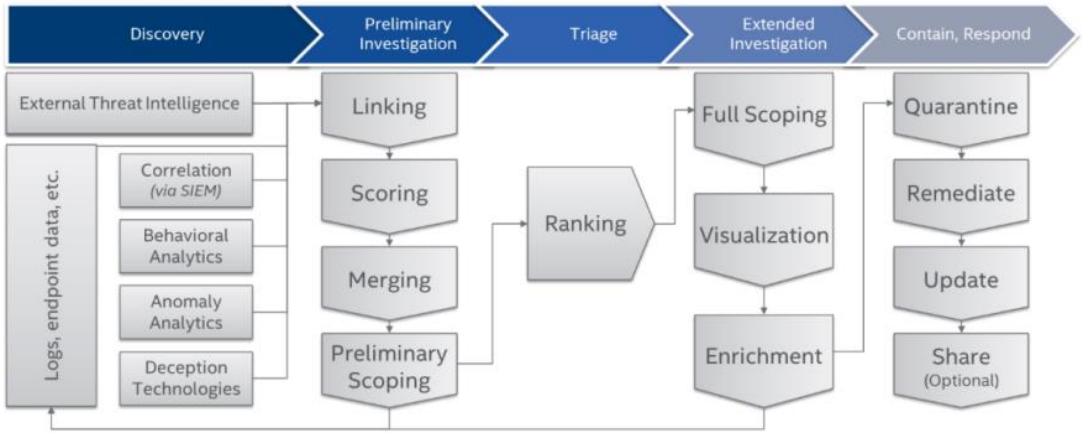
Remediación: Posterior a la materialización de un incidente, se debe establecer acciones para la reanudación de servicios de modo efectivo, veloz y eficaz para minimizar las perdidas, pues las amenazas evolucionan, por lo que se debe invertir en acciones de respuesta y herramientas que facilite la remediación.

Reducir brechas: Como función principal, se tiene el reducir las brechas en controles, ya que no existen dos infraestructuras de TI iguales, dado ello el SOC busca realizar planes de mejoras para minimizar el nivel de madurez en controles.

El SOC tiene como función la detección, prevención y mejora. En la figura 1 se muestra el esquema de funcionamiento de un SOC (Martínez, 2021):

Figura 1

Esquema de funcionamiento de un SOC



Nota. Adaptado de *implementación de un SOC de código abierto con elementos de red para sistemas industriales*, Martínez, 2021.

e) Herramientas de monitorización del SOC

La proliferación de herramientas de monitorización, es una tendencia creciente en organizaciones cuando se requiere mejorar la detección y respuesta ante incidentes cibernéticos, pero hay que considerar el pago por mantenimiento y licencias de las diversas herramientas adquiridas, siendo un factor limitante en software de gestión a utilizar. Sin embargo, las herramientas para la monitorización son importantes para la detección de amenazas, pues constantemente surgen nuevas tendencias de ataques que dejan obsoletas las tecnológicas que probablemente se usen en una organización, ante ello se despliega actualizaciones o mejora de versiones para el correcto funcionamiento (It Digital Security, 2021).

2.2.2. Gestión de información y eventos de seguridad

a) Definición de un SIEM

Una infraestructura gestionada que genera eventos, un SIEM puede recopilar, agregar, almacenar y correlacionar. La plataforma principal de los centros de operaciones de seguridad contemporáneos, recopilan eventos de diversos sensores (como sistemas de detección de intrusiones, antivirus y cortafuegos), los correlacionan y generan vistas de alertas sintéticas para la elaboración de informes de seguridad y la gestión de amenazas. Los sistemas de información de seguridad y gestión de eventos (SIEM) se han

desarrollado para ayudar a los administradores en el desarrollo de políticas de seguridad y la administración de eventos de una variedad de fuentes. En general, un SIEM fundamental se compone de unidades autónomas que pueden interactuar independientemente unas de otras; sin embargo, no podrán funcionar sin la colaboración de todas ellas (SIEM, 2023).

b) Clasificación de un SIEM

Existen herramientas basadas en el sistema SIEM para mejorar la seguridad y la velocidad de reacción ante problemas de seguridad en una institución determinada. Entre los sistemas SIEM más utilizados en el entorno corporativo se encuentran (PURESTORAGE, 2024):

IBM Security QRadar

El objetivo de aumentar la eficiencia y facilitar el trabajo de los analistas de seguridad a lo largo de todo el ciclo de vida de los incidentes, IBM QRadar® Suite es un sistema integral de detección y respuesta a amenazas que, mediante el uso de inteligencia artificial y automatización, aumenta la productividad de los analistas y ayuda así a operar a los equipos de seguridad con recursos limitados (IBM, 2024). Gracias a sus más de 400 módulos, este sistema SIEM se encuentra entre los más completos capaces de gestionar millones de eventos diarios. Esta tecnología proporciona soluciones inteligentes que permiten al personal de seguridad reaccionar de inmediato para detener o disminuir la gravedad de los eventos.

McAfee Enterprise Security Manager

La herramienta SIEM de McAfee, empresa líder en seguridad, permite a los usuarios vigilar sus sistemas para que puedan recopilar, examinar y cotejar los eventos de seguridad con una base de datos exhaustiva de datos documentados para localizar con eficacia las vulnerabilidades. La base de la seguridad más eficaz es el conocimiento en tiempo real de la actividad de todos los sistemas, redes, bases de datos y aplicaciones. Basada en McAfee® Enterprise Security Manager, que ofrece la velocidad y el alcance necesarios para que las organizaciones de seguridad identifiquen, comprendan y respondan a las amenazas ocultas, así como conocimiento de la situación e inteligencia de procesos en tiempo real, la familia de soluciones McAfee Security Information and Event Management (SIEM) es

McAfee, 2023 También comprende una estructura de cumplimiento destinada a simplificar la adhesión (McAfee, 2023).

LogRhythm

El sistema SIEM autogestionado LogRhythm descubre y corrige eventos de forma rápida y asequible. Es rápido y sencillo, lo que ayuda a seguir las normas, detectar peligros y reducir los ataques. Diseñada para pequeñas empresas que no pueden adquirir tecnologías más sofisticadas, esta solución SIEM aborda (LogRhythm, 2024).

c) Componentes de un sistema SIEM

Un sistema SIEM es un conjunto de componentes vinculados que trabajan juntos para proteger el entorno informático de una entidad determinada. Estos elementos comprenden (Equipo de Imagina, 2024):

- **Recolección de datos:** La primera fase del proceso es en la que el sistema SIEM recopila datos de varias fuentes, incluyendo entre otros dispositivos de red, logs de servidor, apps, entre otros.
- **Correlación de eventos:** La correlación de eventos es el análisis que realiza el SIEM de los datos recopilados con el objetivo de identificar tendencias de comportamiento. Este estudio permite identificar peligros probables que, tomados en solitario, pasarían desapercibidos.
- **Alertas y notificaciones:** El SIEM envía alertas en tiempo real cuando se detecta un comportamiento irregular, lo que permite a los equipos de seguridad actuar con rapidez.
- **Almacenamiento seguro:** Los datos recopilados por SIEM se guardan de forma segura para su posterior examen, lo que facilita la realización de auditorías exhaustivas en caso de incidente.

d) Funcionamiento de un SIEM

En el funcionamiento se considera dos tecnologías principales la gestión de incidentes de seguridad (SEM) y la gestión de datos de seguridad (SIM), un sistema de gestión de eventos e información de seguridad (SIEM) es una sofisticada solución de ciberseguridad. Además de recopilar y evaluar registros de eventos, su objetivo es salvaguardar los sistemas de una entidad permitiendo así la detección de amenazas en tiempo real. El SIEM permite responder rápidamente a los incidentes y ayuda a prevenir futuros problemas detectando tendencias extrañas. Agrupa todos los datos en una

base de datos para que se puedan realizar juicios basados en hechos (AMBIT TEAM, 2021).

Este estudio ayuda a separar los falsos positivos de los sucesos reales, aliviando así la carga del personal informático y acelerando la resolución de problemas importantes. Al registrar cada paso del proceso de detección y respuesta, crear alertas automáticas y seguir las políticas de seguridad de datos, los sistemas SIEM proporcionan una supervisión centralizada y una rápida resolución de incidentes. Esto aumenta la eficiencia del equipo y reduce los tiempos de respuesta (AMBIT TEAM, 2021).

2.2.3. Plataformas de monitoreo

a) IDS

Un sistema de detección de intrusos (IDS) es una aplicación informática diseñada para identificar accesos ilegales a ordenadores o redes. Compara el tráfico entrante con una base de datos actualizada de firmas de ataque conocidas. Si surgen actividades sospechosas, alerta a los gestores del sistema para que puedan responder como sea necesario. Estos accesos pueden ser ataques intermitentes de usuarios hostiles, desencadenados por herramientas automatizadas o recurrentes. Estos sistemas no pretenden minimizar la intrusión, sino detectar los accesos inusuales mediante indicios precoces de posible intrusión. Se comportan de forma reactiva (INCIBE, 2024).

Las principales ventajas de un sistema IDS son su capacidad para buscar automáticamente paquetes de datos enviados a través de la red y supervisar la red en tiempo real utilizando los conocimientos que ha adquirido, por lo que detecta cambios en los documentos. Su mayor desventaja es que estos instrumentos -especialmente los pasivos- no están pensados para detener los ataques que encuentran. Además, la herramienta es vulnerable a los ataques DDoS, que quedarían inutilizados (INCIBE, 2024).

b) IPS

Un sistema de prevención de intrusiones (IPS) es un tipo de software destinado a proteger los sistemas contra invasiones y ataques. Se trata de una acción profiláctica. Estas tecnologías examinan las conexiones y los protocolos en tiempo real para determinar si un evento está en desarrollo o a punto de llegar. Pueden controlar el acceso a la red y detectar asaltos mediante tendencias, desviaciones o actividades sospechosas. Basándose en el contenido del tráfico rastreado, el IPS puede crear políticas que incluyen la capacidad de desconectar conexiones, descartar paquetes y establecer alarmas (INCIBE, 2024).

A menudo asociados a cortafuegos y sistemas de Gestión Unificada de Amenazas (UTM), los productos mixtos que ofrecen varios proveedores -a menudo denominados IPS/IDS- permiten un control de acceso basado en reglas sobre los protocolos y sobre el destino u origen del tráfico. Aunque esto último puede limitar la escalabilidad, es decir, la capacidad de ampliar

y gestionar muchos dispositivos en la red; y la protección preventiva, al detectar automáticamente comportamientos anómalos mediante reglas, los sistemas IPS ofrecen varias ventajas, entre ellas la facilidad de instalación, configuración y administración gracias a las configuraciones predefinidas y la gestión centralizada. Además, proporcionan defensa contra varios tipos de ataques, como infecciones de malware, cambios en el sistema de archivos, ataques de fuerza bruta e intrusiones, por lo que mejoran la seguridad y la eficacia a la hora de detener intrusiones en la red o ataques a archivos. Sin embargo, también tienen inconvenientes, como el peligro de falsos positivos que pueden desencadenar reacciones negativas como un aislamiento deficiente de la máquina o la vulnerabilidad a ataques de denegación de servicio (DoS o DDoS) que harían que las máquinas no sirvieran para nada (INCIBE, 2024).

c) SIEM

Compuesta por la gestión de la información de seguridad (SIM) y la gestión de eventos (Security Event Manager), la gestión de eventos e información de seguridad (SIEM) es una solución híbrida centralizada. La generación de alertas de seguridad en tiempo real por parte de varios dispositivos de hardware y software de la red se analiza en la tecnología SIEM. Se trata de una herramienta que centraliza los datos y se conecta con otros sistemas de detección de amenazas para identificar eventos de seguridad, como comportamientos extraños o sospechosos que pueden dar lugar a un incidente. Crea respuestas adecuadas a partir de los informes y evaluaciones que registra y desecha los resultados aberrantes -también conocidos como falsos positivos-INCIBE, 2024. También enlaza varios sistemas agregando registros de actividad de muchas fuentes.

La centralización de la información y los eventos es uno de los beneficios de un SIEM, ya que establece un punto de referencia unificado. La centralización permite la automatización de tareas, lo que a su vez reduce tiempo y costes. Además, permite la monitorización de eventos para identificar anomalías de seguridad o visualizar datos históricos a lo largo del tiempo. Además, los sistemas SIEM notifican a los administradores la existencia de vulnerabilidades y si están siendo explotadas en ataques (INCIBE, 2024)

Los inconvenientes de los sistemas SIEM mantenidos por un departamento interno incluyen una larga curva de aprendizaje, altos costes de implementación y una integración limitada con el resto del sistema, como resultado de la necesidad de formar al personal interno para esta tarea. La externalización de esta tarea conlleva una pérdida de control sobre la información generada o un acceso restringido a determinada información, así como fatiga como consecuencia del elevado volumen de notificaciones recibidas. El proveedor de servicios puede gestionar estos aspectos mediante acuerdos de nivel de servicio (SLA) (INCIBE, 2024).

2.2.4. Tecnología de gestión de eventos e información de seguridad –SIEM

Los beneficios y características que presenta son (IBM, 2020):

Integración con diversos productos.

Gestión del flujo de trabajo en las alertas mediante cuadros de mando personalizados.

Agregación en un único punto diversas fuentes de datos.

El funcionamiento de un SIEM es según los niveles, teniendo en el nivel básico funciones de clasificación, agregación y consolidación de datos para la identificación de amenazas y el cumplimiento de requisitos de cumplimiento de datos. Ahora bien, a medida que crece una organización se requiere adoptar mayores funciones teniendo las que se detallan a continuación (IBM, 2020):

Agregación de datos: Un SIEM requiere que múltiples fuentes de datos sean trasladadas a un solo lugar de procesamiento de información, por ello se recogen los registros SIEM de varios sistemas.

Colectores SIEM: Permiten una configuración que registre los equipos conectados a la red, permitiendo un enlace directo al sistema y la obtención de registros.

Transmisores SIEM: Los SIEM Forwaders permiten el envío de datos a la herramienta SIEM a partir de equipos, por lo que se requiere instalar un software para que los equipos puedan enviar información de eventos al SIEM.

Correlación y análisis de eventos: Es fundamental para comprender y analizar patrones de datos, pues proporciona información de donde localizar y mitigar las amenazas. Las soluciones SIEM influyen considerablemente en

el Tiempo Medio de Recuperación (MTTR) y Tiempo Medio de Detección (MTTD).

Supervisión de incidentes y alertas de seguridad: Al contar con una administración única y con infraestructura local que utiliza la nube, la herramienta SIEM permite la identificación de entidades cercanas de TI, ya que monitorea los dispositivos, aplicaciones y usuarios conectados que se conectan a la red, permitiendo la identificación de comportamiento anormal, siendo esto mediante la regla de correlación predefinida y personalizada por parte de la administración como medida de seguridad.

a) Software de monitorización de seguridad

El SIEM proporciona el control de la red recopilando datos para el análisis de flujos de tráfico básico, por lo que se requiere la monitorización de la seguridad de la red para evitar explotaciones de los activos importantes, pero se requiere el conocimiento de elementos adicionales que aseguren un monitoreo de la seguridad de la red, siendo los que se detallan a continuación:

Cortafuegos: Mecanismo que supervisa la red saliente y entrante con el fin de bloquear los paquetes de datos según un grupo de reglas preestablecidas.

Sistema de detección de intrusos (IDS): Herramienta empleada para reconocer accesos no autorizados a la red o algún ordenador mediante el monitoreo del tráfico entrante que se coteja con una base de información actualizada de firma de ataques reconocidos o explorados. Los IDS permiten la alerta anticipada de posibles intrusos, más no establece una acción para mitigar el efecto (Cabrera, 2021).

Sistema de prevención de intrusiones (IPS): Programa que sirve para la protección ante sistemas que ataquen, pues analiza en tiempo real las protocolos y conexiones para establecer la materialización de un incidente, por lo que su función es vital para identificar sospechosos, patrones de ataques, anomalías desde el análisis en el control de acceso a la red (Gómez et al., 2023).

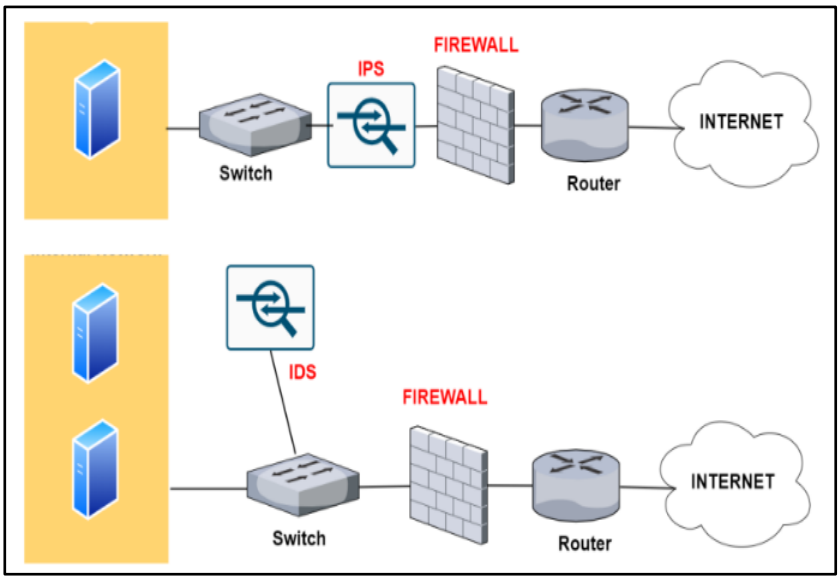
Proxy de navegación: Tecnología utilizada para traducir el tráfico entre protocolos o redes mediante un servidor intermediario que divide a los usuarios de los destinos por la navegación, su importancia es ofrecer una

diversidad en los niveles de inspección de seguridad, privacidad y red según las necesidades, políticas o tráfico de la organización (Avast, 2024).

Sondas: Una sonda cumple como función monitorear la red y facilitar la detección de comportamientos malintencionados de programas, basándose en el análisis de la red en tiempo real con reglas de decisión. Se crea una copia de la red que se necesita analizar, que generalmente son redes críticas, para que funcione correctamente (Harris, 2024). A continuación, en la figura 2 se muestra la comparativa entre un IDS e IPS.

