UNIVERSIDAD INTERNACIONAL SEK

DIGITAL SCHOOL

TRABAJO DE FIN DE CARRERA

TITULADO:

“IMPLEMENTACIÓN DE UN GESTOR DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM) PARA LA PREVENCIÓN Y DETECCIÓN DE CIBER AMENAZAS EN UNA ENTIDAD GUBERNAMENTAL”

Realizado por:

Ing. Luis Alberto Darik Muñoz Alvarez

Director del proyecto:

MSc Ing. Juan Xavier Játiva Alvarez

Como requisito para la obtención del título de:

MÁSTER EN CIBERSEGURIDAD

QUITO, octubre 2022

DECLARACIÓN JURAMENTADA

Por la presente, yo, LUIS ALBERTO DARIK MUÑOZ ALVAREZ, declaro bajo juramento, que el trabajo aquí desarrollado es de mi autoría, que no ha sido previamente presentado para ningún grado a calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento. A través de esta declaración cedo mis derechos de propiedad intelectual de autoría a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente

_____

Luis Alberto Darik Muñoz Alvarez

DECLARACIÓN DE DIRECTOR DE TESIS

El presente trabajo de investigación titulado:

“IMPLEMENTACIÓN DE UN GESTOR DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM) PARA LA PREVENCIÓN Y DETECCIÓN DE CIBER AMENAZAS EN UNA ENTIDAD GUBERNAMENTAL”

Realizado por:

Ing. Luis Alberto Darik Muñoz Alvarez

Como requisito para la obtención del título de:

MÁSTER EN CIBERSEGURIDAD

Ha sido dirigido por mi persona a través de reuniones periódicas con la estudiante y cumple con todas las disposiciones que rigen los trabajos de titulación.

_____

MSc Ing. Juan Xavier Játiva Alvarez

DIRECTOR DEL PROYECTO

LOS PROFESORES INFORMANTES

Los profesores informantes:

MSc Ing. María Fernanda Palma Agama

Ing. José Luis Medina Balseca, Mgtr

Después de revisar el trabajo, lo han calificado como apto para su defensa oral ante el tribunal examinador

El profesor informante:

_____

MSc Ing. María Fernanda Palma Agama

_____

Ing. José Luis Medina Balseca, Mgtr

Quito, octubre de 2022

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es de mi autoría, que se han citado las fuentes correspondientes y que en su desarrollo se respetaron las disposiciones legales vigentes, que protegen los derechos de autor.

_____

Luis Alberto Darik Muñoz Alvarez

DEDICATORIA

Dedico el presente proyecto de
investigación a mi madre y a mi
hermano por su incondicional apoyo.

A un gran hermano y amigo que
siempre estuvo conmigo.
A mis familiares.

AGRADECIMIENTO

A Dios.

A mi hermano.

A mi madre.

A mi padre.

A mi tutor.

A mi tutora.

A mis profesores.

A la Universidad.

A la Entidad Gubernamental.

RESUMEN

En el siguiente proyecto de investigación se llevará a cabo un análisis preliminar del estado actual del sistema de información de la organización, y se implementará un Sistema de Gestión de Información y Eventos de Seguridad (SIEM), conforme a la necesidad de prevenir las amenazas, vulnerabilidades y riesgos que puedan presentarse, con lo cual, permitan alcanzar un mejor desempeño y mejora de la ciberseguridad en la infraestructura tecnológica de la entidad gubernamental. La aplicación de la herramienta apoyada en la ejecución de lineamientos, directrices, procedimientos de control y seguimiento ante posibles incidentes informáticos, permitirá la detección mediante medidas de monitorización, utilizando una herramienta SIEM denominada OSSIM AlienVault. A esto se añade, la posibilidad de evaluar el nivel de seguridad de la infraestructura tecnológica de comunicaciones y sistemas de información actual de la entidad gubernamental, y con ello, gestionar, controlar, resolver y mitigar posibles riesgos, vulnerabilidades y amenazas.

Palabras clave: OSSIM AlienVault, SIEM

ABSTRACT

In the following research project, a preliminary analysis of the current state of the organization's information system will be carried out, and a Security Information and Event Management System (SIEM) will be implemented, according to the need to prevent threats, vulnerabilities and risks that may arise, thereby allowing better performance and improvement of cybersecurity in the technological infrastructure of the government entity. The application of the tool supported by the execution of guidelines, directives, control and monitoring procedures against possible computer incidents, will allow detection through monitoring measures using a SIEM tool called OSSIM AlienVault. To this is added, the possibility of evaluating the security level of the current communications technology infrastructure and information systems of the government entity, and with it, managing, controlling, resolving and mitigating possible risks, vulnerabilities and threats.

Keywords: OSSIM AlienVault, SIEM

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1.1 Planteamiento del Problema

Se hace evidente que las organizaciones actualmente disponen de un elemento importante en el desarrollo de sus actividades, dicho elemento lo constituyen las Tecnologías de la Información y Comunicación. Así mismo, la utilización de sistemas de información para el beneficio de las organizaciones en sus procesos administrativos se ha vuelto fundamental y necesario; sin embargo, el riesgo emergente que surge a partir de la implementación de distintos tipos de sistemas informáticos hace que los activos de información de la organización se vean expuestos ante una serie de dificultades en su manejo y gestión, al igual que el resguardo de dicha información abre un campo de acción en cuanto a la ciberseguridad.

Según un informe oficial de MINTEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información), a través del viceministro de Telecomunicaciones, Patricio Real, en el año 2019, se informó que:

- El país ha recibido más de 40 millones de ataques informáticos, y ha ido incrementándose; a tal punto que el país ha sido ubicado en el puesto 31 a escala mundial en cuanto a volumen de ataques cibernéticos registrados.

- Las principales instituciones que tuvieron intentos de intrusión fueron: la Cancillería, el Banco Central, la Presidencia de la República, el Ministerio del Interior, el Servicio de Rentas Internas, la Corporación Nacional de Telecomunicaciones, algunos GAD's, el Consejo de la Judicatura, el Ministerio de Telecomunicaciones y Sociedad de la Información, el Ministerio de Turismo, el Ministerio del Ambiente y algunas Universidades del país. (MINTEL, 2019)

Según un estudio y análisis de Luis Eduardo Suastegui Jaramillo sobre ataques informáticos en el país durante la pandemia de COVID – 19, en el año 2022, señala que:

- El cibercrimen ha sido una amenaza para la economía mundial y el comercio electrónico; y al no haber controles de seguridad, propician delitos cibernéticos con afectación directa en la seguridad individual y el bienestar público, e impactos graves tanto en organizaciones individuales como corporativas.
- Los delitos cibernéticos suscitados durante la pandemia de COVID – 19 dejó consecuencias en la confidencialidad de los datos, en la integridad de la información y en la disponibilidad de los sistemas de procesamiento de datos.
- Una revisión de los incidentes ocurridos durante la pandemia de COVID – 19, reveló que no existe equilibrio entre los roles de prevención, detección y de respuesta frente a ataques cibernéticos. (Jaramillo, 2022)

En tal situación en la que instituciones públicas se han visto propensas y expuestas a ciberataques, ha puesto en consideración que los sistemas de información manejados en cada entidad se vean comprometidos con riesgo de sufrir la pérdida de información.

En el caso del GAD, se cuenta con antecedentes relacionados a ciberataques de los que ha sido afectado y de los cuales resaltan principalmente los siguientes:

- Expediente fiscal del año 2020, que especifica un presunto delito de ataque a la integridad de los sistemas informáticos, con investigaciones pre procesales pertinentes.
- Documentación referente al año 2020, cuyos informes técnicos señalan problemas de registro de documentos en el sistema de control de documentación, un reporte de encriptaciones de códigos maliciosos en toda la información a consecuencia de ataques cibernéticos, eventos con anomalías e inconsistencias suscitadas en la red de comunicaciones de la entidad.
- Informe técnico del estado de los servidores para el servicio de conectividad a internet del GADPS debido a inconvenientes con las direcciones IP públicas asignadas por el ISP.

1.2 Formulación del Problema

La gran mayoría de organizaciones públicas y privadas, no cuentan con sistemas de gestión de seguridad o centros de operaciones de seguridad, que permitan la supervisión y administración de la seguridad de los sistemas de información, para la oportuna prevención, detección, análisis y mitigación de incidentes de seguridad informática.

Con respecto a entidades públicas la situación es muy similar, la falta de una gestión y gobernabilidad de las TIC, sumado a la falta de un equipo o comité especializado en la seguridad de la información y otros factores asociados, contribuyen al deterioro de los sistemas de información manejados por dichas organizaciones haciendo más compleja la aplicación de medidas de control y diagnóstico que ayuden a la toma de decisiones.

Las entidades gubernamentales descentralizadas, como es el caso de los GAD's, no se encuentran exentos ante ciberataques o amenazas constantes a sus sistemas de información, como los antecedentes de ataques informáticos descritos por el MINTEL en las instituciones públicas del país. La información que manejan los GAD's contiene datos sensibles de las áreas administrativas, financieras, jurídicas, de recursos humanos, gestión de proyectos y obras públicas.

En principio, desde la creación del GADPS, se han realizado diversos cambios por cada administración política y un crecimiento del número de funcionarios de la entidad, dando lugar a una serie de inconvenientes que han ido aumentando en el transcurso del tiempo. El GADPS en la actualidad, mantiene sus actividades administrativas, operativas y tecnológicas en sus instalaciones generales, con una infraestructura de TIC dispuesta en

3 pisos y una torre de telecomunicaciones y a la vez proporciona conectividad a 3 áreas adscritas de campo.

El departamento TIC del GADPS, no cuenta con una gestión de registro o un sistema de análisis, control y monitoreo de eventos e incidentes de ciberseguridad, que permita administrar posibles eventos o amenazas de riesgo. A esto se añade la falta de controles para la infraestructura de comunicaciones de red, dejando a la entidad gubernamental proclive a posibles ciberataques, con afectación a la confidencialidad, integridad y disponibilidad de los sistemas y activos de información. Dado el crecimiento institucional y el desarrollo tecnológico, exige procesos de adaptación, renovación, gestión y control de seguridad prioritarios para un manejo organizado, ordenado de todos los activos de información.

El crecimiento acelerado de las infraestructuras de tecnologías de la información ha hecho que la implementación de un esquema de seguridad sea cada vez más necesario, sobre todo para entornos en organizaciones o entidades que desarrollan gran parte de sus actividades operativas utilizando recursos tecnológicos para su normal desempeño y continuidad diaria. Dicho crecimiento en la infraestructura tecnológica ocasiona un aumento del volumen de datos e información que debe ser analizado, incrementando la asignación de recursos de control y protección de los activos de la organización; lo que disminuye la capacidad de respuesta de los encargados de las TIC ante algún evento o incidente de seguridad. Lo que conlleva a una gestión que consolide y de cumplimiento a las normativas y reglamentos de la organización.

Para suplir las necesidades de seguridad a medida que el tamaño de la organización incrementa, se vuelve más complejo, requiriendo herramientas de seguridad especializada para la prevención, detección y mitigación oportuna con personal especializado que normalmente no disponen tanto las organizaciones privadas como públicas debido a los costos que implica. A esto se añade la falta o inexistencia de documentación de prácticas de seguridad y control de la información, complicando el análisis de datos posteriores. La comprensión de las bitácoras de información y el entorno que se analizará es primordial para determinar las acciones que se tomarán en relación con la actividad general de la red.

También se debe tomar en cuenta que las organizaciones almacenan en sus redes internas gran cantidad de dispositivos de diferentes fabricantes, marcas o proveedores, dando lugar al manejo de distintos tipos de formatos de registros (logs), y a un análisis complejo de datos e información. Otro punto que se debe considerar al garantizar la seguridad de los activos de información de la organización es la dificultad de las medidas de extracción de los datos relevantes a partir de los registros obtenidos, ya que algunos no suelen ser completos; es decir, no son descriptivos o detallados. Y para ello, es necesario que el personal especializado o el equipo de TIC conozca el entorno organizacional y el contexto en el que se generan los registros con ayuda de la implementación de un SIEM que permita la detección, almacenamiento y correlación de eventos a base de un análisis exhaustivo de los registros generados por cada uno de los activos (hosts) pertenecientes a la red de comunicaciones de la organización para el descubrimiento de posibles riesgos y amenazas que puedan surgir. Las herramientas existentes son variadas, pero la correcta elección debe ser examinada y ajustarse a las necesidades y funcionalidades pretendidas por la organización.

1.3 Objetivo general

- Implementar un Sistema de Gestión de Eventos e Información (SIEM), utilizando la herramienta de código libre OSSIM AlienVault, para la prevención y detección de incidentes, amenazas y ataques de seguridad en la infraestructura tecnológica de una entidad gubernamental.

1.4 Objetivos específicos

- Realizar el análisis del estado de situación actual de la infraestructura tecnológica de la entidad gubernamental mediante la inspección de sus instalaciones para el levantamiento de información.
- Implementar un servidor Linux mediante OSSIM AlienVault con sus configuraciones de seguridad para el control y monitoreo de amenazas y riesgos de seguridad.
- Determinar los lineamientos y mecanismos de detección de vulnerabilidades, mediante la utilización de herramientas de monitoreo, y obtención de datos para análisis prospectivos.

1.5 Justificación

1.5.1 Técnica

En un momento de transición, migración y transformación digital a nivel de las tecnologías de la información y comunicación, el uso de las redes de comunicaciones inalámbricas y periféricas es cada vez más frecuente, con usuarios en constante movimiento sin un lugar fijo de permanencia; además de otros factores como: el desarrollo tecnológico, la acelerada obsolescencia de equipos y dispositivos tecnológicos, y el aumento de la cantidad de dispositivos inteligentes sin ningún tipo de seguridad. Lo que conlleva a que los recursos de TI se encuentren expuestos ante constantes riesgos y amenazas como: malware, ransomware, phishing, ataques cibernéticos, entre otros; por tal motivo, organizaciones, empresas, instituciones gubernamentales y entidades corporativas requieren gestionar e implementar controles de seguridad consecuentes a las actividades que cada una desarrolla para establecer la aplicación de modelos, estrategias y mecanismos de prevención, anticipación, detección y reacción ante las amenazas, que proporcionen un aseguramiento y protección de los activos de información.

El control, la supervisión y gestión ininterrumpida de la actividad de datos en las redes de comunicaciones, servidores, equipos terminales, y bases de datos de una organización o empresa ofrece ciertos mecanismos y herramientas para la defensa ante incidentes e intrusiones de seguridad, sin verse al margen de una fuente, tiempo o tipo de ataque. De modo que, un sistema de gestión de eventos e información de seguridad en conjunto con un centro de operaciones de seguridad disminuye la brecha que existe entre el tiempo que demora un ciberataque al comprometer un sistema informático con el tiempo de detección

de una amenaza; logrando un mejor entorno de control propicio para mantener actualizados los sistemas de información.

Disponer de un centro de operaciones de seguridad permitirá proporcionar una mejora en la detección de incidentes de seguridad mediante el control, supervisión y análisis continuos y permanentes de la actividad de los datos e información en una determinada red de comunicaciones sin interrupción de la continuidad del negocio. Entre las razones principales de aplicación de una arquitectura e implementación SIEM por parte de las organizaciones se especifican las siguientes:

- La protección de datos confidenciales y críticos.
- El cumplimiento de normas y controles de seguridad.
- El cumplimiento de normas y regulaciones gubernamentales.

Además, en vista de la nueva era digital por la que atraviesa la sociedad moderna, y en términos del desarrollo de la ciberseguridad en el país, se ha establecido la Estrategia Nacional de Ciberseguridad, que propone lineamientos de seguridad en el ciberespacio con una aplicación de 3 años a partir del año 2022 basándose en 6 ejes de acción que son:

1. Gobernanza y coordinación nacional, que permitirá establecer un enfoque coordinado en relación con la ciberseguridad nacional.
2. Resiliencia cibernética, que permitirá la mejora de la resiliencia tanto a nivel nacional como organizacional que preparen, den respuesta y recuperación ante incidentes cibernéticos.

3. Prevención y lucha contra la cibercriminalidad, permitirá el fortalecimiento de las capacidades de prevención, investigación y seguimiento de delitos cibernéticos.
4. Ciberdefensa nacional, permitirá reforzar las capacidades de ciberdefensa para la protección de las infraestructuras de información crítica nacionales, así como los servicios esenciales del Estado; y desarrollar capacidades en ciber inteligencia que favorezcan la obtención de información relevante y oportuna sobre las amenazas existentes en el ciberespacio para la concerniente toma de decisiones.
5. Habilidades y capacidades de ciberseguridad, permitirá la mejora y ampliación de las habilidades y capacidades cibernéticas de la nación en todos los niveles.
6. Cooperación internacional, permitirá incrementar los beneficios de la cooperación internacional.

La estrategia como tal pretende brindar apoyo e impulsar un crecimiento digital en sectores como: el comercio electrónico, la protección de la información y transacciones financieras, la protección de los datos personales de los ciudadanos, y la protección de la información comercial, sea local o internacional. (MINTEL, Estrategia Nacional de Ciberseguridad del Ecuador, 2022)

La estrategia nacional para la ciberseguridad, puede tomar parte fundamental en la gestión de la ciberseguridad en las diferentes organizaciones, sean públicas o privadas, para el cumplimiento de políticas y el resguardo de los datos e información, considerando 4 principios de aplicación como:

1. Liderazgo y responsabilidad compartida
2. Salvaguardia de los derechos digitales

3. Gestión de riesgos de ciberseguridad y la resiliencia cibernética
4. Visión inclusiva y colaborativa

La Estrategia Nacional de Ciberseguridad se sustenta en 4 principios de aplicación y en 6 ejes de acción, de los cuales se derivan objetivos estratégicos por cada uno de ellos de la siguiente manera:

Objetivos de cada eje de acción:

1. Gobernanza y coordinación nacional:
    a. Establecer un marco integral para la gobernanza de la ciberseguridad.
    b. Fomentar una comunidad consistente y relacionada con expertos en ciberseguridad de las partes interesadas.
    c. Desarrollar un marco legal y regulatorio integral para la gobernanza nacional de la ciberseguridad y la ciberdefensa.
2. Resiliencia cibernética:
    a. Establecer un proceso integral para la gestión de riesgos de ciberseguridad y preparación ante crisis cibernéticas que fortalezcan dichas capacidades a nivel nacional.
    b. Adoptar un marco integral para la identificación, orientación y supervisión de los operadores de las infraestructuras críticas digitales.
    c. Continuar el desarrollo de capacidades de respuesta y gestión de incidentes cibernéticos, incluyendo al CERT nacional.

d. Maximizar el uso de tecnologías avanzadas y la innovación en el diseño de políticas y procesos que sean ágiles para el desarrollo de las capacidades de Ciber inteligencia.

3. Prevención y combate de la ciberdelincuencia
    a. Actualizar el marco legal y regulatorio del país respecto a la ciberdelincuencia que garanticen la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.
    b. Fortalecer la respuesta oportuna y las capacidades operacionales de investigación y judicialización de la cibercriminalidad.
4. Ciberdefensa
    a. Incrementar y fortalecer las capacidades de Ciberdefensa del país para alcanzar la actitud estratégica defensiva definida en la Política de la Defensa Nacional, que protejan la infraestructura crítica digital y los servicios esenciales en el ciberespacio.
5. Habilidades y capacidades de ciberseguridad
    a. Mejorar y ampliar la concientización sobre ciberseguridad en todos los niveles de la sociedad.
    b. Reforzar las habilidades necesarias en ciberseguridad con las partes interesadas.
    c. Asegurar que el sistema educativo imparta conocimientos y fortalezca habilidades referentes a la ciberseguridad.
6. Cooperación internacional
    a. Identificar las prioridades internacionales del país y desarrollar la capacidad de participación en la ciber diplomacia regional e internacional.

b. Fortalecer la participación del país en la cooperación bilateral, regional e internacional como respuesta a las amenazas en el ciberespacio. (MINTEL, Estrategia Nacional de Ciberseguridad del Ecuador, 2022)

1.5.2 Social

Las Tecnologías de la información y comunicación constituyen un punto fundamental en la democratización del conocimiento y la seguridad que implica su manejo; es así que, las TIC se han convertido en un elemento necesario para alcanzar un desarrollo social a nivel de individuos, de grupos sociales, y de naciones que conforman el mundo.

De acuerdo al planteamiento y objetivos de estudio, la investigación se fundamenta en la necesidad de establecer una arquitectura de seguridad que sea adaptable y que permita conocer de manera detallada los componentes requeridos para la implementación de un SIEM, con lo cual la afectación, o posibles impactos en el desarrollo y generación de datos puedan ser prevenidos, mitigados, y corregidos.

No obstante, se hace necesario conocer el estado de los sistemas e infraestructura tecnológica de la entidad gubernamental, debido a los riesgos de seguridad que puedan presentar, y cuyo impacto puede ocasionar afectación directa en el desempeño de los servicios implementados en la red interna de la organización, o impedir el cumplimiento de los objetivos. A esto, se suma la necesidad de un control y monitoreo por medio de mecanismos de alerta ante nuevos riesgos y posibles amenazas de seguridad.

1.5.3 Legal

Según el Decreto No. 1014 del Registro Oficial establece los siguientes artículos:

- Artículo 1.- El establecimiento como política pública para entidades de la Administración Pública Central la utilización de software libre en sus sistemas y equipamientos informáticos.
- Artículo 2.- Se entiende por software libre, a los programas informáticos que se utilizan y se distribuyen sin ninguna restricción, permitiendo el acceso a sus códigos fuente y a sus aplicaciones para realizar mejoras.
- Artículo 3.- Las entidades de la Administración Pública Central previa a la instalación del software libre en los equipos, verificarán la existencia de capacidad técnica de soporte necesario en el uso de este tipo de software.
- Artículo 4.- Se faculta la utilización de software propietario; es decir, que no es libre, únicamente cuando no exista una solución de software libre que pueda suplir las necesidades requeridas, o cuando haya riesgo de seguridad nacional, o el proyecto informático se encuentre en un punto sin retorno.
- Artículo 5.- Sea para software libre como software propietario, siempre y cuando cumplan los requerimientos, se dará preferencia a soluciones con un orden:
    - Nacionales con autonomía y soberanía tecnológica.
    - Regionales con componentes nacionales o con proveedores nacionales.
    - Internacionales con componentes nacionales o con proveedores nacionales.
    - Internacionales.

- Artículo 6.- La Subsecretaría de Informática, al ser un órgano de regulación y ejecución de políticas y proyectos informáticos en las entidades del Gobierno Central, realizará el control y seguimiento del decreto.
- Artículo 7.- Se encargarán de la ejecución del decreto los señores ministros coordinadores y el señor secretario general de la Administración Pública y Comunicación. (Delgado, 2008)

Según el Plan Nacional de Gobierno Electrónico 2018 – 2021 expedido por el MINTEL plantea 14 estrategias, de los cuales tres de ellas se enfocan en el robustecimiento de la ciberseguridad, la protección de los datos e información, y el intercambio de información con GAD municipales, cuyos principales beneficiarios son las personas naturales y jurídicas.

El Plan Nacional de Gobierno Electrónico propone un modelo incluyente con el ciudadano que sea eficaz y eficiente, ajustado a la política pública del Gobierno Nacional, que busca una mayor interacción entre los ciudadanos y el Estado; y comprenden 3 programas de gobernabilidad con sus respectivas estrategias que den cumplimiento a los objetivos del plan. (MINTEL, Plan Nacional de Gobierno Electrónico, 2018 - 2021)
Según el Acuerdo Ministerial Nro. 025-2019 por parte de MINTEL, establece el siguiente acuerdo especificando:

- Artículo 1.- Se expide el Esquema Gubernamental de Seguridad de la Información EGSI, que será de implementación obligatoria en las Instituciones de la Administración Pública Central e Institucional que dependerán de la Función Ejecutiva anexada al Acuerdo.

- Artículo 2.- Las Instituciones de la Administración Pública Central e Institucional que dependan de la Función Ejecutiva, realizarán una Evaluación de Riesgos sobre sus activos de información críticos, con lo cual deberán diseñar un plan de tratamiento de riesgos de la Institución, utilizando como referencia la "Guía para la gestión de riesgos de seguridad de la información".
- Artículo 3.- Se recomienda a las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, el uso de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.
- Artículo 4.- Las Instituciones de la Administración Pública Central e Institucional que dependan de la Función Ejecutiva, actualizarán o implementarán el Esquema Gubernamental de Seguridad de la Información EGSI en un plazo de 12 meses a partir de la publicación del acuerdo. La evaluación de riesgos, y el plan para el tratamiento de los riesgos de cada Institución se realizarán en un plazo de 5 meses y la actualización o implementación de los controles del EGSI (Esquema Gubernamental de Seguridad de la Información) se realizarán en un plazo de 7 meses. La actualización o implementación, se realizará en cada Institución de acuerdo al ámbito de acción, a la estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información.
- Artículo 5.- La máxima autoridad deberá designar, a nivel interno de la Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las áreas: Talento Humano, Administración, Planificación y Gestión Estratégica, Comunicación Social, Tecnologías de la Información, Unidades Agregadores de Valor y Asesoría a través del Área Jurídica. El Comité de Seguridad de la Información garantizará y facilitará la implementación de

iniciativas de seguridad de la información en la Institución o Entidad. En la primera convocatoria los Comités definirán la agenda y reglamento interno respectivamente.

- Artículo 6.- El Comité de Seguridad de la Información tendrá las siguientes responsabilidades:
    - Gestión para la aprobación de la política y normas institucionales de seguridad de la información, por parte de la máxima autoridad de la institución.
    - Seguimiento de cambios significativos de riesgos con afectación a los recursos de información ante posibles amenazas.
    - Conocer y supervisar la investigación y monitoreo de los incidentes de seguridad de la información de alto impacto.
    - Coordinación de la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en relación al EGSI.
    - Difusión de la seguridad de la información dentro de la Institución.
    - Coordinación del proceso de gestión de continuidad de la operación de servicios y sistemas de información de la institución por incidentes de seguridad no previstos.
    - El Comité debe convocarse bimensualmente o cuando sea necesario con sus respectivos registros y actas de reunión.
    - Realizar el informe a la máxima autoridad sobre los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

- Realizar el reporte a la máxima autoridad sobre las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
- Realizar recomendaciones a la máxima autoridad sobre mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

- Artículo 7.- El Comité de Seguridad de la Información (CSI) designará al interior de la Institución a un funcionario como Oficial de Seguridad de la Información (OSI), el cual, tendrá conocimientos de Seguridad de la Información y Gestión de Proyectos, y podrá ser responsable de la Unidad de Seguridad de la Información.
- Artículo 8.- El Oficial de Seguridad de la Información tendrá las siguientes responsabilidades:
  - Identificación de todas las personas o instituciones públicas o privadas, que influyen o tienen impacto en la implementación del EGSI.
  - Generación de propuestas de elaboración de la documentación del EGSI.
  - Asesoría a los funcionarios en la ejecución del Estudio de Gestión de Riegos de Seguridad de la Información en las diferentes áreas de la Institución.
  - Elaboración del plan de concienciación en Seguridad de la Información basado en el EGSI.
  - Elaboración del plan de seguimiento y control de la implementación de las medidas de mejora o de acciones correctivas.
  - Coordinación de la elaboración del Plan de Continuidad de Seguridad de la Información.

- Orientación y generación de un procedimiento adecuado de manejo de incidentes de seguridad de la información que puedan presentarse al interior de la Institución o entidad.
- Coordinación de gestión de incidentes de seguridad de alto impacto a través de otras instituciones gubernamentales.
- Mantenimiento organizado de la documentación de la implementación del EGSI.
- Verificación del cumplimiento de normas, procedimientos, y controles de seguridad institucionales que se hayan establecido.
- Realizar el informe al Comité de Seguridad de la Información sobre el avance de la implementación del EGSI, así como las alertas de impedimento de su implementación.
- Transferencia de la documentación e información de la que fue responsable el Oficial de Seguridad previo a la culminación de sus funciones al nuevo Oficial de Seguridad o al Comité de Seguridad de la Información. (MINTEL, Acuerdo Ministerial 025-2019, 2019)

Según el Acuerdo Nro. 006 – 2021 por parte del MINTEL, establece lo siguiente:

- Artículo 1.- Publicación de la Política de Ciberseguridad, que se encuentra anexa y que forma parte integral del presente Acuerdo Ministerial.
- Artículo 2.- El objetivo de la política es la construcción y fortalecimiento de las capacidades nacionales para garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio.

La política proporciona directrices que buscarán afianzar un ciberespacio seguro para contribuir al desarrollo social, económico y humano del país, así como la creación de confianza digital que favorezca el intercambio de información de bienes y servicios en línea. El enfoque será multisectorial y multidimensional debido al carácter transversal de la ciberseguridad. Por lo tanto, la política alcanza a sectores y actores, públicos y privados del país, con directrices para direccionar las acciones de las entidades de Administración Pública Institucional en dependencia de la Función Ejecutiva, en coordinación con los otros poderes del Estado, sociedad civil y ciudadanía en general.

- Artículo 3.- La ejecución del presente Acuerdo Ministerial, donde la Subsecretaria de Gobierno Electrónico y Registro Civil, ejecute las acciones necesarias para la implementación de la Política de Ciberseguridad. (MINTEL, ACUERDO MINISTERIAL 006-2021, 2021)

Según el Acuerdo Nro. MINTEL-MINTEL-2022-0022 aprobado y publicado, se menciona la Agenda de Transformación Digital 2022 a 2025, donde se indica el Marco Legal y Normativo para el desarrollo de la Transformación Digital, que incluye una Política de Transformación Digital que establece lineamientos políticos de referencia para el proceso de transformación digital enfocándose en los derechos establecidos en la Constitución de la República del Ecuador bajo los siguientes ejes: Gobierno electrónico, Seguridad Digital y Confianza, Infraestructura Digital, Tecnologías Emergentes para el desarrollo sostenible, Economía Digital, Cultura e inclusión Digital, Interoperabilidad, y Tratamiento de los Datos. (MINTEL, ACUERDO N° MINTEL-MINTEL-2022-0022, 2022)

1.5.4 Económica

Uno de los grandes factores que condiciona el desarrollo de proyectos tecnológicos es el financiamiento que se requiere para su desarrollo, sin dejar de lado que un impacto mayor puede producirse por la falta de establecimiento de un esquema de seguridad que permita y garantice la protección de los activos de información. Y de suscitarse un posible incidente de seguridad o delito cibernético que afecte a la organización, el impacto primario se dirige al ámbito financiero, ocasionando pérdidas económicas mayores que puedan superar el valor monetario de los propios activos con los que cuenta una organización.

En tal sentido, se hace imprescindible contar con un conjunto de actividades y procedimientos que ayuden a fortalecer y proteger el ciberespacio contra el uso indebido del mismo; en defensa de la infraestructura tecnológica, y de los activos de información que incluyen a los servicios prestados e información manejada; para con ello evitar un perjuicio económico a la organización.

1.6 Alcance

El presente proyecto permitirá establecer un esquema de seguridad complementario para el manejo, administración, control, detección, análisis, gestión, seguimiento y monitoreo de eventos e incidentes de seguridad que puedan ocurrir en la entidad u organización, siendo un mecanismo que contribuya a tomar medidas preventivas que puedan garantizar la protección de los activos de información y disminuir los riesgos de

seguridad en la infraestructura de red de la organización. Y dado el caso, podrá ser un referente para nuevas implementaciones en organizaciones similares o privadas que lo requieran. Adicionalmente, se busca la optimización en la gestión de control de eventos en tiempo real, aprovechando de forma integral las funcionalidades que incluye la herramienta SIEM; favoreciendo acciones para la gestión de activos, gestión de disponibilidad, gestión de notificaciones, gestión de vulnerabilidades, gestión de riegos, gestión de eventos, gestión de flujo de red, y monitoreo; de tal manera que permitan el desarrollo y desempeño de las actividades con normalidad en la infraestructura general de comunicaciones de red de la entidad gubernamental para una oportuna toma de decisiones.

1.7 Estado del arte

De acuerdo a diferentes fuentes de investigación, las perspectivas para la gestión, control, y monitoreo de eventos e incidentes de seguridad se hace mención en trabajos de investigación que pueden proporcionar un marco de referencia sobre el uso de una herramienta de gestión y monitoreo de la seguridad de una determinada red perteneciente a una organización o entidad para que mediante un análisis y comparativa se pueda seguir los procesos de aplicación en la entidad gubernamental; para lo cual, se presentan los siguientes trabajos que incluyen a diferentes autores para ampliar la óptica que tendrá la investigación:

Según el artículo científico de Ángel Heraldo Bravo, Álvaro Luis Villafuerte Quiroz, y José Patiño S., en el año 2015, denominado: “Implantación de una herramienta

OSSIM para el monitoreo y gestión de la seguridad de la red y plataformas Windows y Linux aplicado a empresas medianas", que indica:

- La herramienta OSSIM, no solo realiza la recolección de logs de diferentes dispositivos, sino que también es un SIEM (Security Information and Event Management) que incorpora diferentes formas de gestión de la seguridad.
- La herramienta OSSIM al ser implementado en una consola centralizada, proporcionará información útil para la toma de decisiones.
- La herramienta OSSIM permitirá la visualización de la disponibilidad de los servidores y dispositivos de una red, además de gran cantidad de información que puede ser analizada.
- La herramienta OSSIM al ser implementado en empresas medianas, permitirá optimizar la gestión y control de una gran cantidad de hosts, cuya administración dependerá de la organización de los equipos que conforman la red de la entidad.
- La factibilidad de la herramienta OSSIM, radica en los recursos que posee, que permitirán tener un mayor control de la seguridad, su puesta en marcha tanto para empresas públicas como privadas sin representar mayor costo para una organización.
- La herramienta OSSIM, permite la obtención de reportes personalizados sobre las posibles vulnerabilidades, amenazas, o ataques existentes en los hosts que conforman la red de una organización. (Ángel Bravo, 2015)

Según la investigación científica de Alexis Fernando Balarezo Chávez, en el año 2015, denominado: "Propuesta de mejoramiento de la herramienta OSSIM SIEM (open

source), para obtener los niveles óptimos de gestión en la administración de la seguridad, en una red implementada en cloud computing", que indica:

- La herramienta OSSIM para monitoreo y detección de incidentes, permite la verificación de amenazas en tiempo real, siendo capaz de correlacionar eventos en busca de patrones que identifiquen un ataque.
- La herramienta OSSIM permite analizar eventos que son recolectados en los archivos de logs que se encuentran en la red, ayudando a descubrir posibles ataques, mediante herramientas integradas de monitoreo y detección.
- OSSIM como una potente herramienta, se caracteriza por correlacionar eventos generados en una red al haber detectado patrones que se relacionen con ataques; y a partir de ello, establecer políticas que prevengan sucesos que puedan perjudicar a la organización, debido a un registro previo de la ocurrencia de eventos. (Poveda, 2015)

Según el trabajo de investigación de Leonela Jackeline Delgado y Jenninson Harolt Suárez, en el año 2015, denominado: "Análisis de la herramienta OSSIM AlienVault de correlación de eventos para la seguridad de la red", señala que:

- Las organizaciones no cuentan con procesos de monitorización para la seguridad de la red, quedando expuestos a constantes problemas que puedan ocurrir, por lo que, es importante el uso de una herramienta de código abierto que agrupe los datos recopilados de seguridad para una eficiente administración y monitoreo de la red, permitiendo optimizar la gestión de detección de anomalías.

- OSSIM AlienVault es una herramienta que permite la correlación de eventos, la detección de intrusos, monitoreo de dispositivos conectados a la red, el envío de alarmas que ayudan al administrador de red a prevenir incidentes y a obtener informes de los eventos suscitados en tiempo real para su respectiva corrección.
- Al contar con un control eficiente de seguridad de la red de una organización mediante procesos de monitoreo con la herramienta OSSIM AlienVault, se puede detectar posibles intrusos y cualquier problema que pueda ocurrir en tiempo real con base en la información de incidentes de seguridad obtenidos. (Asencio, 2015)

Según el trabajo de investigación de Diana Lissette Andrade España, realizado en el año 2016, denominado: "Evaluación del Sistema de Gestión de Seguridad de la Información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE)", se menciona lo siguiente:

- El sistema de gestión de seguridad de la información de una entidad sea pública o privada, debe identificar los riesgos a los que se expone la información, y que deben ser asumidos, mitigados y controlados de forma sistemática.
- Los activos de información dentro de una organización, deben ser protegidos y resguardados mediante la aplicación de estrategias y salvaguardas de alto nivel para alcanzar un control adecuado y una administración efectiva de los recursos informáticos.
- La verificación y cumplimiento de las políticas de seguridad de la información posterior a su elaboración, definición, documentación y sociabilización dentro de la institución, contribuirán al aseguramiento de la confidencialidad, disponibilidad e integridad de la información.