Figura 2

Comparación entre un IDS e IPS



Nota. Comparativa de IDS e IPS. Adaptado de Comparación y diferencias entre IPS vs IDS vs Firewall vs WAF, Shophu, 2019.

b) Servidor Syslog

El protocolo de registro del sistema (Syslog) es un método por el cual los dispositivos de red pueden transmitir datos a un servidor de registro en un formato de mensaje estándar. Fue creado para facilitar la supervisión de los dispositivos de red. Estos dispositivos pueden usar un agente Syslog para enviar mensajes de notificación en diversas situaciones específicas (Progress, 2022).

Los mensajes de registro contienen información detallada sobre el evento, como un ID de dispositivo (incluyendo la dirección IP), una clasificación de gravedad y una marca de tiempo. Syslog tiene limitaciones, pero es muy común gracias a su fácil flexibilidad e implementación y permite la

supervisión de casi cualquier dispositivo de red a través de varias soluciones propietarias. (Progress, 2022).

c) Mensajes de Syslog

El Protocolo de Datagramas de Usuario (UDP) utiliza el puerto 514 para enviar mensajes Syslog. Una desventaja de UDP es que no garantiza la entrega ni el acuse de recibo de los mensajes porque es un protocolo sin conexión. Sin embargo, esta característica facilita la gestión del sistema y reduce la complejidad. Aunque es común que los mensajes Syslog estén en un formato entendible para humanos, no es necesario. Cada mensaje tiene un encabezado con un nivel de prioridad que combina un grado de severidad y una identificación del proceso del dispositivo que generó el mensaje. El sistema UNIX es el origen de los códigos de proceso, también conocidos como "facilidades". Los niveles de severidad oscilan entre 0, que indica una emergencia, y 7, que corresponde a mensajes de diagnóstico y depuración, pasando por niveles intermedios como 6 para mensajes informativos y 1 para atención inmediata (Progress, 2022).

d) Recopilación y gestión de datos

El software debe incluir funciones de gestión y filtrado para que el servidor pueda generar notificaciones, alarmas y alertas de forma automática. El filtrado permite que el administrador acceda fácilmente a registros específicos, como los de un cortafuego, en un periodo concreto. Cualquier desviación del procedimiento estándar puede ser reportada al administrador mediante ventanas emergentes o mensajes de texto. (Progress, 2022).

2.2.5. Estándares y normas de seguridad

a) Normativa ISO/IEC 27001

Estándar internacional que garantiza la confidencialidad, integridad y disponibilidad de los datos y los sistemas que los manejan. Ayuda a las organizaciones a gestionar riesgos de seguridad aplicando controles para mitigarlos o eliminarlos. En su versión 2022, el estándar brinda guías para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), comenzando con el análisis del contexto organizacional para identificar las necesidades de las partes interesadas y definir el alcance del SGSI (EGSInnova Group, 2022).

a) Normativa ISO/IEC 27032

Marco que ofrece técnicas de seguridad en el contexto de ciberseguridad, ya que se centra en características técnicas y otros de protección en internet, redes, información y la preservación de la infraestructura critica para la información. La norma no es certificable, ya que es una directriz de buenas prácticas para la gestión de la ciberseguridad que permite la reducción de riesgos mediante controles, la estructura general de la ISO/IEC 27032. A continuación, en la figura 3 se muestra la estructura general del estándar ISO/IEC 7032 (Cárdenas et al., 2017).

Figura 3

Estructura General del estándar ISO / IEC 27032

Nota. Estructura de la norma ISO/IEC 27032. Adaptado de *Directrices para la administración de ciberseguridad utilizando ISO / IEC 27032*, Parra et al., 2017.

b) CIS Critical Security Controls (CSC)

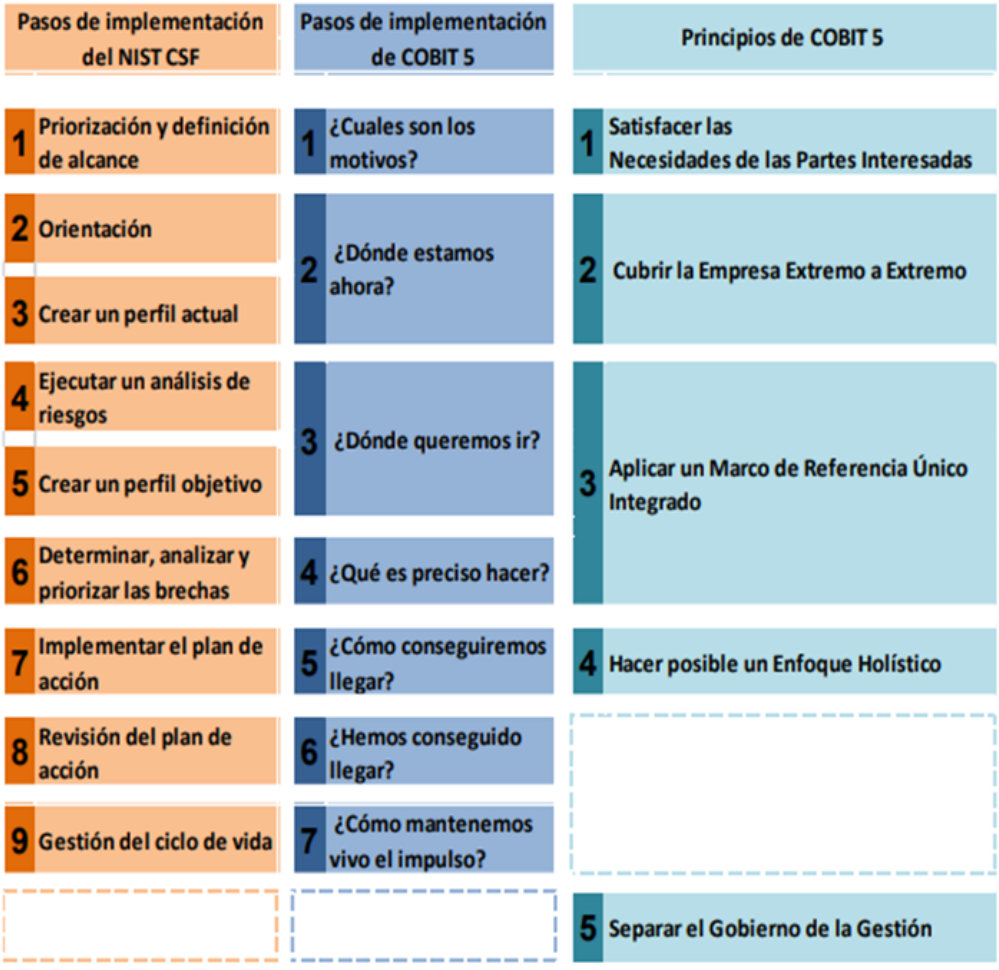
Entidad sin fines de lucro fundada por expertos y voluntarios que tiene como objetivo la búsqueda de medidas que solucionen la ciberseguridad, las cuales puedan aplicarse cualquier organización sin importar el tamaño o rubro, actualmente se encuentra en la séptima versión que establece un conjunto de buenas prácticas para la disminución de ataques contra la infraestructura informática, por lo general el marco CIS es una normal adicional que puede coexistir con otros estándares (Gutiérrez, 2020).

c) COBIT 5

El documento es una guía técnica para la gestión de TI, diseñada para servir como modelo de gobernanza de TI, el control de objetivos, y los marcos y mapas de auditoría. ISACA creó esta guía de mejores prácticas que sirve como referencia para la optimización de la tecnología, el cumplimiento normativo y la reducción de costos. Facilita el cumplimiento de las leyes, optimiza el uso de la tecnología a un costo más bajo y ayuda a gestionar los nuevos tipos de tecnologías de la información (Castillo, 2018). A continuación se muestra la comparativa según diferentes normas de ciberseguridad en la figura 4 (Castaño, 2018):

Figura 4

Comparativa entre el NIS CSF y las buenas prácticas COBIT 5



Nota. Pasos de implementación del NST CSF, COBIT 5 y COBIT 5. Adaptado de *Implementing the NIST Cibersecurity Framework*, ISACA, 2014.

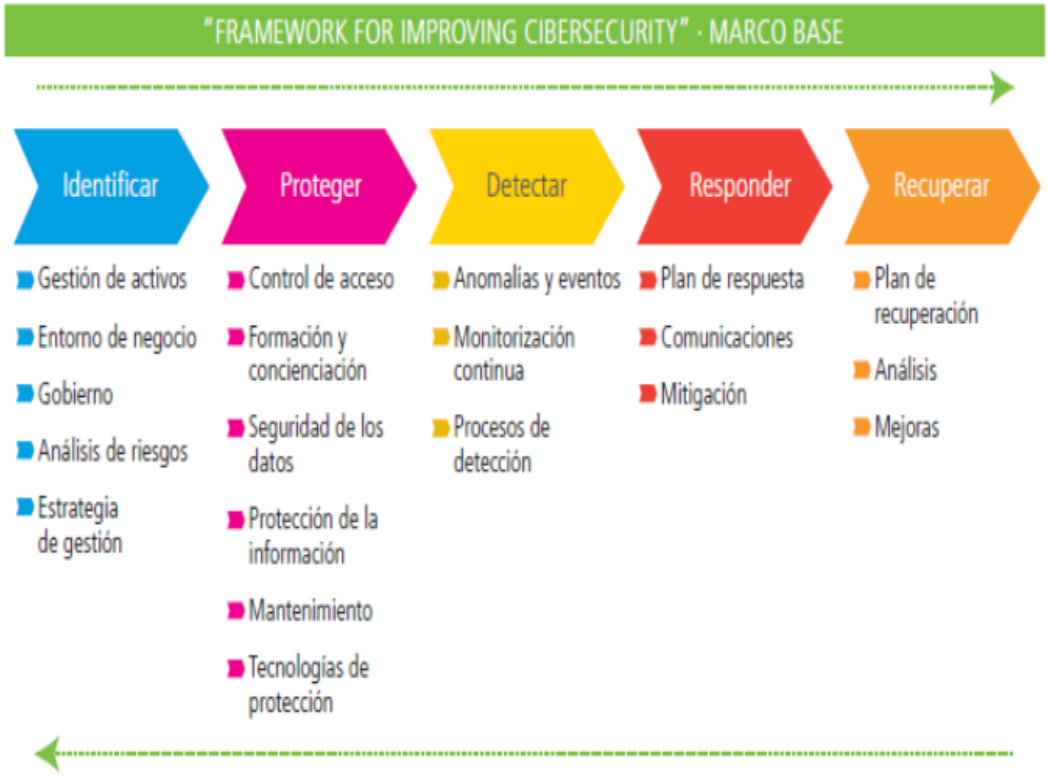
d) NIST v 1.1

El marco ofrece un vocabulario compartido para comprender, controlar y comunicar los riesgos de ciberseguridad. Sirve de plataforma que aúna enfoques tecnológicos, empresariales y políticos para controlar estos peligros, permitiendo así priorizar e identificar los pasos para reducirlos. Además, es aplicable a la gestión de riesgos en toda la empresa o se concentra en salvaguardar servicios importantes en sectores particulares (Parra y Yaqueline, 2018).

NIST v 1.1 permite desarrollar perfiles comunes, que es relevante para una serie de entidades, incluidas instituciones de coordinación sectorial, asociaciones y organizaciones. De carácter práctico, consta de una estructura básica que abarca cinco propósitos principales junto con niveles de implementación y perfiles de aplicación. A continuación, se presentan las cinco fases del marco (Parra & Yaqueline, 2018).

Figura 5

Estructura del marco NIST v 1.1.



Nota. Fases del NIST. Adaptado de *implementación del marco de trabajo para la ciberseguridad NIST CSF desde la perspectiva de Cobit 5*, Castaño, 2018.

2.2.6. Principios básicos de la seguridad informática

a) Confidencialidad

Busca proteger los datos de forma que sólo los usuarios autorizados puedan ver determinada información. Utilizar métodos de encriptación que salvaguarden los datos tanto en tránsito como en almacenamiento ayudará a alcanzar este objetivo y garantizará que sólo aquellos con autorización vean la información. Las contraseñas seguras, que incluyan letras, números y símbolos, también deben evitar palabras comunes o información personal. Por último, implementar la autenticación de dos factores: además de la contraseña, se requiere un segundo código, restringiendo así el acceso de intrusos (Universidad Autónoma del Perú, 2024).

b) Disponibilidad

Se refiere a sistemas y datos que están disponibles cuando se necesitan. Los datos y servicios deben estar siempre accesibles para los usuarios autorizados sin interrupción. El mantenimiento regular de los sistemas, incluyendo actualizaciones de software, aplicación de parches de seguridad, evaluación de hardware, ayuda a garantizar que los sistemas operen según lo previsto evitando fallas imprevistas (Universidad Autónoma del Perú, 2024).

c) Integridad

La integridad es la garantía de que el material es completo y correcto, así como que no ha sido alterado sin permiso. Esto sugiere que los cambios -que deben ser cuidadosamente registrados- sólo pueden ser realizados por personal autorizado. Los controles de acceso ayudan a proteger la integridad de los datos limitando el acceso en función de las funciones y responsabilidades de los usuarios, garantizando así que sólo puedan realizar sus tareas quienes realmente las necesitan. Esto reduce la posibilidad de cambios ilegales (Universidad Autónoma del Perú, 2024).

d) Autenticación

Procedimiento para confirmar la identificación de una persona o dispositivo antes de otorgar acceso al sistema o a la información. Una de las técnicas más utilizadas es la de contraseña. Para evitar accesos no deseados, es fundamental establecer contraseñas seguras y distintas para cada cuenta y actualizarlas con frecuencia. Las contraseñas deben ser complicadas,

incluyendo símbolos, letras y números, y no deben ser fáciles de adivinar Universidad Autónoma del Perú, 2024.

e) No repudio

El no repudio garantiza que alguien no pueda rechazar posteriormente haber participado en una acción dentro de un sistema. Esto es fundamental en las transacciones y comunicaciones digitales ya que asegura que las acciones puedan ser vinculadas a un individuo en particular (Universidad Autónoma del Perú, 2024).

f) Evaluación de riesgos

Implica la identificación, análisis y evaluación de los riesgos para la seguridad de la información. Las organizaciones pueden asignar más eficazmente los recursos y priorizar las medidas de seguridad mediante el uso de una evaluación eficaz (Universidad Autónoma del Perú, 2024).

g) Autorización

Proceso de verificación si un individuo tiene permiso para hacer algo específico. Después de que el usuario se autentica, el sistema revisa si tiene los derechos necesarios para acceder a ciertos recursos o realizar ciertas acciones (Universidad Autónoma del Perú, 2024).

2.3. Definición de términos básicos

- **Análisis de amenazas (Threat Analytics):** Proceso de evaluación y comprensión de los riesgos de seguridad a través de la recolección y estudio de información acerca de amenazas (Villayzan y Gutierrez, 2020).
- **Content-ID:** Tecnología utilizada para identificar y controlar el contenido que circula a través de una red, basado en patrones y firmas de datos (Bechtel, 2019).
- **Firewall de NFGW (Next-Generation Firewall):** Firewall que incorpora funciones avanzadas como inspección profunda de paquetes y control de aplicaciones (Liang y Kim, 2022).
- **IDS (Intrusion Detection System):** Sistema que monitorea una red para identificar actividades sospechosas o no autorizadas (Abdulganiyu et al., 2023).

- **Incidentes de ciberseguridad:** Eventos que afectan negativamente la confidencialidad, integridad o disponibilidad de la información (Santolaria, 2022).
- **IPS (Intrusion Prevention System):** Sistema que detecta y previene actividades maliciosas en una red (Coulibaly, 2020).
- **Optimizador de ancho de banda:** Herramienta que gestiona y distribuye eficientemente el tráfico de red para maximizar el uso del ancho de banda disponible (Serra y López, 2020).
- **Spyware:** Software malicioso diseñado para recopilar información de un sistema sin el consentimiento del usuario (Pierazzi et al., 2020).
- **Syslog:** Protocolo estándar utilizado para el registro de eventos y mensajes generados por dispositivos de red y sistemas de software (Zhou et al., 2022).
- **User-ID:** Funcionalidad que permite asociar el tráfico de red con usuarios específicos para una gestión más precisa de la seguridad (Zeng, 2021).
- **Vulnerabilidad:** Debilidad en un sistema de información que puede ser explotada para comprometer la seguridad (Bernárdez, 2022).

CAPÍTULO III
DESARROLLO DEL TRABAJO PROFESIONAL

3.1. Determinación y análisis del problema

La protección de la infraestructura tecnológica y la información sensible en las entidades públicas es una prioridad en el contexto actual de la ciberseguridad. En el sector salud, el impacto de estas amenazas es especialmente crítico, ya que afecta no solo la privacidad de los pacientes, sino también la operatividad de los sistemas que sostienen la atención médica, lo que podría tener graves consecuencias para la salud de la población (Cando & Medina, 2021).

Aranda (2018) señala que América Latina alberga una diversa gama de delitos cibernéticos. Uno de ellos es el reciente robo de aproximadamente 10 millones de dólares a una institución financiera en Chile. Dicho desfalco podría haberse evitado invirtiendo una pequeña parte de esa suma en ciberseguridad. Aranda subraya que el problema no es específico de un país, sino mundial, ya que las pérdidas anuales derivadas de la ciberdelincuencia oscilan entre el 0,8 y el 1,0% del producto mundial bruto.

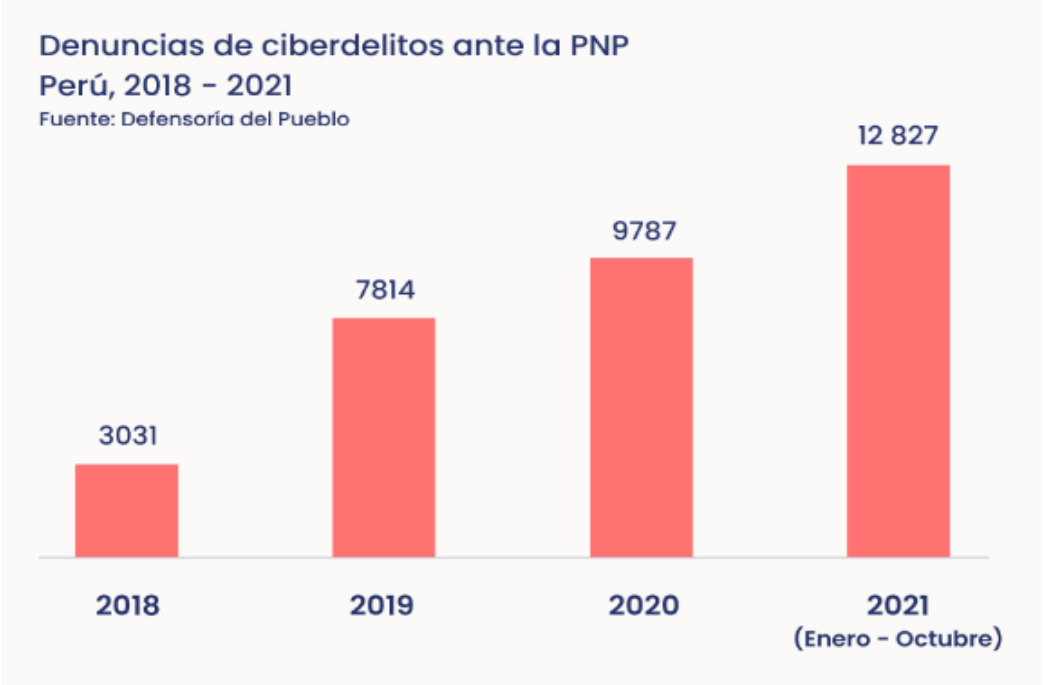
La entidad pública analizada presentaba una infraestructura de seguridad fragmentada, caracterizada por la falta de integración entre los diversos dispositivos y sistemas encargados de monitorear y proteger la red. Esta fragmentación incrementaba los tiempos de respuesta del equipo de ciberseguridad, lo que a su vez exponía a la organización a un mayor riesgo de pérdidas económicas y daños reputacionales (Smart Global, 2024). En el sector sanitario, los datos confidenciales tanto de los pacientes como del personal médico son susceptibles de sufrir estas amenazas potenciales. La exposición de datos confidenciales de diagnóstico e información sensible es perjudicial cuando está en posesión de ciberdelincuentes (Redacción EC, 2022).

A nivel nacional, los ciberdelitos han mostrado un crecimiento en los últimos años, evidenciando la vulnerabilidad de las infraestructuras tecnológicas en el país. Según la Defensoría del Pueblo, en 2021 se registraron 12,827 denuncias de ciberdelitos ante la Policía Nacional del Perú, siendo Lima la

región con mayor incidencia (53%), seguida de Arequipa (5.7%), Callao (5.2%) y La Libertad (5%). Estos datos reflejan un entorno en el que los cibercriminales han encontrado un terreno fértil para explotar las brechas de seguridad en sectores clave (Defensoría del Pueblo, 2023). A continuación, en la figura 6 se muestra la evaluación de las denuncias de ciberseguridad ante la PNP.

Figura 6

Denuncias de ciberseguridad ante la PNP



Nota: la imagen muestra el aumento de denuncias de ciberdelitos ante la Policía Nacional del Perú (Defensoría del Pueblo, 2023)

En el ejemplo concreto de esta empresa investigada, se descubrió que uno de los principales elementos causantes de la exposición a las amenazas eran las deficiencias en el diseño estratégico de la ciberseguridad. La falta de un sistema centralizado de gestión de eventos de seguridad impedía priorizar los riesgos y asignar recursos para mitigar sus efectos. La falta de conocimiento del estado de seguridad de la infraestructura tecnológica elevó la dependencia de procedimientos manuales y reactivos, que resultaban ineficaces e ineficientes ante la velocidad y sofisticación de las amenazas actuales. En el caso del sector salud, los datos que incluyen historiales médicos, diagnósticos y tratamientos son especialmente vulnerables y

pueden ser utilizados para la extorsión, el fraude o incluso la manipulación de historiales médicos.

Las dificultades repercutieron en que la institución pública decida incluir un SIEM en su plan de ciberseguridad, seleccionando el sistema LOG360 para centralizar y analizar en tiempo real los incidentes de seguridad. Esto mejoró enormemente la capacidad de reconocer y disminuir los riesgos. La aplicación implicó un estudio exhaustivo de las necesidades de la entidad, la definición de casos de uso particulares y su interacción con las soluciones de seguridad actuales. Además, se desarrollaron cuadros de mando sencillos para proporcionar métricas importantes, lo que permitió al equipo de ciberseguridad funcionar con mayor eficacia.

Para garantizar el ajuste con la infraestructura actual, el despliegue del SIEM también necesitó una preparación minuciosa. Era esencial configurar y cambiar los puertos de los servidores para garantizar una conexión eficaz entre el SIEM y los dispositivos de seguridad. Además, se realizaron pruebas exhaustivas para garantizar que las notificaciones fueran pertinentes y precisas, así como para confirmar el correcto funcionamiento del sistema. Esta estrategia acortó el tiempo de detección de peligros, reforzando así la capacidad de reacción de la organización ante los sucesos antes de que infligieran daños mayores.

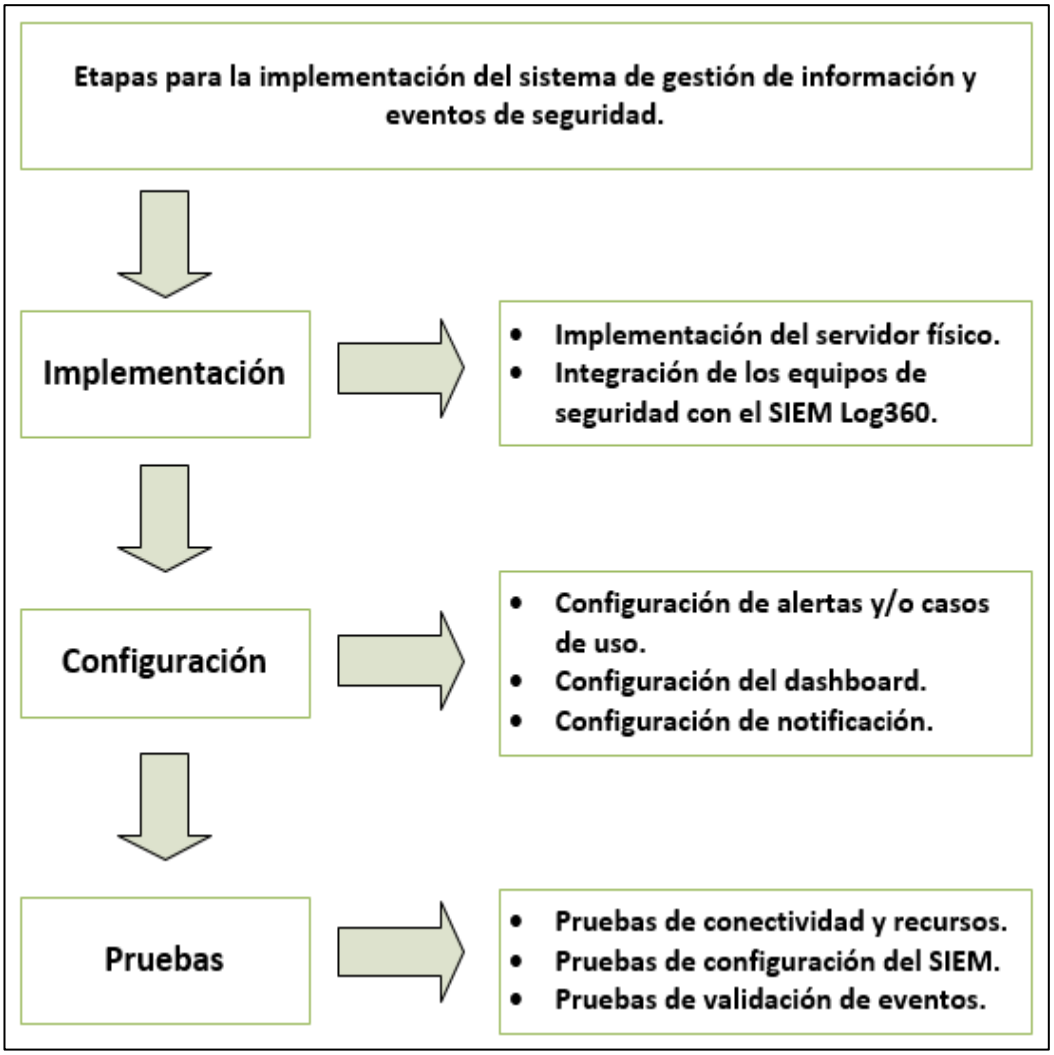
El objetivo de este estudio era aplicar un SIEM acorde a las necesidades de detección de ciber amenazas del sector salud. Este sistema pretende garantizar la preservación de los recursos técnicos, mejorar la identificación temprana de amenazas y aumentar la capacidad de la organización para hacer frente a un entorno de peligros siempre cambiantes. Mediante su implantación, el organismo salvaguarda su infraestructura e información sensible, así como refuerza la garantía de calidad y seguridad que los ciudadanos desean de los servicios públicos prestados.

3.2. Modelo de solución propuesto:

A continuación, se muestra el modelo en la figura 7, el cual contiene las fases de implementación:

Figura 7

Etapas de implementación de proyecto.



Nota. La figura muestra las fases requeridas para implementar un SIEM

En la fase de implementación se realizó la implementación del servidor y la integración de los equipos de seguridad con el SIEM. De acuerdo a las especificaciones técnicas del vendor, para la fase configuración se determinó los casos de usos y alertas a configurar.

En la fase de pruebas se realizó la monitorización en tiempo real del equipo Palo Alto, de acuerdo a los casos de usos y alertas que se configuraron, para la fase del pase operaciones se capacitó al personal del SOC encargado de

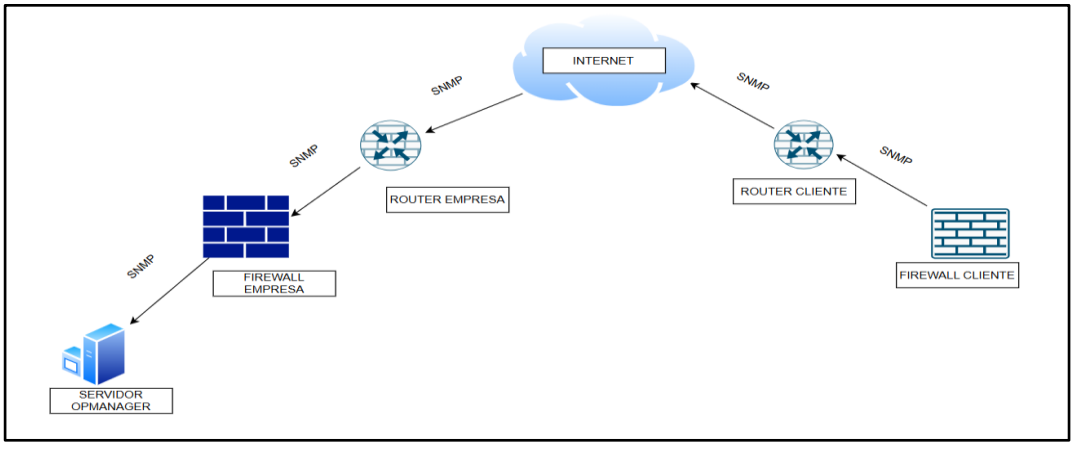
la gestión del SIEM, se les brindó una cuenta de acceso al sistema de monitoreo con los roles y privilegios autorizados por el jefe del SOC.

3.2.1. Determinación inicial del problema.

En el análisis realizado de la situación inicial de la entidad pública del sector salud se validó que el cliente no contaba con un sistema de detección de amenazas en tiempo real, ya que tenía que informar sobre algún tipo de incidencia o evento al equipo SOC con el propósito de que realice acciones a fin de que se logre bloquear los intentos de accesos maliciosos, por ejemplo, en el anexo 3 se muestra que el 21 de noviembre del 2024 a las 10:53 am se reporto una urgencia que debía de bloquearse un link malicioso al equipo SOC y fue atendida a las 11:38 am del mismo día, por lo que se obtuvo 45 minutos de demora que era en promedio las demoras ante urgencias que presentaba el cliente. Por consiguiente, solo realizaban la monitorización de estado de salud de los dispositivos de seguridad a través del protocolo SNMP, en la figura 8 se observa la topología de envió de SNMP desde el firewall a monitorear hacia el servidor Opmanger de la empresa.

Figura 8

Dispositivos de seguridad utilizando protocolo SNMP

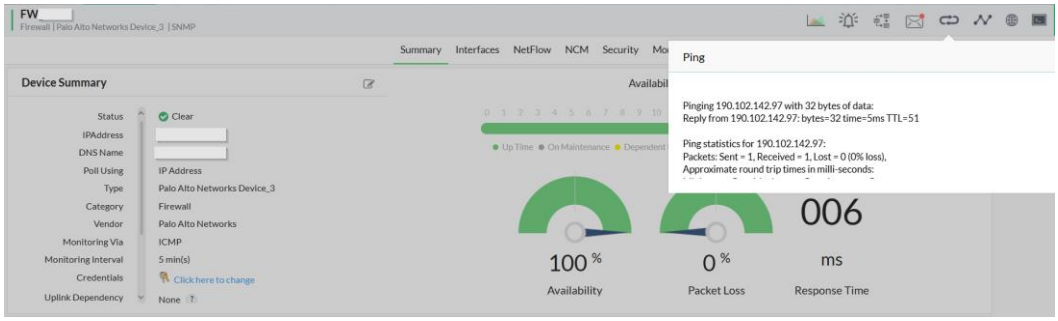


Nota. La figura muestra la topología del protocolo SNMP

El monitoreo se realizaba mediante la plataforma Opmanger donde realizaba un ping al dispositivo firewall para ver la disponibilidad, en la figura 9 se muestra la disponibilidad del equipo.

Figura 9

Monitoreo mediante plataforma Opmanger

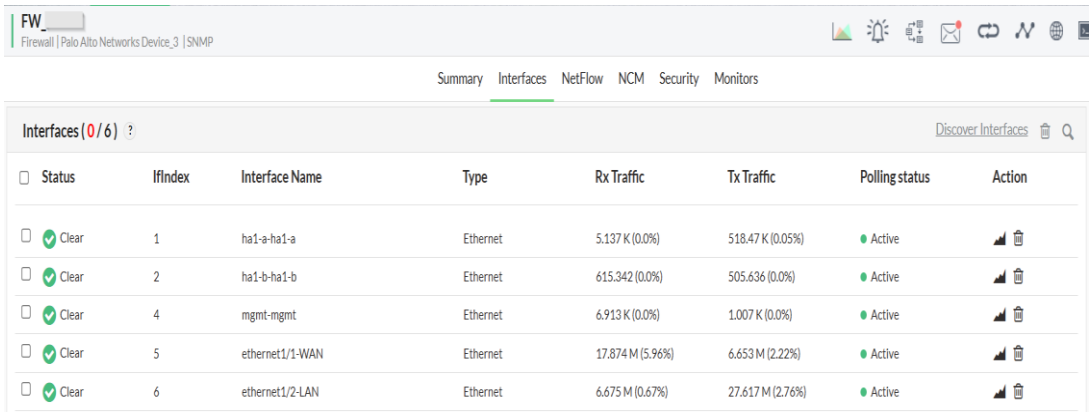


Nota. La figura muestra el monitoreo a través de la plataforma Opmanger

Solo se monitorean las interfaces administradas en el firewall que se está monitoreando, en la figura 10 se observan las interfaces configuras en el firewall perimetral.

Figura 10

Configuración en el portal de monitoreo Opmanger

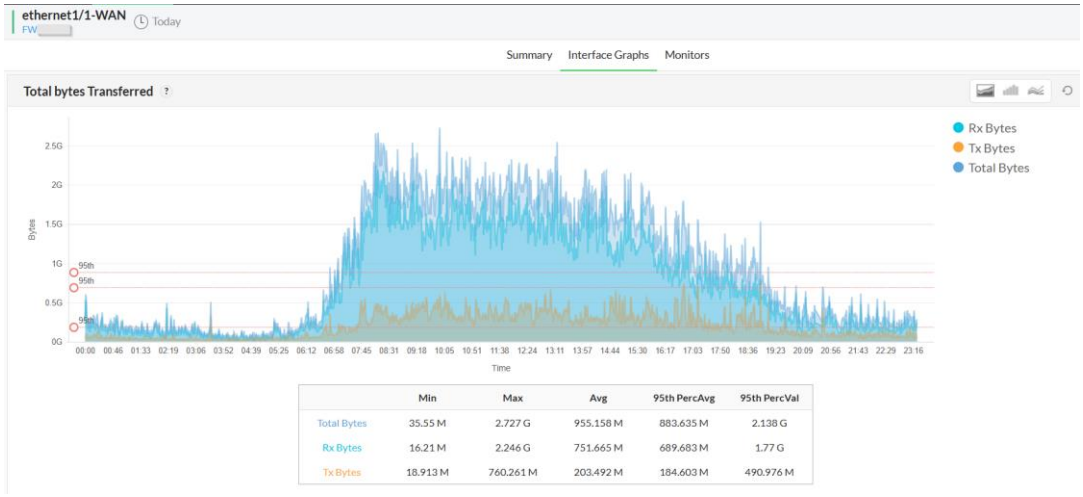


Nota. La figura muestra las acciones de configuración del firewall perimetral

En la figura 11 se observa en la interface ethernet1-1-WAN el total de bytes transferidos de transmisión y recepción.

Figura 11

Transferencia de transmisión y recepción en la interface ethernet1-1-WAN



Nota. La figura muestra el total de bytes transferidos

3.2.2. Fase de implementación

En la fase de implementación es necesario considerar aspectos sobre la instalación del servidor físico y su integración con equipos de seguridad con el SEIM Log360, por lo que se muestra el procedimiento realizado para su instalación.