- Es fundamental dentro de toda organización realizar contantes capacitaciones en cuanto a la seguridad de la información y su tratamiento.
- La norma ISO 27001 permitió conocer las condiciones en las se encontraba el GADPE en términos de seguridad de la información, con resultados alineados con la evaluación del sistema de gestión de seguridad de la información.
- El instrumento de evaluación, basado en COBIT, permitió cuantificar los niveles de riesgo y confianza del GADPE. (España, 2016)

Según el trabajo de investigación de Christian José Castillo Valarezo, en el año 2018, denominado: "Implementación de un sistema de gestión centralizada de seguridad de información y eventos a través del software Open Source OSSIM", indica que:

- Los resultados de una implementación de la herramienta bajo pruebas de concepto ofrece algunos beneficios que comprende: el monitoreo de transacciones en bases de datos en tiempo real, el descubrimiento de servidores y servicios de bases de datos y aplicaciones, la clasificación de información en las bases de datos, el análisis de vulnerabilidades en motores de bases de datos, la gestión de riesgos, la revisión del aprendizaje automático de la base de datos, la creación de reportes de la información monitoreada para que sea almacenada, la creación de políticas de auditoría y seguridad, la configuración de alertas, la administración de roles y usuarios, y un análisis de desempeño.
- La plataforma OSSIM no tuvo problemas durante las pruebas de concepto sin presentar alertas de disponibilidad o rendimiento.
- Un análisis de vulnerabilidades permite evidenciar la exposición al riesgo al que se encuentra la institución implicada.

- Los reportes para el análisis de tráfico monitoreado, proporcionan información relevante a los administradores de bases de datos. (Valarezo, 2018)

Según el trabajo de investigación de Díaz Lima Francisco de Jesús, en el año 2018, denominado: “Implementación modular de un sistema de centralización y correlación de eventos de seguridad de la información (SIEM)”, indica que:

- Un factor importante de acuerdo a las diferentes soluciones SIEM es la arquitectura en la que se establecen sus operaciones, donde una arquitectura modular proporciona una correlación minuciosa y centralizada de los eventos de seguridad debido a las mejoras identificadas, que permiten un análisis de información segmentado y delimitado de forma más precisa de acuerdo a los niveles de abstracción de datos.
- La existencia de herramientas SIEM es variado, con un aporte diferente por cada producto, y un enfoque distinto de funcionalidades que pueden ofrecer un sistema funcional de administración, análisis, correlación y almacenamiento de registros al haber un adecuado procedimiento de planificación e implementación para el cumplimiento de requisitos que se adapten a las necesidades de cada organización.
- Un SIEM puede proveer información relevante que permitirá la mejora de la inteligencia operativa, efectividad de respuesta ante incidentes, y la detección de falencias en los sistemas; convirtiéndose en una pieza importante mediante una planificación previa. (Lima, 2018)

Según el trabajo de investigación de Joel Fernando Banchón Montaleza y Alexandra Mabel Zalabarria Zamora, en el año 2019, denominado: “Monitoreo y gestión

de seguridad sobre la infraestructura de red mediante la implementación de una herramienta OSSIM aplicando al sector de la mediana empresa", señala que:

- OSSIM AlienVault permite no solo realizar la recolección de logs (registros) de los hosts (equipos terminales), sino que permite la gestión de la seguridad.
- OSSIM permite la visualización de los recursos de servidores y dispositivos de red para la detección y mitigación de riesgos y vulnerabilidades que hayan sido generados por los usuarios en la red interna de una organización.
- La implementación de la herramienta OSSIM, permitió el desarrollo de seguridades informáticas para la mitigación de vulnerabilidades dentro de una infraestructura de red, la optimización de la gestión y control del tráfico generado con una previa administración organizada y detallada de toda la infraestructura y equipos de red. (Alexandra, 2019)

Según el trabajo de investigación de Mariella Anabel Estela Campos, en el año 2020, denominado: "Implementación de un Security Information and Event Management (SIEM) para detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de una entidad financiera", señala que:

- La implementación de una plataforma SIEM, con apoyo de controles de endpoints (dispositivos informáticos remotos), checkers (verificadores) y redes, se puede mitigar riesgos, evitar pérdidas económicas y pérdidas de información.
- Una herramienta SIEM de seguridad puede garantizar la disponibilidad de los activos de información, el cumplimiento de las normativas, el aseguramiento de

la continuidad del servicio y dar un seguimiento de la confidencialidad, integridad, y disponibilidad de los activos de información.

- La entidad donde fue implementado el SIEM, pudo reducir la carga laboral, los costos empresariales, consiguiendo una escalabilidad en la economía.
- La implementación del SIEM, permitió priorizar alertas de seguridad, haciendo que el SOC se concentre en incidentes sospechosos con alta probabilidad de ocurrencia. (Campos, 2020)

Según un artículo de Jorge Enrique Alvarado Chang, realizado en el año 2020, denominado: "Análisis de ataques cibernéticos hacia el Ecuador", señala lo siguiente:

- Los ataques cibernéticos han sido uno de los delitos informáticos que se han incrementado desde el año 2005, donde el robo y pérdida de información con afectación en las entidades tanto públicas como privadas son sus principales consecuencias.
- El país, presenta falencias que deben considerarse para una identificación de riesgos, a esto se añade la falta de organización en las instituciones de control, la falta de un plan de respuesta ante ciberataques; donde una implementación adecuada de ciberseguridad recae en la creación de una entidad enfocada a la protección cibernética a nivel nacional, mediante procesos de identificación y clasificación de las infraestructuras críticas y sectores vulnerables del país en caso de ataques cibernéticos.
- Las personas deben estar informadas sobre los riesgos que pueden presentarse al utilizar el ciberespacio; donde las entidades de control deben publicar un informe

anual que contenga información de todos los ataques cibernéticos suscitados, y las medidas de contingencia utilizadas para mitigarlos. (Chang, 2020)

Según el trabajo de investigación de Nicole Mónica Moran Maldonado, realizado en el año 2021, denominado: "Estado de la ciberseguridad en las empresas del sector público del Ecuador: una revisión sistemática", menciona que:

- El aumento de ataques cibernéticos exige en las instituciones públicas el diseño de soluciones de mejora de la seguridad tecnológica, que prevengan pérdidas de información confidencial, y recursos del estado.
- La identificación del estado de la ciberseguridad en la gestión de empresas públicas del Ecuador, mediante una revisión sistemática y aplicando un estudio exploratorio de datos encontrados; se concluyó, que el estado de la seguridad en las instituciones públicas está en constante exposición a ciberataques, siendo una vía de alto riesgo que puede ser identificable por medio de controles.
- Un modelo de seguridad basado en herramientas de seguridad y gestión de información de usuarios externos e internos con controles de acceso a información crítica dentro de organizaciones públicas se traslada al uso de arquitecturas de verificación de identidad que permitan disminuir riesgos para tomar control de las vulnerabilidades presentes por el uso de tecnologías.
- La tecnología de seguridad de las redes en el Ecuador se ha utilizado para el resguardo de la información y de recursos tecnológicos, mediante una revisión de gestión sistemática de seguridad, ya sea de la información circundante a los servicios como de los medios tecnológicos de transmisión de datos soportados por las plataformas de las entidades públicas. (Maldonado, 2021)

Según el artículo de investigación de Enrique Colon Ferruzola Gómez, Óscar Xavier Bermeo Almeida, Lissett Margarita Arévalo Gamboa, en el año 2021, denominado: “Análisis de los sistemas centralizados de seguridad informática a través de la herramienta AlienVault OSSIM”, indica que:

- Al haber efectuado un análisis sobre los procesos actuales que tienen las organizaciones o empresas, mediante pruebas en distintos escenarios de la red, se logró identificar que las organizaciones no poseen procesos de monitorización para la seguridad de una red, que en cierta medida se vuelve un factor perjudicial debido a la exposición ante las constantes amenazas que puedan presentarse. Por tal razón, el uso de una herramienta de agrupación de datos de seguridad informática para una administración y monitoreo de la red en una organización o empresa es de gran utilidad por la facilidad de manejo que proporciona a los administradores de red, permitiendo el seguimiento de eventos, la optimización de la gestión de seguridad debido a posibles intrusiones, anomalías o ciberataques; siendo a la vez una solución ante problemas que puedan suscitarse en la red.
- OSSIM AlienVault es una herramienta independiente que permite la correlación de eventos, la detección de intrusos, el monitoreo de dispositivos conectados a la red, y el envío de alarmas que informan sobre posibles eventos de riesgo; lo que ayuda al administrador de red a efectuar la prevención de incidentes y a obtener informes en tiempo real para su debida corrección y seguridad de la red de la organización o empresa. (Ferruzola Gómez & Arévalo Gamboa, 2021)

Según el trabajo de investigación de Unai Abrisqueta Sánchez, en el año 2021, denominado: “Diseño, despliegue e Inteligencia de una herramienta SIEM”, señala que:

- Mediante la implementación de un sistema SIEM se puede alcanzar el aseguramiento y control de una infraestructura de red privada para su monitoreo, proporcionando una capa de seguridad. (Sanchez, 2021)

Según el artículo científico de Gustavo González Granadillo, Susana González Zarzosa, y Rodrigo Díaz, publicado en el año 2021, denominado: "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures", señala que se han desarrollado sistemas de gestión de eventos e información de seguridad (SIEM) como una respuesta de ayuda a los encargados de TI para el diseño de políticas de seguridad y administración de eventos desde diferentes fuentes.

El SIEM, normalmente se compone de bloques separados que incluyen: dispositivo fuente, recopilación de registros, normalización de análisis, motor de reglas, almacenamiento de registros, supervisión de eventos, entre algunos más; con un funcionamiento independiente entre cada uno de ellos, pero de no haber un trabajo en conjunto, el SIEM no funcionará correctamente.

Las tecnologías desarrolladas para plataformas SIEM proporcionan un análisis en tiempo real sobre eventos e incidentes de seguridad generados por los dispositivos de red y aplicaciones; y aunque tengan la capacidad de dar respuesta para automatizar procesos de selección y despliegue de contramedidas, los sistemas de respuesta actuales realizan una selección y despliegue de medidas de seguridad sin efectuar un exhaustivo análisis de impacto de ataques y escenarios de respuesta.

La investigación también menciona que:

- De acuerdo a un análisis de comportamiento y análisis e implementación de riesgos, las técnicas y herramientas de análisis, evaluación, y guía de implementación óptima de mecanismos de seguridad en la infraestructura que sea administrada deben desarrollarse para implementar diferentes sensores que puedan ser redundantes.
- Aunque la mayoría de las soluciones SIEM proporcionan interfaces gráficas, las capacidades de visualización y reacción se limitan por el manejo de grandes cantidades de eventos recopilados. De modo que, se deben desarrollar extensiones de visualización y análisis, que proporcionen a los usuarios el conocimiento para una eficiente toma de decisiones.
- La mayoría de las soluciones SIEM incluyen capacidades de almacenamiento de datos, que están limitadas por la disponibilidad del hardware, requiriendo productos adicionales que van con el aumento del precio. (Gustavo González Granadillo, 2021)

Según el trabajo de investigación de Andy Alcides Mora y José David Villacreses, en el año 2022, denominado: “Plan de fortalecimiento ante ataques informáticos del hospital de especialidades Portoviejo basados en sistemas de correlación de log”, señala que:

- La implementación de una herramienta de gestión y monitoreo de seguridad centralizado basado en la correlación de logs (registros), permite una optimización de los recursos de red de una organización; por lo que OSSIM AlienVault es

recomendable por las características de administración, de requerimiento de sistema, soporte, y uso de las que dispone.

- Entre los sistemas de correlación de logs (registros) existentes, la herramienta OSSIM AlienVault permite la recolección de información desde dispositivos que se encuentren conectados a la red, los cuales convergen con herramientas de monitoreo y detección integradas en OSSIM para el descubrimiento de posibles anomalías.
- La implementación de un sistema de seguridad centralizado y de correlación de eventos de log como OSSIM AlienVault a un costo mínimo, proporciona información de utilidad a un administrador de red, ayudando a la mejora continua y toma decisiones a través de una consola de gestión centralizada. (Villacreses, 2022)

CAPÍTULO II

MARCO TEÓRICO

La administración y centralización de un sistema de gestión de incidentes agrupa diferentes conceptos que permiten establecer parámetros referenciales que sustenten el trabajo de investigación, los cuales se describen a continuación para la comprensión de la seguridad de la infraestructura tecnológica de red, activos de información, políticas y herramientas de gestión de seguridad.

2.1 Seguridad de la información

Se puede definir como el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información; es decir, la preservación de la confidencialidad, integridad, y disponibilidad de la información, a través de políticas, mecanismos, y medidas que afectan al tratamiento de los datos utilizados en una organización. (IEC, 2018)

La seguridad de la información asegura la confidencialidad, la integridad, y la disponibilidad de la información con el fin de garantizar un desarrollo sostenido de una organización, así como también su continuidad, minimizando las posibles consecuencias ante incidentes de seguridad de la información y aplicando una gestión de controles

adecuados que requieren ser especificados, gestionados, implementados, monitorizados, revisados y mejorados. (IEC, 2018)

2.2 Seguridad informática

La seguridad informática cada vez toma más importancia, por lo que empresas, organizaciones, entidades e instituciones gubernamentales, así como también la gran mayoría de usuarios conectados a la red de internet; se han visto en la necesidad de encontrar formas de protección ante posibles incidentes. Por lo que, la seguridad informática consiste en un conjunto de medidas que impiden la ejecución de las operaciones no autorizadas sobre un sistema o red informática, que pueden ocasionar daños sobre la información, y comprometer su integridad, confidencialidad, autenticidad, y disponibilidad, disminuyendo el rendimiento de los equipos o bloqueando el acceso de los usuarios que están autorizados para ingresar al sistema. (Vieites, 2014)

2.3 Principios de la seguridad informática

La relevancia que va tomando la seguridad de la información frente a los diferentes acontecimientos de ataques cibernéticos a nivel global, está ocasionando que todos los actores que están involucrados con la tecnología concienticen el valor que tienen los recursos de información y su constante exposición, en la continuidad de las actividades y procesos en los que se desarrollan.

Es por ello, que garantizar la protección y el correcto funcionamiento de los activos de información deberá estar sujeto a principios fundamentales de seguridad que son:

2.3.1 Confidencialidad

Es un principio de seguridad que garantiza que la información solo sea accesible e interpretada por personas o sistemas autorizados. (Santos, 2006)

2.3.2 Integridad

Es un principio de seguridad informática que garantiza que la información solo pueda ser alterada o modificada por personas autorizadas o usuarios legítimos. (Santos, 2006)

2.3.3 Disponibilidad

Es otro principio de seguridad que asegura que la información sea accesible en el momento que sea necesario por personas autorizadas. (Santos, 2006)

Existen adicionalmente 2 principios deseables que también pueden incluirse en la protección de los datos e información como: la autenticación y el no repudio.

2.3.4 Autenticación

Es un principio de seguridad adicional que permite la comprobación de la identidad de las personas en una comunicación para garantizar que son quienes dicen ser, asegurando así el origen de la información. (Santos, 2006)

2.3.5 No repudio

Este principio de seguridad adicional conocido también como irrenunciabilidad que permite probar la participación de las partes involucradas en una comunicación. (Santos, 2006)

2.4 Ciberseguridad

La ciberseguridad se puede definir como un conjunto de medidas de protección de la información, mediante el tratamiento de amenazas que pueden afectar y poner en riesgo la información tratada por los sistemas de información que se encuentran interconectados. (ISACA, 2015) Se hace necesario conocer ciertos conceptos que normalmente se presentan en la seguridad:

2.5 Incidente de seguridad

Puede definirse como un evento singular o una serie de eventos de seguridad de la información, que son inesperados o no deseados, con una probabilidad significativa de comprometer las operaciones de un negocio, de provocar la interrupción de los servicios suministrados por un sistema informático, y sobre todo de amenazar los activos, y la seguridad de la información de una organización. (IEC, 2018)

2.6 Evento de seguridad

Puede describirse como la ocurrencia o cambio de un conjunto particular de circunstancias, considerando que:

- Un evento puede ser único o repetido, debido a varias causas.
- Un evento puede consistir en algo que no se llega a producir.
- En ocasiones, un evento puede calificarse como un incidente o un accidente. (IEC, 2018)

2.7 Vulnerabilidad de seguridad

Puede entenderse como cualquier debilidad en un sistema informático que pueda permitir a cualquier amenaza posible causar daños y generar grandes pérdidas en una organización. (Vieites, 2014)

2.8 Amenazas de seguridad

Se considera amenazas a cualquier evento accidental o intencionado que pueda ocasionar algún posible daño en un sistema informático, cuya afectación puede ser significativa con pérdidas materiales, económicas, financieras, u otros similares en una organización. (Vieites, 2014)

2.9 Impacto de seguridad

Se puede definir como la medición y valoración del daño que podría ocasionar a una organización un incidente de seguridad. Para la medición del impacto del daño en una organización puede ser categorizada como: alto, medio, o bajo. (Vieites, 2014)

2.10 Riesgo de seguridad

Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático; es decir, la posibilidad de que las amenazas puedan explotar las vulnerabilidades de un activo o grupo de activos de información, provocando un determinado impacto en una organización. (Vieites, 2014)

Controlar la seguridad de la infraestructura general de red de una organización puede ser aplicable mediante políticas de seguridad que proporcionen una guía de acciones

acertadas de gestión para garantizar la protección de los datos e información. Para ello, es necesario conocer algunos conceptos.

2.11 Políticas de seguridad

La planificación permite el planteamiento de objetivos y la definición de líneas de acción para su ejecución; donde el modo para representar las mejores acciones, y expectativas de una organización es la elaboración de políticas de seguridad. Las políticas describen las reglas que una organización espera que se cumplan por sus miembros, y de no ser acatadas, establecer las correspondientes sanciones debido a las consecuencias ocasionadas. Las políticas pueden afectar a todos los recursos de una organización como: hardware, software, accesos, personal, comunicaciones, redes, contratación de personal, sistemas, entre otros; lo que hace necesario considerar las áreas importantes para la organización.

Normalmente, el número de políticas corresponde al número de áreas identificadas en los objetivos de seguridad, con lo cual, una política de seguridad de la información comprende tres tipos:

- Política de seguridad de la información a nivel empresarial (Enterprise Information Security Policy o EISP): se ocupa de los aspectos de interés para una organización o empresa, siendo la primera en ser creada, y a partir de ella se elaboran las demás con un enfoque hacia la resolución de problemas específicos. La política no debe experimentar cambios frecuentes, porque pierde credibilidad,

y debe ser firmada por la alta Dirección y estar alineada con las estrategias generales de la organización.

- Políticas de seguridad de asuntos específicos (Issue-Specific Security Policy o ISSP): se ocupa de asuntos específicos, como un determinado servicio de red, departamento o función, que no afectan a una organización. Estas políticas constituyen una guía detallada para instruir al personal en cuanto al uso de sistemas basados en la tecnología. El objetivo es el establecimiento de bases sobre el uso adecuado o inadecuado de la tecnología, como: el uso del correo electrónico, el uso de la navegación web, el uso de fotocopiadoras e impresoras, el uso del teléfono móvil, el uso de dispositivos y equipos de comunicaciones, o el uso de recursos de la organización en el hogar, etc.
- Políticas de seguridad de sistemas específicos (System-Specific Policy o SysSP): se ocupan en los sistemas individuales o tipos de sistemas, y prescriben el hardware y software aprobados, diseñan los métodos para fortalecer un sistema, especifican los tipos de cortafuegos, u otras medidas de control. Normalmente, estas políticas funcionan como estándares o procedimientos para configurar o mantener sistemas. (García, 2004)

También desde otra perspectiva, las políticas pueden clasificarse como:

- Regulatorias: que discuten las regulaciones y procedimientos a seguir cuando se aplica algún tipo de legislación o cumplimiento a la actividad de una organización.
- Consultivas: que definen los comportamientos, actividades aceptables y las consecuencias de su transgresión.

- Informativas: que proporcionan información o conocimientos sobre temas específicos, como los objetivos de la organización, las interacciones con clientes y proveedores, sin que sean de cumplimiento obligatorio. (García, 2004)

Las políticas deben implementarse en una organización con el fin de que los objetivos de seguridad se formalicen, se concreten, y se desarrollan mediante la creación de una jerarquía de documentación, donde cada nivel se consolida en un tipo o categoría de información y problema. En el nivel más alto, se encuentran las políticas de seguridad, que resumen las necesidades de seguridad de una organización, el siguiente nivel lo constituyen los estándares, que definen los requisitos obligatorios para el uso homogéneo de hardware, software, tecnología, y controles de seguridad; y en el último nivel se encuentran las normas, directrices y procedimientos. (García, 2004)

- Políticas: Son los documentos estratégicos que especifican las reglas que deben seguirse o requisitos de seguridad que deben cumplir los activos de una organización.
- Estándares: Son documentos tácticos que especifican el uso de la tecnología con el propósito de cumplir los objetivos definidos en las políticas de seguridad. La estandarización de los procedimientos operativos favorece a una organización, al especificar metodologías que se utilizarán en la implantación de medidas de seguridad. Los estándares normalmente son de carácter obligatorio y se implantan en toda la organización para conseguir la homogeneidad.
- Normas, directrices y procedimientos: Las normas definen el mínimo nivel de seguridad que cada sistema de una organización debe cumplir. Las directrices, son recomendaciones que deben seguirse, aunque no de manera obligatoria; ya que

pueden adecuarse para cada sistema o situación. Los procedimientos, comprenden los pasos a seguir para realizar una tarea específica, proporcionando los pasos para implantar las políticas, estándares, normas, y directrices creadas previamente. (García, 2004)

2.12 Gestión de seguridad

La gestión de la seguridad implica actividades para dirigir, controlar, y mejorar de forma continua una organización dentro de estructuras adecuadas, y dichas actividades incluyen la acción, la forma, la práctica, el manejo, la dirección, la supervisión y control de los recursos. Las estructuras de gestión se extienden desde un único individuo hasta grupos de individuos en organizaciones pequeñas, medianas, o grandes. En términos del SGSI, la gestión implica la supervisión, y la toma de decisiones que permitan alcanzar los objetivos de negocio mediante la protección de los activos de información de una organización. La gestión de seguridad de la información involucra la formulación, y el uso de políticas, normas, procedimientos, y guías de seguridad de la información, aplicadas en una organización; que se lleva a cabo por los individuos vinculados a la misma. (IEC, 2018)

2.13 Sistema de gestión

Un sistema de gestión utiliza un conjunto de recursos que permiten conseguir los objetivos planteados por una organización, incluyendo la estructura organizacional, la

planificación de actividades, la gestión de los activos de información, el cumplimiento de las regulaciones, las políticas, las prácticas, las responsabilidades, los procedimientos, los procesos, y los recursos. (IEC, 2018)

2.14 SIEM

SIEM (Security Information and Event Management), que quiere decir: "Gestión de Eventos e Información de Seguridad", es un sistema de seguridad que proporciona a las organizaciones una respuesta oportuna y precisa para la detección y respuesta ante cualquier amenaza sobre sus sistemas informáticos. Los sistemas SIEM tienen un control sobre todos los eventos que se susciten en una organización para la detección de cualquier patrón o tendencia desconocida, y tomar acción inmediata. SIEM es la evolución y combinación de dos tecnologías de seguridad que fueron desarrolladas anteriormente:

- Gestión de eventos de seguridad (SEM): detecta patrones de acceso poco convencional en tiempo real. Un gestor de eventos de seguridad permite la administración de eventos, análisis de amenazas de seguridad en tiempo real, la visualización y etiquetado, respuesta ante incidentes de seguridad. Los datos son tomados desde el equipo terminal hasta un repositorio central mediante el uso de protocolos como: SNMP (Simple Network Management Protocol), Syslog (System Logging Protocol), entre otros. El almacenamiento seguro de eventos y alertas de seguridad registrados durante el funcionamiento se realiza en el repositorio central, y la información recolectada se analiza mediante el uso de algoritmos y cálculos estadísticos para la identificación de amenazas,

vulnerabilidades y riesgos que puedan ocurrir en una red. Un SEM proporciona capacidades de normalización de entradas para la identificación de información relevante para su debida notificación. Entre las soluciones de tipo SEM que están disponibles en el mercado está: SolarWinds Log & Event Manager, Nagios Log Server, GFI EventsManager, entre otros.

- Gestión de información de seguridad (SIM): centraliza los registros de seguridad para que sean interpretados y almacenados en tiempo real, permitiendo una acción inmediata. Un gestor de información de seguridad reúne de forma automática los registros de eventos de equipos de seguridad como: cortafuegos, servidores Proxy, sistemas de prevención de pérdida de datos, entre algunos otros. Un SIM proporciona capacidades robustas para la administración y almacenamiento de logs (registros) y traducirá los datos registrados a formatos simplificados que se correlacionen entre sí; permitiendo la generación de reportes de seguridad que pueden presentarse para auditorías de seguridad. Entre las soluciones de tipo SIM que están disponibles en el mercado son: Splunk, LogLogic, IBM TCIM, ArcSight, RSA enVision, entre otros. (David R. Miller, 2011)

Los sistemas SIEM permiten incrementar y fortalecer el nivel de seguridad de una organización o empresa, con una visión integral de seguridad de las tecnologías de la información.

2.14.1 Arquitectura de sistemas SIEM

Los sistemas SIEM se componen por diferentes partes en el que cada una realiza un proceso diferente e independiente, pero que trabajan en conjunto basándose en una gestión de registros. Cada parte ejecuta distintos procesos que son:

- Dispositivo fuente: realiza la captura de la información, recuperando registros que se almacenan y procesan en el SIEM.
- Registro de Colección: realiza la obtención o recopilación de todos los registros de los dispositivos fuentes para transportarlos al SIEM.
- Análisis / Normalización de Registros: realiza la asignación de un formato estándar de lectura de registros y generación de reglas del sistema para su uso en el SIEM.
- Núcleo de Reglas / Núcleo de Correlación: está dividido en 2 segmentos, el núcleo de reglas y el núcleo de correlación de reglas; donde el primero realiza la ampliación de la normalización de eventos para la activación de alertas en el SIEM; mientras que el núcleo de correlación realiza la comparación de todos los eventos normalizados de distintas fuentes de acuerdo a reglas creadas previamente.
- Almacenamiento de Registros: favorece el trabajo en un único almacén de datos centralizado o distribuido, ayudando que la relación entre las diferentes funciones del SEM y las funciones forenses e informes del SIM sean acopladas, dependiendo de la cantidad de datos recogidos, y de la infraestructura de TIC.
- Monitoreo: mediante una interfaz de consola y una interfaz web, permiten visualizar y analizar todos los datos almacenados en el SIEM, facilitando la

gestión del sistema con una visión amplia e integral del entorno. (Walter Baluja García, 2012)

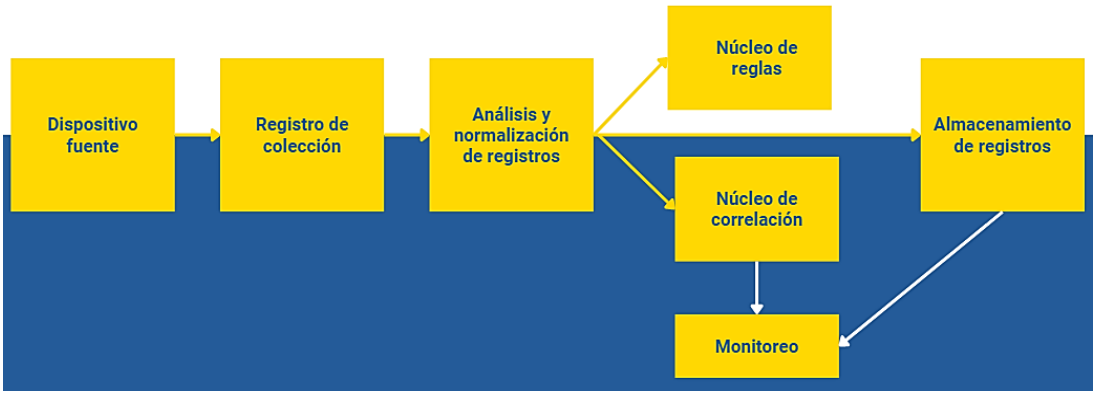


Figura 1: Arquitectura de un sistema SIEM

Fuente: El Autor

2.14.2 Funciones SIEM

Las funciones principales que realiza un sistema SIEM son: el almacenamiento, y la interpretación de los registros, en tiempo real. Con lo cual, contribuye a una oportuna reacción y detección que puede impedir o solucionar cualquier incidente de seguridad.

Un sistema SIEM realiza la recopilación de toda la información de manera centralizada en una base de datos, para posteriormente realizar un análisis profundo, y así poder detectar patrones y tendencias de comportamiento inusuales. Las principales características de un sistema SIEM para la seguridad y respuesta ante incidentes son las siguientes:

- La identificación entre amenazas reales y falsos incidentes.

- La monitorización centralizada de amenazas potenciales.
- El redireccionamiento a personal especializado y cualificado para la resolución de incidentes con la información previamente recopilada.
- La documentación de todo el proceso de detección, análisis, actuación y resolución.
- El cumplimiento de las normas y legislaciones vigentes en relación con la protección de datos y seguridad. (David R. Miller, 2011)

2.15 Proveedores SIEM

El desarrollo de soluciones SIEM en el transcurso del tiempo hasta la actualidad ha contribuido en la gestión de seguridad de las organizaciones, permitiendo realizar diferentes tareas como: la monitorización en tiempo real, la flexibilidad de consulta de registros, la correlación, la identificación de anomalías, la centralización de recursos de control, entre otros. Para lo cual, se recogieron datos de los productos líderes y su evolución en el tiempo, en el campo de la seguridad de la información, tomando como referencia las investigaciones de los analistas de Gartner. Las métricas de desempeño que se consideran incluyen la protección de acceso a la web, la protección de servicios en la nube y aplicaciones privadas, el control de acceso, la protección contra amenazas, la seguridad de datos, el monitoreo de seguridad y control de uso aceptable basado en la red.

El avance de tecnologías para productos SIEM en los últimos años, han sobrepasado los límites de la gestión de cumplimiento, dado que a medida que las organizaciones se dan cuenta de la utilidad y de los beneficios de la incorporación de una inteligencia de

seguridad para la mejora de su capacidad de respuesta ante amenazas emergentes y al aumento de ataques dirigidos; han empezado a implementarlos en sus infraestructuras de red. No obstante, el progreso en cuanto a soluciones SIEM, ha permitido inclusive una mejoría en el monitoreo de seguridad, en la detección oportuna de anomalías para una respuesta eficaz frente a incidentes de riesgo, y en la prevención de intrusiones. Al evaluar cualquier tecnología, es esencial determinar sus funcionalidades y características más relevantes tales como: el procesamiento en tiempo real, volumen de información, visualización, complejidad, escalabilidad, resiliencia, precio, capacidad de respuesta, rendimiento y almacenamiento.

2.16 Comparación de sistemas SIEM

La variedad de sistemas SIEM existentes es muy amplia, aunque según las características de rendimiento y funcionalidades se han destacado algunos que agrupan a sistemas SIEM de pago y de código libre. De acuerdo, a los resultados arrojados por las investigaciones de Gartner, se tiene la siguiente tabla comparativa que establece diferentes proveedores SIEM que presentan condiciones favorables para su implementación, clasificados por categorías; que proporcionan una guía referencial para la toma de decisiones en las empresas u organizaciones que vayan a implementarlo.

Tabla 1: Categorías de comparación de sistemas SIEM

Categorías	
Líder	
Retador	
Participante	
Visionario	

Fuente: El Autor

A continuación, el cuadro comparativo de soluciones SIEM líderes en el mercado.

Tabla 2: Cuadro comparativo de sistemas SIEM

TABLA COMPARATIVA	Año											
Proveedor	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
AccelOps												
AlienVault / AT&T												
Azure Sentinel / Microsoft												
Blackstratus SIEMStorm												
CA												
ClearSkies / Odyssey												
CorreLog												
Dell Technologies / RSA / EMC												
elQnetworks												
Elastic												
EventTracker												
Exabeam												
FireEye												
Fortinet / FortiSIEM												
Gurucul												
HanSight												
HP / ArcSight / HPE / Micro Focus												
Huawei												
Huntsman / Tier-3												
IBM												
LogLogic												
LogMatrix												
LogPoint												
LogRhythm												
Manage Engine												
McAfee / Intel												
netForensics												
NetIQ Sentinel / Micro Focus												
NetWitness												
Novell												
Prism Microsystems												
Q1Labs												
Quest Software												
Rapid7												
S21sec												
Securonix												
SenSage												
SolarWinds												
Splunk												
Sumo Logic												
Symantec												
Tango / 04												
Tenable Network Security												
Tibco-LogLogic												
TriGeo												
Tripwire												
Trustwave												
Venustech												

Fuente: El Autor / (Gartner, 2022)

OSSIM AlienVault compite con un gran grupo de soluciones SIEM que han conseguido posicionarse como líderes en el mercado, donde la mayoría son de pago; sin embargo, también compite con soluciones SIEM de código abierto donde se destacan algunos, y al ser un sistema SIEM que permite una implementación accesible, versátil y adaptable al administrador de TI en organizaciones y empresas de todo tipo, con herramientas de apoyo integradas, centralizadas y configurables de acuerdo a las necesidades que puedan surgir; posibilita una gestión más acertada, logrando sobresalir entre ellos.

Al ser soluciones SIEM de código abierto, posibilitan la apertura de su diseño de ciberseguridad, con lo cual los encargados de TI pueden realizar modificaciones y después compartirlos libremente; permitiendo una adaptabilidad y personalización según las necesidades de la entidad u organización.

Estas herramientas de código abierto pueden obtenerse de forma gratuita por parte de las organizaciones que lo deseen, lo cual permite una capacidad de administración de registros, la reducción de costos de implementación, y el establecimiento de un esquema de mantenimiento de los mismos.

A continuación, se presenta un listado de herramientas SIEM gratuitas y de código abierto existentes y con mayor presencia y aceptación en el mercado,

Tabla 3: Cuadro de sistemas SIEM de código abierto

Proveedor		Características
Apache Metron		Evolucionó a partir del proyecto Open SOC de CISCO, vinculando varias soluciones en una plataforma centralizada. Permite analizar, normalizar, indexar y almacenar eventos de seguridad para el análisis. Adicionalmente, puede proporcionar alertas de seguridad y detección de alertas cibernéticas.
Elasticsearch		Permite el almacenamiento de los datos de forma centralizada, para ser consultados en base a diferentes tipos de búsqueda que facilitan el manejo de registros con una perspectiva general y detallada; sin embargo, no proporciona alertas o correlación de eventos.
ELK Stack		Se compone de varias herramientas SIEM gratuitas como: el motor de análisis y búsqueda distribuido basado en JSON, la interfaz de visualización de usuario Kibana , la plataforma de envío de datos Beats, y Logstash para el procesamiento y recopilación de datos.
Graylog		Es una plataforma de administración de registros centralizados que analiza y recopila datos. Permite la escalabilidad, normalización, notificaciones, alertas, detección de incidentes de amenazas, respuesta ante incidentes de riesgo.
MozDef		Desarrollado por Mozilla que cuenta con herramientas de características escalables y configurables, correlación de eventos y alertas de seguridad.
OSSEC		Es un sistema de detección de intrusos que proporciona un agente de host para la recopilación de registros con una aplicación central de procesamiento de esos registros. La herramienta supervisa los archivos de registro y la integridad ante posibles ataques cibernéticos. Permite analizar registros de múltiples servicios de redes y opciones de alerta.
OSSIM AlienVault		Es una plataforma centralizada completa que permite la recopilación de datos, normalización y correlación de eventos, para la detección de amenazas. Tiene capacidades de registro y monitoreo, descubrimiento de activos, evaluación de amenazas y respuestas automatizadas integradas, análisis forense, y la gestión de registros y alarmas.
Prelude		Es un sistema que recopila, normaliza, ordena, agrega, correlaciona e informa todos los eventos de seguridad, con agentes externos como: Auditd, OSSEC, Suricata, Kismet y ClamAV. La herramienta permite detectar y manejar cualquier intento de intrusión en el sistema de seguridad.
Sagan		Desarrollado por Quadrant Information Security, la herramienta de alto rendimiento que permite análisis y correlación en tiempo real, la configuración y mantenimiento de recursos, el tiempo de ocurrencia de eventos, y la generación de alertas. Su uso es complejo.
Security Onion		Es una distribución de Linux diseñada para la detección de intrusos basados en host y en red, recopilación de eventos, captura de paquetes, análisis estático, y el monitoreo de seguridad empresarial. También reúne herramientas como: Elasticsearch, Logstash, Kibana, Suricata, Zeek, Wazuh, Stenographer, CyberChef, NetworkMiner y otros. herramientas de seguridad.
SIEMonster		Es una plataforma centralizada que permite la personalización según las necesidades organizacionales que proporciona inteligencia ante amenazas en tiempo real, protección contra ataques en tiempo real, correlación, aprendizaje automático, y puede ser ejecutable en al nube.
Snort		Es un sistema de prevención de intrusiones que permite el análisis de tráfico de red en tiempo real, y cuenta con capacidades de análisis de registro, visualización de tráfico, rastreador y registrador de paquetes, volcado de flujos de paquetes en archivos de registro. Aunque su interfaz tiene cierta complejidad de uso.
Splunk		Al ser una versión gratuita no comparte algunas funciones respecto a su versión comercial, limitando el manejo y su viabilidad a largo plazo. Sin embargo, permite detectar, investigar, monitorear y responder a ciber amenazas; cuenta con inteligencia artificial y aprendizaje automático, visualización en tiempo real, lo que le permite automatizar la recopilación, indexación y alertas.
Suricata		Es una herramienta con capacidades de detección y prevención de intrusos, monitoreo de seguridad de red, control de tráfico, registro de solicitudes, almacenamiento de certificados, y extracción de archivos de flujos.
Wazuh		Es una herramienta equipada con capacidades de detección de amenazas, monitoreo de integridad, cumplimiento y gestión de incidentes; siendo escalable y flexible. Permite recopilar, agregar, indexar, analizar datos de seguridad, e identificar amenazas o anomalías. Aunque limitado en el manejo de alertas.

Fuente: El Autor / (Gartner, 2022)

Fundamentalmente, todos los SIEM tienen capacidades de recolección, almacenamiento y correlación de eventos generado por una infraestructura gestionada. Aunque existen otras capacidades, OSSIM AlienVault logra destacar entre soluciones comerciales y de

código abierto que se resume de acuerdo al análisis y evaluación de cada característica SIEM basado en categorías como: básico (no implementado), promedio (parcialmente implementado), y alto (totalmente implementado). La evaluación considera configuraciones básicas que debe cumplir un SIEM para proporcionar una funcionalidad óptima para una gestión adecuada de la seguridad en las empresas u organizaciones.

Tabla 4: Categorías de las capacidades SIEM

Categorías	
Alto	
Promedio	
Bajo	

Fuente: El Autor / (Gartner, 2022)

Entre las capacidades proporcionadas por un sistema SIEM, se encuentran algunos que comprenden desde factores económicos, de rendimiento, de funcionalidad, de complejidad, de mantenimiento, de escalabilidad y de procesamiento de grandes volúmenes de datos e información.

De tal manera que, la plataforma de seguridad y gestión OSSIM AlienVault proporciona una herramienta completa, sencilla, confiable, segura y accesible para todo tipo de organizaciones, pero en especial para aquellas que cuentan con personal, equipos de seguridad y presupuesto limitados.

Tabla 5: Cuadro de características SIEM

Capacidades / SIEM	QRadar	LogRhythm	OSSIM AlienVault	Splunk	ArcSight	McAfee	SolarWinds	RSA
Almacenamiento								
Análisis de datos								
Análisis de riesgo								
Complejidad								
Escalabilidad								
Fuentes de datos								
Precio								
Procesamiento en tiempo real								
Reacción y reportes								
Reglas de correlación								
Rendimiento								
Resiliencia								
Seguridad								
Seguridad forense								
UEBA								
Visualización								
Volumen de datos								

Fuente: El Autor / (Gartner, 2022)

2.17 AlienVault SIEM

OSSIM AlienVault (Open Source Security Information Manager) es un SIEM que fue desarrollado por Julio Casal y Dominique Karg en los años 2000, y cuya empresa se formalizó en 2007 en Madrid por Julio Casal, Dominique Karg, Alberto Román, e Ignacio Cabrera; llegando a ser un referente en la ciberseguridad que tenía como propósito convertirse en una plataforma comunitaria gratuita de respuesta ante amenazas de seguridad. Actualmente, la empresa española AlienVault fue adquirida por la multinacional AT&T.

AlienVault cuenta con una amplia comunidad de usuarios experimentados en el uso de AlienVault SIEM en diferentes tipos de aplicaciones que van desde el cumplimiento

hasta las operaciones, desde el gobierno hasta sistemas de control, desde las finanzas hasta la fabricación. AlienVault SIEM corresponde a un sistema de gestión de seguridad totalmente unificado, con herramientas manejables a través de la interfaz de AlienVault, e integradas con otros componentes funcionales del sistema. Los productos AlienVault también se integran con herramientas de seguridad externas de todo tipo que permiten la creación de una solución unificada ajustada a las necesidades específicas de una organización. (Lorenzo, 2011)

2.17.1 Arquitectura OSSIM

La arquitectura OSSIM tiene cierta similitud con la arquitectura SIEM, que incluye 3 componentes básicos y uno adicional disponible únicamente para la versión comercial de OSSIM denominada USM Anywhere (Unified Security Management). (Lorenzo, 2011)

Los componentes se describen de la siguiente manera:

- SIEM (Gestor de eventos): Proporcionará capacidades de búsqueda, detección, filtrado, de datos e información (minería de datos) al sistema de seguridad, además de evaluación de riesgos, indicadores de riesgos, análisis de vulnerabilidades, control y monitoreo en tiempo real, y correlación de registros basándose en reglas. El SIEM incluye una base de datos SQL (Structured Query Language), que permite el almacenamiento de información normalizada para facilitar el análisis de los datos; también está diseñado para proporcionar un alto rendimiento y escalabilidad debido al gran flujo de información que pueda generarse.

- LOGGER (Registrador): Almacenará cada uno de los eventos que hayan ocurrido (sin modificaciones) en un dispositivo de seguridad forense; dichos eventos se almacenan y se firman digitalmente, lo que asegura su admisibilidad.
- COLLECTOR (Colector): Reunirá los registros de los eventos que se hayan generado por los sensores de OSSIM u otro sistema externo para clasificarlos y normalizarlos previo a ser enviados al SIEM y al Logger (registrador). Los colectores pueden ser implementados como un sistema autónomo o ser incorporados en el sensor o dispositivo SIEM de acuerdo a las necesidades de desempeño que sean requeridos.
- SENSOR (Sensor): Recogerán la información del entorno local, para procesarla; y coordinar la detección y respuesta de la red OSSIM ante amenazas. Los sensores se instalan en los segmentos de la red y sitios remotos donde realizarán la inspección de todo el tráfico de red generado, de tal manera que, puedan detectar y recolectar información sobre el tipo y forma de los posibles ataques utilizando diferentes métodos sin que afecten el rendimiento de la red. (Lorenzo, 2011)

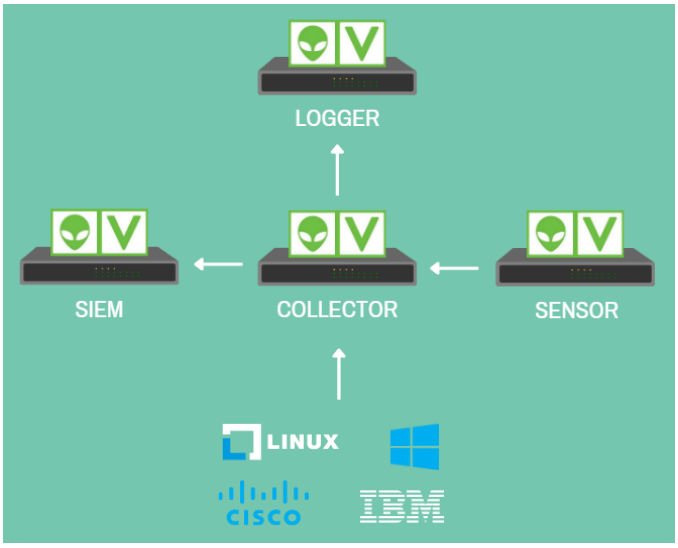


Figura 2: Arquitectura OSSIM AlienVault

Fuente: El Autor

2.17.2 Herramientas del sistema OSSIM AlienVault

Dentro del sistema OSSIM AlienVault se integran herramientas complementarias centralizadas para la administración y gestión de eventos e incidentes de seguridad. OSSIM AlienVault integra herramientas que intervienen en conjunto para proporcionar un control centralizado en los procesos de análisis, detección y monitoreo de la red de una organización.

Tabla 6: Cuadro de herramientas de OSSIM AlienVault

Herramienta	Función
ARPwatch	Detección de cambios o anomalías en direcciones MAC.
Cisco PIX	Control del tráfico entre la red externa e interna.
IPTables	Filtrado del tráfico y recolección de eventos.
Nagios	Monitoreo de la disponibilidad de hosts y servicios.
Nessus	Escaneo de vulnerabilidades de la red.
NfSen	Visualización y generación de gráficos de flujo de la red.
Nikto	Escaneo de vulnerabilidades de la red.
Nmap	Escaneo de redes, descubrimiento de hosts y servicios activos.
Ntop	Monitorización y visualización estadística del tráfico de red.
NTsyslog	Analizador de registros en Windows.
OpenVAS	Escaneo, detección, evaluación y gestión de vulnerabilidades.
Osiris	Detección de intrusos a nivel de hosts.
OSSEC	Detección de intrusos a nivel de logs.
OSSIM agent	Supervisión y recolección de datos de dispositivos o equipos terminales.
P0f	Detección del sistema operativo y versión de los hosts conectados a la red.
PADS	Detección de equipos terminales conectados a la red y anomalías en servicios.
Snare	Recolección de registros en sistemas Windows.
Snort	Detección de intrusos a nivel de red.
Spade	Detección de cambio o anomalías en paquetes.
Syslog	Analizador de registros en Linux.
Tcptrack	Monitoreo de conexiones TCP de la red.

Fuente: El Autor

2.17.3 Implementación de OSSIM AlienVault

Para la implementación del sistema OSSIM AlienVault, se precisa de un listado de verificación de requisitos básicos previo a su instalación, que son los siguientes:

- Dirección de correo electrónico para registro.
- Lista de subredes, rangos o zonas a monitorear.
- Dirección IP estática para la instancia de OSSIM.
- Acceso a un puerto o nodo para el monitoreo de red.
- Información de cuenta de dominio para la instalación del agente HIDS.
- Información de acceso al cortafuegos para la habilitación de gestión de registros.

El proceso de aplicación, instalación e implementación de OSSIM AlienVault será:

2.17.3.1 Despliegue e implementación de OSSIM AlienVault

Se instalará el paquete virtual del SIEM en un determinado hipervisor.

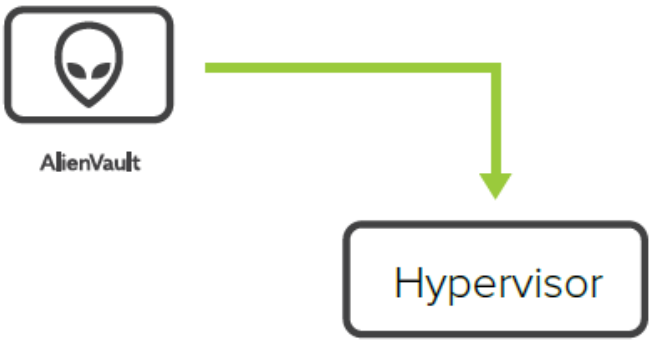


Figura 3: Despliegue OSSIM AlienVault

Fuente: El Autor / (AT&T, AlienVault - Quick Start Guide, 2021)

2.17.3.2 Monitoreo del tráfico de red

Se configura las interfaces y se monitorea el tráfico de red para detectar amenazas.

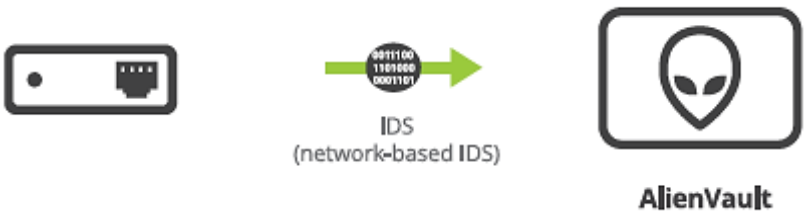


Figura 4: Monitoreo de tráfico de red

Fuente: El Autor / (AT&T, AlienVault - Quick Start Guide, 2021)

2.17.3.3 Descubrimiento de activos

OSSIM AlienVault realizará un escaneo de descubrimiento para detectar los activos.

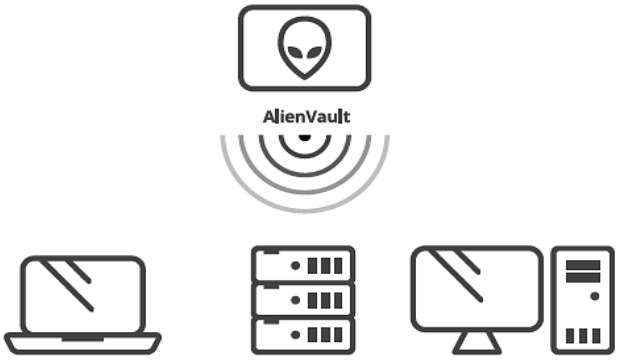


Figura 5: Descubrimiento de activos

Fuente: El Autor / (AT&T, AlienVault - Quick Start Guide, 2021)

2.17.3.4 Recopilación de logs y monitoreo de activos

Se supervisa el registro de activos y la alarma sobre alguna actividad que sea sospechosa.

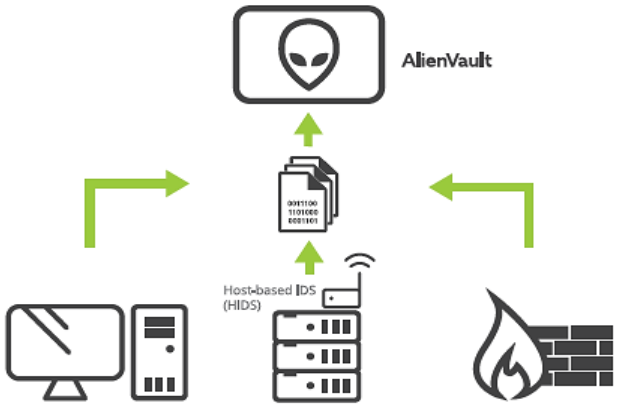


Figura 6: Recopilación de registros y monitoreo de activos

Fuente: El Autor / (AT&T, AlienVault - Quick Start Guide, 2021)

2.17.3.5 Investigación y respuesta

Se identifica las amenazas y se investiga los incidentes.

Figura 7: Investigación y respuesta

Fuente: El Autor / (AT&T, AlienVault - Quick Start Guide, 2021)

2.18 Controles de seguridad CIS

Se ha hecho muy evidente que la seguridad de la información, se ha visto vulnerado porque los ataques informáticos han ido superando los mecanismos defensivos de las organizaciones, pese a que los presupuestos han aumentado; los riesgos de pérdida de datos e información crítica, siguen vigentes y las acciones de intrusión y penetración a los sistemas informáticos no cesan. Por tal motivo, surgen controles de seguridad para la protección de la información.

Los CIS (Critical Security Controls) – Controles críticos de seguridad, tuvieron sus inicios como una actividad de identificación de los ciberataques que afectan a las organizaciones o empresas constantemente en sus actividades diarias, hasta convertirse en una comunidad conformada por expertos, especialistas e instituciones voluntarias liderados por el Center for Internet Security (CIS). Las actividades desempeñadas son:

- El intercambio de conocimientos sobre ataques y atacantes.
- La identificación de las causas fundamentales de los ataques y la elaboración de acciones defensivas.
- La creación e intercambio de herramientas.
- La elaboración de guías de trabajo para la resolución de problemas.
- La asignación de controles de CIS que se adapten al marco regulatorio.
- El cumplimiento para garantizar los lineamientos requeridos de manera colectiva con un enfoque hacia la identificación y resolución de problemas que puedan presentarse.

2.19 Estructura de los controles CIS

Los controles se encuentran sujetos a ciertos elementos:

- Visión general: Hace referencia a una breve descripción de la intención del control y su utilidad como una acción defensiva.
- Procedimientos y herramientas: Hace referencia a una descripción técnica de los procesos y tecnologías que permiten la implementación y automatización de los controles.
- Descripciones de salvaguardas: Hace referencia a una tabla de acciones específicas que las organizaciones o empresas deben considerar para implementar un control.

2.20 Los 18 Controles de Seguridad Críticos del CIS

Anteriormente, los controles de seguridad críticos de SANS (SysAdmin Audit, Networking and Security Institute) eran 20; ahora se denominan oficialmente CIS – Controles Críticos de Seguridad (Controles CIS).

Los controles CIS en su última versión 8, combina y consolida los controles CIS por actividades, en lugar de por quién gestiona los dispositivos, dando como resultado la disminución del número de controles de 20 a 18. Los controles CIS son los siguientes:

- Control CIS 1: Inventario y Control de Activos Empresariales.
- Control CIS 2: Inventario y Control de Activos de Software.

- Control CIS 3: Protección de datos.
- Control CIS 4: Configuración segura de activos y software empresarial.
- Control CIS 5: Gestión de cuentas.
- Control CIS 6: Gestión de control de acceso.
- Control CIS 7: Gestión continua de vulnerabilidades.
- Control CIS 8: Gestión de registros de auditoría.
- Control CIS 9: Navegador web de correo electrónico y protecciones.
- Control CIS 10: Defensas contra malware.
- Control CIS 11: Recuperación de datos.
- Control CIS 12: Gestión de infraestructura de red.
- Control CIS 13: Supervisión y defensa de la red.
- Control CIS 14: Concientización sobre seguridad y capacitación en habilidades.
- Control CIS 15: Gestión de proveedores de servicios.
- Control CIS 16: Seguridad del software de aplicación.
- Control CIS 17: Gestión de respuesta a incidentes.
- Control CIS 18: Pruebas de penetración. (CIS, CIS Critical Security Controls V8, 2021)

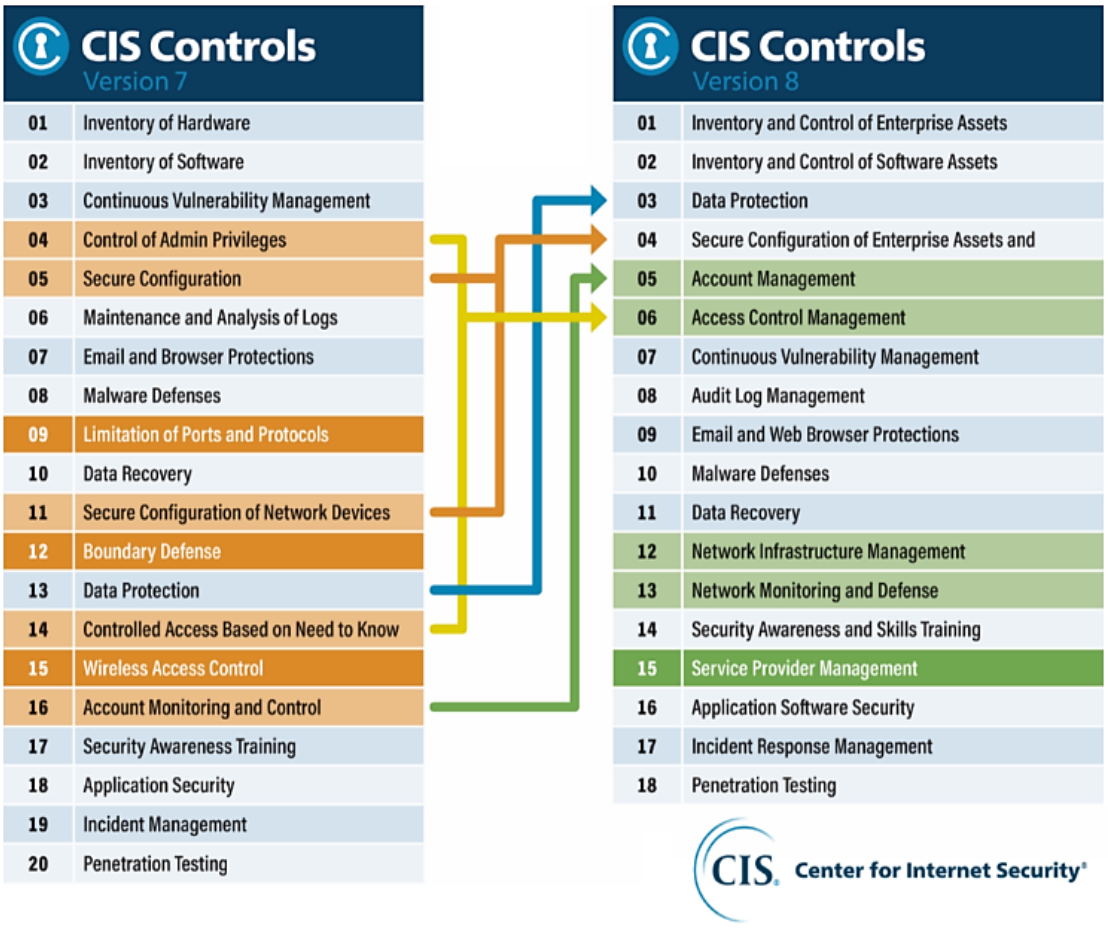


Figura 8: Controles CIS v8

Fuente: (CIS, cisecurity.org, 2022)

En relación a los cambios en la nueva versión, algunos de los controles se han fusionado, como el control 4 (control de privilegios de administrador) con el control 14 (acceso controlado basado en la necesidad de saber), dando como resultado el control 6 (gestión de control de acceso). También, algunos de los controles han quedado obsoletos, como el control 15 (control de acceso inalámbrico), surgiendo un nuevo control 15 (gestión de proveedores de servicios). Y controles como el control 5 (configuración segura) con el control 11 (configuración segura de dispositivos de red), generaron el control 4 (configuración segura de activos y software empresarial).

Bajo un esquema de evaluación de control de seguridad crítica CIS se puede determinar como punto de partida el porcentaje de riesgo abordado con relación al riesgo aceptado. (Anexo 5) Y a base de los resultados obtenidos se identifican ciertas falencias en la seguridad de la entidad gubernamental en el que algunos parámetros de control no han sido implementados, tales como: inventario de activos de software, gestión de vulnerabilidades, configuración segura de activos y software, gestión de registros; lo que conlleva a un alto porcentaje de riesgo aceptado con posibles consecuencias perjudiciales a largo plazo si no son resueltos. Y apenas un 11% de riesgo abordado cumple con los controles básicos de seguridad de la entidad en cuestión.

2.20.1 Esquema de controles

De acuerdo a las falencias encontradas, se pretende establecer un esquema de control referencial que permita una mejora significativa en la gestión y administración de la seguridad de la infraestructura tecnológica y activos de información de la entidad, a base de los siguientes parámetros generales:

Tabla 7: Descripción de análisis de controles de seguridad

Descripción	Observaciones
Control e inventario de activos	Se debe aplicar un inventario completo de los activos de información que serán protegidos y que preferiblemente se efectúen en cada sistema, y sea automatizado.
Control e inventario de activos de software	Se deberá implementar herramientas de escaneo para la identificación de aplicaciones de software que se encuentren instaladas.
	Se debe implementar un inventario de los activos de software que permitan la ejecución de programas autorizados.
Control de gestión de vulnerabilidades	Se debe implementar herramientas de escaneo que permitan la identificación de vulnerabilidades en cada sistema.
	Se deberá implementar un sistema de control y administración de actualizaciones para cada sistema, y si es posible que sea autmatizado.
Control de administración de cuentas	Se debe implementar una herramienta de escaneo para efectuar un inventario de usuarios que tengan derecho de acceso a los sistemas de la entidad.
Control de configuración segura de activos y software	Se deberá implementar herramientas de escaneo para la identificación de configuraciones incorrectas realizadas en cada sistema.
	Se debe implementar un sistema de cumplimiento de configuraciones de seguridad en los sistemas.
Control de gestión de registros	Se debe implementar un esquema de registro de auditoría completo para cada sistema que maneje información crítica de la entidad.
	Se debe implementar un sistema de gestión de eventos e información de seguridad que permitan una centralización de registros para auditorías.

Fuente: El Autor

CAPÍTULO III

ANÁLISIS Y SITUACIÓN ACTUAL

3.1 Entidad Gubernamental

El Gobierno Autónomo Descentralizado de la Provincia de Sucumbíos, es una institución que fue creada en el año 1989, según el Registro Oficial No. 127; que cumple la función de GAD Provincial dentro del territorio Nororiental del país.

3.1.1 Propósito

"Mejorar las condiciones de vida de las y los sucumbisenses, a través del fortalecimiento de las capacidades y talentos locales, la asistencia técnica y transferencia de tecnología, impulso a la agroindustria y emprendimientos, financiamiento y generación de espacios y servicios públicos dignos y eficientes". (GADPS, 2022)

3.1.2 Funciones

Según lo establecido en el Art. 29 del Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD), el GAD de la provincia de Sucumbíos cumple las siguientes funciones:

- Legislación, normatividad y fiscalización.
- Ejecución y administración.
- Participación ciudadana y control social.

3.1.3 Competencias

Según lo establecido en el Art. 42 del Código Orgánico de Organización Territorial, Autonomía y Descentralización (COOTAD), el GAD de la provincia de Sucumbíos cumple las siguientes competencias exclusivas:

- Planificación, en conjunto con otras instituciones públicas y actores de la sociedad, para el desarrollo provincial, formulación de planes de ordenamiento territorial, en el ámbito de sus competencias, de manera articulada con la planificación nacional, regional, cantonal y parroquial, en el marco de la interculturalidad y plurinacionalidad y el respeto a la diversidad.
- Planificación, construcción y mantenimiento del sistema vial de ámbito provincial, que no incluye zonas urbanas.
- Ejecución, en coordinación con el gobierno regional y los demás gobiernos autónomos descentralizados, de obras en cuencas y micro cuencas.
- Gestión ambiental provincial.
- Planificación, construcción, operación y mantenimiento de sistemas de riego de acuerdo con la Constitución y la Ley.
- Fomento de actividades productivas provinciales, especialmente agropecuarias.

- Gestión para la cooperación internacional para el cumplimiento de sus competencias.
- Determinación de políticas de investigación e innovación del conocimiento, desarrollo y transferencia de tecnologías necesarias para el desarrollo provincial, en el marco de la planificación nacional. (Oficial, 2019)

3.2 Capacidad Institucional

La entidad gubernamental, cuenta con una infraestructura y terrenos (escriturados y actas de comodato). Principalmente, se encuentran dispuestos en:

- Edificio de tres plantas.
- Recinto Ferial, utilizado como centro de exposiciones y ferias agropecuarias, comerciales y culturales.
- Bodegas y talleres.
- Edificio de 2 plantas donde funciona Sucumbíos Solidario.
- Edificio y finca donde funciona el Centro de Investigaciones y Servicios Agropecuarios de Sucumbíos (CISAS).
- Terreno para el sindicato de trabajadores.
- Terreno donde funciona el Colegio a Distancia Juan Jiménez.

(GADPS, 2022)

3.3 Estructura organizacional de la Entidad Gubernamental

La estructura organizacional del GADPS comprende una serie de procesos que están administrados y gestionados para el desarrollo provincial, que son:

- Proceso de Gobierno Legislativo, Ejecutivo y de Participación Ciudadana.
- Proceso de Gobernabilidad y Asesoría.
- Proceso de Control y de Participación Ciudadana.
- Proceso Operativo de Apoyo.
- Proceso Agregado de Valor.
- Procesos Desconcentrados.

(GADPS, 2022)

La entidad gubernamental cuenta con un manejo de talento humano por cada nivel de proceso, considerando al personal de nombramiento, contrato y servicios profesionales. La estructura organizacional se establece con base en el siguiente organigrama:

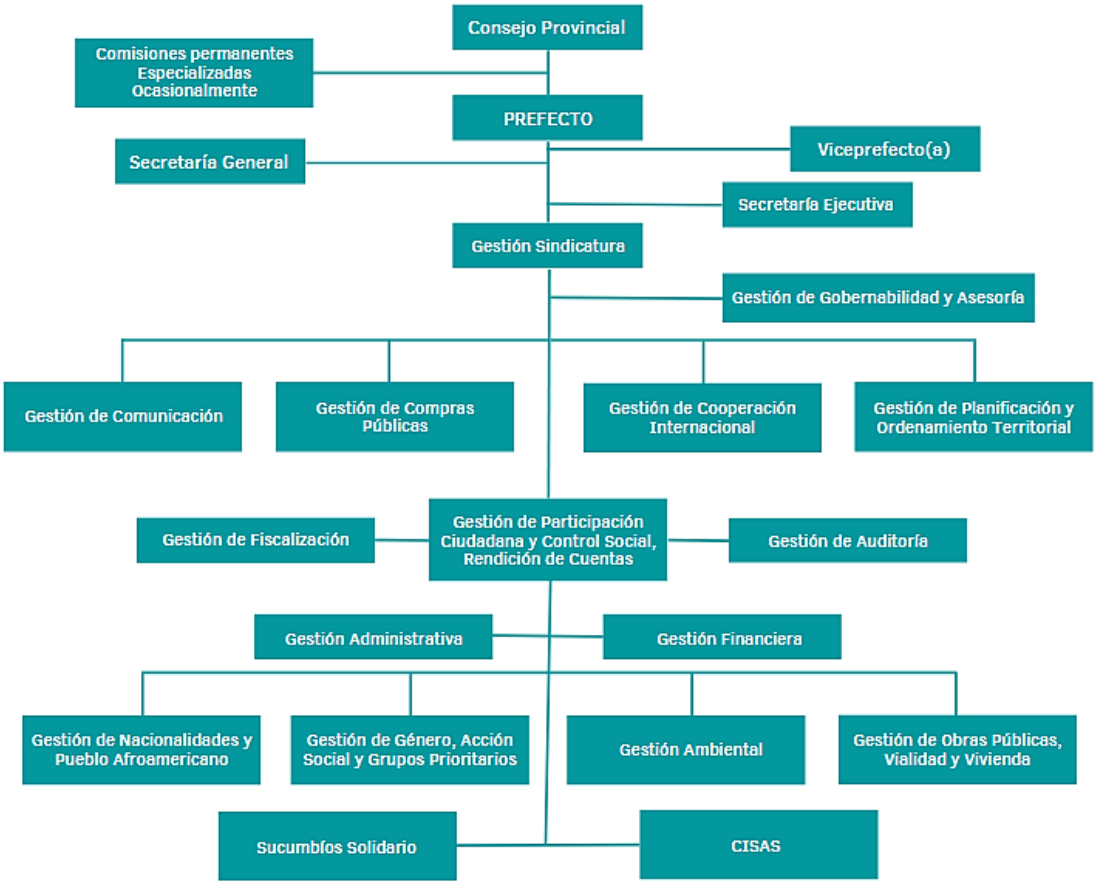


Figura 9: Estructura Organizacional de la entidad gubernamental

Fuente: (GADPS, 2022) / El Autor

3.4 Situación Tecnológica de la Entidad Gubernamental

El GADPS desde sus inicios ha llevado un crecimiento organizacional en conformidad a las necesidades que se iban presentando, ocasionando la generación de un mayor volumen de datos en los diferentes sistemas de información. (Anexo 5) El incremento de la cantidad de nodos de red debido a la incorporación de nuevos usuarios, ha dificultado una gestión integral de los diferentes departamentos y áreas que conforman la entidad gubernamental y ha hecho que se originen algunos riesgos de seguridad.

El esquema general de la red de la institución, se encuentra descontinuado, lo que ha dificultado su administración, gestión y control; y ha desembocado en la implementación de soluciones parciales que solo proporcionan una salida temporal a la problemática general. (Anexo 5)

3.5 Infraestructura de la entidad gubernamental

El GADPS realiza sus actividades principales en el Edificio de 3 plantas ubicado en el centro de la ciudad. Dentro de las instalaciones intervienen varios departamentos dispuestos en cada piso y cuya infraestructura tecnológica es gestionada y administrada por el Departamento de Informática.

La entidad cuenta con su propio proveedor de servicios de Internet, el cual es distribuido a través del Data Center (Centro de Datos) y sus respectivos cuartos de máquina hacia todos los usuarios de la institución. La red de datos implementada está segmentada por VLAN's, y los usuarios disponen de sus estaciones de trabajo con conectividad alámbrica e inalámbrica.

La distribución de la infraestructura general de la red del GADPS, ubica los racks (bastidores) de comunicaciones en cada piso, con una accesibilidad directa sin protecciones, dejando expuesto el acceso hacia el exterior, lo que ocasiona un posible riesgo de los activos de comunicación de red. El centro de datos es el único que cuenta con mecanismos de autenticación física para su acceso, mientras que los cuartos de máquinas se encuentran directamente expuestos al entorno de las actividades diarias de

los diferentes departamentos que conforman el GAD; por lo que cualquier usuario, funcionario, o atacante puede tratar de ingresar para desconectar, interrumpir u ocasionar algún daño en los equipos de comunicaciones de red dispuestos en el rack (bastidor).

Figura 10: Cuartos de máquinas del GADPS

Fuente: (GADPS, 2022)

En relación con el centro de datos, presenta un acceso mediante un mecanismo de autenticación físico para el acceso a los racks (bastidores), convirtiéndose en un punto vulnerable para la entidad gubernamental.

Figura 11: Centro de Datos del GADPS

Fuente: (GADPS, 2022)

Al interior del Data Center (Centro de datos), se cuenta con una seguridad mínima de acceso a los racks (bastidores) donde el cableado se ve expuesto y se interconecta a la infraestructura de red del edificio de la entidad gubernamental.

Figura 12: Racks del Centro de Datos del GADPS

Fuente: (GADPS, 2022)

Desde el Data Center se reparte el cableado y la red de comunicaciones hacia los demás cuartos de máquinas e instalaciones de la entidad gubernamental.

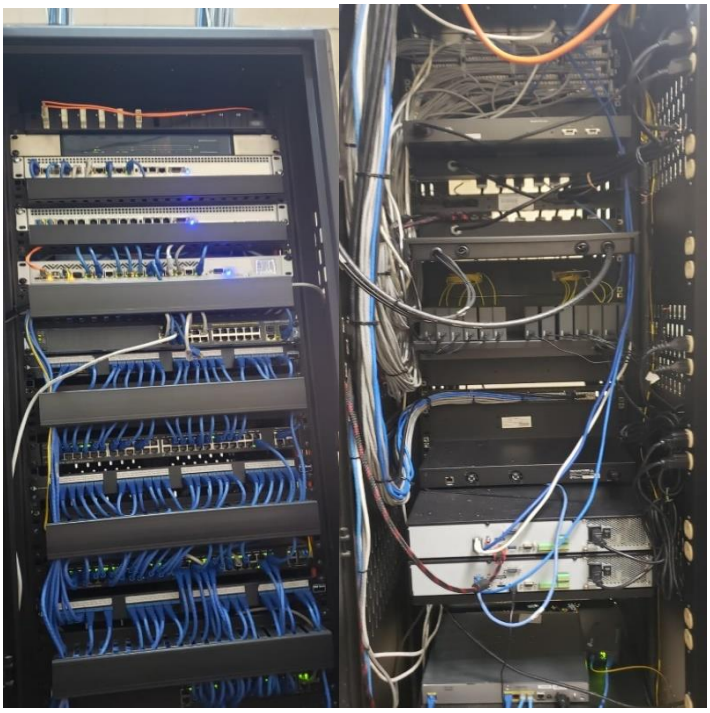


Figura 13: Cableado y conexiones de Racks del Centro de Datos del GADPS

Fuente: (GADPS, 2022)

Los cuartos de máquinas se encuentran dispuestos en cada piso con sus Racks (Bastidores) donde los equipos y cableado presentan una mínima seguridad, haciendo que se encuentre vulnerable ante el personal de mantenimiento que pueda acceder y ocasionar algún daño o interrupción del sistema y red de comunicaciones del GADPS.

El piso 1 se encuentra conectado a la infraestructura de red de la entidad y comunicado con el Data Center mediante cableado estructurado.