Para la instalación del SIEM, se deben tener en cuenta los recursos de hardware necesarios, así como los requisitos de software especificados por ManageEngine Log360, que es compatible con varias versiones del sistema operativo Microsoft Windows. Según la información obtenida de www.manageengine.com, para propósitos de evaluación, el software requiere al menos Windows 8 o Windows Server 2012, mientras que para entornos de producción se recomienda Windows Server 2022, 2019, 2016, 2012 R2 o 2012. En este proyecto específico, se optó por instalar Windows Server 2022 para asegurar la compatibilidad y el rendimiento óptimo del sistema, siendo presentado en la tabla 1 las características que se recomienda para el hardware.

Tabla 1

Característica recomendadas según el hardware

Hardware	Minimum	Recommended
Base Speed	2.4 Ghz	3 Ghz
Core	12	16
RAM	64	64
Disk Space	1.2 TB	1.5 TB
Disk Type	SSD	SSD

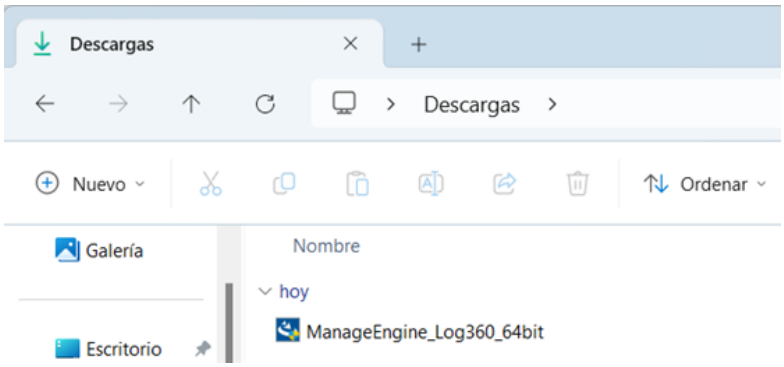
Nota. Tomado de ManageEngine Log360

Instalación del LOG360

Para comenzar la instalación de Log360, primero se validaron los recursos del sistema recomendados. Luego, se descargó el software desde la página de Manageengine, específicamente el archivo ManageEngine_Log360_64bit, que fue utilizado para iniciar el proceso de instalación como se muestra en la figura 12.

Figura 12

Descarga del software LOG360



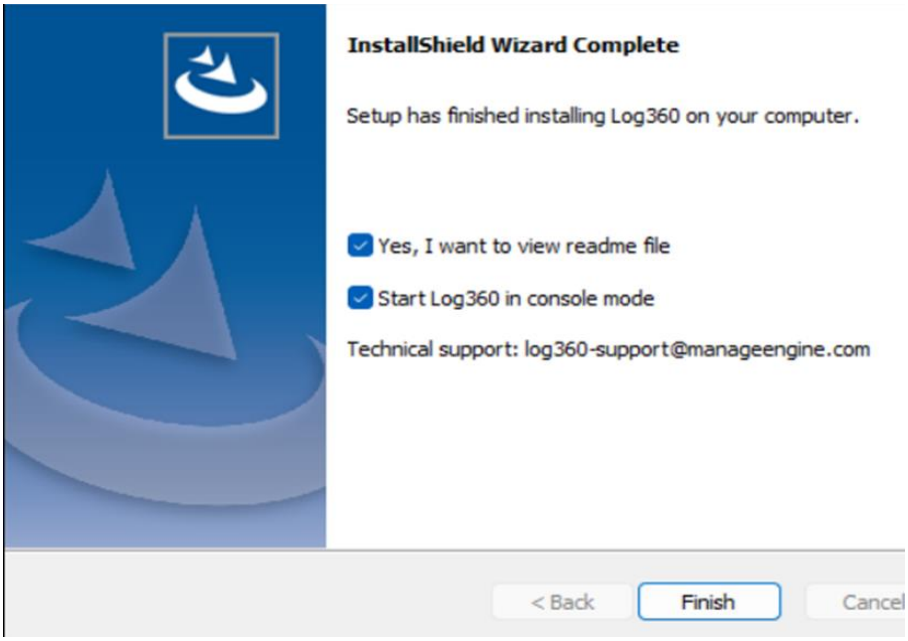
Nota. Tomado de ManageEngine Log360

Para instalar ManageEngine Log360, se inicia seleccionando el archivo descargado ManageEngine_Log360_64bit y se procede con la opción "Next" en el asistente de instalación. A continuación, revise y acepte el acuerdo de contrato de licencia, y seleccione el tipo de instalación deseado—estándar, mínimo o personalizado. Especifique también la ubicación de la carpeta destino donde se alojará el software. En la figura 13 se muestra la descarga

del software Log360, en la cual se muestra las configuradas estas opciones, el sistema comenzará la copia de archivos necesaria para la instalación, que culminará con la finalización del proceso.

Figura 13.

Descarga del software LOG360



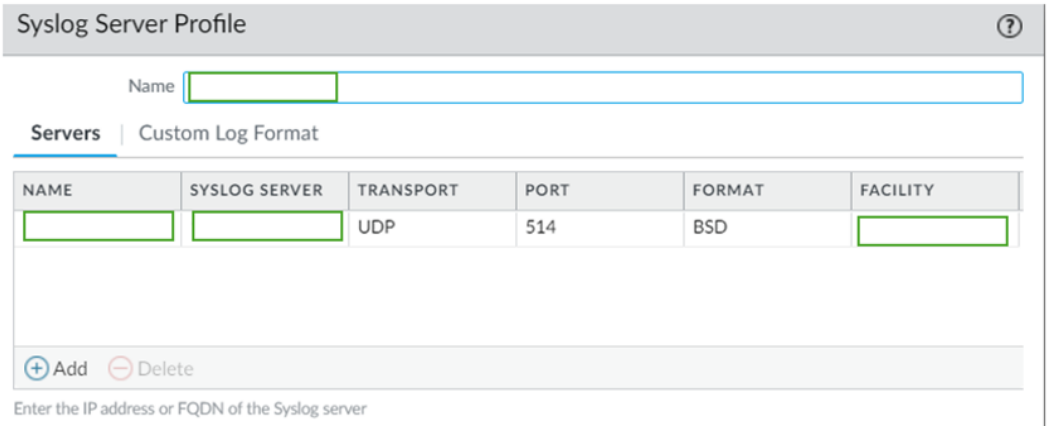
Nota. Tomado de ManageEngine Log360

Para el funcionamiento del sistema, es necesario que los siguientes puertos estén abiertos en el servidor: el puerto 8400 (TCP), utilizado para el servidor web; los puertos 513 (UDP) y 514 (TCP y UDP), requeridos para que el servidor Syslog reciba mensajes; y el puerto 33335 (TCP), destinado al acceso de la base de datos. Esto asegura la correcta comunicación y gestión de datos dentro de la infraestructura del sistema.

Para gestionar el módulo SIEM de LOG360, es clave configurar Syslog en un firewall Palo Alto. Es necesario asegurarse de que el firewall esté bien configurado para enviar los eventos de seguridad a través de Syslog al EventLog Analyzer, lo que permitirá una integración efectiva y un monitoreo constante de los eventos de seguridad. A continuación, se presenta el perfil de servidor Syslog en la figura 14.

Figura 14

Perfil de servidor Syslog



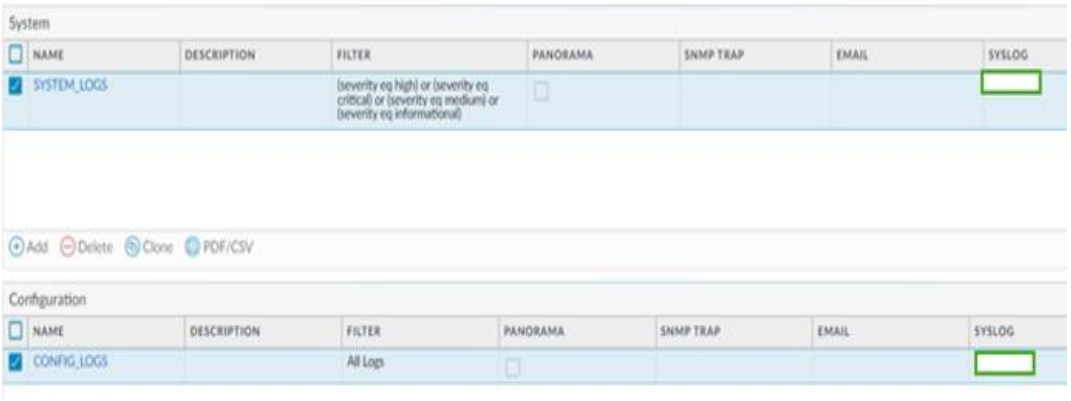
Nota. Tomado de la empresa Smart Global SAC, 2024

En la figura 14 se muestra la interfaz para configurar un perfil de servidor Syslog, donde se pueden añadir detalles de varios servidores. En la configuración visible, se emplea UDP como protocolo de transporte en el puerto 514, típico para Syslog, y el formato de mensaje es BSD. Los usuarios pueden administrar los servidores ingresando la dirección IP o el FQDN y utilizando los botones 'Add' y 'Delete' para modificar la lista.

Para enviar eventos de seguridad a una herramienta de monitoreo, se debe configurar un perfil de reenvío de logs denominado "SIEM", especificando la dirección del servidor Syslog como 133.156.45.9 y seleccionando "LOG" como la facility. A continuación, en la figura 15 se muestra la interfaz de configuración.

Figura 15

Interfaz de Configuración de Perfiles de Reenvío de Logs

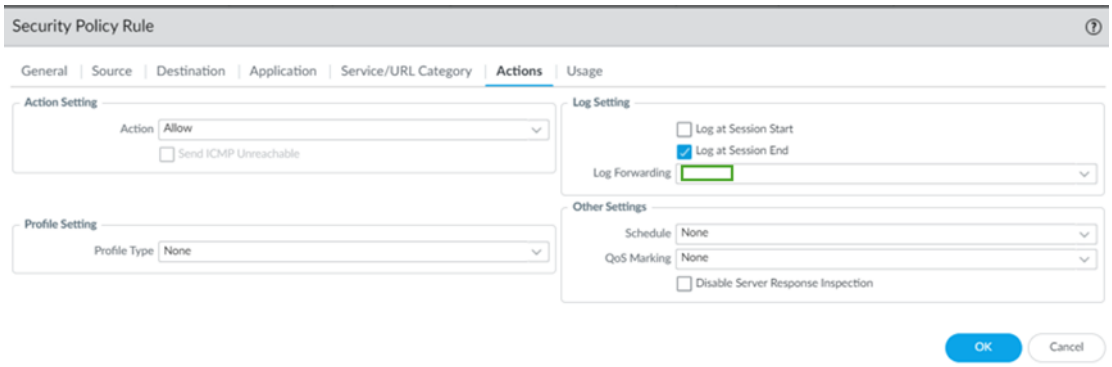


Nota. Tomado de la empresa Smart Global SAC, 2024.

Posteriormente, se realiza valida que todas las políticas de seguridad se encuentren enviando los logs al perfil Forwarding, por lo que se muestra en la figura 16 las reglas de política de seguridad.

Figura 16

Reglas de política de seguridad



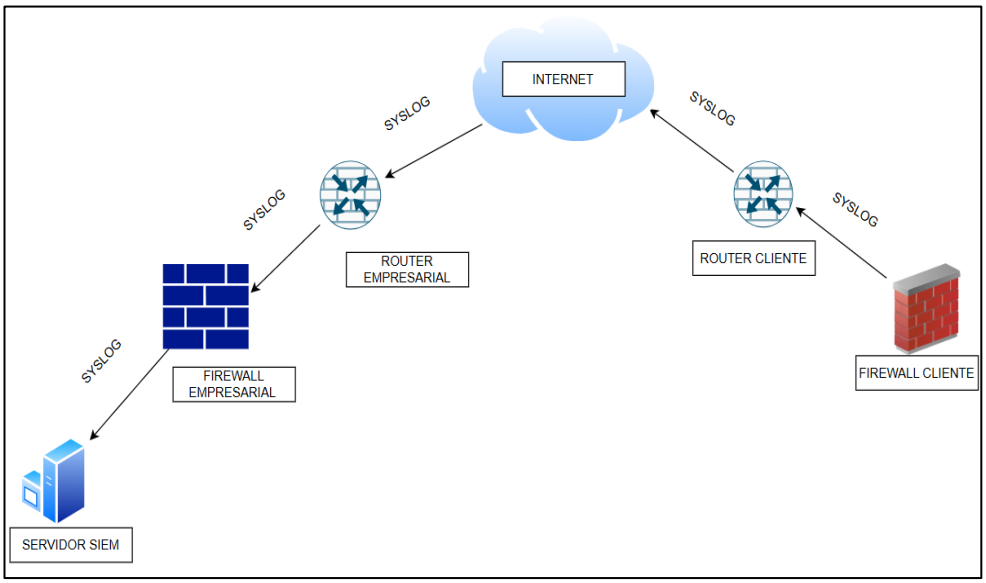
Nota. La figura muestra las opciones establecidas para acciones permitidas, ajustes de registro de eventos al final de sesiones, redirección de registros

3.2.3. Fase de configuración

En la fase de configuración se realizó las configuraciones de casos de usos y acondicionamiento del SIEM para una buena gestión del sistema, es importante validar que los dispositivos de la entidad pública deben enviar logs al SIEM LOG360, en la siguiente figura 17 se observa la topología de la sincronización del equipo firewall al servidor SIEM.

Figura 17

Topología de sincronización del equipo firewall al servidor SIEM



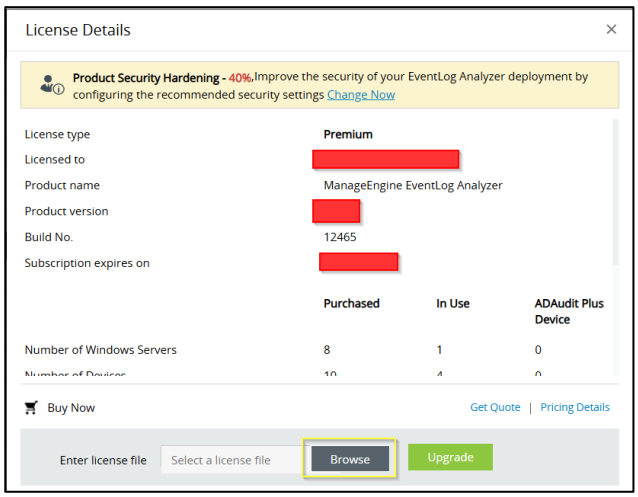
Nota. Se observa la topología en arquitectura de red

Instalación de licencias

En la figura 18 se muestra la licencia que debe cargarse una vez completado el proceso de instalación.

Figura 18

Licencia del SIEM Log360



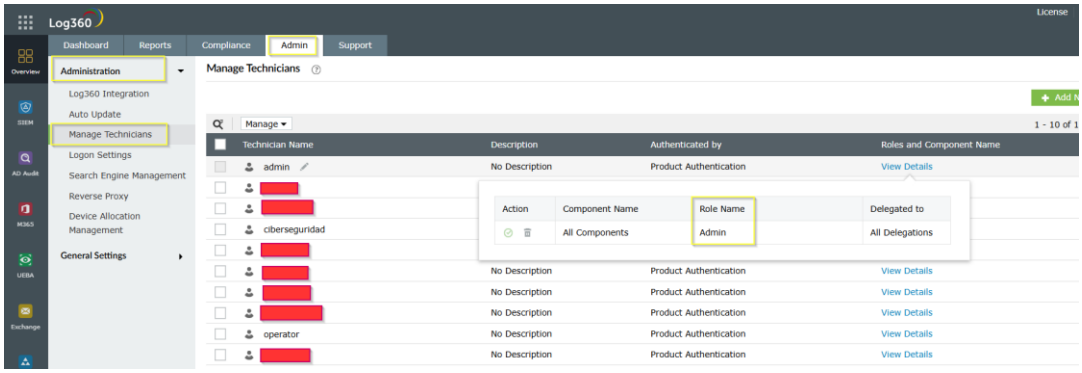
Nota. La figura muestra detalles de la licencia en Manage Engine EventLog Analyzer

Acceso al SIEM para los interesados del proyecto

Esta sección detalla la descripción de accesos y roles al SIEM Log360, en donde se asigna un nuevo técnico para el acceso al sistema, es importante saber que rol y privilegios tendrá la cuenta de cada especialista de ciberseguridad.

Figura 19

Descripción de accesos y roles al SIEM Log360



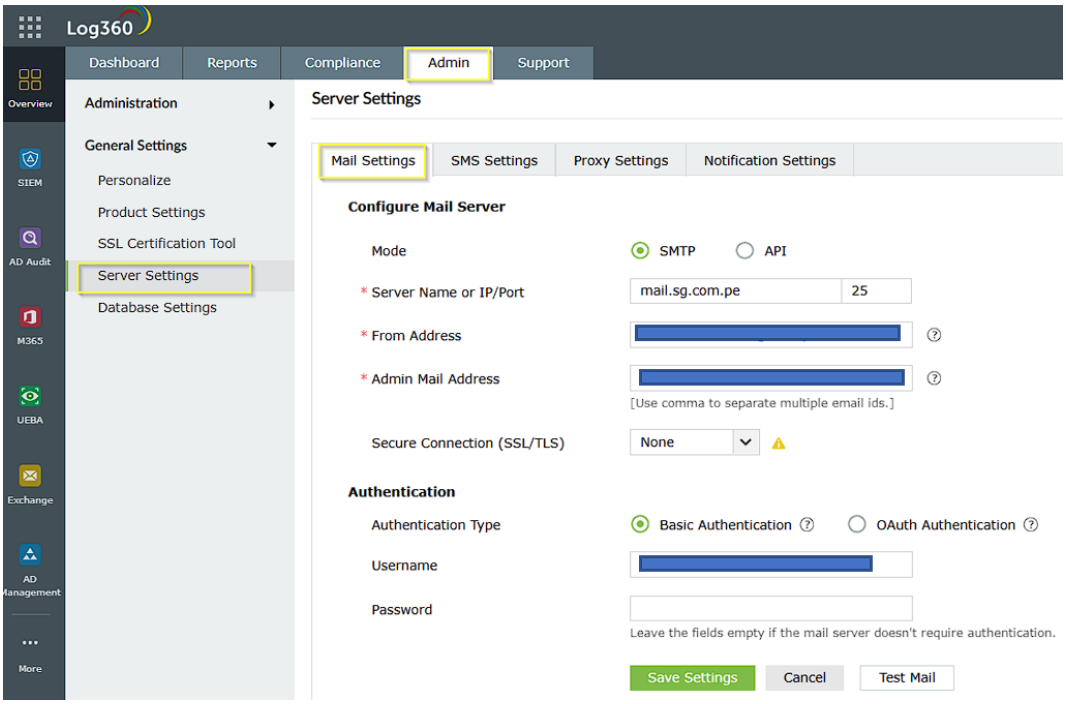
Nota. La figura muestra la gestión de técnicos en SIEM Log360

Configuración de correos

Para las notificaciones se configuró el servidor de correos para enviar notificaciones y alertas. Se añadieron los correos que se utilizaron para recibir las notificaciones como se muestra en la figura 20.