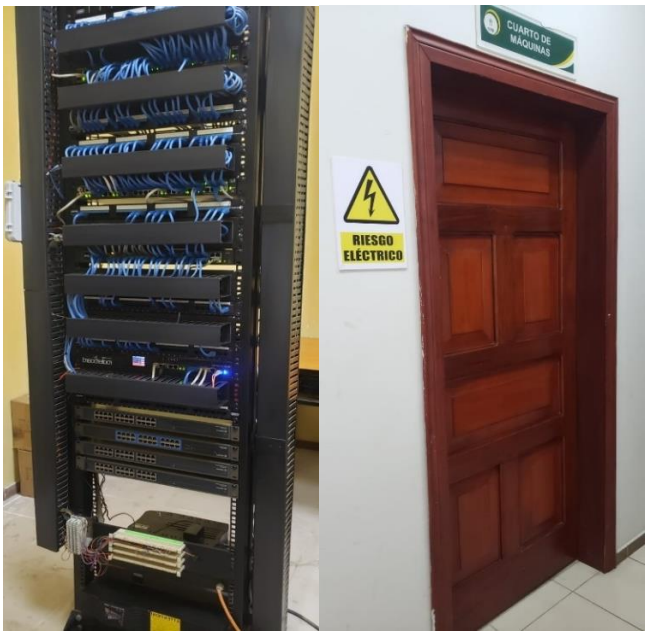


Figura 14: Cuarto de máquinas P1 del GADPS

Fuente: (GADPS, 2022)

El piso 2 se encuentra conectado a la infraestructura de red de la entidad y comunicado con el Data Center mediante cableado estructurado, con mayor proximidad.

Figura 15: Cuarto de máquinas P2 del GADPS

Fuente: (GADPS, 2022)

El piso 3 se encuentra conectado a la infraestructura de red de la entidad y comunicado al Data Center mediante cableado estructurado.

Figura 16: Cuarto de máquinas P3 del GADPS

Fuente: (GADPS, 2022)

También, se cuenta con enlaces RF que proporciona la red de comunicaciones de la entidad gubernamental hacia otros sitios adscritos.

Figura 17: Enlaces RF del GADPS

Fuente: (GADPS, 2022)

3.6 Sistemas y servicios de información

Dentro de las instalaciones de la entidad gubernamental se utilizan en la intranet una serie de aplicaciones y servicios para efectuar procesos de registro, documentación, gestión, proyectos, presupuestos, nómina y otros. Adicionalmente, los usuarios de los departamentos de la entidad tienen acceso a portales que se encuentran alojados en el centro de datos, para procesos administrativos; también pueden acceder a los aplicativos para solicitar procesos de soporte manejados por el departamento de TIC. Otros servicios web de información se encuentran expuestos al público y son administrados por personal de tecnología designado para esos departamentos de la entidad. Sin embargo, existen usuarios que también tienen acceso para gestionar los servicios y páginas web de ciertos departamentos, lo que representa un factor de riesgo a nivel interno de la entidad.

3.6.1 Sistemas internos

Entre los sistemas internos que se maneja en la entidad gubernamental para cumplir con las actividades cotidianas se encuentran alojados en diferentes servidores, a los cuales todos los usuarios de la entidad tienen acceso. Los sistemas que forman parte de los activos de información son: sistema de asistencia, sistema de comunicadores, sistema de correo, sistema de documentación, sistema de roles, sistema de asistencia y mesa de ayuda, sistema financiero, sistema de planificación, sistema de información, sistema de base de datos.

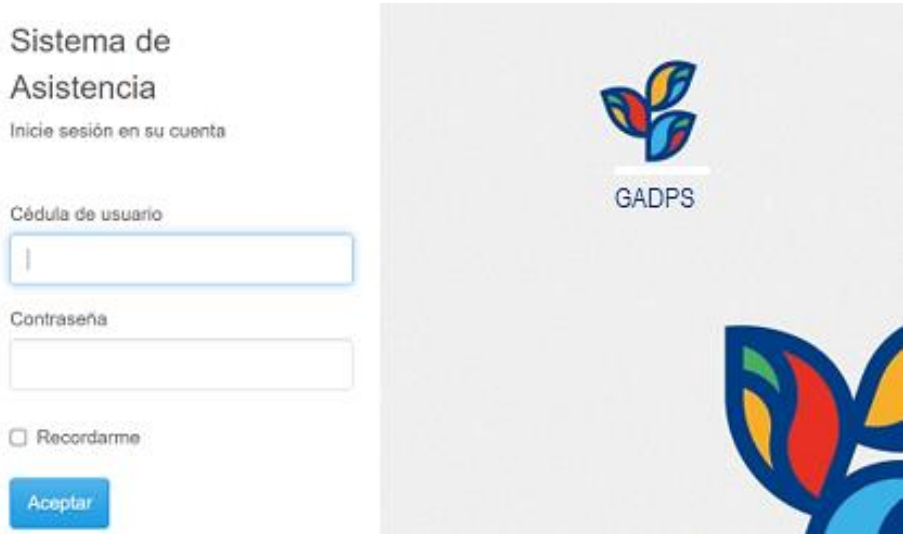


Figura 18: Sistema de asistencia

Fuente: (GADPS, 2022)

3.6.2 Sistemas externos

Entre los sistemas externos que se maneja en la entidad gubernamental para el cumplimiento de actividades informativas y de comunicación cotidianas, además de otros servicios, se encuentran alojados en diferentes servidores, a los cuales todos los usuarios sean internos o externos pueden acceder. Entre los sistemas que forman parte de los activos de información son: sitio web del GADPS, sitio web de correo, sistema de información local, sistema de cartografía, sistema de información general.

Figura 19: Sitio web de la entidad gubernamental

Fuente: (GADPS, 2022)

Uno de los sitios que permite el manejo de proyectos de cartografía, georreferenciación, etc., es el sistema de información local que se incorpora al sitio web.

Figura 20: Sistema de información local de la entidad gubernamental

Fuente: (GADPS, 2022)

Por lo tanto, tanto los sistemas internos como externos de la entidad gubernamental requieren incluir acciones de control y monitoreo que permitan resguardar la integridad, disponibilidad y confidencialidad de la información generada, almacenada y transferida o compartida a través de una herramienta de gestión de eventos e incidentes de seguridad.

3.7 Usuarios de la entidad gubernamental

Un aspecto muy importante en las organizaciones es el factor humano en el uso de las TIC, lo que implica una mayor gestión de control. En tal situación, se hace necesario incluir cuántos usuarios aproximadamente se encuentran utilizando el servicio de red de la entidad, y dada la actividad habitual, lo ha vuelto un riesgo potencial de seguridad.

En principio, desde el inicio de las actividades en la entidad, se han dado algunos cambios sumados al incremento progresivo del número de usuarios que tienen un flujo de actividades constantes, lo que aumentó el grado de control. Los valores aproximados del número de usuarios son:

Tabla 8: Usuarios de la entidad gubernamental

Usuarios	Cantidad
Personal de TIC	10
Personal administativo	641
Personal operativo	51
Total	**702**

Fuente: (GADPS, 2022), el Autor

Con los datos cuantitativos que fueron obtenidos, se puede determinar la cantidad de usuarios que disponen de conectividad directa a la red de comunicaciones de la entidad,

convirtiéndose en un objetivo principal ante posibles ciberataques; no obstante, pueden inclusive convertirse en posibles canales de vulnerabilidad, lo que conlleva a tomar en consideración todas las posibles vías de ocurrencia de eventos e incidentes de seguridad ya sea por amenazas externas, riesgos internos y externos.

3.8 Esquema de red

La entidad gubernamental se compone de diferentes nodos de red que se distribuyen respectivamente, el diagrama de red del GADPS, muestra la arquitectura de interconexión de los segmentos de red que incluyen a la torre de comunicaciones.

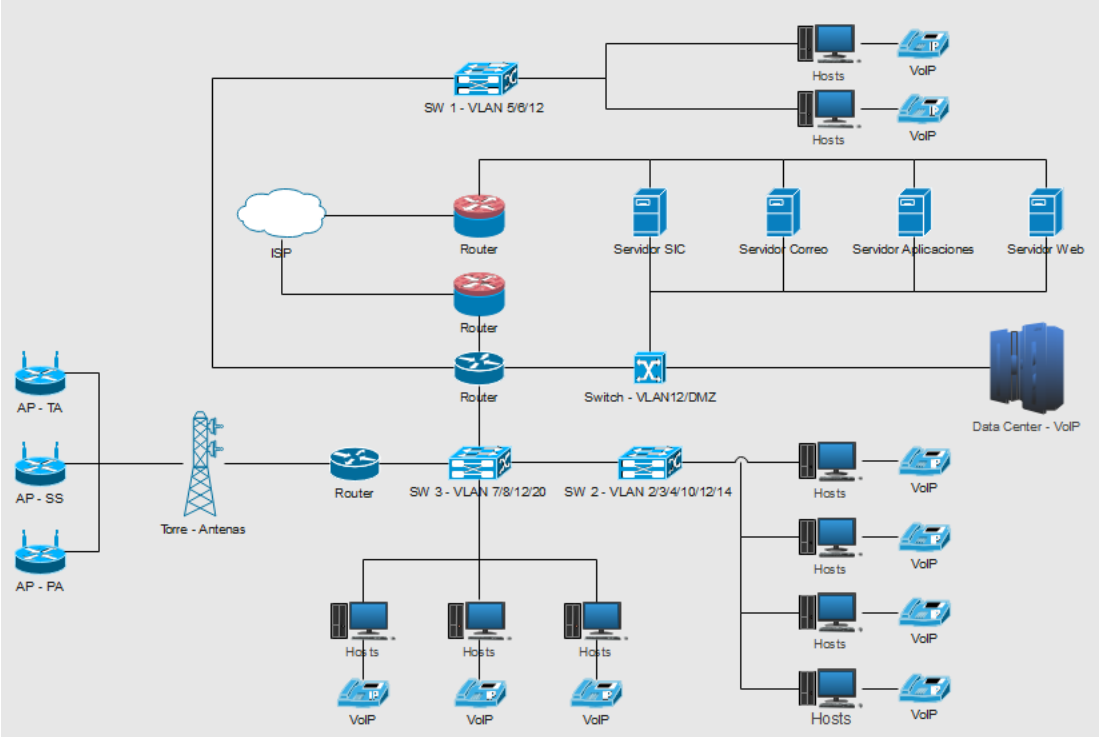


Figura 21: Diagrama de red de la entidad gubernamental

Fuente: (GADPS, 2022)

CAPÍTULO IV

PROPUESTA

En relación a la problemática general, se plantearon algunos aspectos que ayudaron a solucionar los puntos críticos que presentaba la infraestructura general de telecomunicaciones de red de la entidad gubernamental.

4.1 Introducción

Las distintas vulnerabilidades, riesgos, o ciberataques a los que se enfrentan las organizaciones públicas y privadas pueden traer consigo afectaciones tanto en los sistemas de información como en los datos e información que sea utilizada en las actividades diarias. En referencia a la entidad gubernamental, la seguridad de su infraestructura tecnológica, red de comunicaciones, y equipos presentan ciertas deficiencias que pueden originar eventos o incidentes que tengan gran impacto en el desarrollo y la continuidad de las actividades de cada departamento; de modo que, una propuesta de solución es la gestión de incidentes, eventos y ciber amenazas a través de un sistema de gestión de eventos e información de seguridad para el control y monitoreo de los diferentes activos de información que permitan una detección preventiva y su mitigación respectiva.

Con la propuesta se pretende como finalidad, una administración centralizada de la seguridad de los activos y servicios de información, buscando una mejora y sobre todo

mantener la integridad, disponibilidad y confidencialidad de toda la infraestructura de comunicaciones de red de la entidad.

4.2 Requerimiento de confidencialidad

Previo al inicio de la implementación del sistema de gestión de incidentes y eventos de seguridad, se llevó a cabo el planteamiento de los términos del manejo y exposición de los datos e información sensible de la entidad gubernamental mediante un "Acuerdo de Confidencialidad", el mismo que deberá ser firmado en mutuo acuerdo entre el jefe del departamento de TIC y el investigador del proyecto. Dicho documento habilita el manejo de cierta información crítica vinculada a la entidad para efectos de la investigación. (Anexo 1)

4.3 Requerimientos de implementación

Se realizará la instalación de las siguientes herramientas:

- Plataforma software de virtualización VirtualBox versión 6.1.34
- Sistema operativo Linux – Debian (64 bit)
- OSSIM AlienVault versión 5.8.1
- Interfaz de red

La instalación de la herramienta de código abierto OSSIM AlienVault requerirá contar con la información de la infraestructura de red de la entidad gubernamental, y de acuerdo a ello, determinar las configuraciones que permitan el funcionamiento adecuado de la herramienta.

La configuración para la máquina virtual comprende la especificación del nombre, el tipo de sistema operativo como Linux que corresponde al sistema que tendrá el SIEM a instalar, la versión con Debian (64-bit) (distribución) correspondiente al sistema operativo del SIEM, y el tamaño de la memoria RAM como mínimo de 2048 MB hasta unos 8000 MB debido a los requerimientos de procesamiento que necesita y de acuerdo a la recomendación por defecto del fabricante.

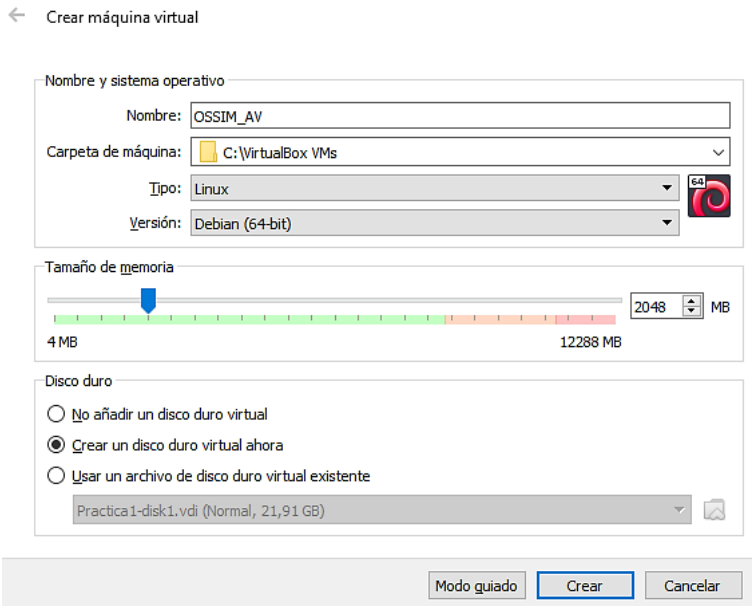


Figura 22: Configuración de OSSIM AlienVault – Nombre y tamaño de memoria

Fuente: El Autor

Se especifica el tamaño de almacenamiento de disco para la máquina virtual con un mínimo de 20 GB hasta unos 100 GB o más por recomendación del fabricante, y debido

al flujo de información que almacenará el gestor mediante la recopilación de información en registros (logs) para ser enviados al servidor donde se realizará el procesamiento y análisis.

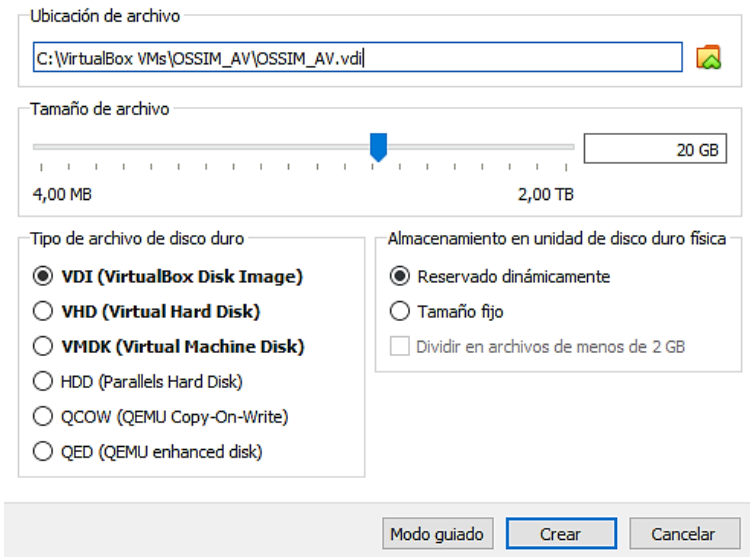


Figura 23: Configuración de OSSIM AlienVault – Ubicación y tamaño de archivo

Fuente: El Autor

Dentro del apartado ‘Almacenamiento’ de las configuraciones de la máquina virtual, se agrega la imagen ISO para la instalación de OSSIM AlienVault, en la opción ‘Atributos’.

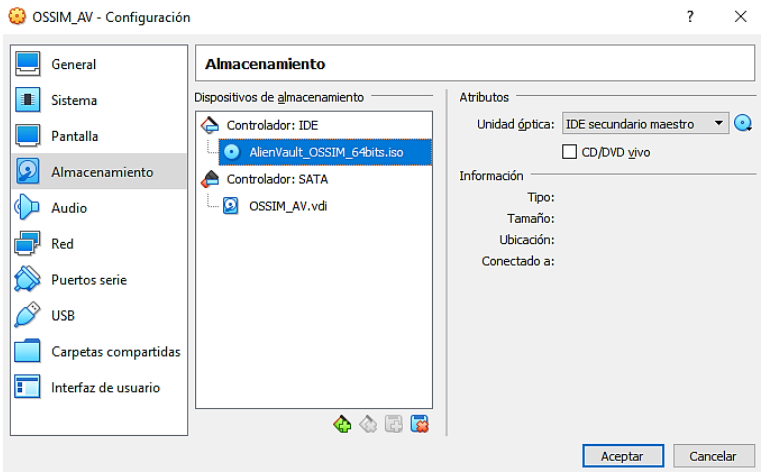


Figura 24: Configuración de OSSIM AlienVault – Almacenamiento

Fuente: El Autor

Para las configuraciones de instalación se solicitará la elección de una de las 2 opciones sugeridas, una para efectuar la instalación completa (Install AlienVault OSSIM 5.8.11 (64 Bit)), y la otra opción será para la instalación de un sensor (Install AlienVault Sensor 5.8.11 (64 Bit)). Al seleccionar la primera opción, permite trabajar no solo con un servidor centralizado, sino con un servidor que va a recolectar la información de varios sensores a nivel de toda la organización.

Figura 25: Configuración de OSSIM AlienVault – Inicio de instalación

Fuente: El Autor

Al haber seleccionado la primera opción, se abrirá una nueva ventana para escoger el idioma de acuerdo a lo que se requiera.

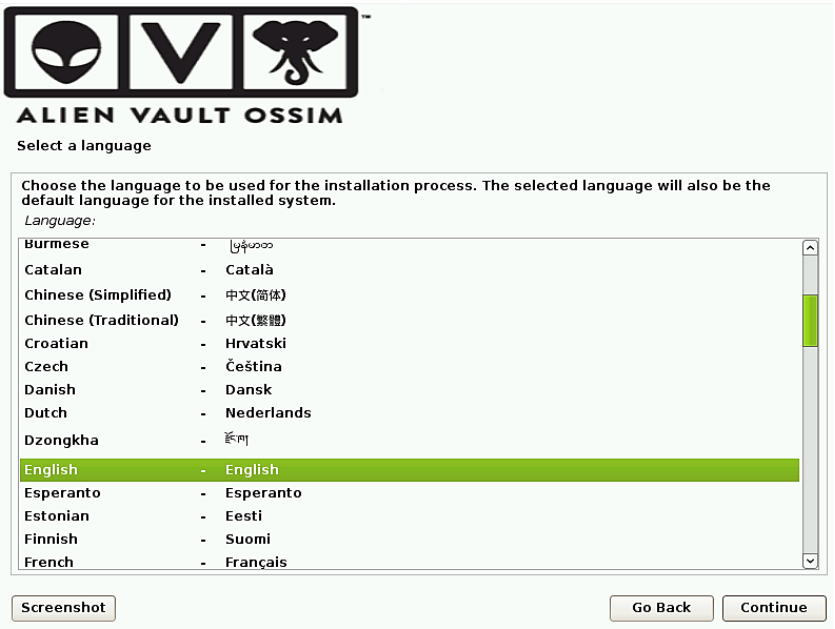


Figura 26: Configuraciones OSSIM AlienVault – Selección de idioma

Fuente: El Autor

Se elegirá la ubicación indicando el país de procedencia.

Figura 27: Configuraciones OSSIM AlienVault – Selección de ubicación

Fuente: El Autor

Se elige la configuración del teclado indicando el idioma respectivo.

Figura 28: Configuraciones OSSIM AlienVault – Configuración del teclado

Fuente: El Autor

Al continuar con el proceso, se seguirán descargando algunos componentes necesarios para la instalación total de la herramienta SIEM.

Figura 29: Configuraciones OSSIM AlienVault – Instalación de componentes

Fuente: El Autor

Mientras está ejecutándose el proceso de instalación de componentes, se debe verificar en el apartado de Red de la máquina virtual de OSSIM AlienVault que en la opción Adaptador 1 (interfase de red) se encuentre conectado a la opción: ‘Adaptador puente’.

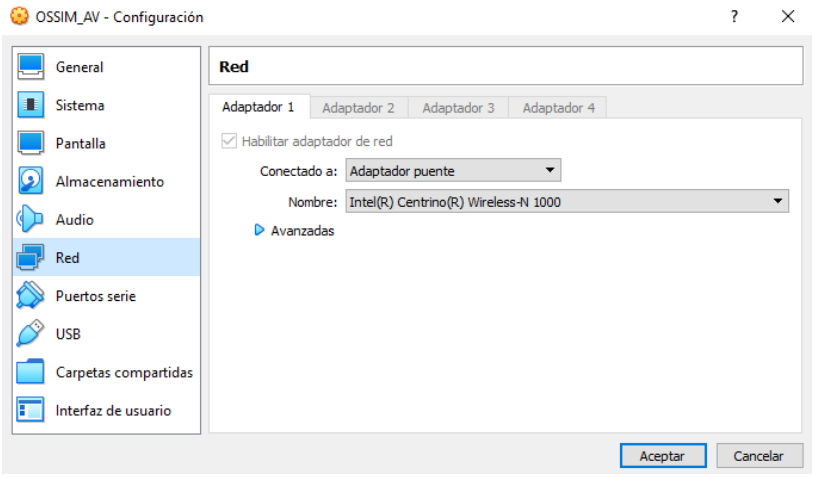


Figura 30: Configuraciones OSSIM AlienVault – Configuración del adaptador de red

Fuente: El Autor

En la siguiente ventana se realizará la configuración de la dirección IP de OSSIM AlienVault para un ambiente de pruebas.

Figura 31: Configuraciones OSSIM AlienVault – Configuración de la dirección IP

Fuente: El Autor

Se especificará la máscara de red correspondiente a la dirección IP configurada previamente para un ambiente de pruebas.

Figura 32: Configuraciones OSSIM AlienVault – Configuración de la máscara de red

Fuente: El Autor

A continuación, se indica la dirección IP para el Gateway (puerta de enlace) que tendrá el servidor.

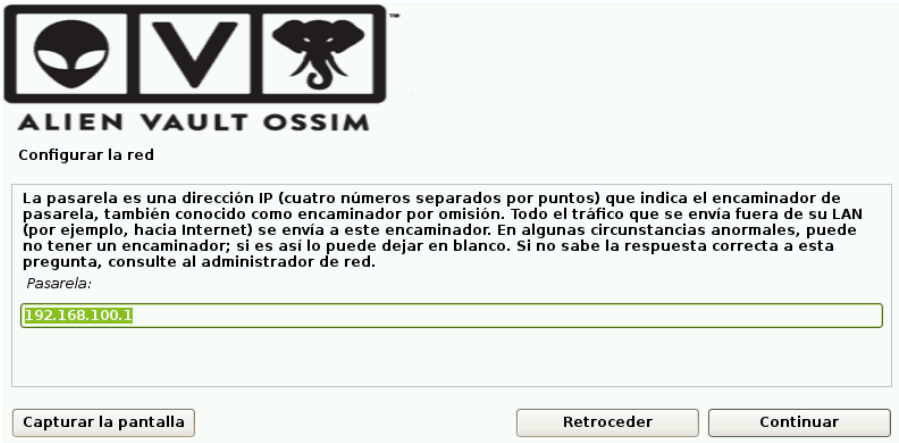


Figura 33: Configuraciones OSSIM AlienVault – Configuración del Gateway

Fuente: El Autor

Se realiza la configuración de la dirección de DNS para la resolución del nombre de dominio, e iniciar con la configuración de la red.

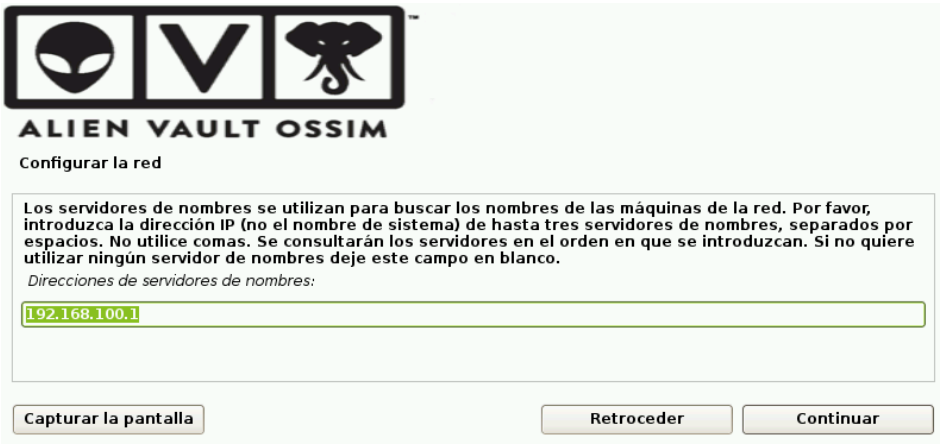


Figura 34: Configuraciones OSSIM AlienVault – Configuración DNS

Fuente: El Autor

En la siguiente ventana, se ingresará una contraseña robusta para el super usuario (root).

Figura 35: Configuraciones OSSIM AlienVault – Configuración de contraseña

Fuente: El Autor

Se configura la zona horaria deseada de acuerdo a las configuraciones previas.

Figura 36: Configuraciones OSSIM AlienVault – Configuración de zona horaria

Fuente: El Autor

Al indicar la zona horaria, se dará paso a la instalación del sistema base de OSSIM AlienVault en el disco duro del equipo.

Figura 37: Configuraciones OSSIM AlienVault – Instalación del sistema base

Fuente: El Autor

Al terminar la instalación del sistema base de OSSIM AlienVault, el equipo se reiniciará para cargar la pantalla de inicio.

Figura 38: Configuraciones OSSIM AlienVault – Inicio del sistema base

Fuente: El Autor

Al culminar toda la instalación de OSSIM AlienVault, se tendrá acceso al sistema.

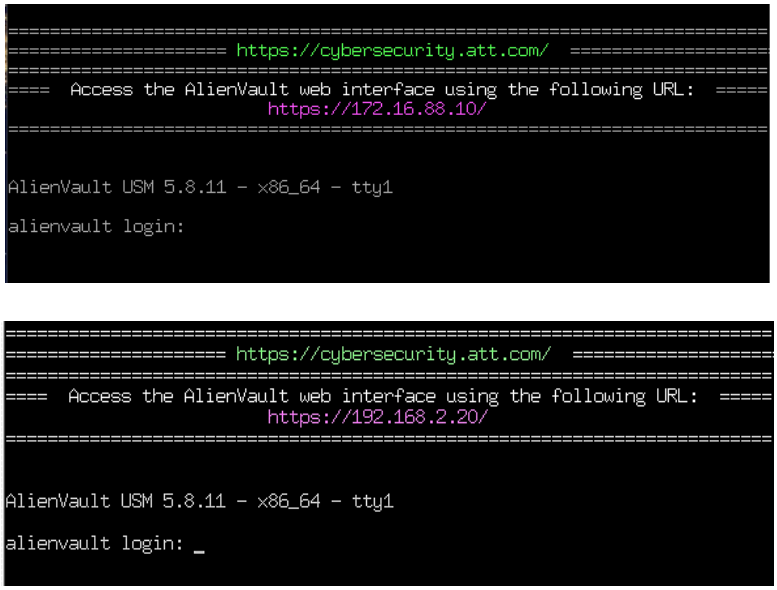


Figura 39: Configuraciones OSSIM AlienVault – Inicio del sistema

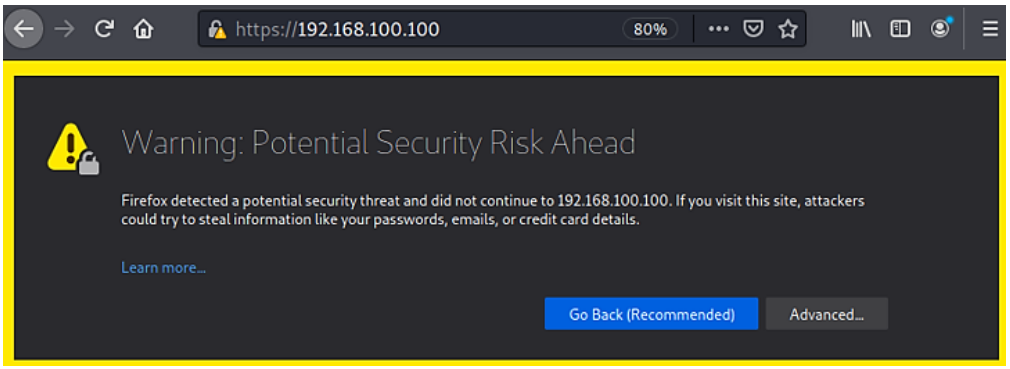
Fuente: El Autor

Para verificar se ingresan las credenciales de acceso configuradas anteriormente que corresponden al usuario y contraseña. Dentro del sistema de OSSIM AlienVault se desplegará un menú con varias opciones de configuración disponibles.

Figura 40: Configuraciones OSSIM AlienVault – Menú de opciones del sistema

Fuente: El Autor

Para acceder a la interfaz web de OSSIM AlienVault, se deberá ingresar a la dirección IP configurada previamente para la administración de la consola web, utilizando un navegador.



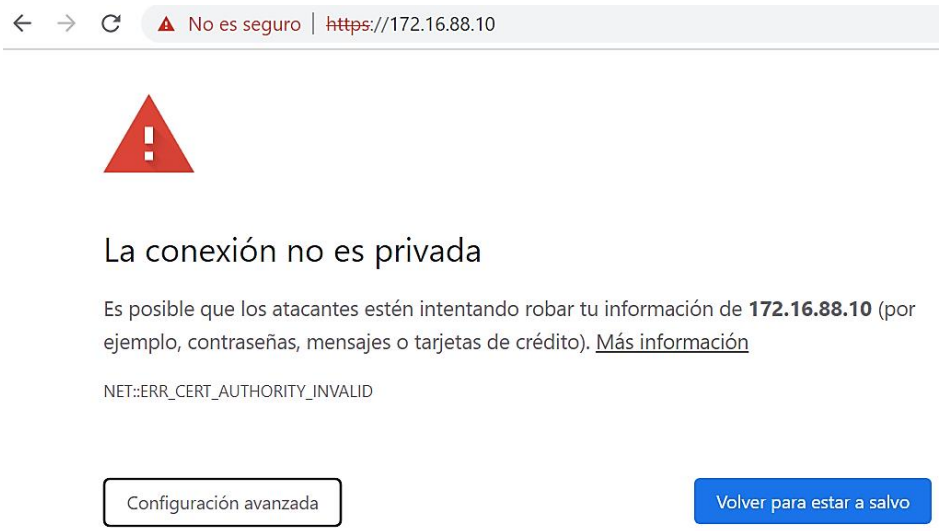


Figura 41: Configuraciones OSSIM AlienVault – Acceso a la interfaz web

Fuente: El Autor

La validación del servidor se realiza al ingresar de forma local la dirección IP en el navegador, que mostrará un mensaje de sitio no seguro. Se ingresa a la opción 'Advanced settings' y se accede seleccionando la opción 'Accept the Risk and Continue'.

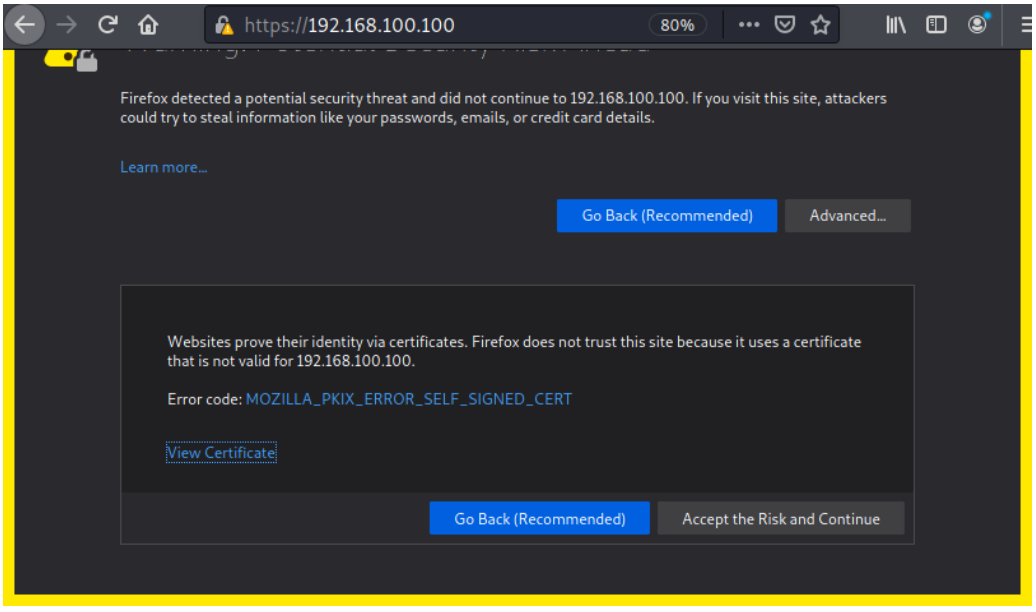


Figura 42: Configuraciones OSSIM AlienVault – Acceso a la interfaz web

Fuente: El Autor

Una vez que se ha ingresado a la opción seleccionada anteriormente, se podrá visualizar la siguiente página, donde se ingresará la información solicitada en el formulario de creación de cuenta.

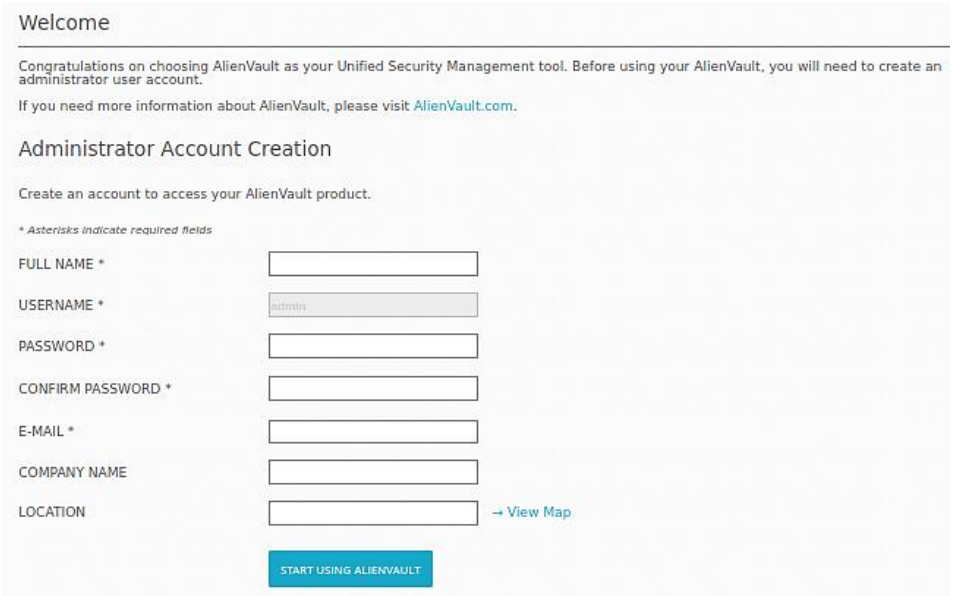


Figura 43: Configuraciones OSSIM AlienVault – Formulario de creación de cuenta

Fuente: El Autor

Una vez ingresados los datos y seleccionado la opción ‘Start using AlienVault’, se tendrá el acceso para iniciar sesión a la cuenta con el usuario y contraseña previamente asignados.

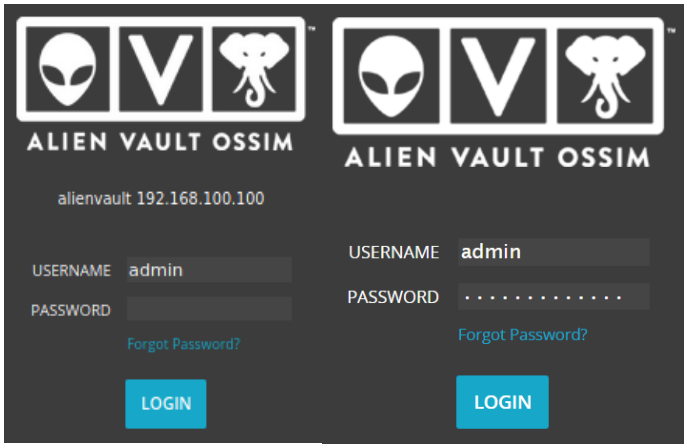


Figura 44: Configuraciones OSSIM AlienVault – Ingreso de credenciales de acceso

Fuente: El Autor

Al ingresar a la interfaz web de OSSIM AlienVault, se despliega una ventana de bienvenida para iniciar con la configuración del servidor.

Figura 45: Configuraciones OSSIM AlienVault – Inicio del sistema

Fuente: El Autor

Al ingresar a la interfaz web, se despliega el asistente de OSSIM AlienVault para realizar configuraciones preliminares.

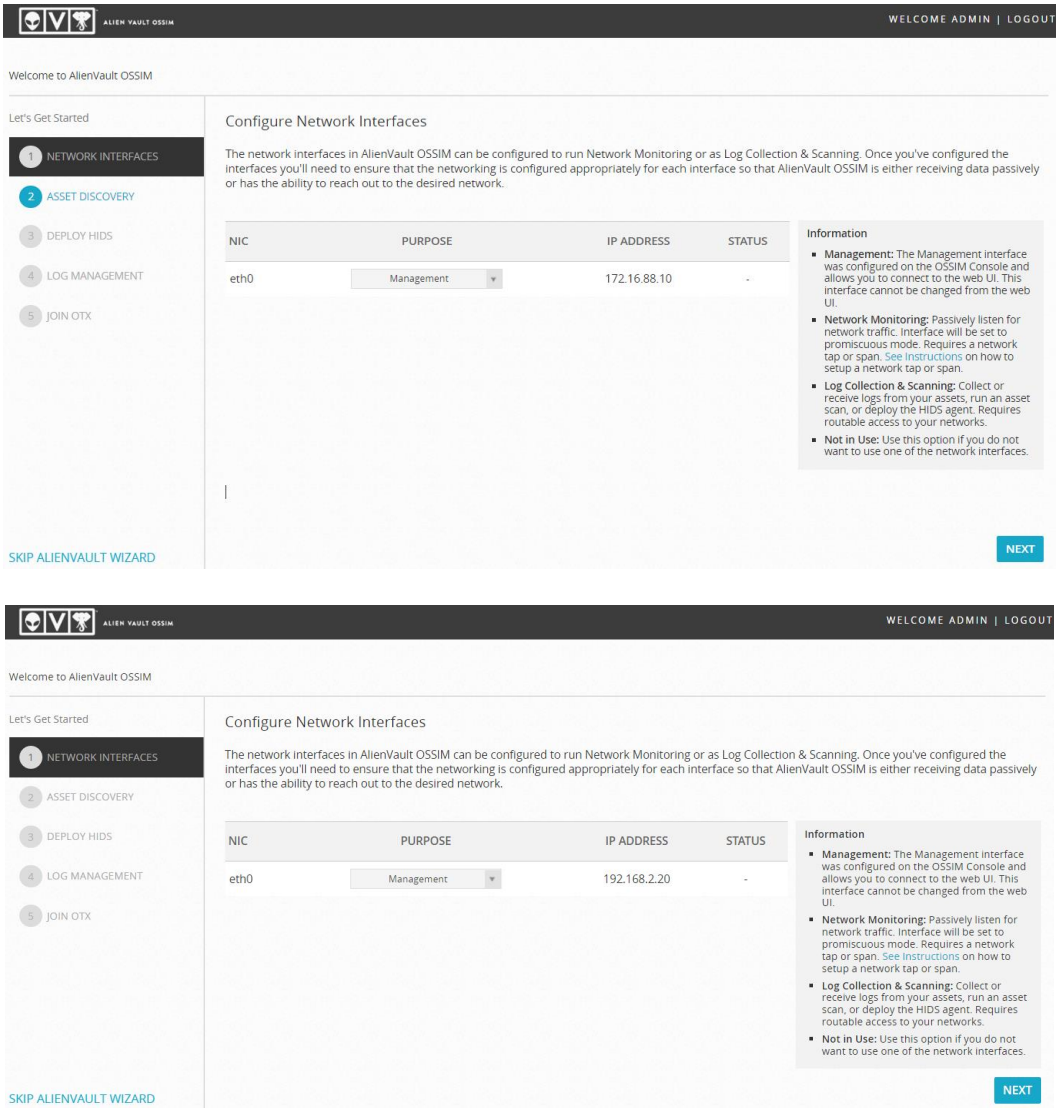


Figura 46: Configuraciones OSSIM AlienVault – Interfaces de red

Fuente: El Autor

En la siguiente ventana, se muestra el descubrimiento de activos con opción de añadir nuevos activos o dispositivos de red; lo que permite conocer el listado de equipos que componen el sistema. A la vez se puede realizar un escaneo de la red o importar un listado desde un archivo de formato ‘csv’.

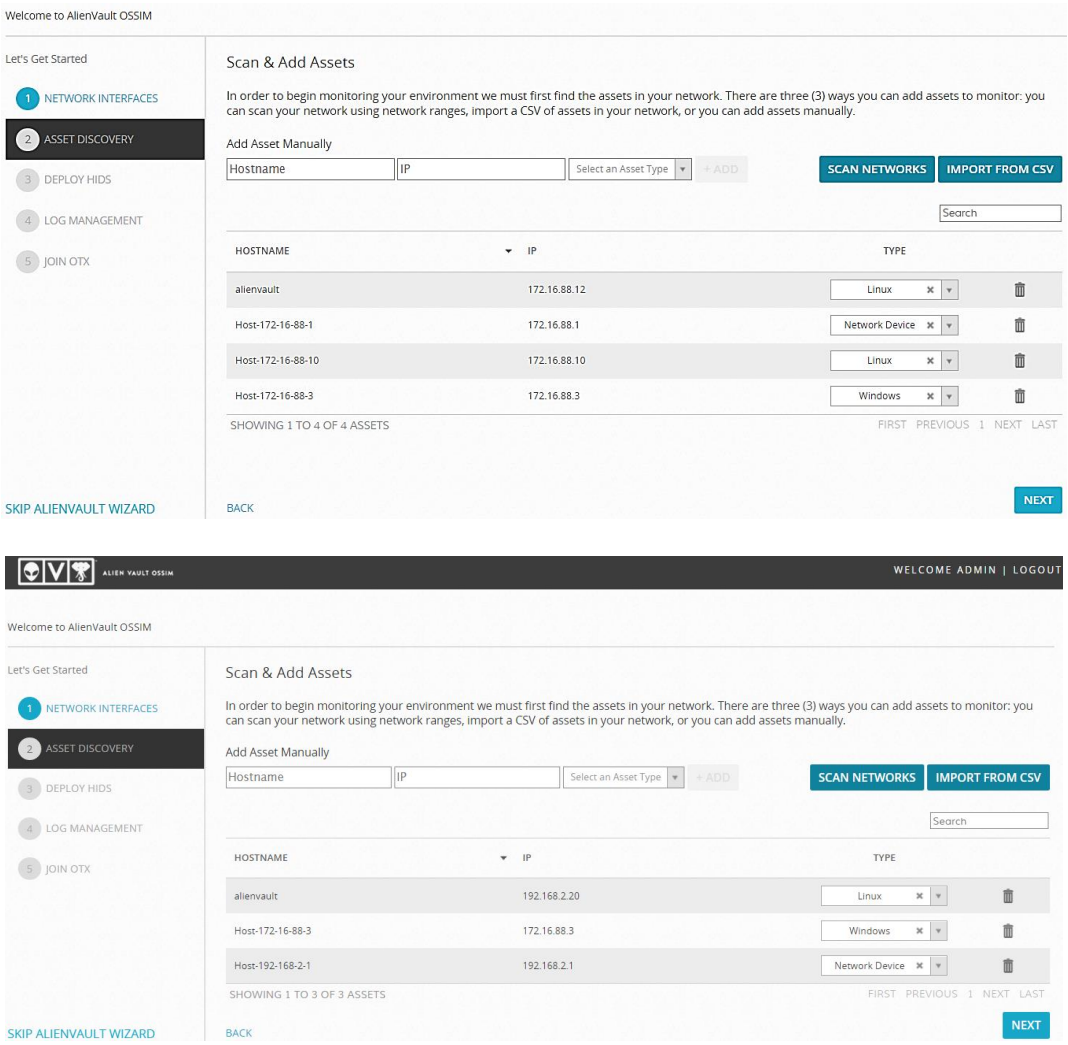


Figura 47: Configuraciones OSSIM AlienVault – Descubrimiento de activos

Fuente: El Autor

Al continuar, se muestra el despliegue de implementación del HIDS (Sistema de detección de intrusiones basado en host) en servidores o equipos para su monitoreo, donde es necesario incluir un usuario, contraseña y un dominio opcional.

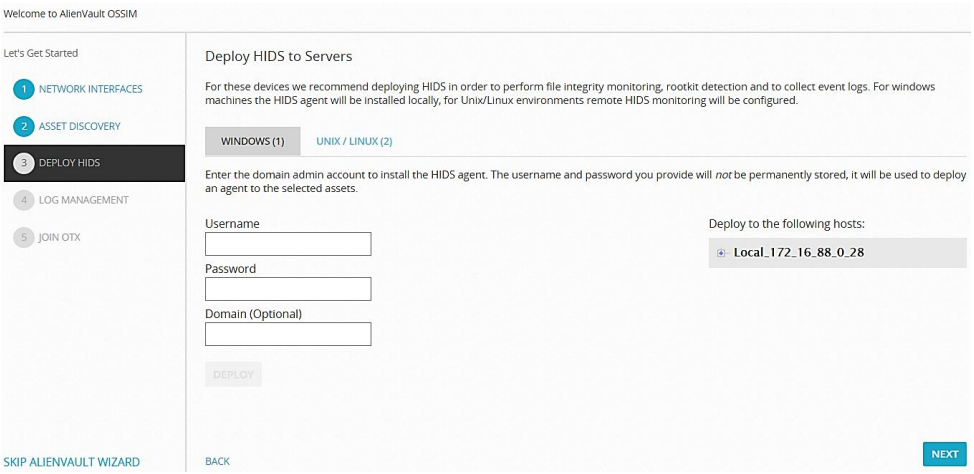


Figura 48: Configuraciones OSSIM AlienVault – Despliegue HIDS

Fuente: El Autor

Para la siguiente ventana se despliega la sección para la gestión de registros, efectuando un escaneo previo al activo sugerido en la sección de 'Asset discovery'.

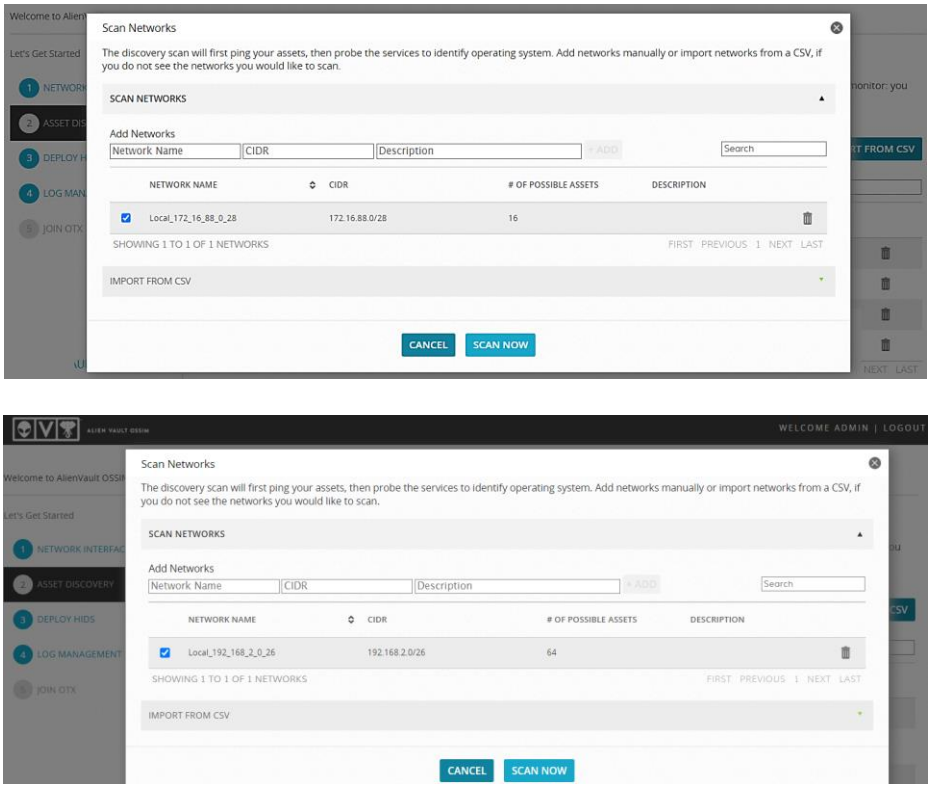


Figura 49: Configuraciones OSSIM AlienVault – Escaneo de red

Fuente: El Autor

Al terminar el escaneo, los resultados pueden mostrar los dispositivos de red encontrados, aunque inicialmente no puedan haberse encontrado.

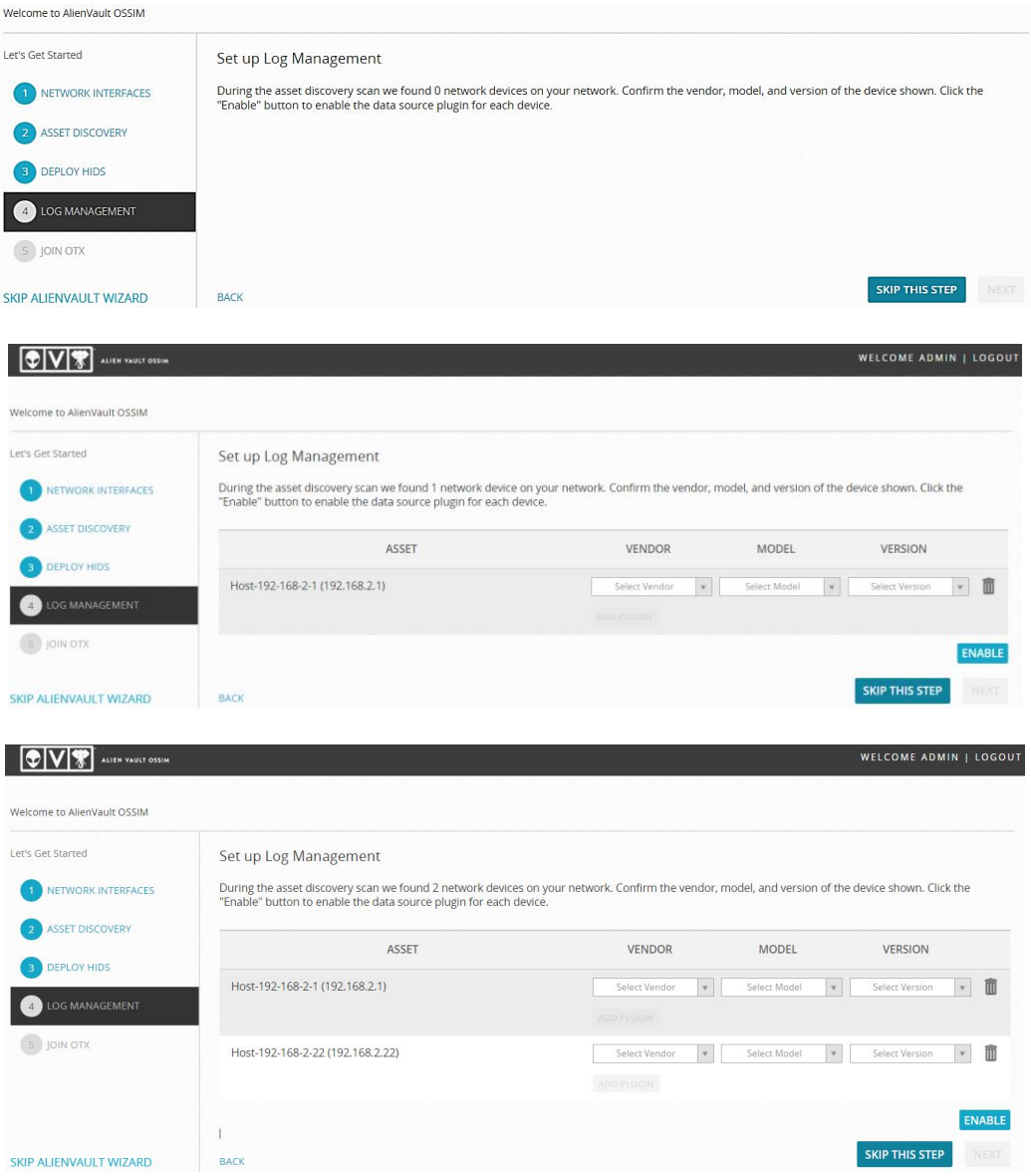


Figura 50: Configuraciones OSSIM AlienVault – Gestión de registros

Fuente: El Autor

En la sección final se solicitará el registro de una cuenta para el ingreso del código OTX, que permitirá la integración del sistema de detección de amenazas. El código OTX se obtendrá al registrar una cuenta que será verificada.

Al concluir si es requerido se podrán hacer configuraciones adicionales o iniciar la exploración de OSSIM AlienVault.

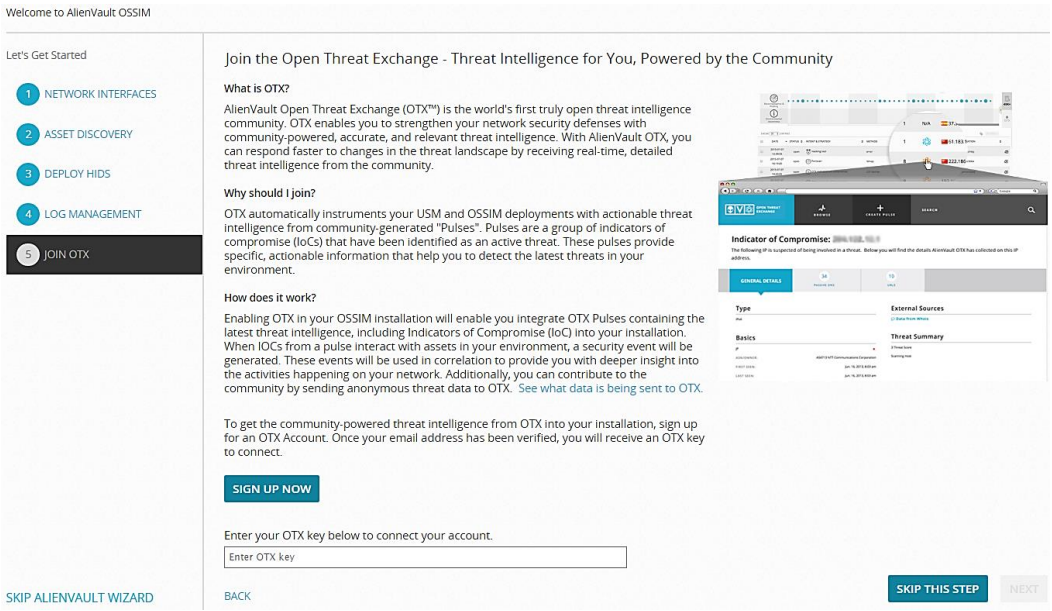


Figura 51: Configuraciones OSSIM AlienVault – Registro de código OTX

Fuente: El Autor

Se muestra un mensaje de finalización de registro para el intercambio de información referente a las amenazas encontradas.

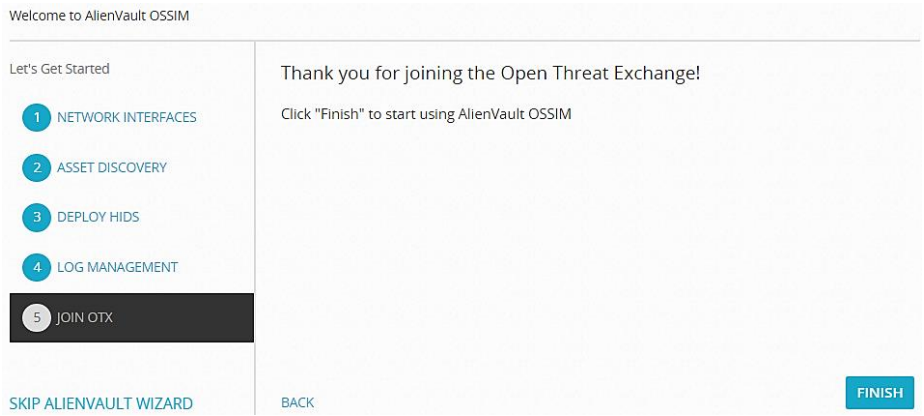


Figura 52: Configuraciones OSSIM AlienVault – Finalización de registro

Fuente: El Autor

Se cargará toda la interfaz web con sus diferentes opciones de configuración.

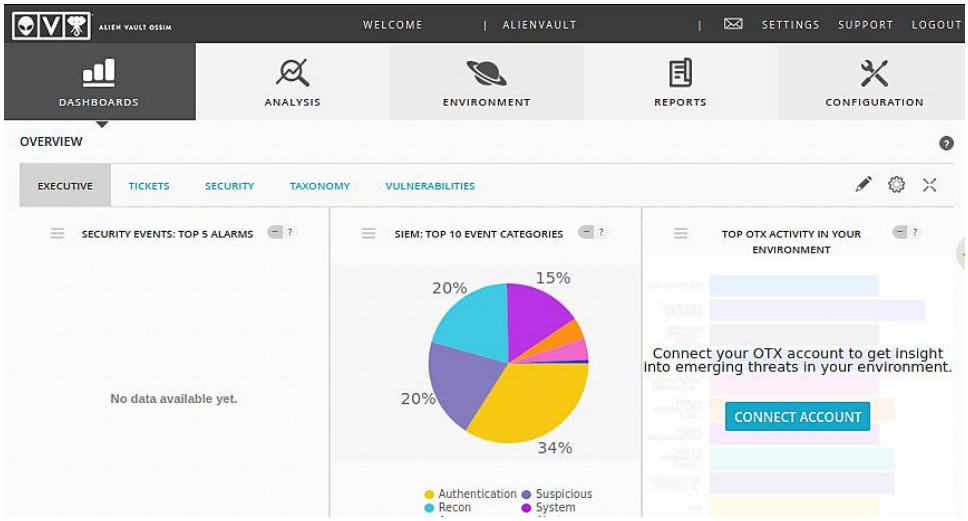


Figura 53: Configuraciones OSSIM AlienVault – Interfaz web

Fuente: El Autor

Al haber ingresado directamente a la consola de administración web de OSSIM AlienVault para efectuar ajustes adicionales de comprobación, se tendrá el menú habilitado con las 8 opciones de configuración por consola.

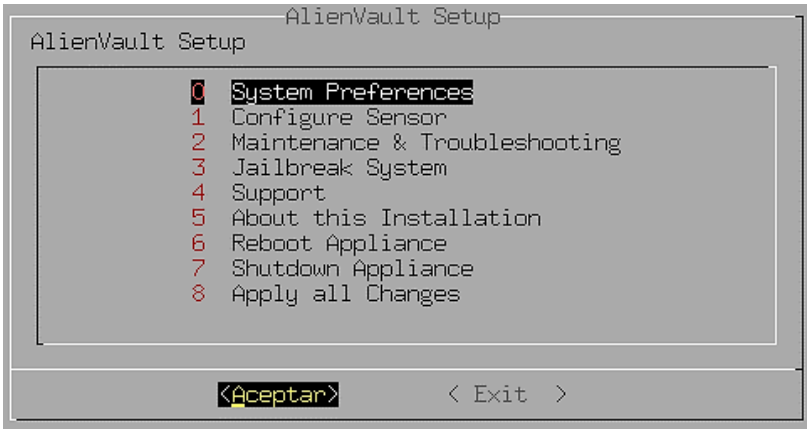


Figura 54: Configuraciones OSSIM AlienVault – Menú de opciones general

Fuente: El Autor

Se elegirá la opción ‘System Preferences’, que desplegará otro menú con 6 opciones; de los cuales la opción ‘Configure Network’ permitirá realizar las configuraciones de la red.

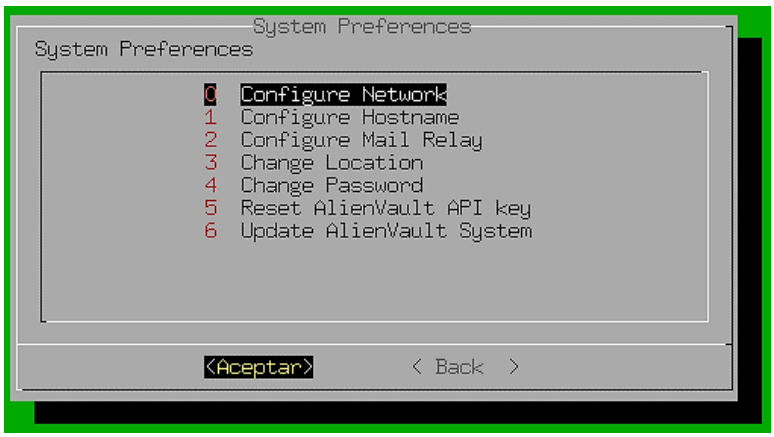


Figura 55: Configuraciones OSSIM AlienVault – Menú de opciones de preferencia

Fuente: El Autor

En el siguiente menú de opciones se podrá realizar la configuración de la tarjeta de red, ingresando a ‘Setup Management Network’.

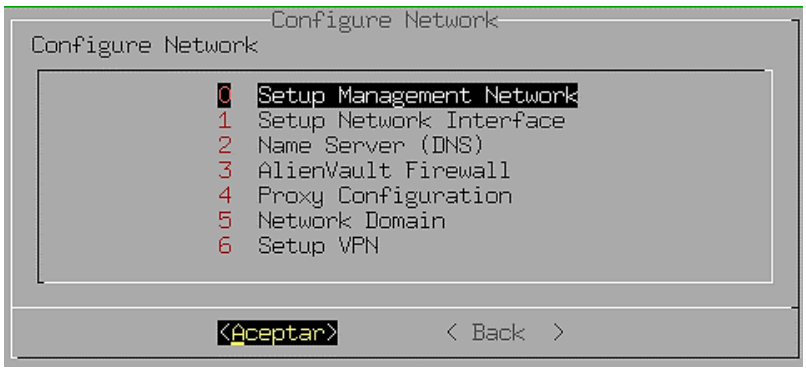


Figura 56: Configuraciones OSSIM AlienVault – Menú de opciones de red

Fuente: El Autor

Al abrirse la siguiente ventana, se muestra una lista con las diferentes tarjetas de red configuradas del sistema operativo que dispone el servidor (interfaces de red). Si se tiene

otra tarjeta de red, se puede añadir para que sea configurado específicamente como recolector de información.

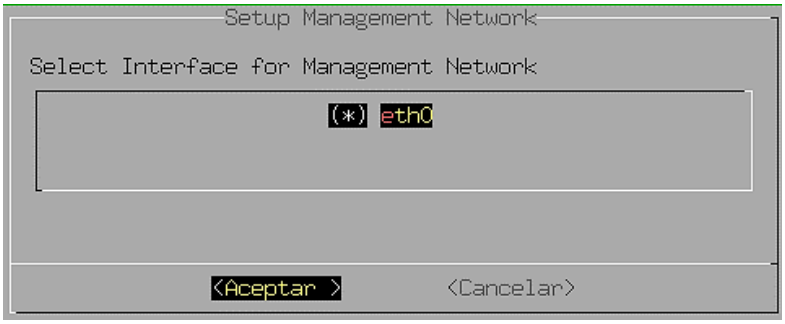


Figura 57: Configuraciones OSSIM AlienVault – Configuración de la red de gestión

Fuente: El Autor

Al seleccionar y aceptar la interfaz de red indicada ‘eth0’, se muestra la configuración del direccionamiento IP del equipo.

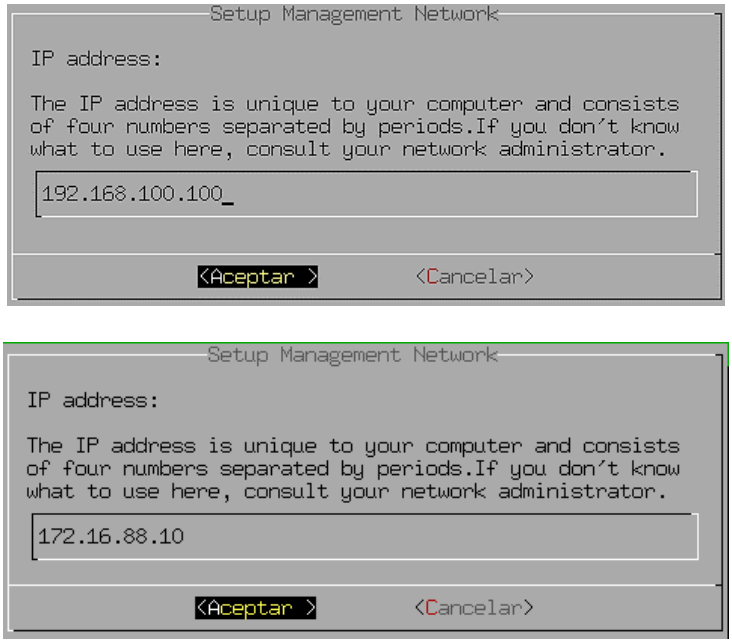


Figura 58: Configuraciones OSSIM AlienVault – Configuración de la dirección IP

Fuente: El Autor

Al aceptar y especificar la dirección IP, se muestra la configuración de la máscara de red que tendrá el equipo.

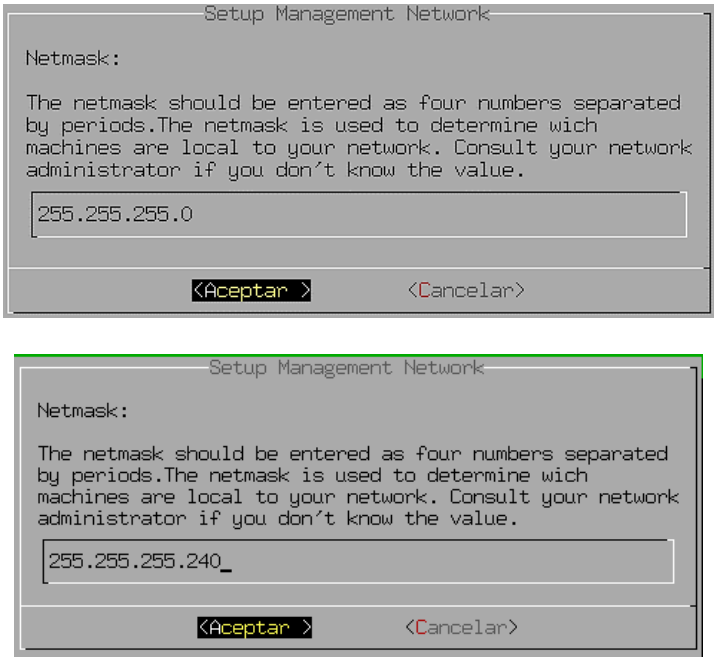
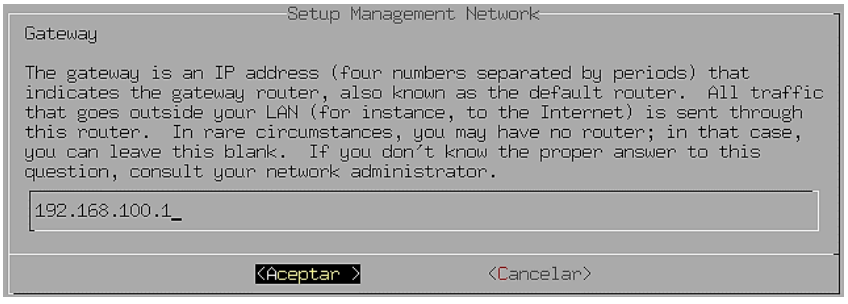


Figura 59: Configuraciones OSSIM AlienVault – Configuración de la máscara de red

Fuente: El Autor

Al aceptar y especificar la máscara de red, se muestra la configuración de la puerta de enlace (Gateway) que tendrá el equipo.



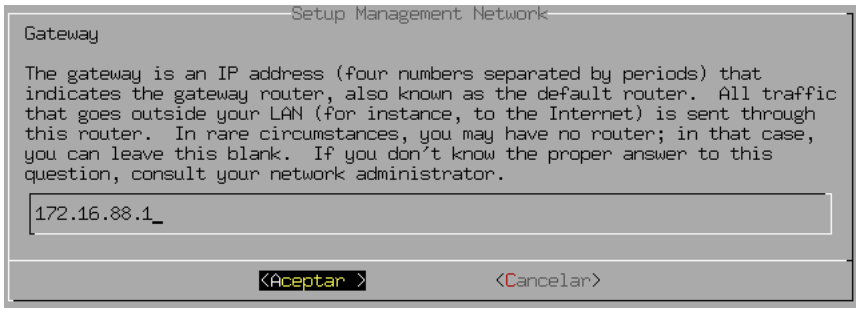


Figura 60: Configuraciones OSSIM AlienVault – Configuración de la puerta de enlace

Fuente: El Autor

Se podrá verificar si el 'Firewall' (corta fuegos) se encuentra habilitado por defecto en la opción 'AlienVault Firewall' del menú de opciones de red. De igual manera, se podrá configurar el direccionamiento del nombre de dominio (DNS), el Proxy, la configuración de una red privada virtual (VPN) o el nombre de dominio.

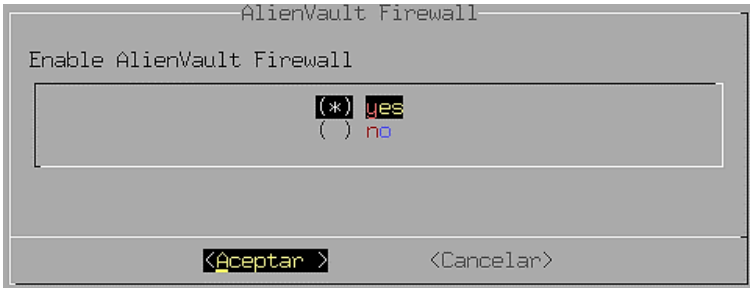


Figura 61: Configuraciones OSSIM AlienVault – Configuración del Firewall

Fuente: El Autor

En el menú de opciones de red, se puede seleccionar la opción 'Network Domain' para indicar el nombre de dominio de la organización respectivamente, aunque para efectos de pruebas se dejará por defecto lo sugerido por la herramienta.

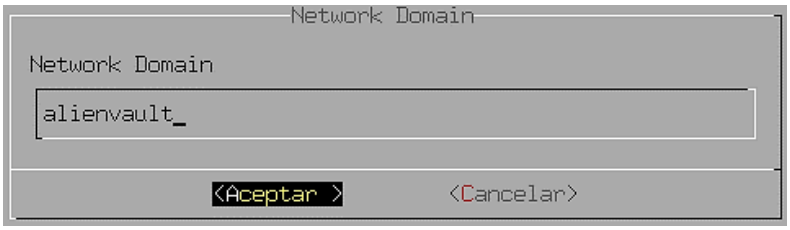


Figura 62: Configuraciones OSSIM AlienVault – Configuración de nombre de dominio

Fuente: El Autor

Al haber especificado el nombre de dominio del servidor, se regresa al menú de preferencias del sistema, donde se indicará el nombre del host (hostname) en la opción 'Configure Hostname'. Se tendrá un nombre sugerido y se aceptará. También dentro del mismo menú, habrá opciones para configurar la retransmisión de correo para el envío de alertas, el cambio de la ubicación, el cambio de la contraseña y la actualización del sistema de OSSIM AlienVault.

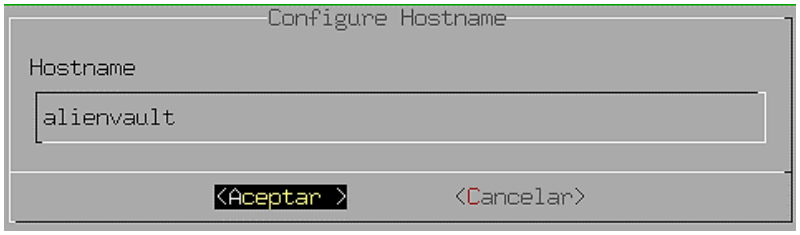


Figura 63: Configuraciones OSSIM AlienVault – Configuración de hostname

Fuente: El Autor

Al regresar al menú principal, se deberá seleccionar la opción 'Configure Sensor' que desplegará el menú de opciones para la configuración del sensor.