Figura 20

Configuración de correos para el envío de notificaciones y alertas



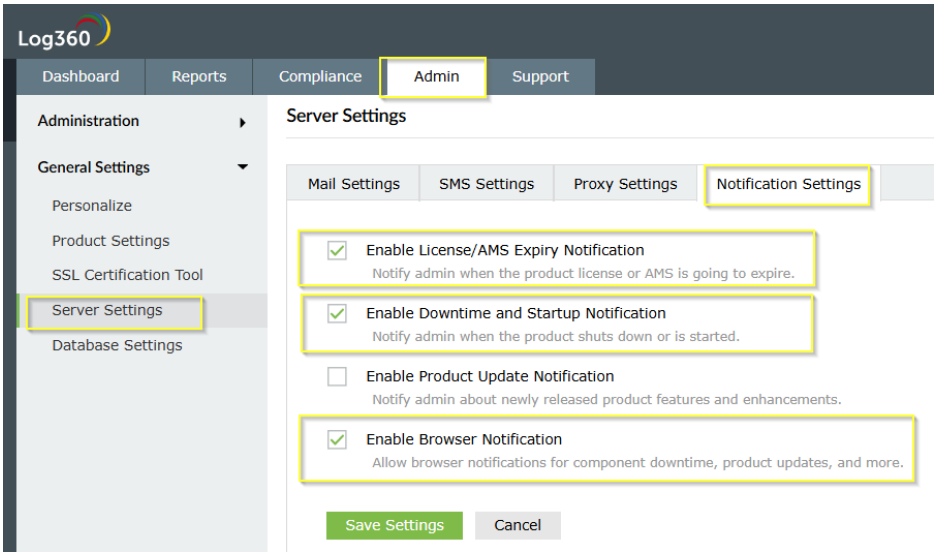
Nota. La figura detalla la configuración del modo SMTP, incluyendo el nombre del servidor, puerto, direcciones de correo de origen y administrador

Configuración de notificaciones

Para la configuración de notificaciones se definieron los siguientes parámetros como caducidad de licencia el tiempo de inactividad, notificaciones de actualización del producto, notificaciones del navegador. Se configuró las siguientes notificaciones Como se observa en la figura 21.

Figura 21

Configuración de notificaciones del SIEM Log360



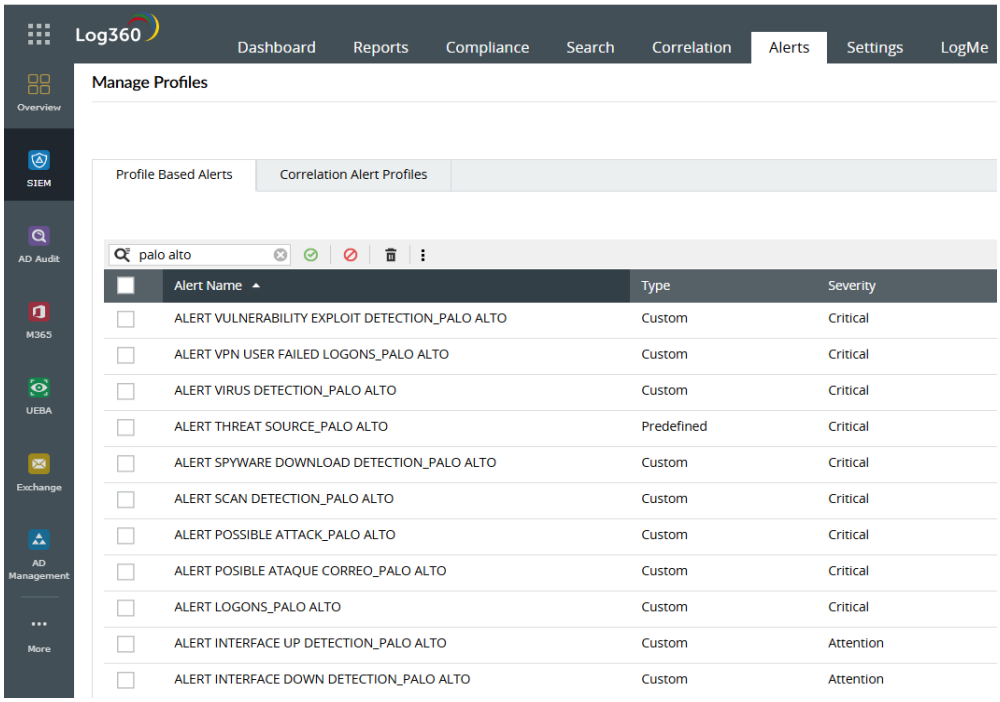
Nota. Configuración de notificaciones en los ajustes del servidor de Log360

Configuración de los casos de uso

Luego de las validaciones de la integración del Palo Alto con el SIEM LOG 360, se definieron los casos de usos de acuerdo con el problema detectado en la entidad pública como se muestra en figura 22.

Figura 22

Alertas registradas del SIEM Log360

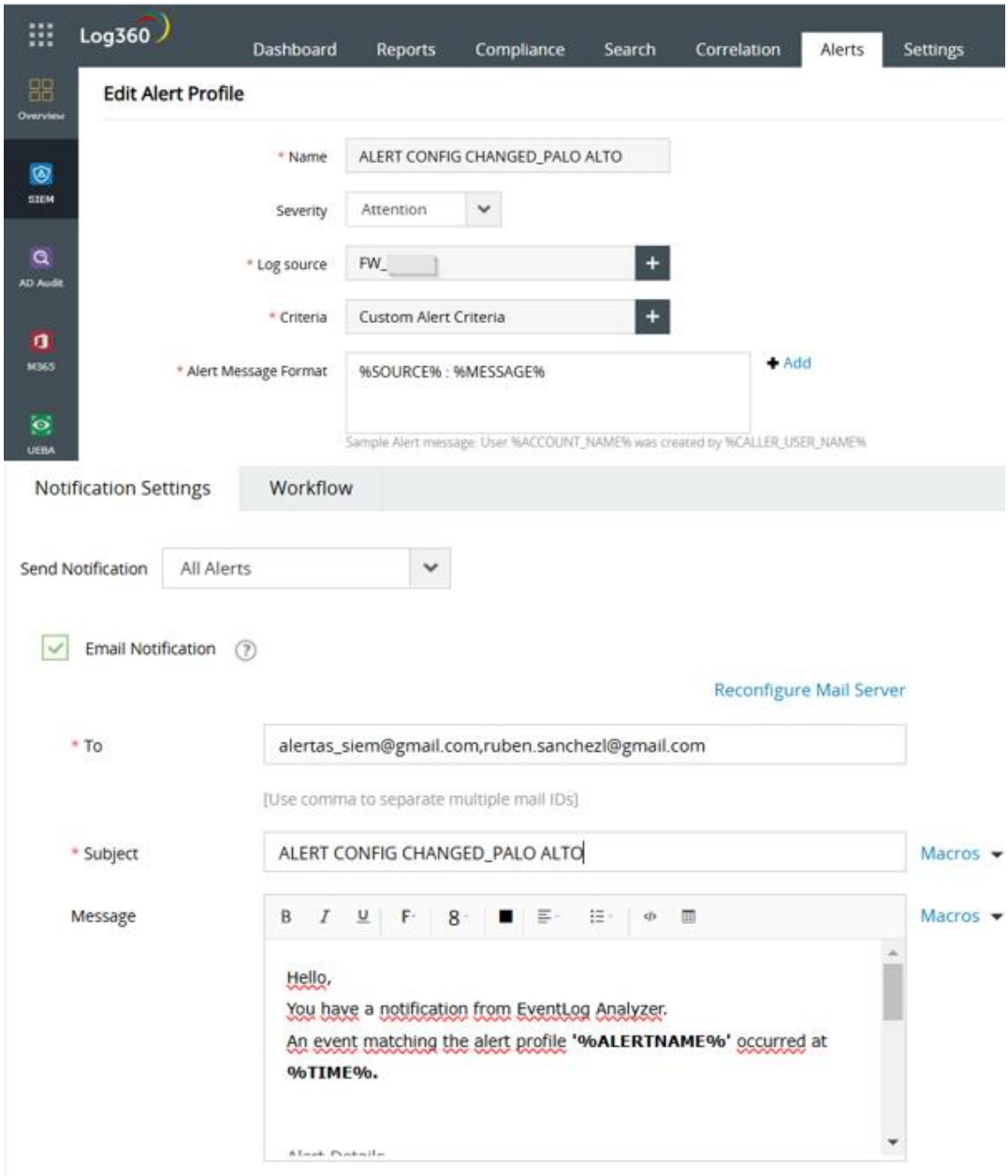


Nota. Listado de perfiles de alerta configurados en Log360 relacionados con dispositivos Palo Alto

El caso de uso cambios en la configuración del equipo es de suma importancia porque en ello podemos observar los diferentes tipos de cambios realizados por los diferentes usuarios que tienen administración del equipo Palo Alto. En la figura 23 se observan los parámetros a configurar.

Figura 23

Configuración de parámetros en el SIEM Log360

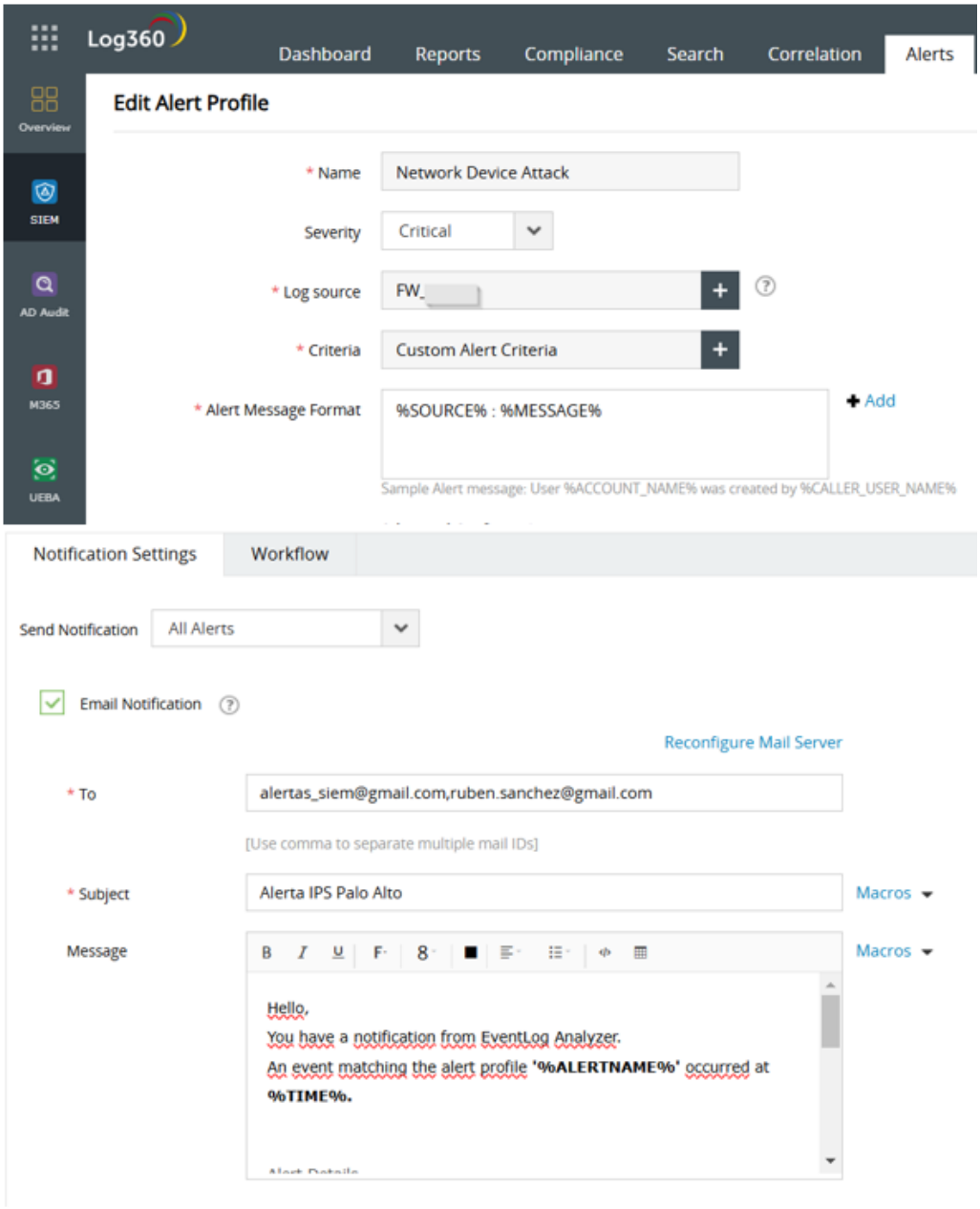


Nota. Configuración de perfil de alerta en Log360 para notificaciones relacionadas con cambios en la configuración de dispositivos Palo Alto

Respecto al caso de uso Network Device Attack es de suma importancia, ya que se valida en los logs del Palo Alto tráfico entrante desde diferentes IPs maliciosas validadas por los motores de búsqueda como se muestra en la figura 24.

Figura 24

Configuración de Perfil de Alerta en Log360 para Notificaciones de Ataques



Nota. Captura de pantalla que muestra la configuración de un perfil de alerta en Log360

Fase de pruebas

Respecto a las pruebas se realizó un checklist con las pruebas realzadas para mostrar los resultados obtenidos como se observa en la tabla 2.

Tabla 2

Cumplimiento de pruebas realizadas

Pruebas de conectividad y recursos	Cumplió	No cumplió
Disponibilidad del servicio mediante un ping constante a la url	Si	
Validación estable de recursos de CPU	Si	
Validación estable de recursos de Memoria	Si	
Pruebas de configuración del SIEM		
Validación de expiración de licencias	Si	
Validación de sincronización del Palo Alto con el SIEM	Si	
Validación de notificaciones de los casos de uso	Si	
Pruebas de validación de eventos		
Validación de eventos Syslog	Si	
Validación de eventos de seguridad	Si	
Validación de eventos Windows	Si	

Nota. Se muestra el cumplimiento en las distintas pruebas

En la tabla 2 se muestra el check list de pruebas que se han realizado durante la fase de validación, en donde se incluye la configuración del SIEM y validación de eventos, por lo que mediante el cumplimiento de los distintos ítems se demuestra que se ha cumplido el plan de pruebas presentado.

En el desarrollo de la investigación sobre la implementación de un sistema de gestión de información y eventos de seguridad para la detección de amenazas en una entidad pública del sector salud, las contribuciones primordiales en términos de competencias y habilidades, se orientaron hacia:

Conocimientos en administración de redes y comunicaciones:

Con las habilidades que adquirí durante la formación académica en la universidad se obtuvo conocimientos en administración de redes de ciberseguridad y comunicaciones con el fin de determinar y realizar diagnóstico de sistemas de información de clientes con el propósito de mitigar posibles amenazas de ciberseguridad.

Manejo de un SIEM para el monitoreo y acciones ante amenazas cibernéticas que complementan la seguridad a través de un equipo SOC.

Las habilidades que se fueron adquiriendo durante la etapa profesional a permitido obtener conocimientos con relación a la seguridad informática, en cuanto a la implementación de un SIEM para consolidar una estrategia de ciberseguridad, siendo utilizado el software Log360 para el monitoreo y acciones de respuestas a fin de brindar al cliente una mayor seguridad en sus diferentes sistemas.

Manejo de habilidades blandas:

Las habilidades blandas son de vital importancia para el trabajo en equipo, ya que la instalación del Log360 requiere que se forme un equipo multidisciplinario, por lo que una comunicación asertiva y trabajo en equipo se aprendieron durante la formación académica, lo cual es importante para el éxito de los proyectos.