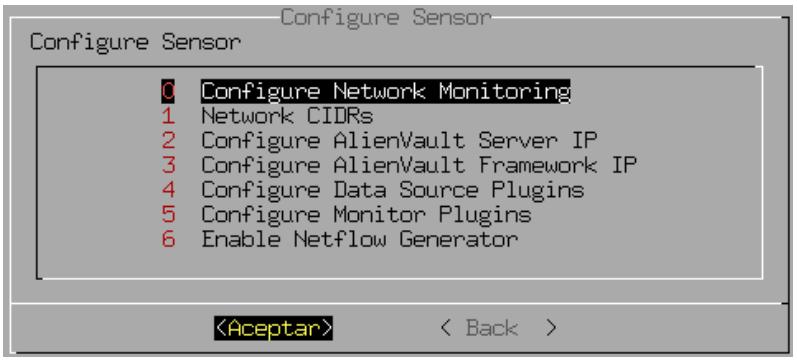


Figura 64: Configuraciones OSSIM AlienVault – Configuración de sensor

Fuente: El Autor

Al seleccionar la primera alternativa 'Configure Network Monitoring', se podrá configurar la tarjeta de red (interfase) para el monitoreo y captura del tráfico de red.

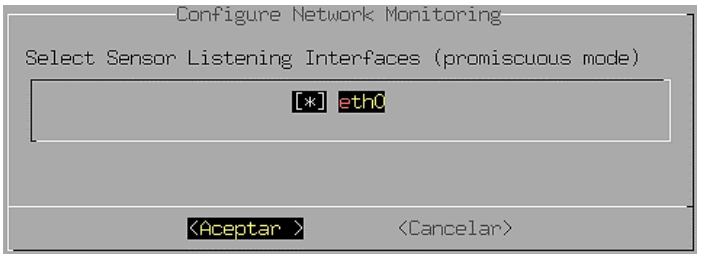


Figura 65: Configuraciones OSSIM AlienVault – Configuración de la interfaz de red

Fuente: El Autor

Al configurar la interfaz de red del sensor, en el menú de configuración se configura la red o redes que se va a monitorear, ingresando en la opción 'Network CIDRs'. Por defecto, la herramienta sugerirá algunas redes, las mismas que serán adoptadas o eliminadas para especificar o cambiar por una red deseada.

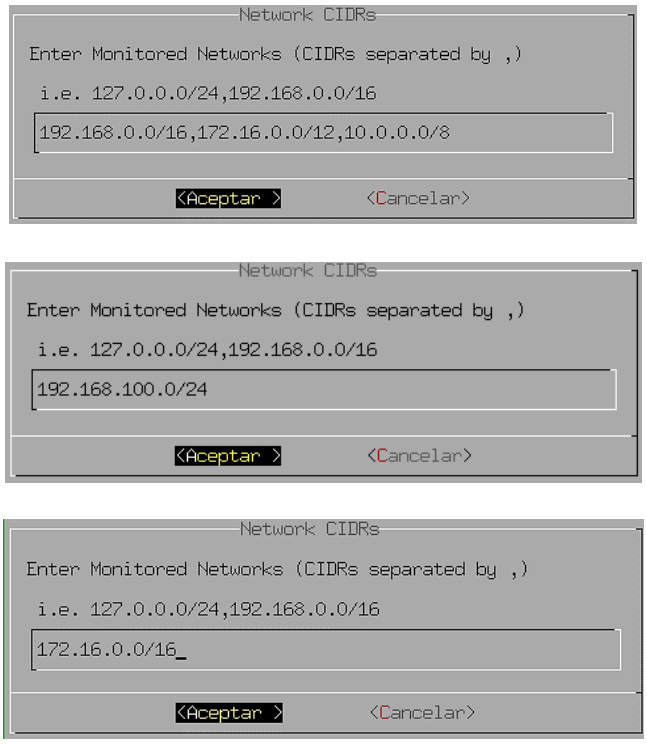


Figura 66: Configuraciones OSSIM AlienVault – Configuración de la red monitoreada

Fuente: El Autor

Dentro del menú de configuraciones de sensor, en la opción 'Configure AlienVault Server IP', se especifica una dirección IP sugerida para que recolecte la información.

Figura 67: Configuraciones OSSIM AlienVault – Configuración de la dirección IP

Fuente: El Autor

En la opción 'Configure AlienVault Framework IP', se especifica una dirección IP sugerida para el marco de trabajo del servidor en el ambiente de pruebas.

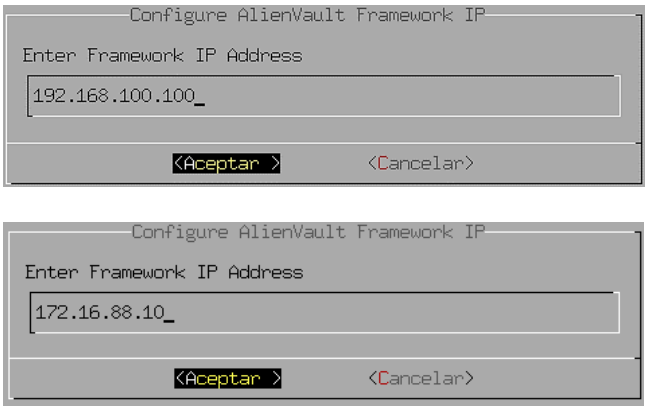


Figura 68: Configuraciones OSSIM AlienVault – Configuración del framework

Fuente: El Autor

La siguiente opción 'Configure Data Source Plugins' que permitirá determinar los plugins (complementos) que están habilitados en el servidor o se podrán habilitar otros que sean necesarios para que sean incluidos en el monitoreo.

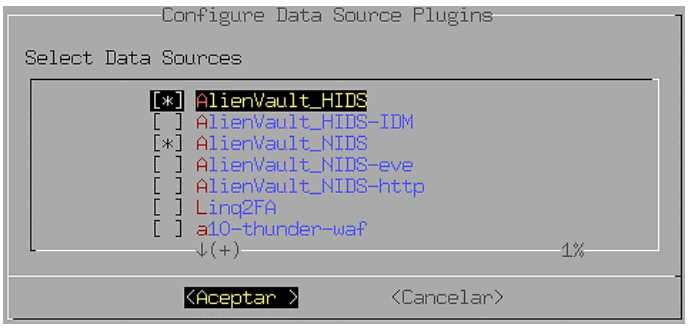


Figura 69: Configuraciones OSSIM AlienVault – Configuración de complementos

Fuente: El Autor

Al regresar al menú principal se puede acceder a la opción de 'Maintenance & Troblueshooting' para el mantenimiento y solución de problemas o la opción 'Jailbreak System' para tener acceso a la consola; además de reiniciar el servidor, apagar el servidor y aplicar todos cambios realizados mediante la opción 'Apply all changes'. Al efectuarse los cambios se despliega un aviso con los cambios que serán aplicados.

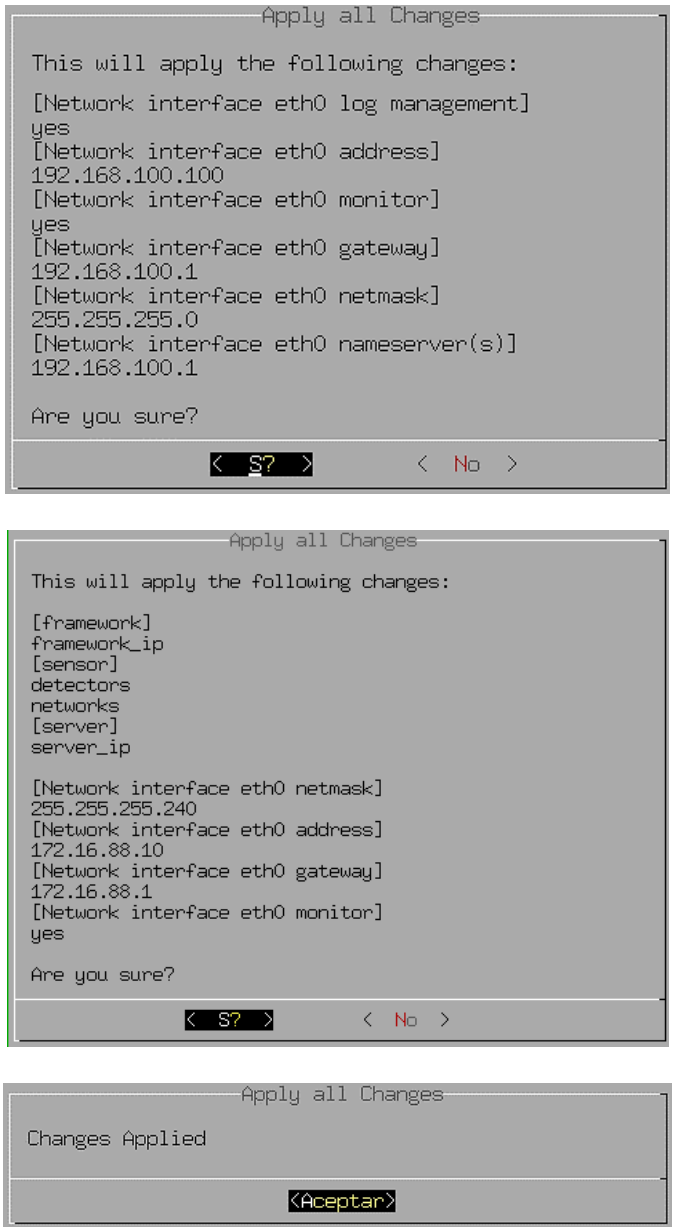


Figura 70: Configuraciones OSSIM AlienVault – Aplicación de cambios

Fuente: El Autor

Al finalizar y guardar los cambios, en la opción ‘About this Installation’ del menú principal se puede verificar la versión del sistema.

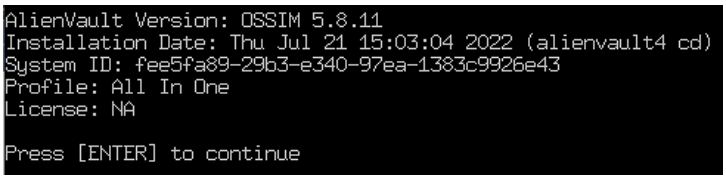


Figura 71: Configuraciones OSSIM AlienVault – Versión del sistema instalado

Fuente: El Autor

Dentro del menú principal se puede ingresar a la opción 'Jailbreak System', para iniciar el modo de consola del servidor.

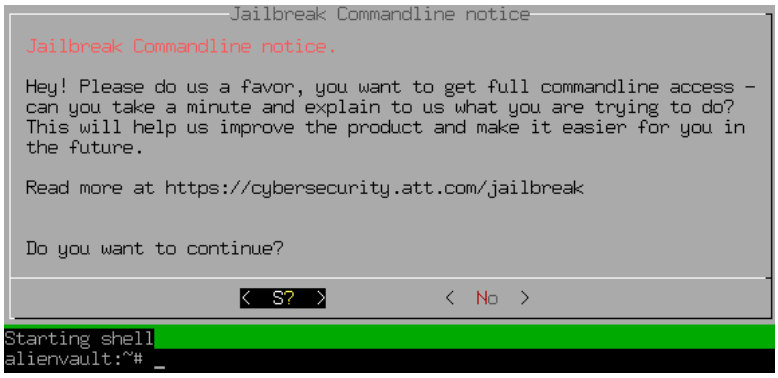
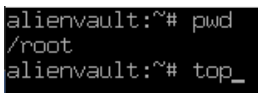


Figura 72: Configuraciones OSSIM AlienVault – Modo de línea de comandos

Fuente: El Autor

Al ejecutar los siguientes comandos se puede determinar:

- pwd – permite mostrar el directorio actual.
- top – permite mostrar los procesos en ejecución.
- df -lh – permite mostrar el espacio en disco utilizado por el sistema de ficheros.



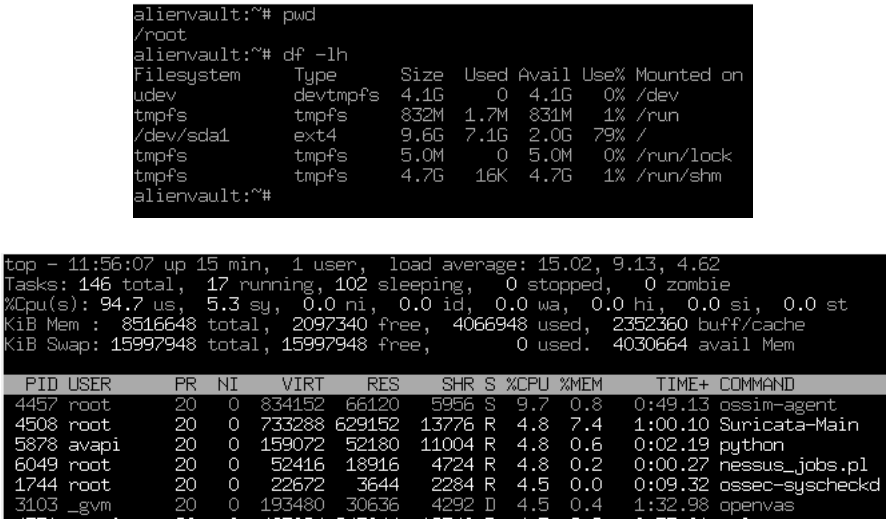


Figura 73: Configuraciones OSSIM AlienVault – Línea de comandos

Fuente: El Autor

4.4 Gestión de activos

Al ingresar con las credenciales de acceso a la consola en la interfaz web de OSSIM AlienVault, se ingresa a la opción ‘Assets & Groups’ dentro del apartado de ‘Environment’, el cual mostrará los activos (dispositivos) que haya detectado el sistema operativo. Si se requiere añadir otros activos, se necesita elegir la opción ‘Add Assets’ seguido de Scan for new Assets’.

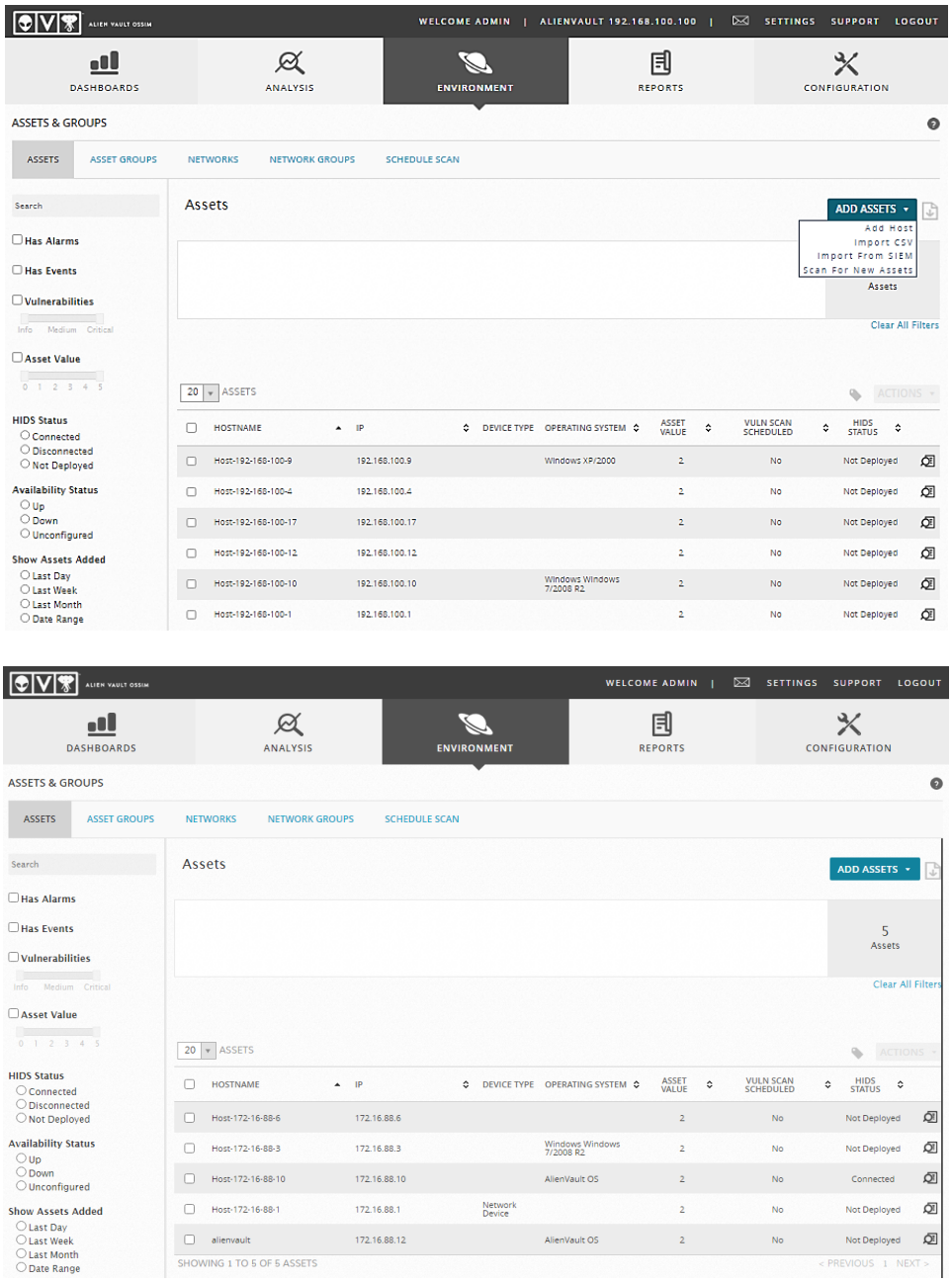


Figura 74: Interfaz web OSSIM AlienVault – Gestión de activos

Fuente: El Autor

Al elegir la opción de escaneo de nuevos activos se abrirá un espacio para añadir los activos que se van a buscar en la red, se podrá seleccionar el sensor que será utilizado como el sensor que se encuentra en el servidor OSSIM AlienVault; también se podrá seleccionar el tipo de escaneo, la plantilla de tiempo, la autodetección de servicios y

sistemas operativos, la habilitación de resolución de DNS inversa para conocer los nombres de los equipos y se inicia con el escaneo. El tiempo de escaneo dependerá del tamaño y la cantidad de equipos, servidores y dispositivos conectados a la red para recabar información y almacenarlo dentro de la base de datos de OSSIM AlienVault con el fin de detectar vulnerabilidades, y posibles riesgos.

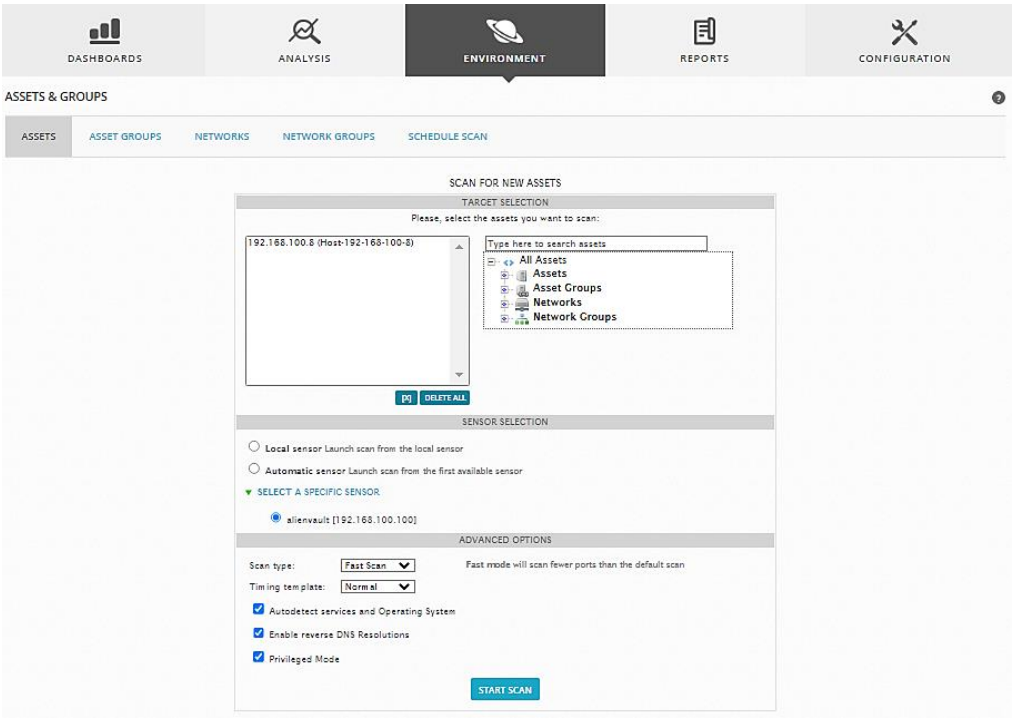


Figura 75: Interfaz web OSSIM AlienVault – Ingreso de activos

Fuente: El Autor

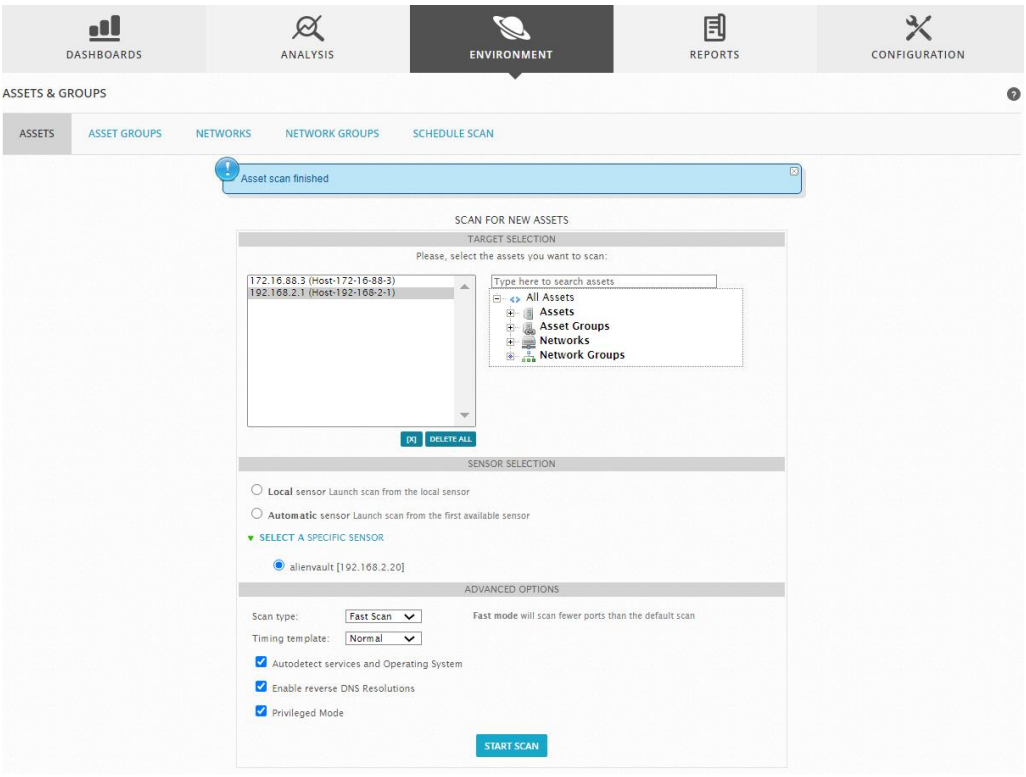


Figura 76: Interfaz web OSSIM AlienVault – Escaneo de activos

Fuente: El Autor

Los resultados del escaneo mostrarán un listado con los dispositivos encontrados, donde se podrá realizar la actualización de la gestión de activos en la opción 'Update managed assets'.

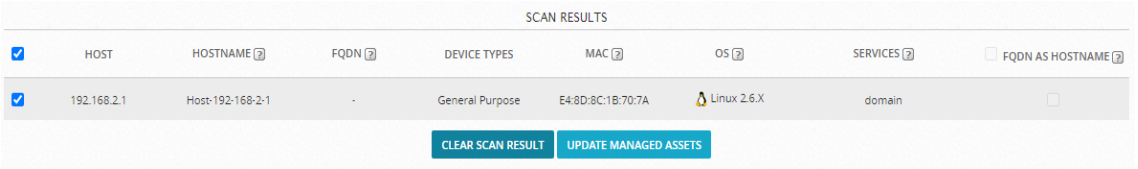


Figura 77: Interfaz web OSSIM AlienVault – Resultados de escaneo de activos

Fuente: El Autor

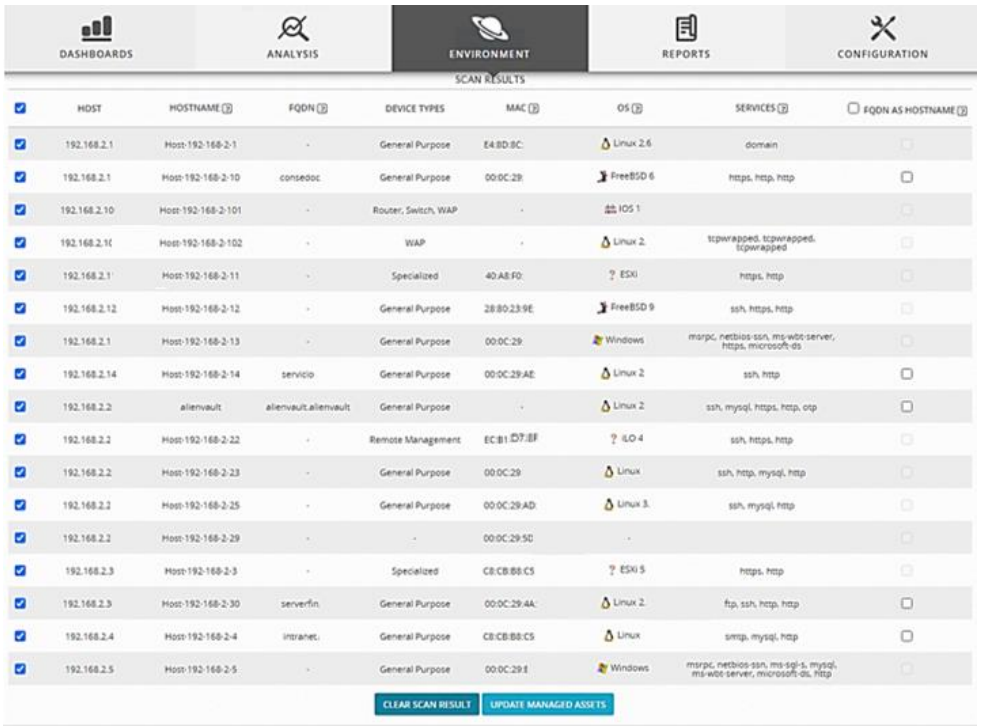


Figura 78: Interfaz web OSSIM AlienVault – Actualización de gestión de activos

Fuente: El Autor

Los campos que se habilitan corresponden al nombre del grupo en el cual se incluirán los activos asociados con una descripción breve del mismo, el valor de criticidad del activo con una escala que va entre 1 a 5 dependiendo del tipo o clase de activos manejados en la organización, el sensor o red distribuida de sensores para realizar la administración del grupo de servidores mencionado, también se indicará que el activo no pertenece a una entidad externa y se guardan los cambios para que la información encontrada del inventario sea actualizada.

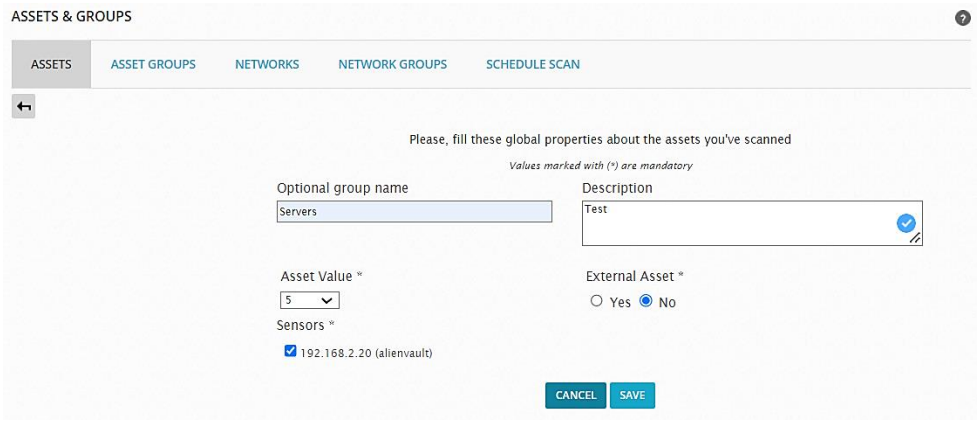


Figura 79: Interfaz web OSSIM AlienVault – Nombre del grupo de activos

Fuente: El Autor

Se actualizará el listado en un resumen descriptivo de los nuevos activos de la red.

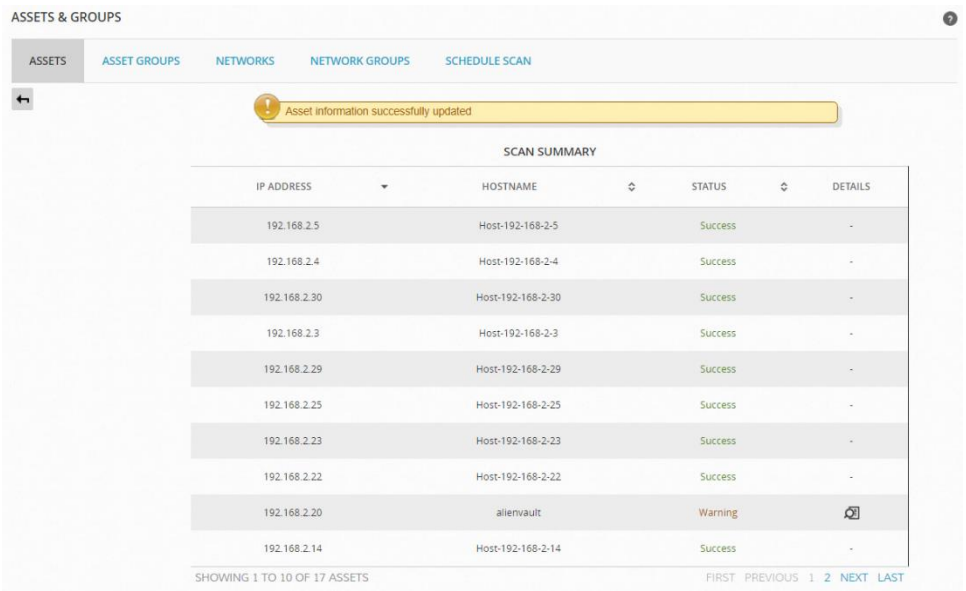


Figura 80: Interfaz web OSSIM AlienVault – Activos y grupos

Fuente: El Autor

Al haberse actualizado el inventario con la información del grupo de servidores perteneciente al grupo que fue creado, el mismo aparecerá en la opción ‘Assets Groups’ dentro del apartado ‘Environment’ mostrando el número de activos asociados al grupo,

aunque sin datos estadísticos de vulnerabilidades, alarmas, disponibilidad, y notas debido a que aún no están desplegados los módulos OpenVas, Snort, Nagios para que haya los resultados correspondientes.

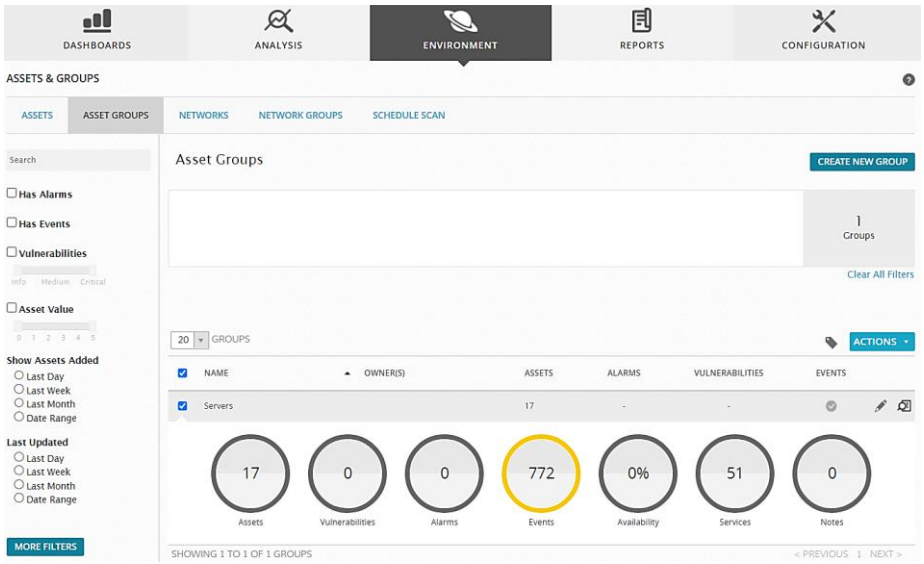


Figura 81: Interfaz web OSSIM AlienVault – Grupos de activos

Fuente: El Autor

En la siguiente pestaña de 'Networks', se muestran las redes que podrán configurarse y ser monitorizadas por OSSIM AlienVault.

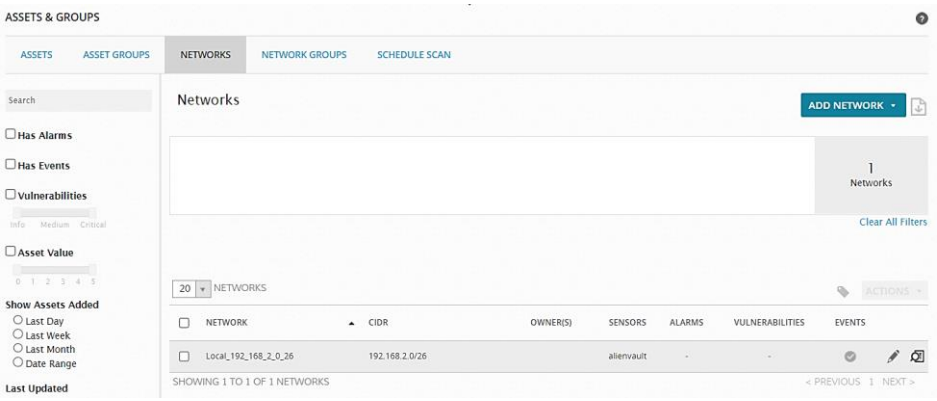


Figura 82: Interfaz web OSSIM AlienVault – Redes

Fuente: El Autor

En la pestaña ‘Networks Groups’, se muestra el conjunto de redes que pueden agruparse.

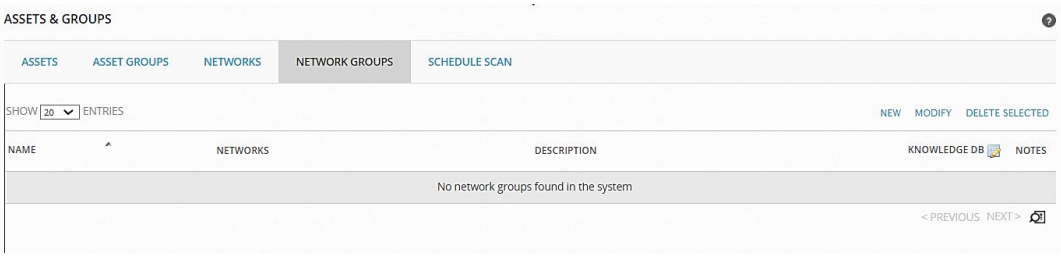


Figura 83: Interfaz web OSSIM AlienVault – Grupos de redes

Fuente: El Autor

De igual forma, si se requiere contar con más grupos de activos, se pueden crear y añadir grupos para conmutadores, ruteadores, VPNs, estaciones de trabajo, con el fin de organizar la red para obtener un mapa de los activos con los que cuenta la organización o entidad. Para evidenciar la información de cada host (activo), se puede seleccionar en el apartado ‘Environment’ la opción ‘Assets’ y elegir un activo.

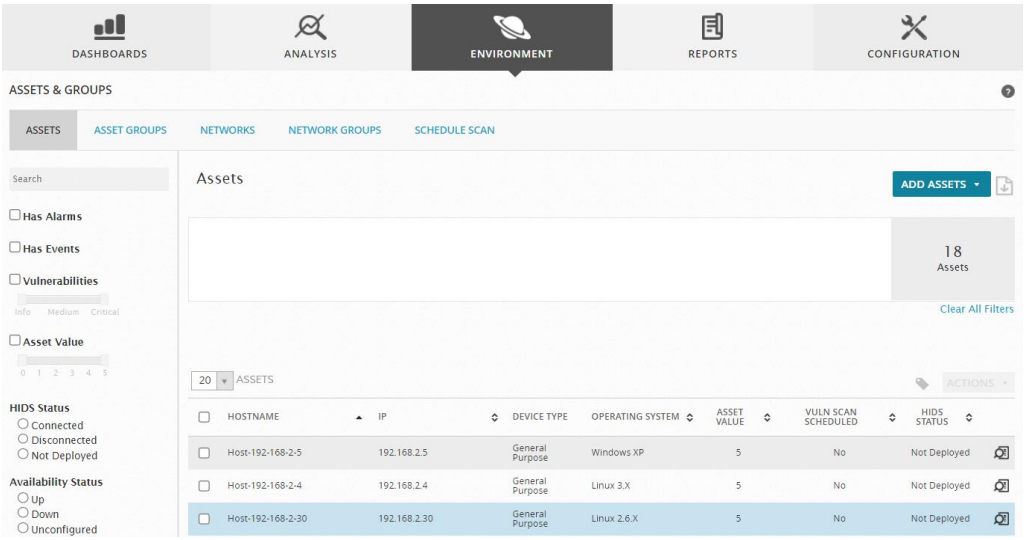


Figura 84: Interfaz web OSSIM AlienVault – Activos

Fuente: El Autor

Al elegir un determinado activo de la lista desplegada, para verificar la información que presenta el mismo, y si es necesario realizar alguna modificación, se lo puede hacer mediante la opción ‘Actions’ para editar el activo que fue seleccionado.

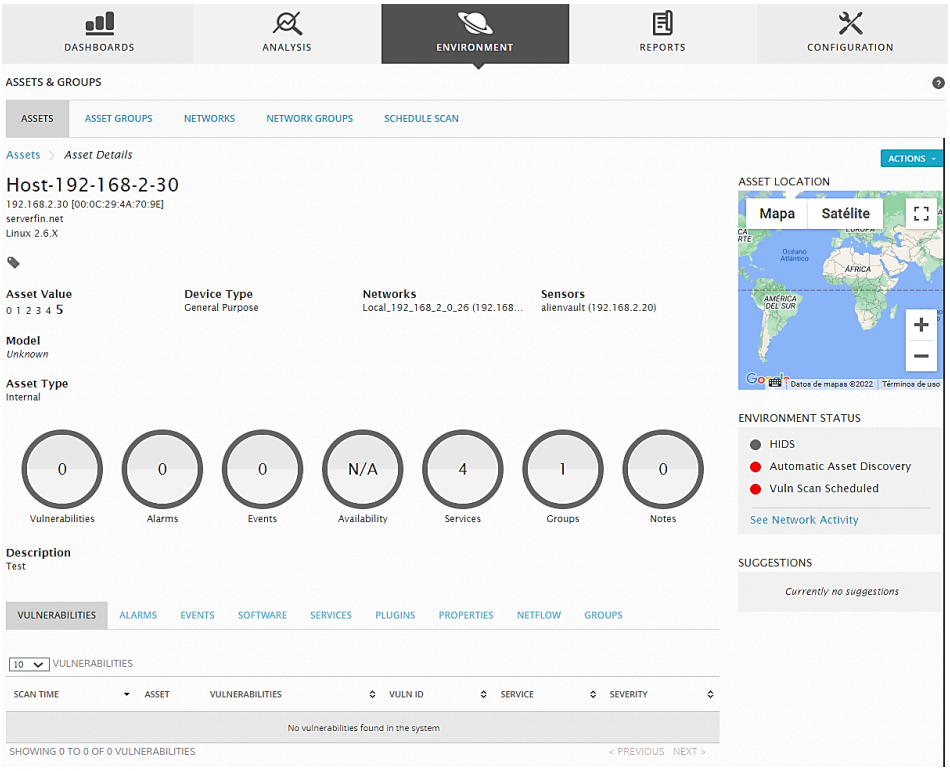


Figura 85: Interfaz web OSSIM AlienVault – Detalles de activos

Fuente: El Autor

Al ingresar en la opción ‘Actions’, se pueden realizar diferentes acciones de los cuales para la edición se debe seleccionar ‘Edit’.

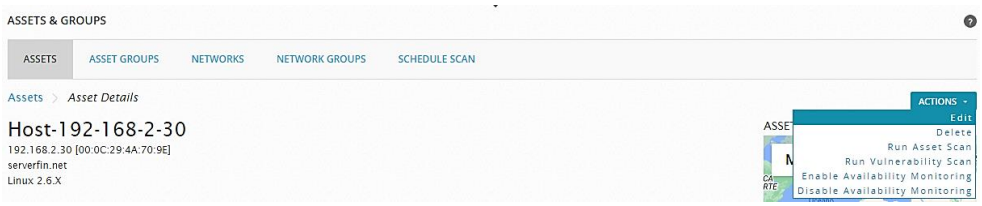


Figura 86: Interfaz web OSSIM AlienVault – Edición de los detalles de activos

Fuente: El Autor

Se abrirá una ventana de edición que permitirá la actualización y configuración del activo.

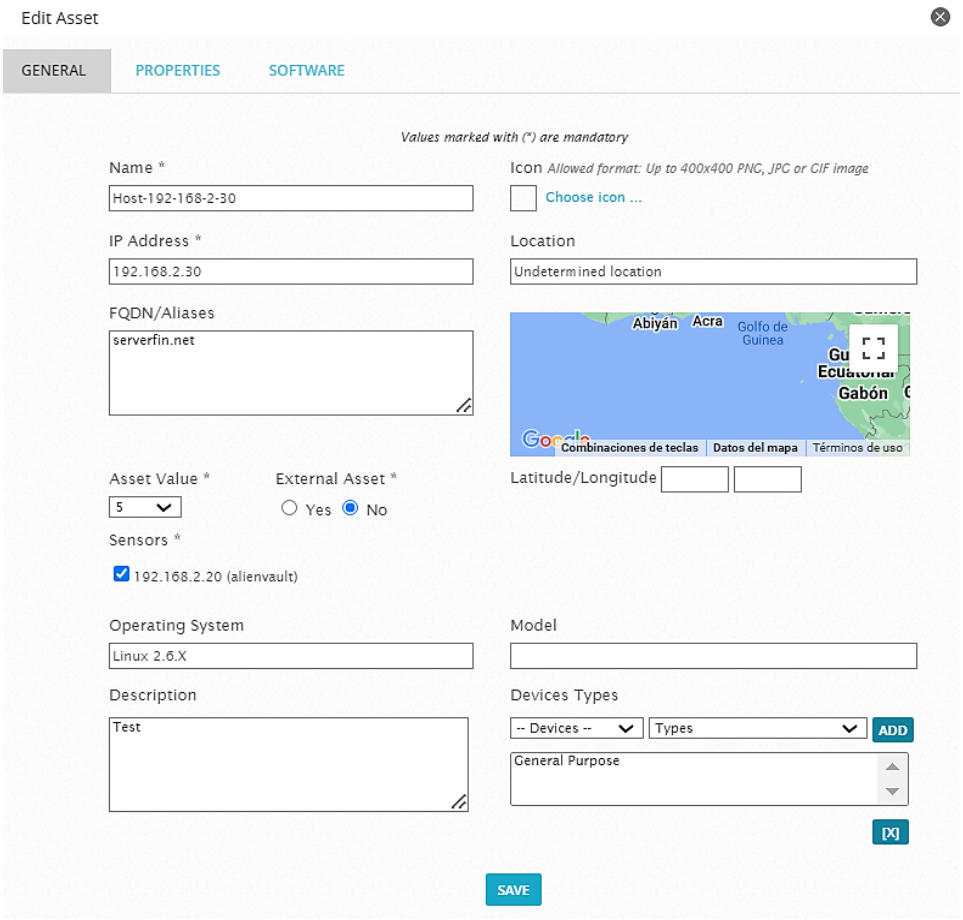


Figura 87: Interfaz web OSSIM AlienVault – Edición del activo

Fuente: El Autor

Dentro de la información obtenida del activo, en el ambiente de prueba, se puede seleccionar la opción 'Services' para identificar los servicios que están activos. Los servicios encontrados pueden también editarse y mostrar información como puertos, protocolos, nombres, estado y monitoreo.

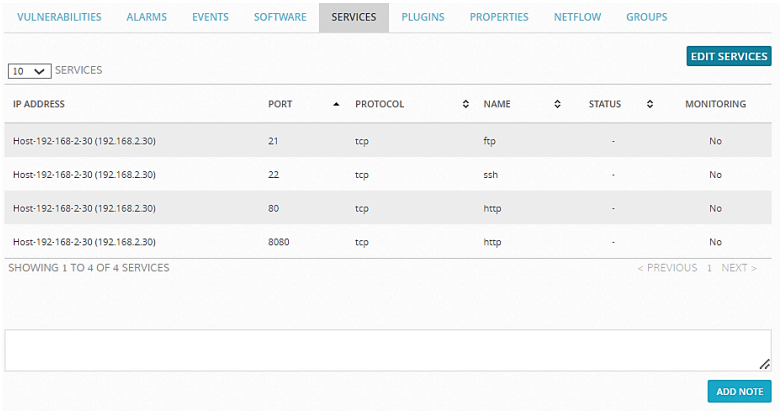


Figura 88: Interfaz web OSSIM AlienVault – Servicios de los activos

Fuente: El Autor

4.5 Gestión de disponibilidad

En el apartado 'Environment' de la interfaz web de OSSIM AlienVault, se debe ingresar a la sección 'Assets' y se selecciona un activo de la lista desplegada en el ícono de visualización; una vez dentro de la información mostrada, se debe ingresar a la opción 'Actions' para escoger la habilitación del monitoreo de disponibilidad en 'Enable Availability Monitoring', con una confirmación de que el monitoreo para el activo seleccionado ha sido habilitado.

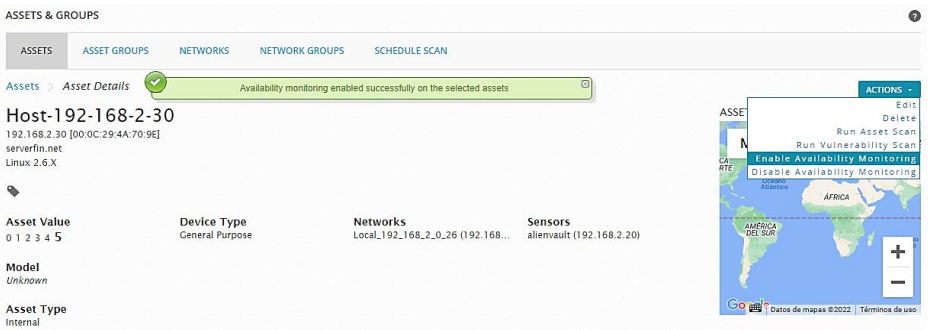


Figura 89: Interfaz web OSSIM AlienVault – Gestión de monitoreo de disponibilidad

Fuente: El Autor

A continuación, dentro de los detalles e información del activo, se habilita el monitoreo de los servicios en la opción ‘Services’ en la sección de ‘Description’ del activo que fue seleccionado.

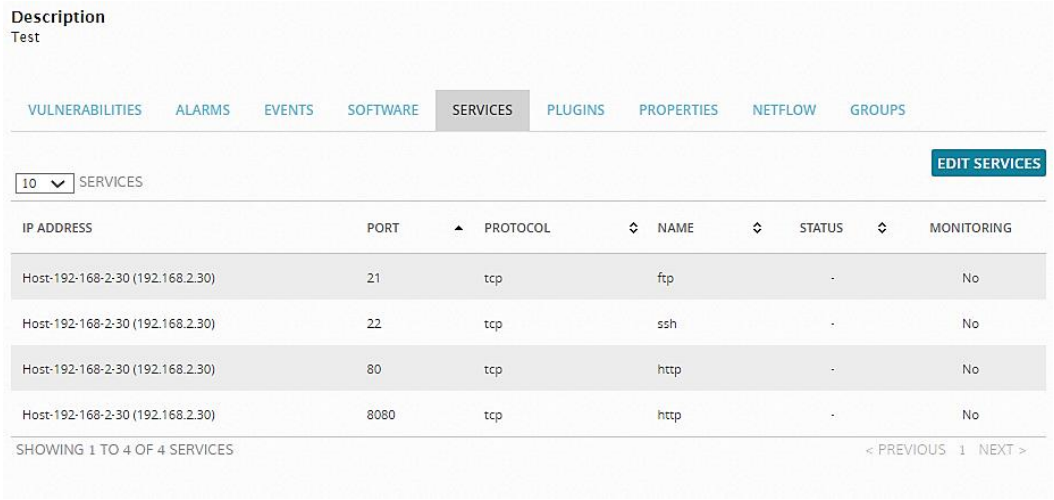


Figura 90: Interfaz web OSSIM AlienVault – Servicios del activo

Fuente: El Autor

En el listado que se haya desplegado se ingresa a la opción ‘Edit services’, para realizar la edición de monitoreo de los servicios correspondientes que están contenidos en el servidor. Dependiendo de la criticidad, se podrán monitorear algunos servicios o todos a la vez, seleccionando la opción ‘yes’ de la sección ‘Monitoring’ en cada uno respectivamente.

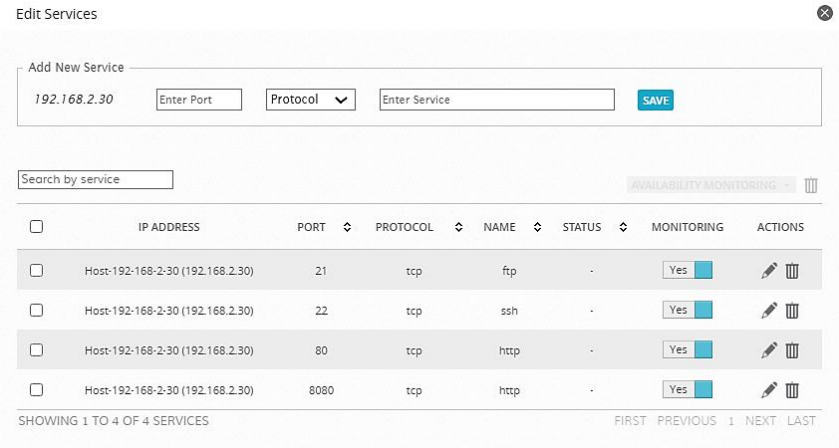


Figura 91: Interfaz web OSSIM AlienVault – Habilitación de servicios del activo

Fuente: El Autor

Al habilitarse el monitoreo de cada uno de los servicios contenidos, se actualizará la información estadística concerniente al activo.

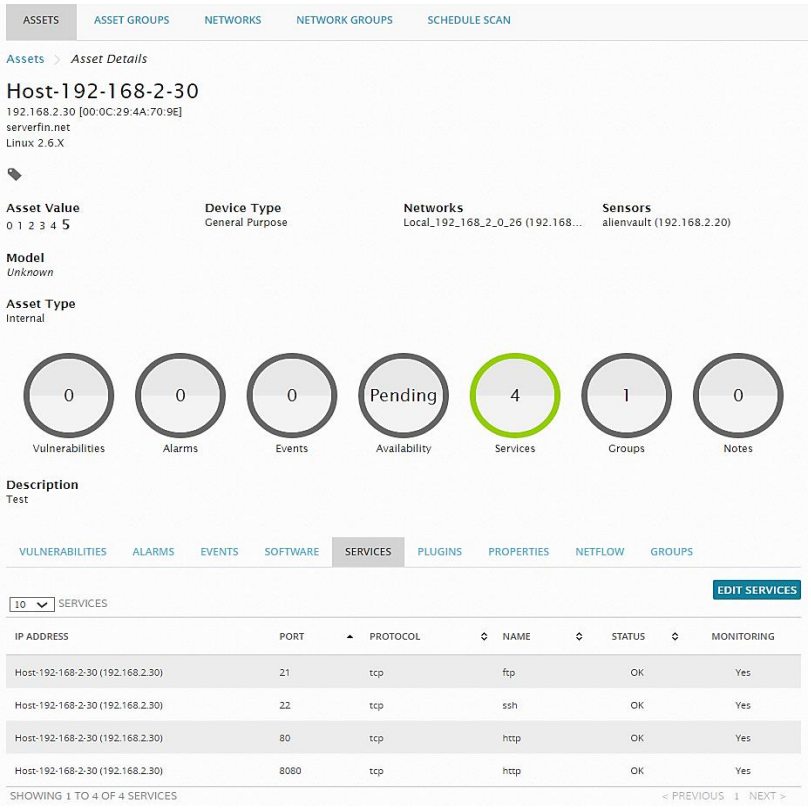


Figura 92: Interfaz web OSSIM AlienVault – Actualización de información del activo

Fuente: El Autor

Luego, en el apartado ‘Environment’, en la opción ‘Availability’, se puede tener acceso a la visualización global de estadísticas de la monitorización en tiempo real de los servicios previamente configurados.

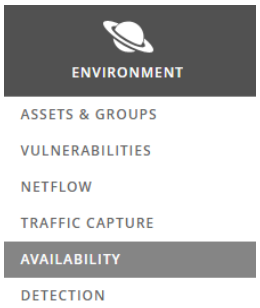


Figura 93: Interfaz web OSSIM AlienVault – Opción de acceso a disponibilidad

Fuente: El Autor

Una vez se haya ingresado a la opción ‘Availability’, se tendrá el despliegue de la información estadística de todos los servicios de los activos que se encuentren monitorizados.

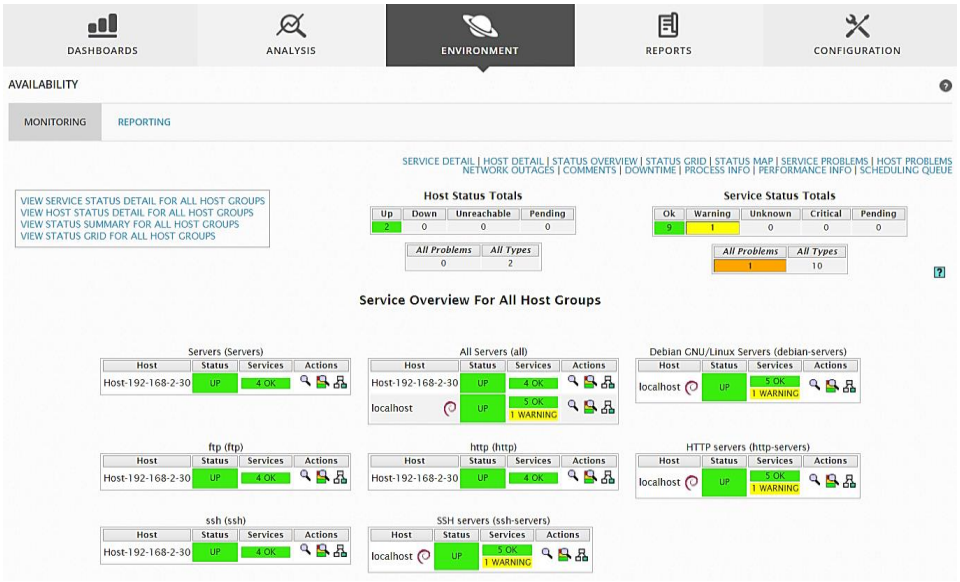


Figura 94: Interfaz web OSSIM AlienVault – Monitoreo de disponibilidad de activos

Fuente: El Autor

La información obtenida contendrá el host, con su estado activo o inactivo y sus servicios que pueden estar pendientes o activos, y continuará actualizándose mientras se realiza la exploración. Para efectuar la revisión de los mensajes de alerta se puede seleccionar el mensaje de advertencia, considerando que el color verde indica que el servicio de un determinado activo se encuentra habilitado y disponible, y según el grado de criticidad e inconveniente encontrado, el color podrá ser gris, rojo, naranja o amarillo con información referente al estado.

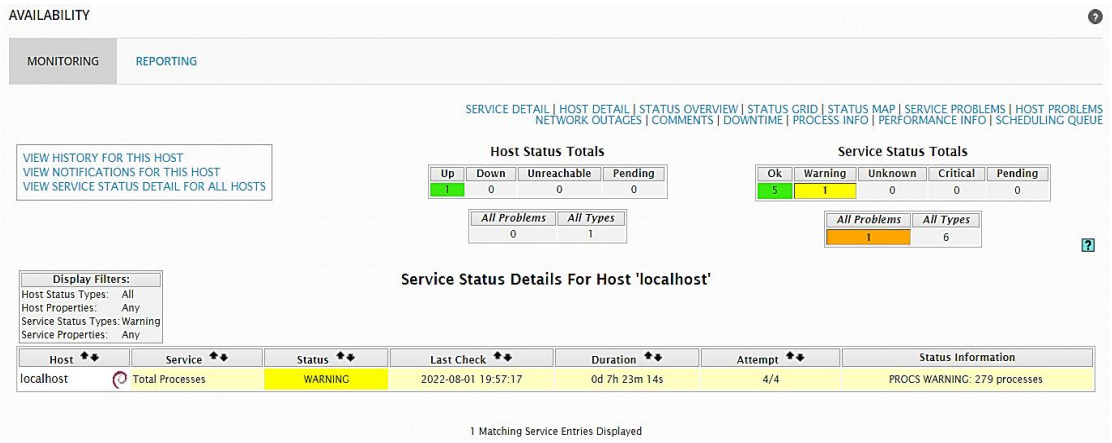


Figura 95: Interfaz web OSSIM AlienVault – Estado del servicio de un activo

Fuente: El Autor

Si se agregan más activos, los mismos serán reflejados en el listado de la opción ‘Availability’ con estados que indicarán su criticidad.

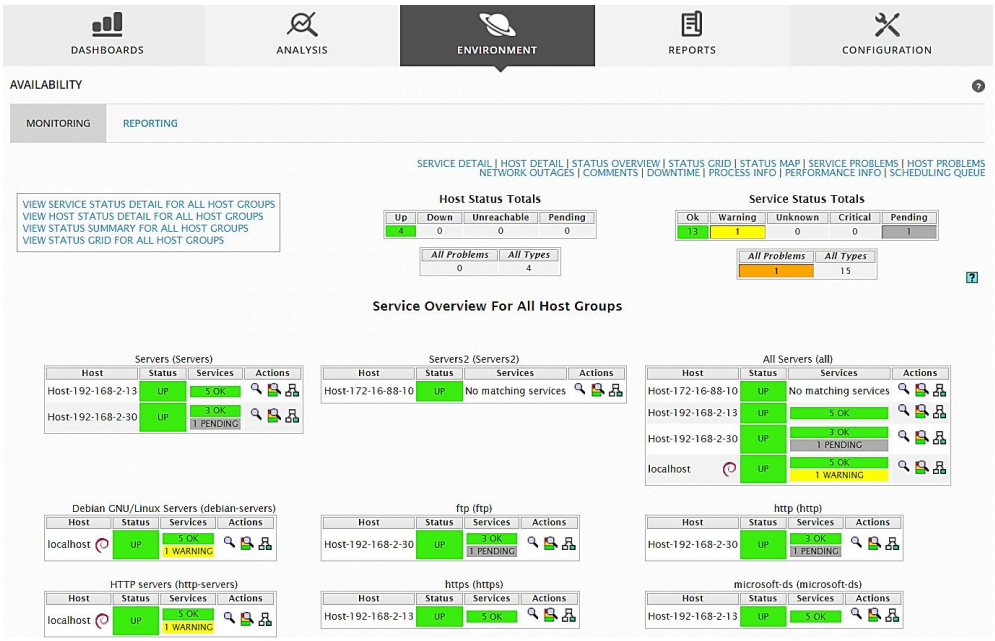


Figura 96: Interfaz web OSSIM AlienVault – Monitoreo del estado de activos

Fuente: El Autor

Para obtener información detallada de los activos monitorizados, se debe seleccionar la opción ‘Service detail’ dentro de la sección ‘Monitoring’ perteneciente al apartado ‘Availability’; el cual muestra un listado con la información del estado por cada uno de los servicios.

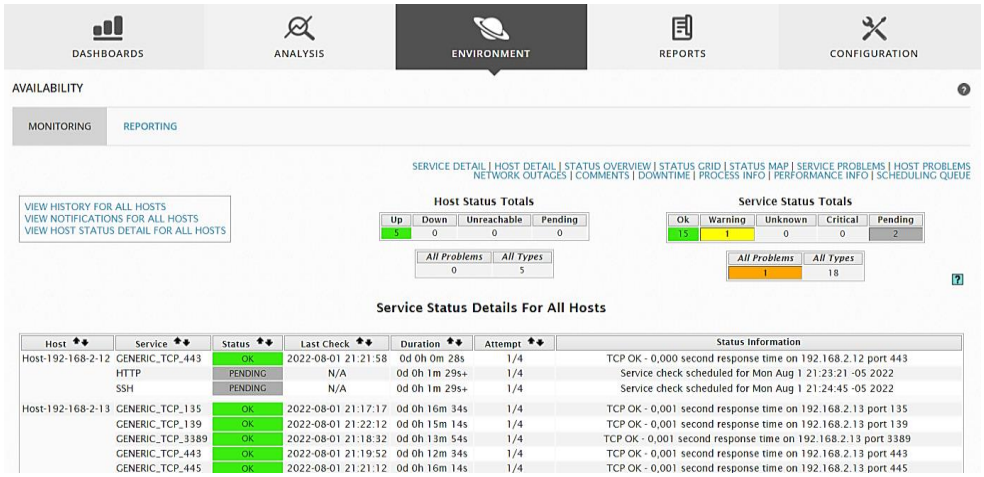


Figura 97: Interfaz web OSSIM AlienVault – Detalle de servicios

Fuente: El Autor

Para obtener información sobre los equipos (hosts), se deberá seleccionar la opción ‘Host detail’, donde se muestra los equipos que se encuentran activos con su respectiva información sobre su última revisión, su duración e información de su estado.

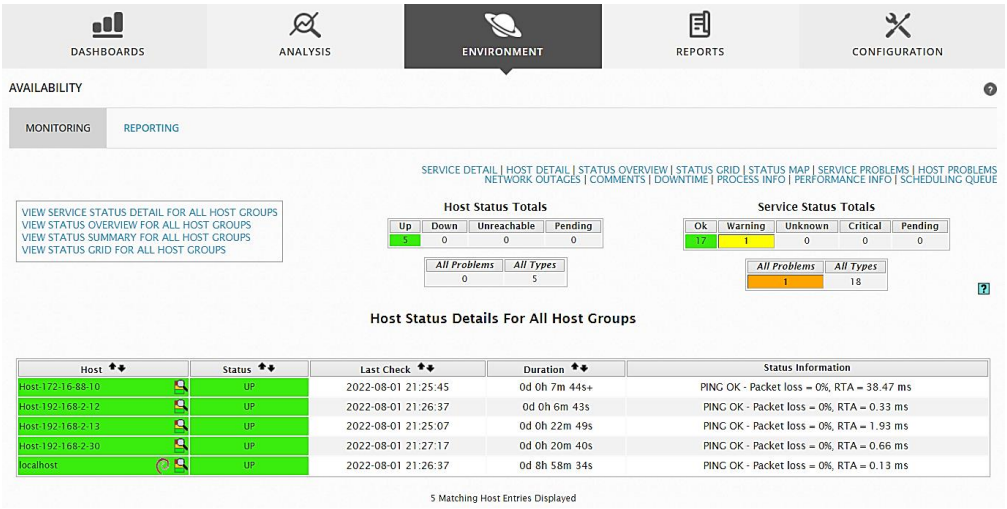


Figura 98: Interfaz web OSSIM AlienVault – Detalle del estado de los activos

Fuente: El Autor

También se puede revisar las opciones de: ‘Status overview’ (Descripción del estado), ‘Status grid’ (Malla de estado), ‘Status map’ (Mapa de estado), ‘Service problems’ (Problemas de servicio), ‘Host problems’ (Problemas de equipos), ‘Network outages’ (Interrupciones en la red), ‘Comments’ (Comentarios), ‘Downtime’ (Tiempo muerto), ‘Process info’ (Información de procesos), ‘Performance info’ (Información de funcionamiento), y ‘Scheduling queue’ (Lista de programación).

Si se presentará algún inconveniente en un determinado servidor (host), se puede visualizar en la opción de ‘Monitoring’, un mensaje que establece un valor cualitativo de ‘Down’ (Inactivo o caído) mostrándose de color rojo.

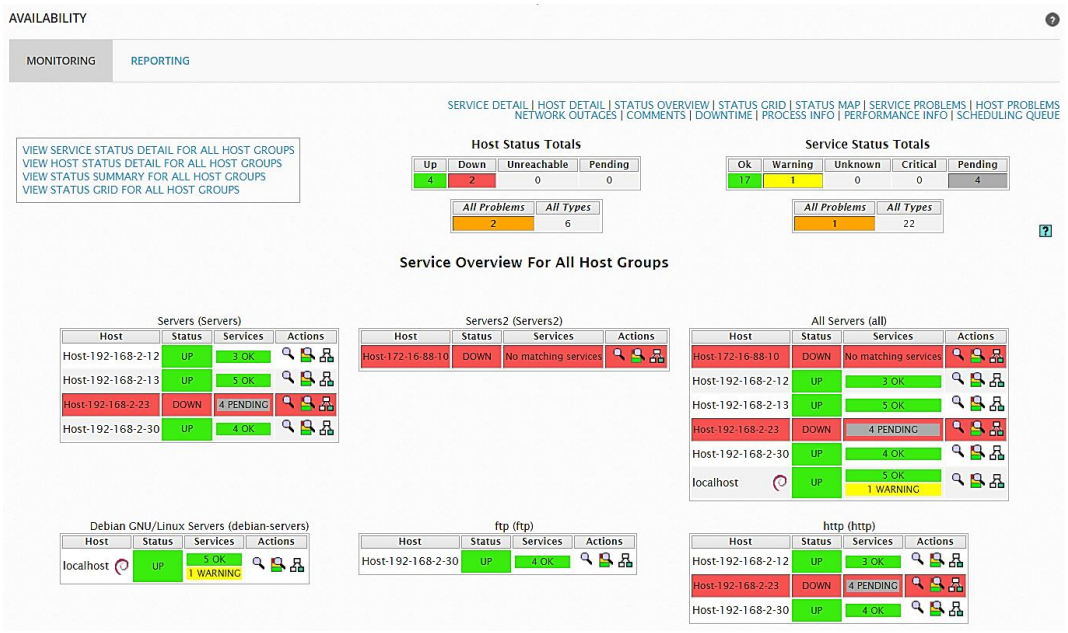


Figura 99: Interfaz web OSSIM AlienVault – Monitoreo y revisión de disponibilidad

Fuente: El Autor

Dentro de la opción ‘Host detail’ (Detalle del equipo) se puede validar los valores resultantes del monitoreo.

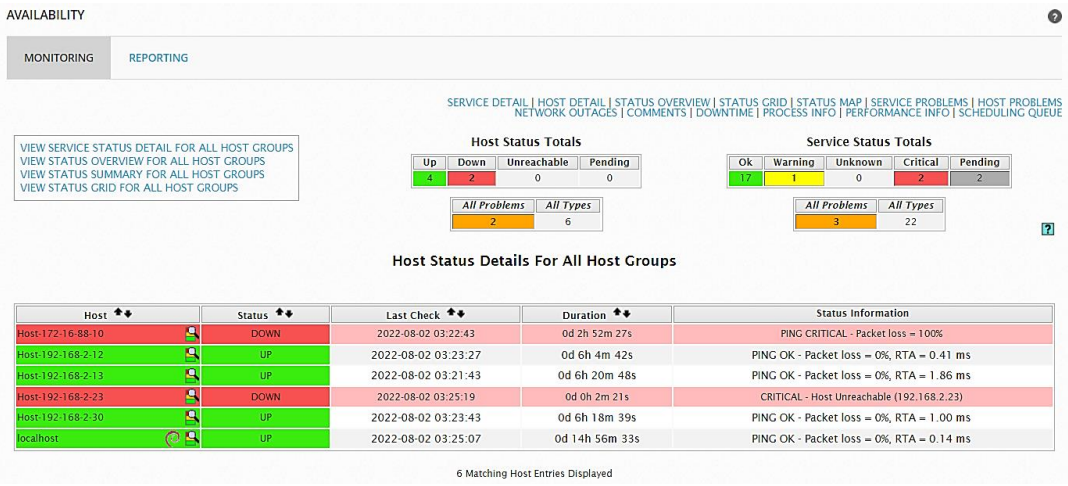


Figura 100: Interfaz web OSSIM AlienVault – Detalle del estado del activo detenido

Fuente: El Autor

Sin embargo, si se realiza la verificación del servidor o dispositivo que presenta el problema, se deberá efectuar acciones correctivas para mitigar el evento o inconveniente presentado, dando como resultado la continuidad de la operatividad del servidor. Lo que hace que el servidor monitoreado cambie su valor cualitativo de 'Down' (Inactivo) a 'Up' (activo) reflejándose en el cuadro de descripción general del servicio.

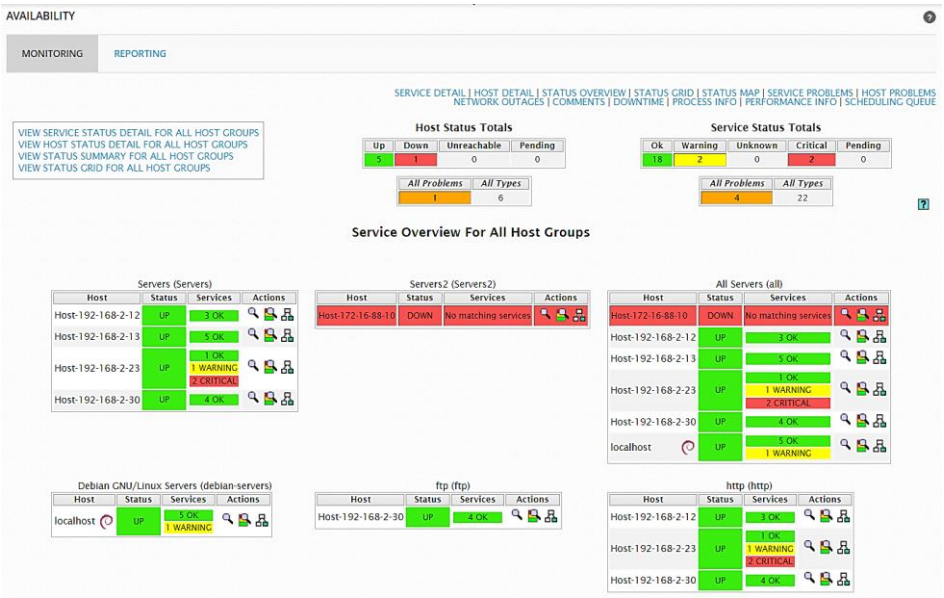


Figura 101: Interfaz web OSSIM AlienVault – Comprobación de disponibilidad

Fuente: El Autor

Dentro de la opción 'Availability' (Disponibilidad), hay otra funcionalidad que permite la generación de reportes a nivel de servicio, dispositivo, equipo, grupo de servicios, o grupo de dispositivos, ingresando a la opción 'Reporting' (informes), lo que permite obtener un el porcentaje de disponibilidad de acuerdo a un determinado tiempo y dependiendo de los reportes o informes que sean requeridos; en donde el paso inicial será acceder a 'Trends' (Tendencias) para elegir el tipo de informe sea por equipo (host) o servicio (service) para la determinación de su disponibilidad.

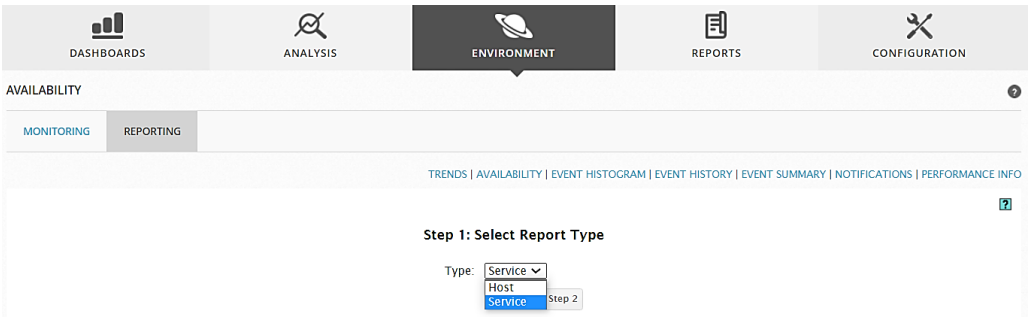


Figura 102: Interfaz web OSSIM AlienVault – Selección del tipo de reporte

Fuente: El Autor

El siguiente paso es la selección del equipo o servicio del que se requiera generar el reporte correspondiente.