Conocimiento en SIEM

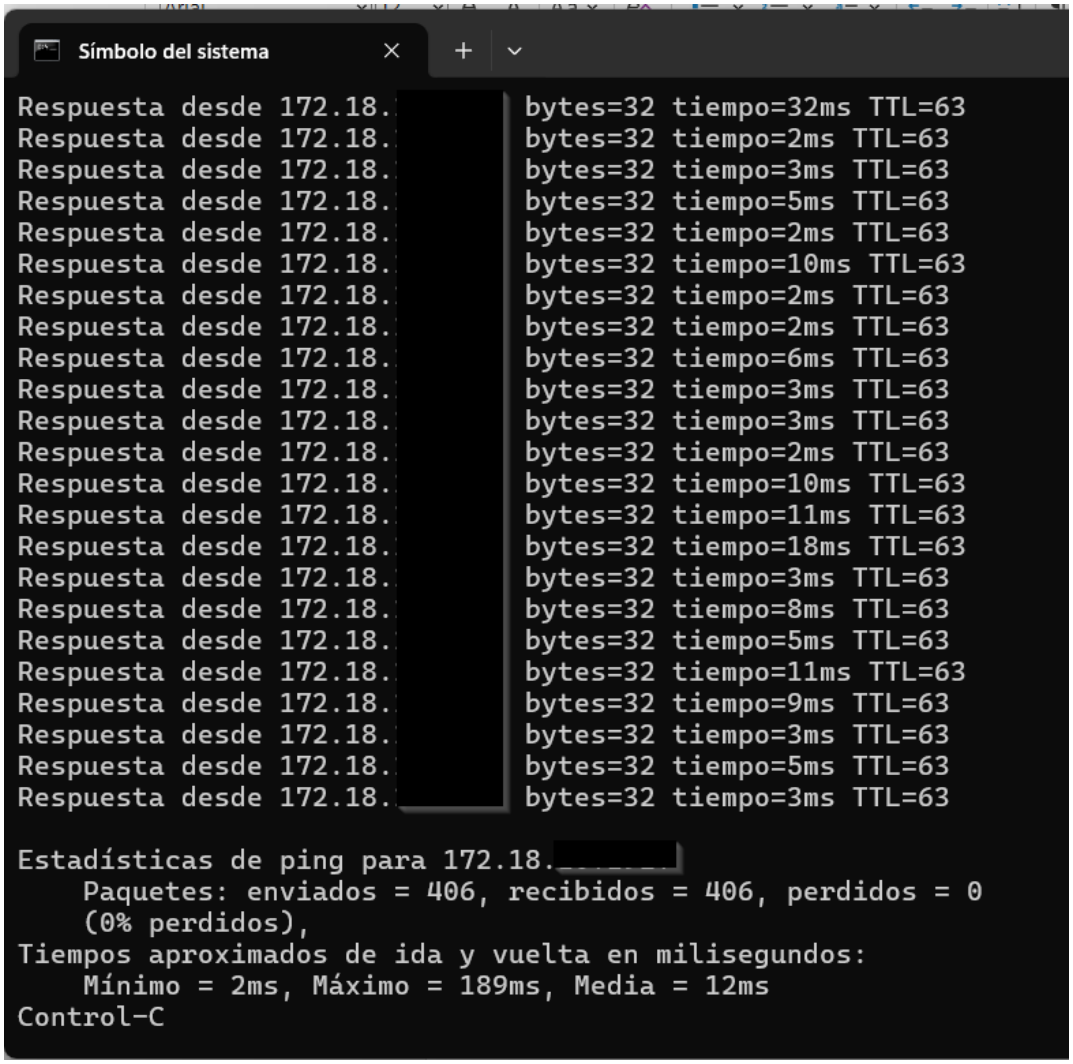
Se adquirieron sólidos conocimientos en la configuración y optimización de dispositivos de seguridad, asegurando la integración efectiva del sistema SIEM con las plataformas existentes, lo cual es importante en el campo de la seguridad informática, ya que el Perú es un país que posee una enorme brecha en este campo, en ese sentido, la implementación de un Log360 permite detectar amenazas e incidentes de seguridad de una forma centralizada a través de la identificación y correlación de eventos críticos para dar respuesta ante posibles incidentes de ciberseguridad.

3.3. Resultados

En los resultados de la implementación de un SIEM que permita detectar las amenazas en una entidad pública del sector salud, se realizaron pruebas de conectividad y recursos que demostraran su funcionamiento. En los resultados se muestra la conectividad, como se demostró en la figura 25, donde se obtuvo un ping constante: de los 406 paquetes enviados, no se perdió ninguno.

Figura 25

Comprobación de conectividad mediante comando ping

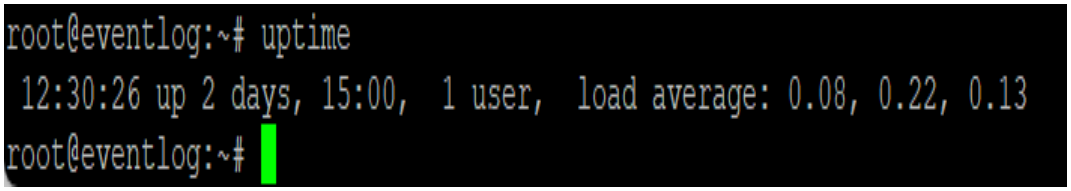


Nota. Captura de pantalla del símbolo del sistema que muestra los resultados de un ping continuo hacia la dirección

Asimismo, se realizó la validación de la disponibilidad del servicio mediante el comando CLI uptime como se muestra en la figura 26.

Figura 26

Monitorización del tiempo de actividad y carga del sistema

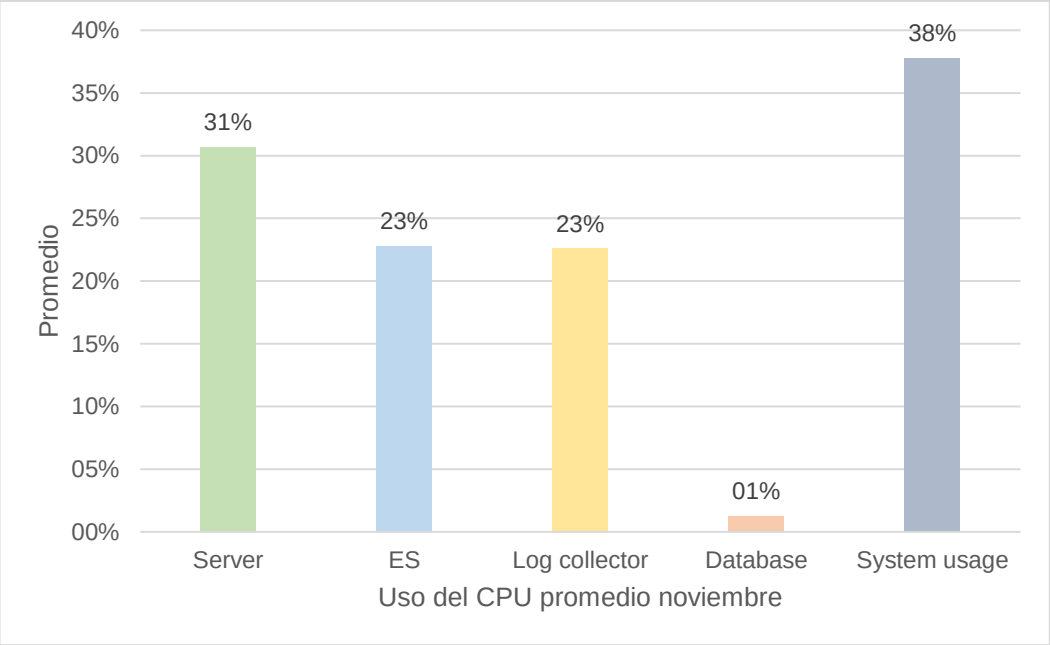


Nota. Se muestra la captura de pantalla del comando uptime

De igual manera, se realizó la revisión del CPU durante el periodo de 30 días, en el que se revisaron los datos registrados en intervalos reguladores, por lo que se puede demostrar la ausencia de picos de sobrecargas o fluctuaciones inusuales que pudieran afectar el rendimiento del CPU (Ver anexo 1), en ese sentido, se garantiza la confiabilidad y estabilidad del sistema durante el periodo que se ha realizado el análisis como muestra la figura 27.

Figura 27

Promedio de uso del CPU durante noviembre del 2024

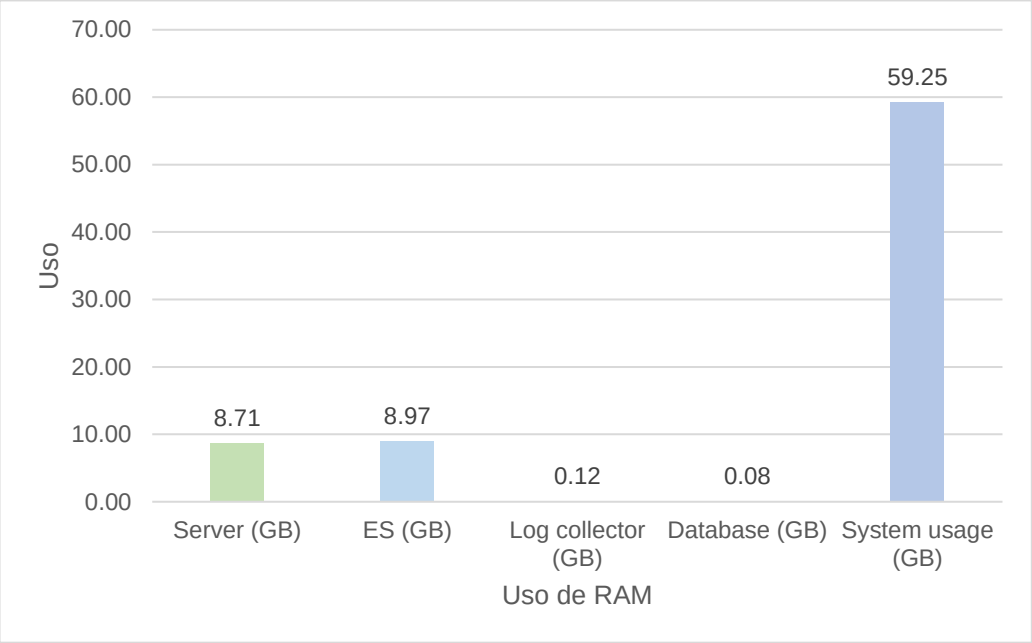


Nota. Se muestra el promedio del uso del CPU durante noviembre del 2024

En la figura 27 se muestra que en promedio el system usage obtuvo un 38%, el server del 31% y como menor uso el database con 1%, esto demuestra que el SIEM es de utilidad al servir en la búsqueda de amenazas que pudieran afectar los procesos claves de la entidad en estudio. Posterior a ello, se monitoreo el uso de la RAM a fin de identificar su capacidad de dar seguimiento a las consultas realizadas (Ver anexo 2), como se muestra el promedio en el mes de noviembre del 2024 en la figura 28:

Figura 28

Promedio de uso del RAM durante noviembre del 2024



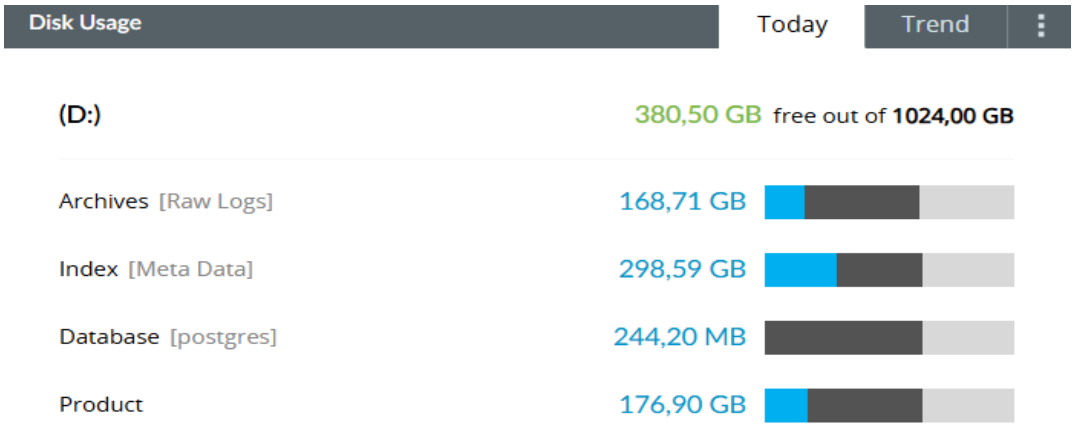
Nota. Gráfico que muestra el promedio del uso del CPU, desglosado por componentes como el servidor, ElasticSearch (ES), Log Collector y la base de datos

En la figura 28 se muestra que en el promedio de uso de la memoria RAM se identificó que el Server tuvo 8.71 GB en promedio, el Elasticsearch (ES) 8.97 GB, mientras que el System usage 59.25 GB, lo cual evidencia una alta demanda de los recursos por parte del sistema y posee una capacidad el sistema para que soporte consultas durante el uso de los sistemas de la entidad en estudio. Por lo mencionado, se demuestra que el uso de la memoria opera dentro de lo recomendado, es decir, el system usage no supera el 70 GB que el umbral recomendado por el fabricante.

En la figura 29 se muestra el uso del disco un valor disponible 380.50 GB libre de 1 TB, cabe mencionar que encriptamos los logs para tener una mayor disponibilidad del disco después de un periodo de 3 meses.

Figura 29

Uso de disco en la unidad D



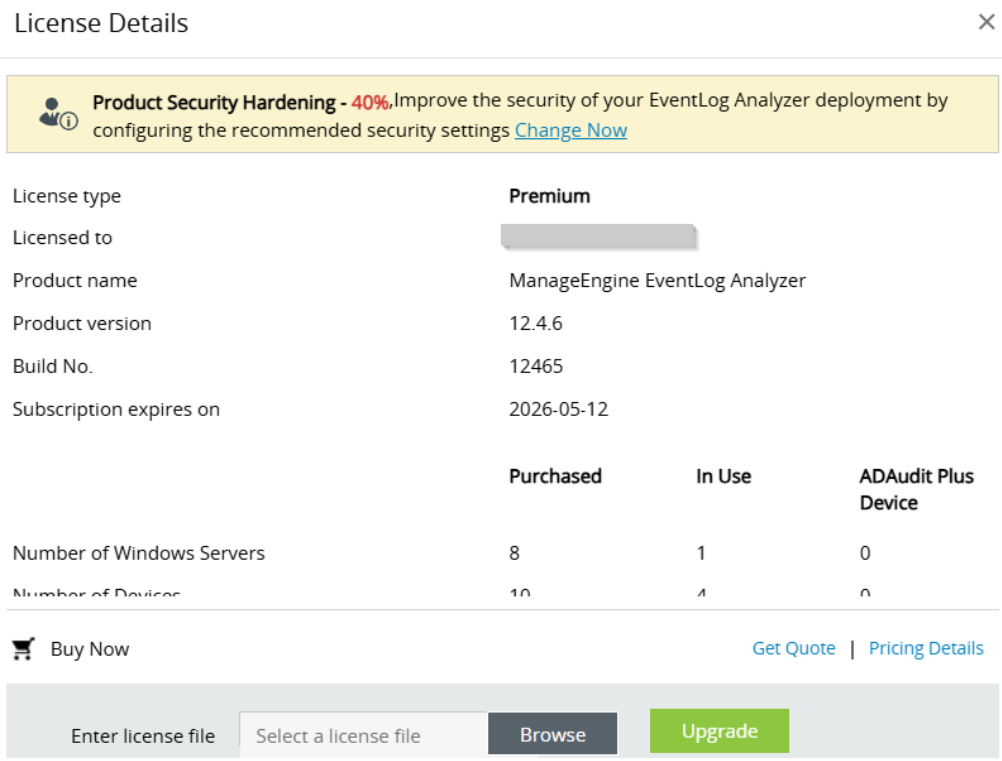
Nota. Segmentación del espacio utilizado en la unidad de almacenamiento D

Resultados de configuración del SIEM

En la figura 30 se observa que se tiene una licencia premium cuya subscription vence el 12 de mayo del 2026 es importante realizar la validación de la licencia ya que esto podría generar una afectación en el rendimiento del servicio.

Figura 30

Detalles de la licencia de ManageEngine EventLog Analyzer

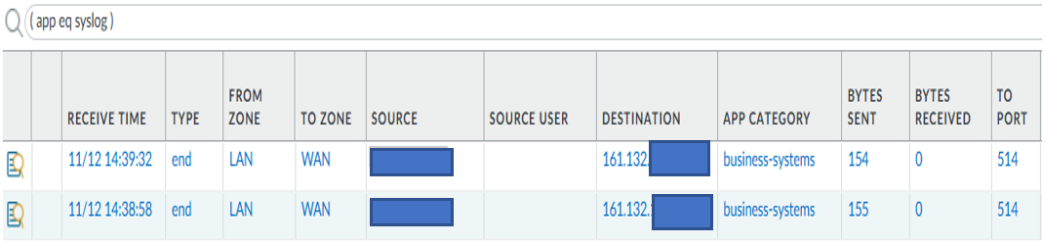


Nota. Información detallada sobre la licencia del software ManageEngine EventLog

Se observó que mediante los logs del palo alto se está envinado syslog desde la red LAN hacia la WAN que representa el servidor SIEN ya que el servidor se encuentra fuera de la red del cliente como se muestra la figura 31.

Figura 31

Registro de tráfico Syslog en el firewall



Nota. La figura muestra los registros de tráfico de la aplicación Syslog en el firewall

Resultados de monitoreo de eventos SIEM

Tabla 3

Eventos del syslog monitoreados por el SIEM en 2024

Eventos del Syslog	Setiembre	Octubre	Noviembre
Información	636271301	513095257	531271049
Recuento de eventos	7349	6292	5544
Error	3522	2637	2675
Critico	749	577	655
Noticias	9	4	7

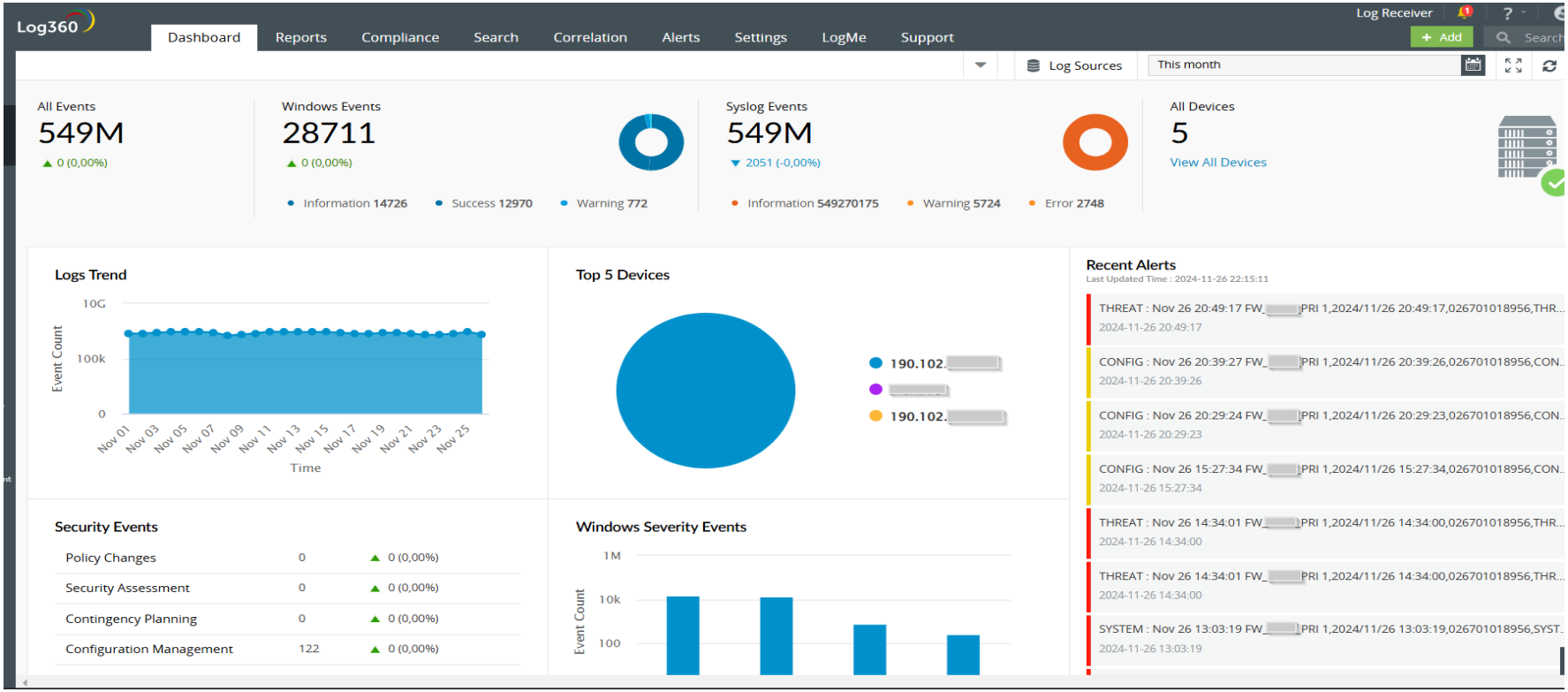
Nota. Se muestra el cumplimiento en las distintas pruebas

La tabla 3 muestra una disminución en los eventos registrados en el Syslog entre septiembre (636271301) y noviembre (531271049), destacando que los eventos informativos y de error presentan una reducción general, mientras que en los eventos críticos se muestra una detección de 749 en setiembre, 577 en octubre y 655 en noviembre, lo cual demuestra que el SIEM detecta las amenazas a la entidad de salud para tomar acciones correctivas y puedan mitigarse su efecto.

A continuación, se muestra el tablero de monitoreo del Log360 en la figura 32 empleado por el equipo SOC y el personal de TI de la entidad del sector salud, como se muestra en la figura 32.

Figura 32

Tablero de monitoreo Log360

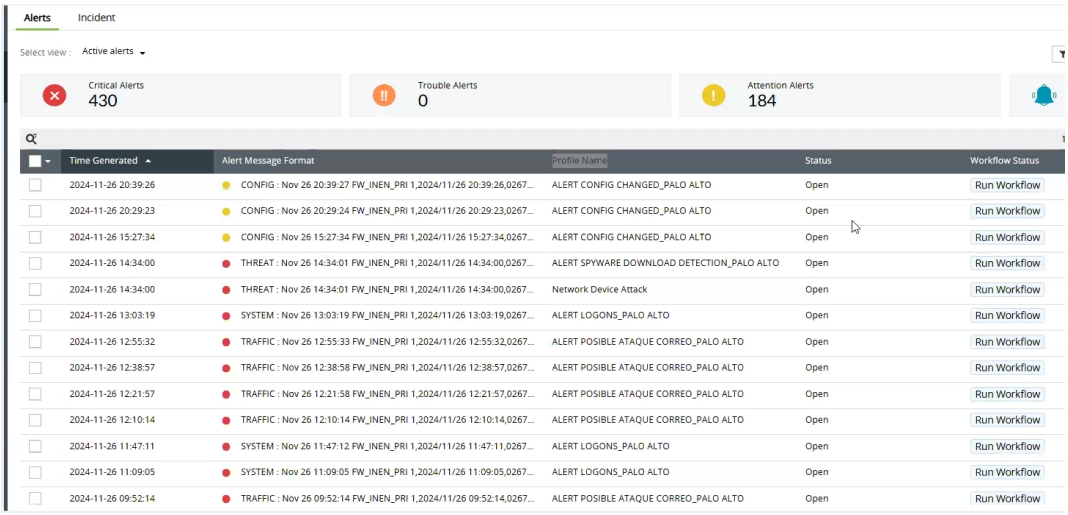


Nota. Se muestra principales indicadores del Log360

La figura 33 muestra el monitoreo normal de alertas en la entidad de salud durante el mes, con 614 alertas reportadas, de las cuales 430 son críticas y 184 requieren atención, mientras que no se registraron alertas menores. Destacan incidentes críticos como cambios en la configuración del firewall (Config Changed, Palo Alto) y detección de amenazas, incluyendo descargas de software malicioso y posibles ataques de red. Todas las alertas permanecen abiertas, lo que requiere intervención inmediata mediante los flujos de trabajo establecidos para mitigar riesgos y garantizar la seguridad de la infraestructura tecnológica. A continuación, en la figura 33 se muestra las alertas reportadas en la entidad de salud el 26 de noviembre del 2024.

Figura 33

Alertas reportadas en la entidad de salud



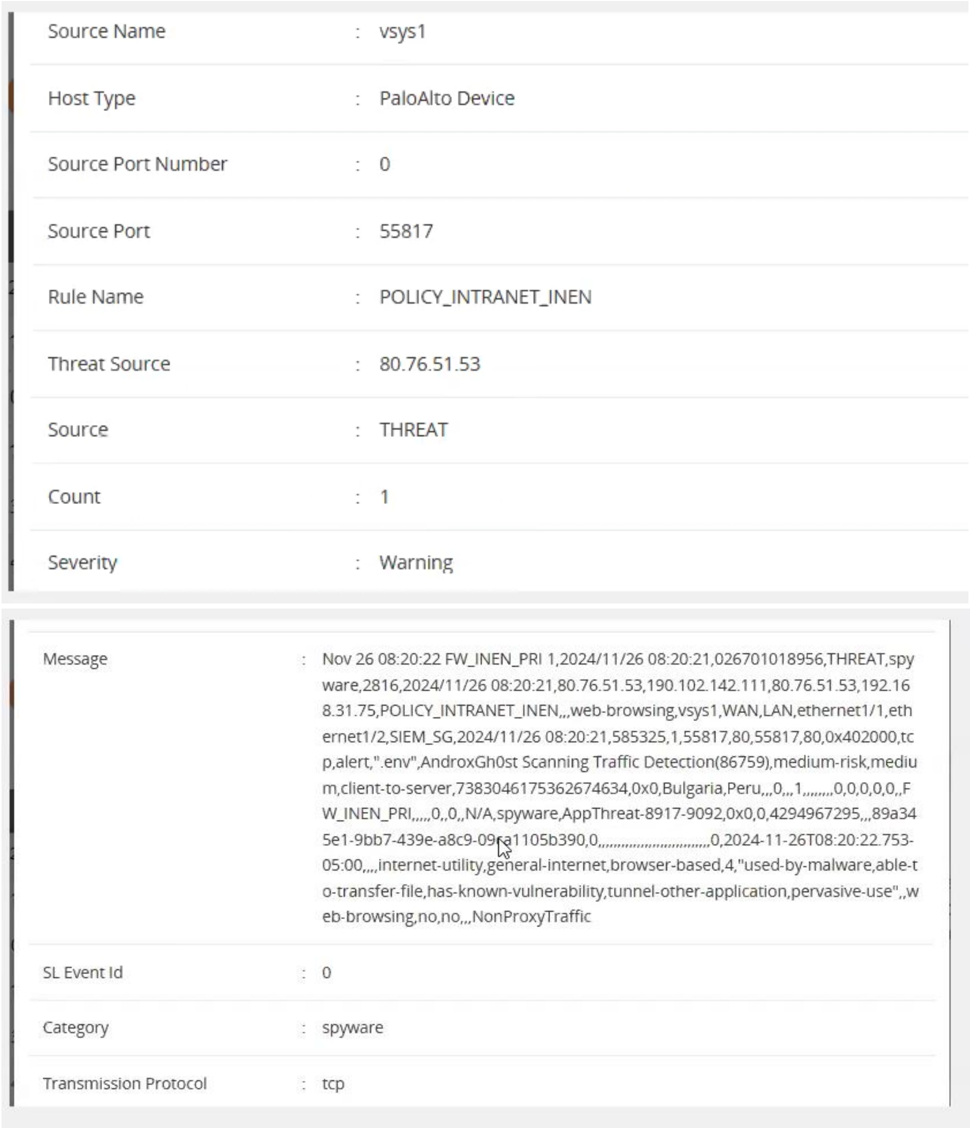
Nota. Se muestra principales indicadores del Log360

La gráfica 34 muestra una alerta generada por un dispositivo Palo Alto, donde se ha identificado una consulta al servidor desde Bulgaria. El evento está relacionado con un intento de acceso o actividad sospechosa detectada en la red interna, específicamente bajo la regla POLICY_INTRANET_INEN. El origen de la amenaza se encuentra en la dirección IP 80.76.51.53, que corresponde a Bulgaria, y se ha clasificado como una alerta de advertencia (Warning) debido a la actividad asociada con un spyware. El mensaje de la alerta describe un intento de ejecución de AndroxGhost Scanning Traffic

Detection, que es un tipo de malware utilizado para la transferencia de datos de forma no autorizada a través de protocolos de navegación web.

Figura 34

Alertas generada por Palo Alto



Nota. Se muestra una alerta y su interpretación

CONCLUSIONES

- La implementación del sistema SIEM estableció un mecanismo efectivo para detectar amenazas e incidentes de ciberseguridad en tiempo real lo cual mejoró la capacidad de respuesta del equipo seguridad frente a riesgos en la infraestructura tecnológica de la entidad pública del sector salud.
- El análisis de la situación inicial reveló principalmente que las alertas demoraban 45 minutos en promedio para tomar acciones reactivas, por lo que mediante la implementación del SIEM se toma acciones de manera inmediata y proactiva, validando las alertas generadas en el sistema.
- La implementación del SIEM identificó eventos de amenazas e incidente en un promedio trimestral de eventos de información 560212535.6 y detectando 660.3 alertas criticas en el periodo trimestral.
- En la validación se cumplieron el 100 % de las pruebas establecidas, sin pérdidas de paquetes en la prueba de conectividad, con un uso del CPU del 38 % y una memoria RAM de 59,25 GB durante el mes de noviembre de 2024, lo que demostró que el SIEM funciona de manera estable durante el periodo de evaluación.

RECOMENDACIONES

- Se recomienda realizar el monitoreo constante y actualizaciones periódicas del sistema SIEM para mantener su efectividad frente a nuevas amenazas.
- Dentro de la política de la empresa se recomienda un plan de capacitación al personal técnico en el uso y gestión del sistema SIEM para que se garantice las respuestas rápidas y eficaces ante incidentes.
- Se recomienda establecer políticas de seguridad informática para que se complementen el sistema SIEM, como la gestión de accesos y auditorías regulares.
- A futuros trabajos se recomienda integrar el SIEM con otras herramientas de seguridad como, por ejemplo, antimalware, anti DDoS, firewall de aplicaciones web para garantizar una mejora continua en la detección y respuesta efectiva ante nuevas amenazas de ciberseguridad.

REFERENCIAS BIBLIOGRÁFICAS

Alanazi, A. T. (2023). Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. *Cureus*, *15*(10), e47026. https://doi.org/10.7759/cureus.47026

AMBIT TEAM. (2021). *¿Qué significa SIEM y cómo funciona?* [En línea]. Blog de Ambit. https://www.ambit-bst.com/blog/qué-significa-siem-y-cómo-funciona

Añazco, J. D. (2021). *Sistema de gestión de eventos e información de seguridad (SIEM) de la infraestructura tecnológica de la universidad internacional SEK del Ecuador* [Universidad Internacional SEK]. https://repositorio.uisek.edu.ec/bitstream/123456789/4385/1/Tesis%20Jorge%20A%c3%b1azco%20final_14-10_2021.pdf

Aranda, O. (2018). Ciberseguridad y ciberdefensa: Prioridad nacional postergada. *Revista de Marina*, *956*(1), 1-15.

Ariffin, M. A. M., 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), Article 20. https://doi.org/10.3991/ijet.v17i20.32901

Avast. (2024). *¿Qué es un servidor proxy?* [En línea]. Blog Avast. https://www.avast.com/es-es/c-what-is-a-proxy-server

Bayona, L., & Palacios, L. E. (2019). *Implementación del software LOG360 para el cumplimiento del requerimiento 10 del estándar de seguridad de datos para la industria de tarjeta de pago* [[Tesis de grado, Universidad San Martin de Porres]]. https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/5431/lavado_sda.pdf?sequence=1&isAllowed=y

Bermudez, M. A. (2024). *Aplicación de estándares de ciberseguridad para proteger la información de las organizaciones* [Pontificia Universidad Católica del Perú]. https://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/27284/BERMUDEZ_TORRES_MARCO_ANTONIO.pdf?sequence=1&isAllowed=y

Broeders, D. (2021). Private active cyber defense and (international) cyber security—Pushing the line? *Journal of Cybersecurity*, *7*(1), 1-10.

Cabrera, G. (2021). *Implementación de un Sistema de Detección de Intrusos (IDS) mediante la inspección de tráfico de la red* [Trabajo de Universidad Oberta de Catalunya]. Universidad Oberta de Catalunya.

Cando, M. R., & Medina, R. P. (2021). Prevención en ciberseguridad: Enfocada a los procesos de infraestructura tecnológica. *3 c TIC: cuadernos de desarrollo aplicados a las TIC*, *10*(1), 17-41.

Cárdenas, H. P., Lorenzo, A. F., & Herrera, L. R. (2017). Directrices para la gestión de la Ciberseguridad utilizando el estándar ISO/ECT 27032. *Estudios en Seguridad y Defensa*, *12*(24), Article 24. https://doi.org/10.25062/1900-8325.253

Cervera, A., & Goussens, A. (2024). Ciberseguridad y uso de las TIC en el Sector Salud. *Atencion Primaria*, *56*(3), 102854. https://doi.org/10.1016/j.aprim.2023.102854

Cujabante, X. A., Bahamón, M. L., Venegas, J. C., & Quiroga, J. A. (2020). Ciberseguridad y ciberdefensa en Colombia: Un posible modelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, *18*(30), 357-377.

Defensoría del Pueblo. (2023). *La ciberseguridad en el Perú: Estrategías y retos del estado*. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

EGSInnova Group. (2022). ISO 27001—Sistemas de Gestión de Seguridad de la Información. *Software ISO*. https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

Equipo de Imagina. (2024). *¿Qué es la tecnología SIEM de Ciberseguridad?* [En línea]. Tutoriales de Imagina. https://imaginaformacion.com/tutoriales/que-es-la-tecnologia-siem

Gomero, R., & Sánchez, D. (2024). Ciberseguridad en servicios de apoyo al médico ocupacional de la ciudad de Lima. Estudio piloto. *Revista Médica Herediana*, *35*(1), 38-43. https://doi.org/10.20453/rmh.v35i1.5298

Gómez, J. C., Castaño, N. J., & Correa, L. C. (2023). Sistemas de detección y prevención de intrusos: Una taxonomía experimental basada en código abierto orientada a la industria 4.0. *Ciencia e Ingeniería Neogranadina*, *33*(1), 75-86. https://doi.org/10.18359/rcin.6534

Harris, A. (2024). *Comparison and Differences Between IPS vs IDS vs Firewall vs WAF* [En línea]. Networks Training. https://www.networkstraining.com/firewall-vs-ips-vs-ids-vs-waf/

IBM. (2024). *Paquete QRadar de IBM* [En línea]. Blog IBM. https://www.ibm.com/qradar

INCIBE. (2024). *¿Qué son y para qué sirven los SIEM, IDS e IPS?* [En línea]. INCIBE Empresas. https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips

Kriptos. (2024). *Informe de Ciberseguridad en el sector de la salud*. Kriptos. https://www.kriptos.io/es/es-post/ciberseguridad-sector-salud

LogRhythm. (2024). *LogRhythm SIEM*. Productos de Widefense. https://widefense.com/productos/logrhythm

Lopez, V. (2024, junio 26). *Ciberseguridad en el sector salud: Radiografía y cómo protegerse*. S2 Grupo. https://s2grupo.es/ciberseguridad-en-el-sector-salud-radiografia-y-como-protegerse/

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

Martínez, M. (2021). *Implementación de un centro de operaciones de seguridad (SOC) de código abierto con elementos de red para sistemas industriales.* [En línea]. Universidad Politécnica de Valéncia.

McAfee. (2023). *McAfee Enterprise Security Manager* [En línea]. Onasystems. https://www.onasystems.net/wp-content/uploads/2017/01/Ficha-tecnica-siem.pdf

Mishima. (2021). *EY Perú: Más del 60% de empresas peruanas muestra preocupación por su capacidad para enfrentar ataques de ciberseguridad*. https://www.ey.com/es_pe/news/2021/10/empresas-peruanas-preocupacion-ataques-ciberseguridad

Montalván, P. C. (2020). *Proyecto de actualización de los sistemas Firewall para mejorar la ciberseguridad en la Marina de Guerra del Perú* [Universidad de Piura]. https://pirhua.udep.edu.pe/backend/api/core/bitstreams/637cdc06-2e09-442d-895d-7b492cdbaa2f/content

Parra, C., & Yaqueline, X. (2018). Normatividad de ciberseguridad en el sector financiero colombiano. *Seminario de investigación aplicada de la gestión de la seguridad y el riesgo*, *1*(1). http://polux.unipiloto.edu.co:8080/00004756.pdf

Pérez, A. D. (2023). *Guía de implementación de un SOC* [En línea]. Universidad Oberta de Catalunya. https://openaccess.uoc.edu/bitstream/10609/147343/3/antoniodTFM1223memoria.pdf

Progress. (2022). *¿Qué es un servidor Syslog y cómo funciona?* https://www.whatsupgold.com/es/blog/que-es-un-servidor-syslog-y-como-funciona

PURESTORAGE. (2024). *¿Qué es SIEM? Definición y funcionamiento* [En línea]. Blog de PURESTORAGE. https://www.purestorage.com/es/knowledge/what-is-siem.html

Redacción EC. (2022, septiembre 21). El 62% de ciberataques tienen como objetivo los sectores de gobierno, minería y salud. *El Comercio*. https://elcomercio.pe/tecnologia/actualidad/el-62-de-ciberataques-tienen-como-objetivo-los-sectores-de-gobierno-mineria-y-salud-ciberseguridad-cibercriminales-espana-mexico-colombia-noticia/

Ruiz, Y. (2023). *Riesgos de la obsolescencia tecnológica para las organizaciones (Hardware y Software)*. https://www.b-secure.co/blog/riesgos-de-la-obsolescencia-tecnologica-para-las-organizaciones

SIEM. (2023). *¿Qué es la gestión de eventos e información de seguridad (SIEM)?* [En línea]. Topicos de IBM. https://www.ibm.com/es-es/topics/siem

Smart Global. (2024). *SmartGlobal Pagína Oficial* [En línea]. Ciberseguridad. https://www.smartglobal.pe/

Universidad Autónoma del Perú. (2024, julio 9). *Conoce los principios básicos de la seguridad informática* | *Blog Autónoma*. Universidad Autónoma del Perú. https://www.autonoma.pe/blog/principios-basicos-seguridad-informatica/

Vargas, M. (2023). *Ciberseguridad en Perú*. e ICEX España Exportación e Inversiones. https://www.icex.es/content/dam/es/icex/oficinas/065/documentos/2023/12/anexos/FS_Ciberseguridad%20en%20Per%C3%BA%202023_REV.pdf

Vasquez, W. F. (2023). *ImplementaciÛn de servicio de centro de operaciones de ciberseguridad (CYBERSOC) con plataformas opensource a entidad financiera* [Universidad Nacional Mayor de San Marcos]. https://cybertesis.unmsm.edu.pe/backend/api/core/bitstreams/7e3bac47-f219-4c12-94fc-5dab1667120d/content

Zegarra, J. C. (2020). *Desarrollo de un gestor de notificaciones multiagente para la reducción de los tiempos de diagnóstico y mitigación de fallos en redes IP* [[Tesis de posgrado, Universidad Nacional Mayor de San Marcos]]. https://cybertesis.unmsm.edu.pe/backend/api/core/bitstreams/fe9ed9da-ec2a-463f-8725-0885bb904b3b/content

ANEXOS

Anexo 1. Uso del CPU del SIEM durante noviembre del 2024

Uso de CPU	3-11	4-11	5-11	6-11	7-11	8-11	9-11	10-11	11-11	12-11	13-11	14-11	15-11	16-11	17-11	18-11	19-11	20-11	21-11	22-11	23-11	24-11	25-11	26-11	Promedio
Server	16.4%	25.8%	13.6%	15.5%	16.4%	10.7%	12.1%	23.1%	80.9%	64.1%	39.0%	61.7%	56.7%	18.9%	44.9%	53.5%	26.2%	12.4%	11.9%	10.5%	22.5%	56.6%	35.4%	6.8%	30.7%
ES	1.2%	0.7%	0.3%	1.2%	0.5%	0.3%	30.0%	30.0%	2.1%	2.2%	1.5%	2.3%	1.1%	50.0%	1.1%	90.0%	1.6%	50.0%	40.0%	40.0%	90.0%	1.0%	70.0%	40.0%	22.8%
Log collector	0.4%	0.4%	0.3%	0.4%	0.3%	0.2%	30.0%	40.0%	30.0%	40.0%	30.0%	30.0%	30.0%	30.0%	30.0%	30.0%	30.0%	30.0%	30.0%	20.0%	30.0%	30.0%	30.0%	20.0%	22.6%
Database	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	10.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	10.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	10.0%	1.3%
System usage	29.0%	36.3%	22.7%	22.2%	25.2%	16.7%	18.1%	28.1%	89.0%	69.3%	44.8%	70.0%	64.7%	24.6%	50.7%	58.8%	33.1%	18.5%	17.8%	16.4%	29.0%	65.0%	43.5%	12.9%	37.8%

Anexo 2. Uso de RAM del SIEM durante noviembre del 2024

Uso de RAM	3-11	4-11	5-11	6-11	7-11	8-11	9-11	10-11	11-11	12-11	13-11	14-11	15-11	16-11	17-11	18-11	19-11	20-11	21-11	22-11	23-11	24-11	25-11	26-11	27-11	28-11	Promedio
Server (GB)	8.8	7.5	8.1	8.3	8.3	8.3	8.8	9.1	9.4	9.7	8.8	9	8.1	8.8	9.1	7.5	8.1	8.1	8.1	8.2	8.8	9.3	9.5	9.6	9.6	9.6	8.71
ES (GB)	10.4	10.2	10.7	10.4	10.3	10.3	10.3	9.2	9	8.5	8.9	9	9.6	9.6	9.4	8.8	8.9	8.6	8.3	7.6	6.9	7.4	7.6	7.7	7.8	7.9	8.97
Log collector	0.12	0.10	0.11	0.11	0.11	0.11	0.11	0.12	0.12	0.13	0.12	0.12	0.11	0.12	0.12	0.12	0.13	0.13	0.13	0.14	0.14	0.12	0.12	0.12	0.12	0.12	0.12
Database	0.07	0.13	0.07	0.08	0.06	0.07	0.06	0.08	0.09	0.09	0.11	0.09	0.06	0.06	0.07	0.09	0.06	0.06	0.06	0.05	0.07	0.07	0.09	0.07	0.07	0.09	0.08
System usage	44.3	38.2	38.5	43.4	48	54.3	60.6	65.8	65.7	64.8	60.8	60.4	58.1	64.8	65.3	65.3	62.2	64.9	65.2	65.1	65.9	64.4	62.8	63.4	63.7	64.6	59.25

Anexo 3. Evidencia de reporte reactivo del cliente al equipo SOC antes de implementación del SIEM

De:
Enviado: lunes, 21 de octubre de 2024 10:53
Para:
Cc:
Asunto: Bloque de link ante posible ataque de PHISHING 21/10/2024 -

Buenos días Sres. del SOC

El presente correo es para saludarlos y al mismo tiempo, carácter de urgencia y previa coordinación con el Ing. euesolicitarles el bloqueo del siguiente link:

https://ddei5-0-ctp.trendmicro.com/wis/clicktime/v1/query?url=http%3a%2f%2fd0bdbe5b.verifiedsecure.net%2f&umid=BEB444E0-24F7-B406-81C8-900F6C17BDD8&auth=87669afb3f4a1f96264475959879ec1656b2c448-10a47017451dc5bb9166bae0e838c23f8cfb9459

Con el fin de evitar un posible ataque de phishing que pueda afectar a la información institucional.

Agradeciendo por su atención prestada, y esperando que la solicitud sea atendida a la brevedad posible, me despido.

Atte.

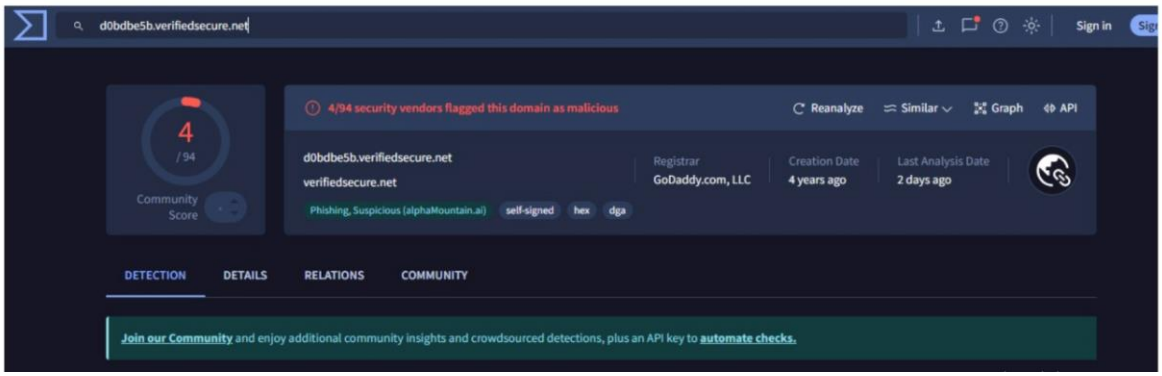
Enviado el: lunes, 21 de octubre de 2024 11:38
Para:
CC:
Asunto: RE: [Solicitud ID :#RE-30682#]: Bloqueo de link ante posible ataque de PHISHING 21/10/2024 || SG ||

REMITENTE EXTERNO
PrecauciÃ³n: Este mensaje es de un REMITENTE EXTERNO. No hagas clic en los ENLACES, ni abras los archivos ADJUNTOS si no reconoce al remitente.

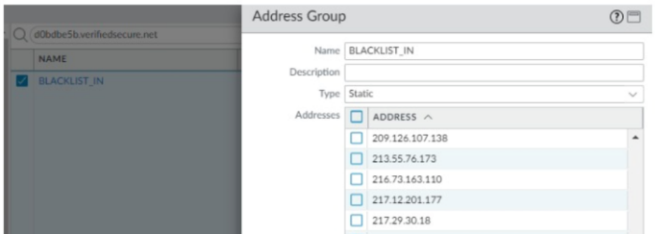
Estimado

Se procedió con el bloqueo del link indicado

Se adjunta la captura de pantalla con la(s) alerta(s) observada(s).



Política donde el link fue bloqueada.



Anexo 4. Evidencia de un correo posterior a tomar a realizar acciones reactivas

Re: [Solicitud ID :#RE-29733#]: CyberSOC - Network Device Attack ||[redacted]

N nsoc

Reply | Reply all | Forward

To: manyaypoma@inen.sld.pe

Sun 9/8/2024 1:16 AM

Cc: [redacted]com.pe; [redacted]sld.pe; [redacted]; Oscar[redacted]; **+4 others**

Estimados,

Se ha detectado y bloqueado una alerta sobre una actividad sospechosa hacia la red interna.

El tráfico malicioso se originó desde la IP 92.118.39.167 (zona WAN) y estaba dirigido a la IP interna 190.1[redacted] (zona LAN).

Prioridad: Critica

Sistema Fuente: Sistema de Detección de Amenazas: SIEM(EventLogAnalyzer)

Atacante (Origen):

- Dirección IP: 92.118.39.167
- Puerto/Protocolo: 65421/ TCP
- Aplicación: web-browsing
- Reputación: USA
- IOC / HASH: AndroxGh0st Scanning Traffic Detection(86760)

Víctima (Destino):

- Dirección IP: 19[redacted]
- Puerto/Aplicación: 80 /web-browsing
- Hostname: N/A
- Usuario: N/A

Análisis:

Se observó que la política 192[redacted]del dispositivo Palo Alto permitió inicialmente el tráfico entrante desde la IP 92.118.39.167 en USA hacia una dirección IP interna 19[redacted]en Perú. Esta IP maliciosa presenta las siguientes características:

- Comunicación detectada como tráfico de spyware.
- La IP reportada se encuentra en plataformas de detección de amenazas.

Recomendaciones:

Considerar la restricción de conexiones a países específicos, como USA para reducir el riesgo de exposición a amenazas que se originan desde regiones específicas.

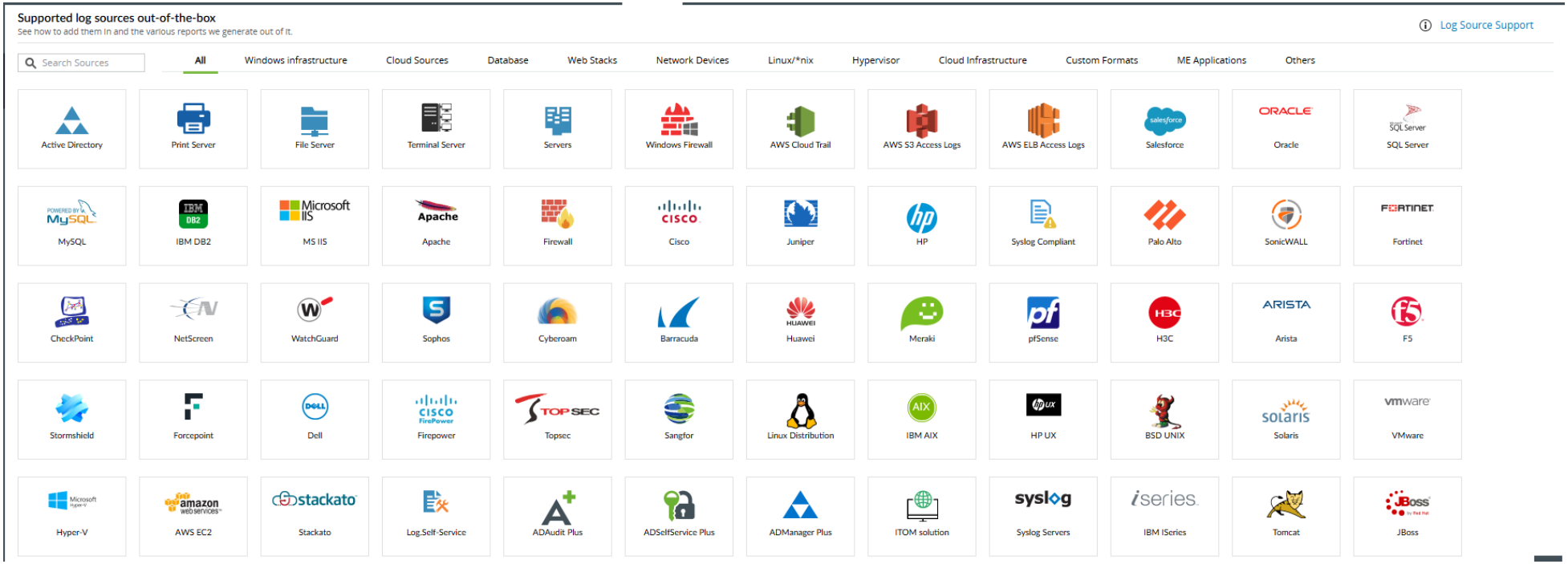
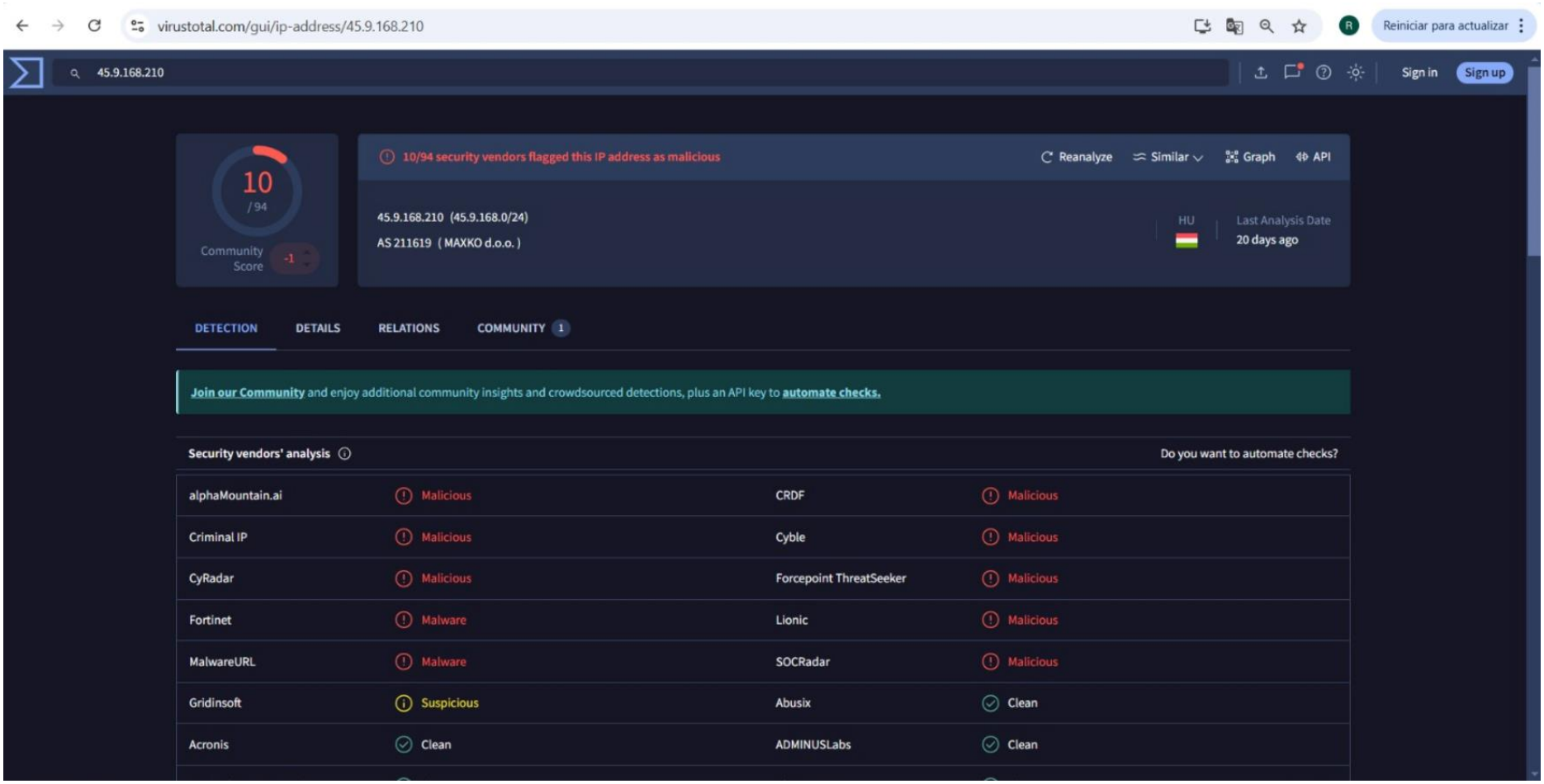
Política donde fue bloqueada la IP reportada.

76	POLICY-IP-BLOQUEO	PUBLICACION	WAN	BLACKLIST_IN	any	LAN	ALL-VIP-GRO DNAT_190.1

De lo comentado, se procede al cierre del ticket.

Saludos cordiales.

Anexo 5. Marcas de equipos compatibles con el Log360



Anexo 6. Motores de búsqueda para validar la reputación de la IP