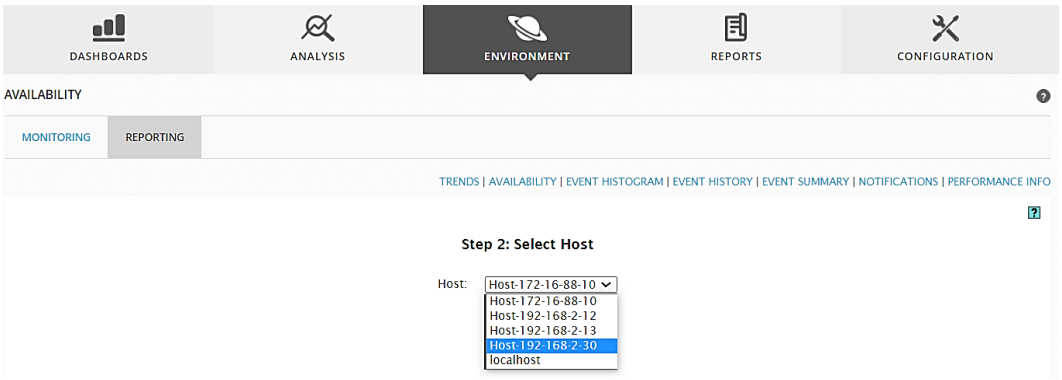


Figura 103: Interfaz web OSSIM AlienVault – Selección del host del reporte

Fuente: El Autor

En el tercer paso es especificar el periodo que tendrá el reporte o si será personalizado, y se procede a crear el reporte con la opción ‘Create Report’. Otras opciones dentro de la opción ‘Reporting’ (Informes) para reportes serán: ‘Availability’ (Disponibilidad), ‘Event histogram’ (Histograma de eventos), ‘Event history’ (Historia de eventos), ‘Event summary’ (Resumen de eventos), ‘Notifications’ (Notificaciones) y ‘Performance info’ (Informe de funcionamiento).

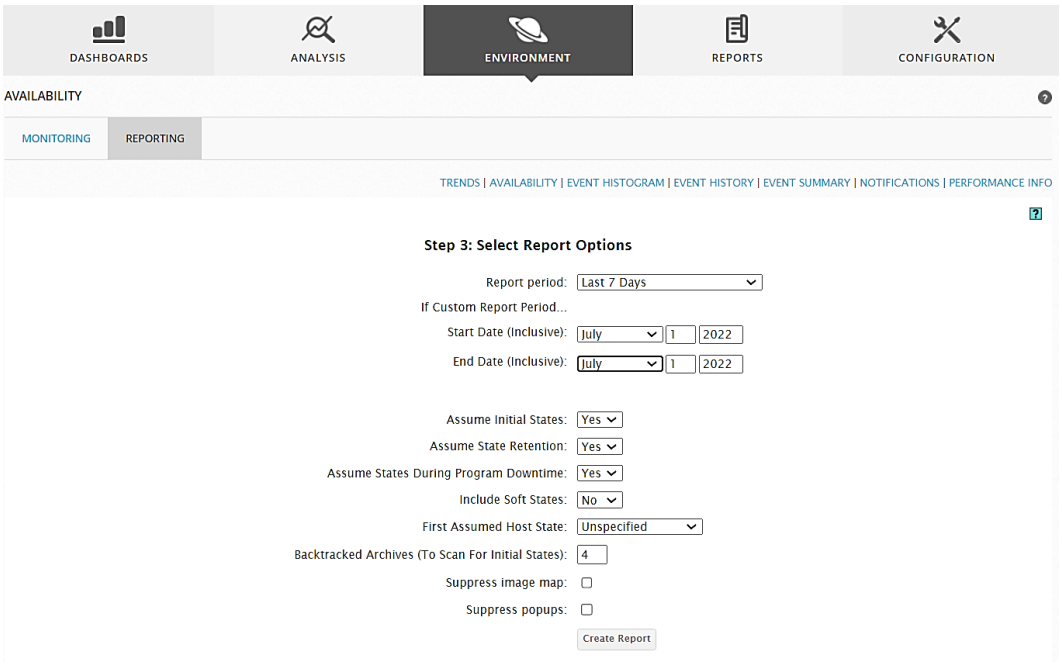


Figura 104: Interfaz web OSSIM AlienVault – Selección de opciones de reporte

Fuente: El Autor

Cuando se crea el respectivo informe de acuerdo a lo especificado en los pasos anteriores, se puede visualizar los porcentajes que dependerán del tiempo y de la captura de información, lo cual mostrará el estado inicial de los servicios dentro del servidor seleccionado. Como la información preliminar que se ha obtenido comprende un lapso de tiempo corto, el gráfico no mostrará mayores cambios, considerando los indicadores 'Up' (Activo), 'Down' (Inactivo), 'Unreachable' (Inalcanzable), 'Indeterminate' (Indeterminado), ya que aún se estarán recopilando datos e información relevante para la generación del informe. Los informes permitirán contribuir a todos los indicadores de disponibilidad con los que cuenta la organización o entidad.

Si es requerido, se puede añadir nuevos equipos para efectuar la monitorización con sus respectivos informes.

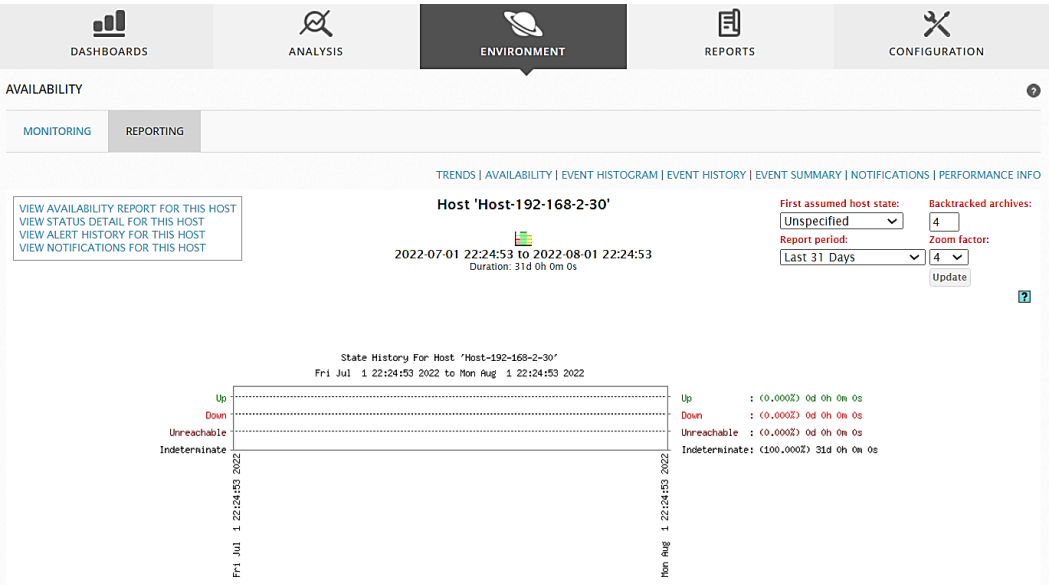


Figura 105: Interfaz web OSSIM AlienVault – Informes de disponibilidad

Fuente: El Autor

4.6 Gestión de notificaciones

La gestión de notificaciones permitirá el envío de notificaciones mediante correo electrónico, para lo cual se debe ingresar a la consola del servidor OSSIM AlienVault ya sea generando una Shell (consola de administración) o por una conexión de 'ssh'.

Dentro del intérprete de comandos del sistema del servidor, se edita el archivo 'contacts_nagios2.cfg' mediante un editor 'nano'. Los comandos que se ejecutan son:

- cd /etc/nagios3/ (permite el ingreso al directorio 'nagios3')
- ls (permite listar el contenido del directorio)
- cd conf.d/ (permite el ingreso al directorio 'conf.d')
- ls (permite listar el contenido del directorio)
- nano contacts_nagios2.cfg (permite la edición del archivo)

```
alienvault:~# cd /etc/nagios3/
alienvault:/etc/nagios3# ls
apache2.conf  cgi.cfg  commands.cfg  conf.d  nagios.cfg  resource.cfg  stylesheets
alienvault:/etc/nagios3# cd conf.d/
alienvault:/etc/nagios3/conf.d# ls
contacts_nagios2.cfg  generic-host_nagios2.cfg     hostgroups_nagios2.cfg  ossim-configs         timeperiods_nagios2.cfg
extinfo_nagios2.cfg   generic-service_nagios2.cfg  localhost_nagios2.cfg   services_nagios2.cfg
alienvault:/etc/nagios3/conf.d# nano contacts_nagios2.cfg
```

Figura 106: Consola OSSIM AlienVault – Configuración inicial

Fuente: El Autor

Al ingresar al archivo de configuración ‘contacts_nagios2.cfg, se muestra el contenido para efectuar las configuraciones requeridas, donde se modificarán los campos ‘contact_name’ (nombre), ‘alias’ (alias), ‘email’ (correo electrónico) y ‘members’ (usuario miembro) respectivamente.

```
  GNU nano 2.7.4                                File: contacts_nagios2.cfg

##############################################################################
# contacts.cfg
##############################################################################



##############################################################################
##############################################################################
#
# CONTACTS
#
##############################################################################
##############################################################################

# In this simple config file, a single contact will receive all alerts.

define contact{
        contact_name                    root
        alias                           Root
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,r
        service_notification_commands   notify-service-by-email
        host_notification_commands      notify-host-by-email
        email                           root@localhost
        }



##############################################################################
##############################################################################
#
# CONTACT GROUPS
#
##############################################################################
##############################################################################

# We only have one contact in this simple configuration file, so there is
# no need to create more than one contact group.

define contactgroup{
        contactgroup_name       admins
        alias                   Nagios Administrators
        members                 root
        }
```

Figura 107: Consola OSSIM AlienVault – Configuración del archivo ‘contacts.cfg’

Fuente: El Autor

Se guardan los cambios realizados y se reinicia el servicio de ‘nagios3’ ejecutando el comando: ‘service nagios3 restart’ para que sean aplicadas las nuevas configuraciones. Y de haber algún inconveniente o problema suscitado mediante pruebas de disponibilidad, se recibirá la notificación respectiva al correo electrónico (email).

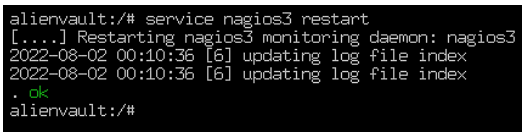


Figura 108: Consola OSSIM AlienVault – Reinicio del servicio ‘nagios3’

Fuente: El Autor

A continuación, se configura el servidor Postfix para que se pueda realizar el envío de correos electrónicos sin depender de otro servidor, para lo cual, se ingresa el comando: ‘dpkg-reconfigure postfix’ para abrir un asistente de configuración. Se elige la opción ‘Internet Site’ para el tipo general de configuración de correo y se acepta para continuar.

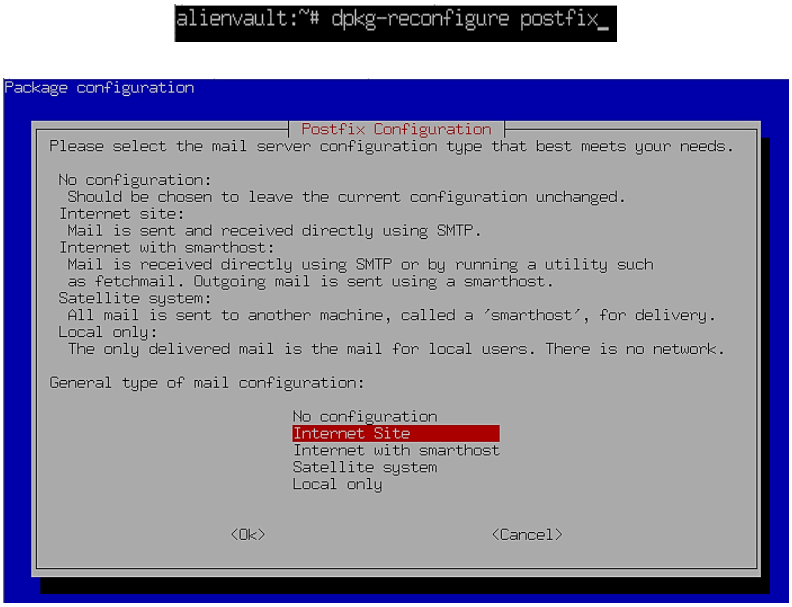


Figura 109: Consola OSSIM AlienVault – Configuración de Postfix

Fuente: El Autor

Luego, aparecerá el nombre por defecto del servidor, que puede ser modificado o cambiado según lo requerido.

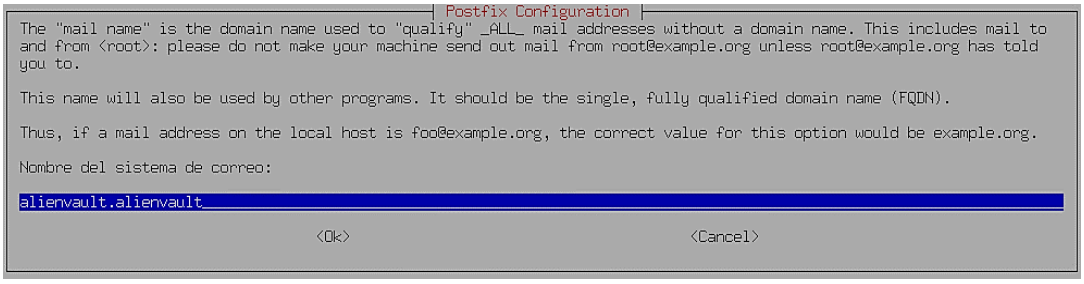


Figura 110: Consola OSSIM AlienVault – Asignación de nombre del sistema de correo

Fuente: El Autor

Se solicitará el ingreso de un destinatario para la administración de correo raíz, el cual puede ser 'root' para super administrador.

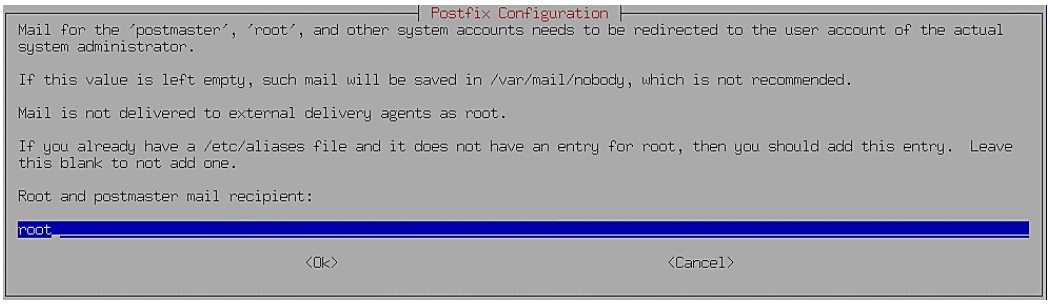


Figura 111: Consola OSSIM AlienVault – Destinatario de correo

Fuente: El Autor

También se tiene por defecto otros destinatarios, aunque lo necesario es el envío de correos electrónicos.

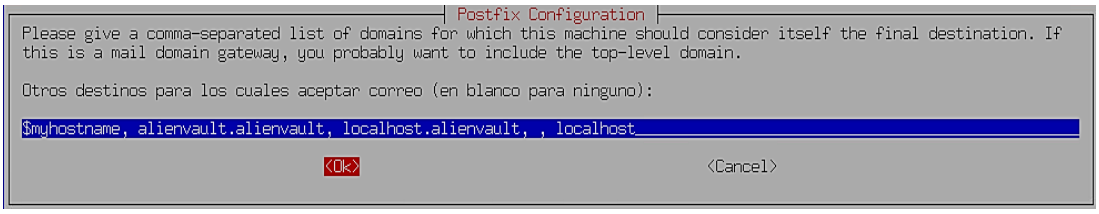


Figura 112: Consola OSSIM AlienVault – Otros destinatarios

Fuente: El Autor

Se acepta las actualizaciones sincrónicas en la cola de correo.

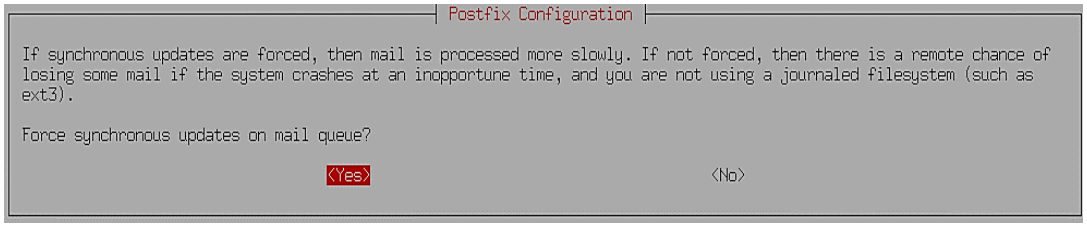


Figura 113: Consola OSSIM AlienVault – Actualizaciones sincrónicas

Fuente: El Autor

Se aceptan las redes locales sugeridas por defecto, especificándose los bloques de red para los que el host va a retransmitir los correos.

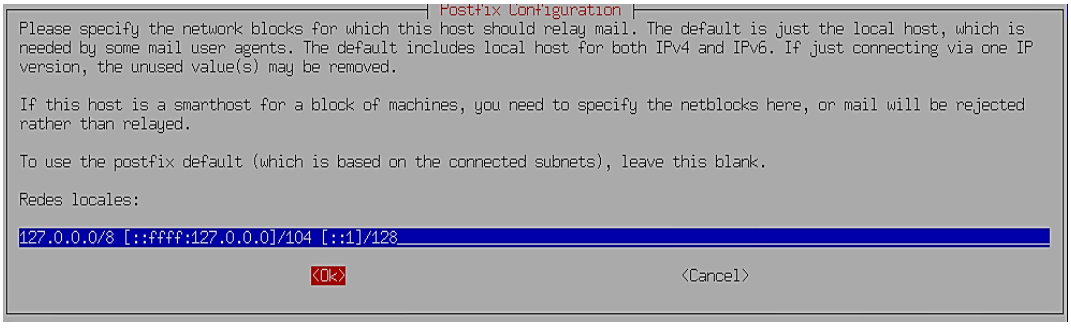


Figura 114: Consola OSSIM AlienVault – Redes locales

Fuente: El Autor

Se debe dejar el límite de tamaño del buzón con el valor por defecto.

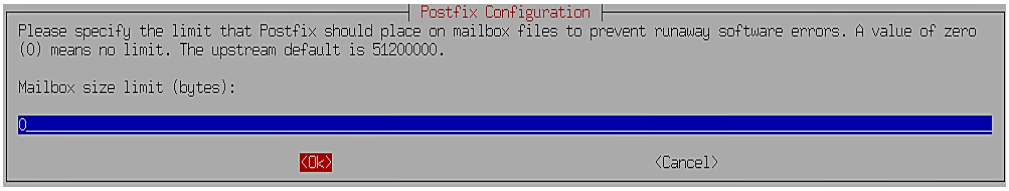


Figura 115: Consola OSSIM AlienVault – Límite de tamaño de buzón

Fuente: El Autor

Para los caracteres de extensión de dirección local, se dejarán tal como se muestra por defecto.

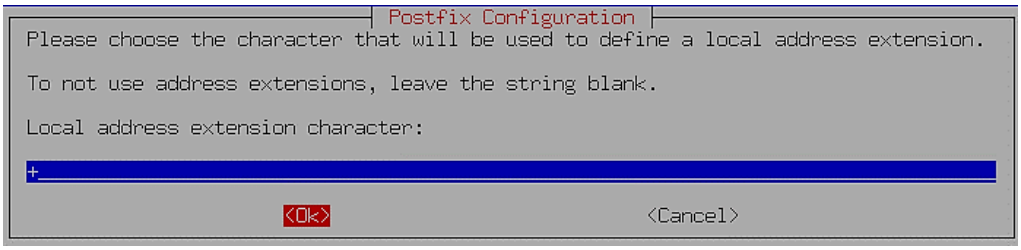


Figura 116: Consola OSSIM AlienVault – Caracteres de extensión de dirección local

Fuente: El Autor

Se selecciona el protocolo de Internet que se utilizará y que esté habilitado por el sistema al momento de la instalación, que por defecto es ‘ipv4’.

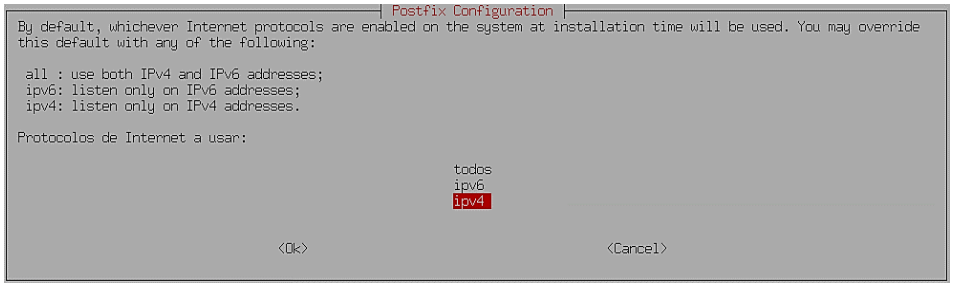


Figura 117: Consola OSSIM AlienVault – Configuración de protocolo de internet

Fuente: El Autor

Al término del proceso de configuración previa de Postfix, se puede hacer una comprobación enviando un correo de prueba. El comando que permite abrir el esquema de envío es ‘mail’ seguido del correo electrónico al que se desea enviar las notificaciones, se añade el asunto, el cuerpo del mensaje, y si se requiere una copia hacia otro correo se ingresa ‘Control + d’ e ‘Intro’ para el envío correspondiente.

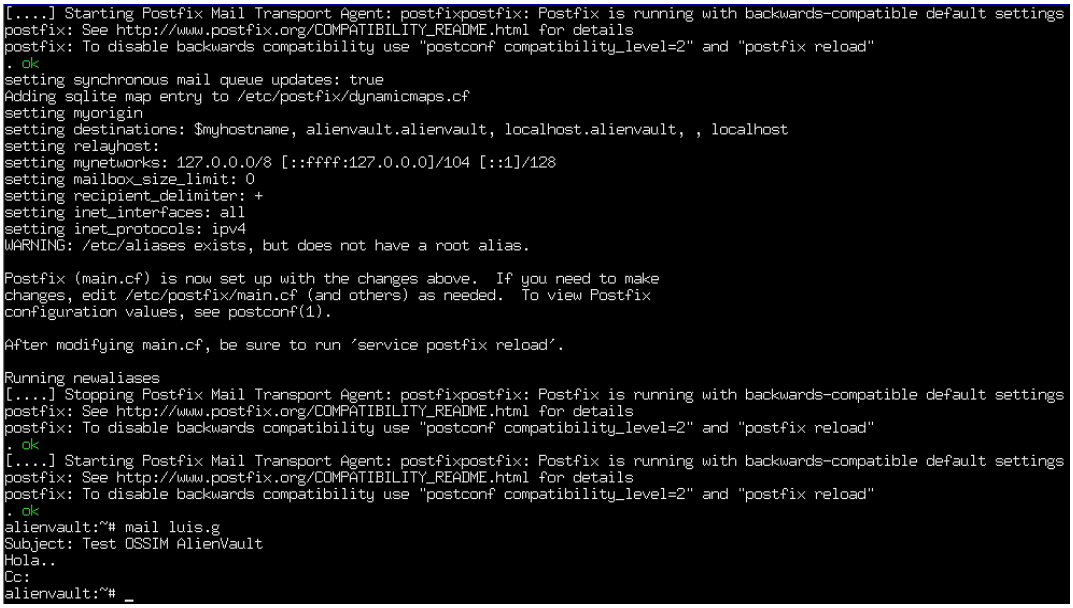


Figura 118: Consola OSSIM AlienVault – Envío del correo electrónico de prueba

Fuente: El Autor

Se puede corroborar la recepción del envío del correo electrónico de prueba en el buzón respectivo y validar el mensaje recibido desde la consola intérprete de comandos del servidor OSSIM AlienVault.

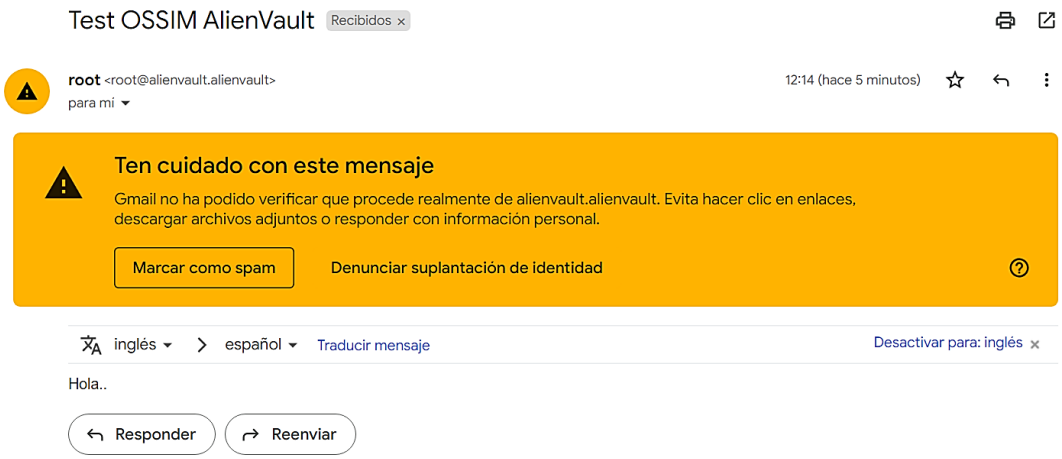


Figura 119: Consola OSSIM AlienVault – Recepción del correo electrónico de prueba

Fuente: El Autor

Si se suscita un evento, el sistema de OSSIM AlienVault enviará una notificación al correo electrónico correspondiente con la información pertinente del caso.

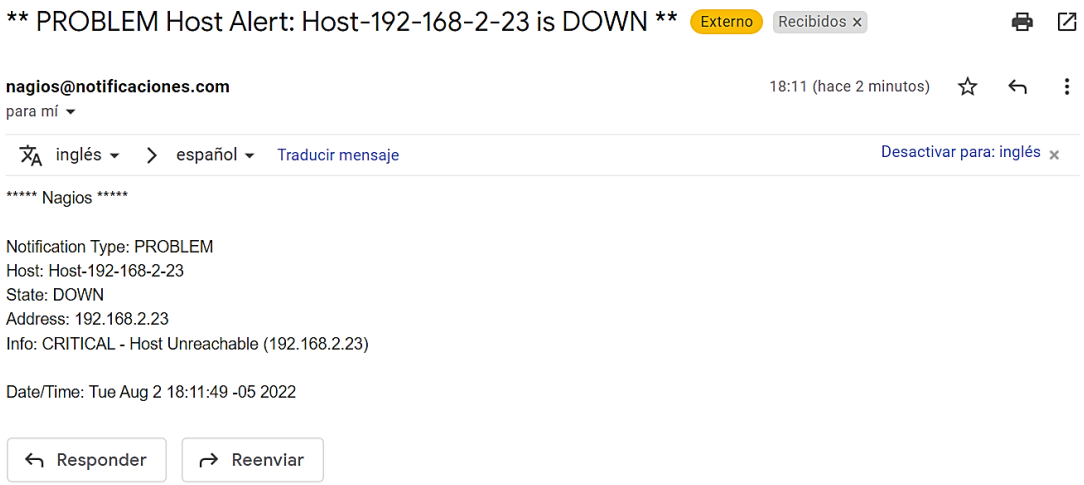


Figura 120: Consola OSSIM AlienVault – Recepción de notificación de evento

Fuente: El Autor

La información puede ser verificada ingresando al terminal de comandos para ejecutar:

- cd /etc/nagios3/ (permite ingresar al directorio)

- ls (permite listar en pantalla el contenido del directorio)
- nano commands.cfg (permite editar el archivo)

```
alienvault:/# cd /etc/nagios3/
alienvault:/etc/nagios3# ls
apache2.conf  cgi.cfg  commands.cfg  conf.d  nagios.cfg  resource.cfg  stylesheets
alienvault:/etc/nagios3# nano commands.cfg
```

Figura 121: Consola OSSIM AlienVault – Configuración de archivo 'commands.cfg'

Fuente: El Autor

El archivo 'commands.cfg' se mostrará y se podrá editar de acuerdo a lo requerido.

```
  GNU nano 2.7.4                                File: commands.cfg

##############################################################################
# COMMANDS.CFG - SAMPLE COMMAND DEFINITIONS FOR NAGIOS
##############################################################################


##############################################################################
# NOTIFICATION COMMANDS
##############################################################################


# 'notify-host-by-email' command definition
define command{
        command_name    notify-host-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nSt$
        }

# 'notify-service-by-email' command definition
define command{
        command_name    notify-service-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService: $SERVICED$
        }




##############################################################################
# HOST CHECK COMMANDS
##############################################################################

# On Debian, check-host-alive is being defined from within the
# nagios-plugins-basic package

##############################################################################
# PERFORMANCE DATA COMMANDS
##############################################################################


# 'process-host-perfdata' command definition
define command{
        command_name    process-host-perfdata
        command_line    /usr/bin/printf "%b" "$LASTHOSTCHECK$\t$HOSTNAME$\t$HOSTSTATE$\t$HOSTATTEMPT$\t$HOSTSTATETYPE$\t$HOSTEX$
        }
```

Figura 122: Consola OSSIM AlienVault – Archivo 'commands.cfg'

Fuente: El Autor

Si se toma acción inmediata del evento suscitado en algún activo de la red de la organización, se puede ver reflejado en el monitoreo y verificación de disponibilidad de OSSIM AlienVault.

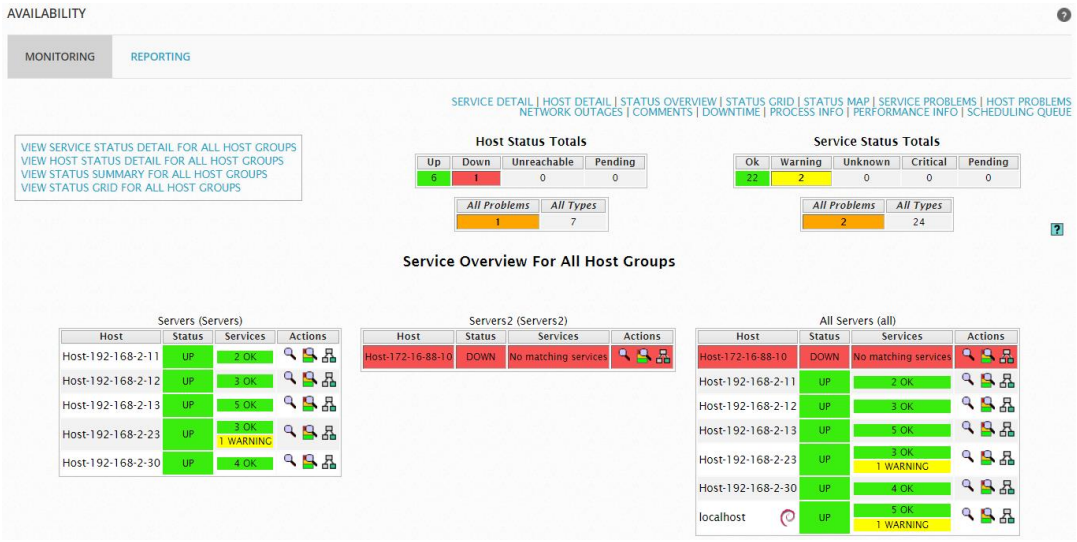


Figura 123: Consola OSSIM AlienVault – Acción correctiva de evento

Fuente: El Autor

De igual manera, se recibirá una notificación indicando que el evento suscitado fue mitigado.

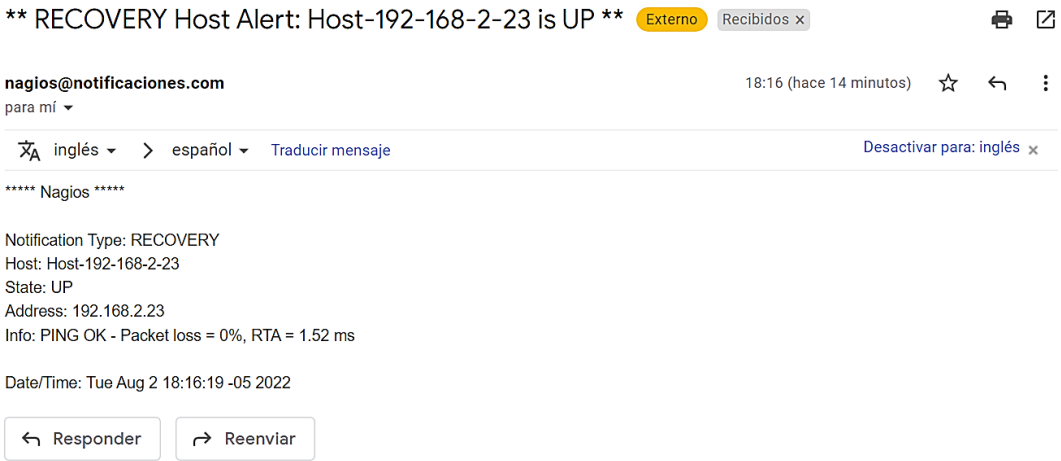


Figura 124: Consola OSSIM AlienVault – Notificación de evento mitigado

Fuente: El Autor

4.7 Gestión de vulnerabilidades

Para iniciar la gestión de vulnerabilidades se debe ingresar al apartado de 'Environment' en la opción de 'Vulnerabilities' dentro de la consola de administración de la interfaz web de OSSIM AlienVault.

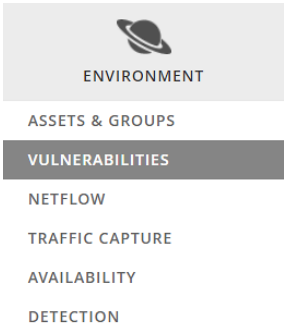


Figura 125: Interfaz web OSSIM AlienVault – Opción de acceso a vulnerabilidades

Fuente: El Autor

Dentro de la opción escogida, se tendrá acceso al tablero general de configuraciones para la administración y generación de reportes. Previamente, se verificará los activos con los que cuenta la red de la organización.

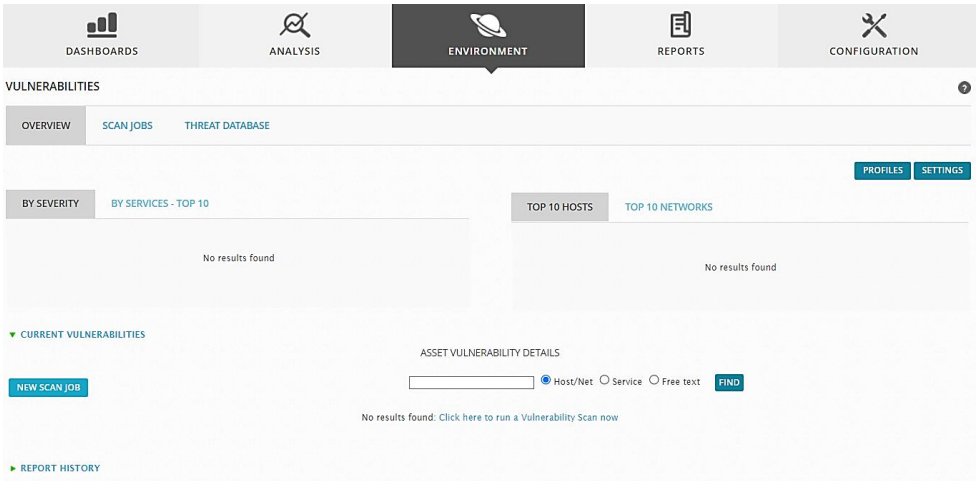


Figura 126: Interfaz web OSSIM AlienVault – Tablero general de vulnerabilidades

Fuente: El Autor

En el ‘Dashboard’ (tablero) desplegado, en la pestaña ‘Scan jobs’ (Trabajos de escaneo) se puede llevar a cabo la programación de escaneo de vulnerabilidades de acuerdo a los activos existentes y dependiendo de los requisitos disponibles al momento de efectuarse el proceso.

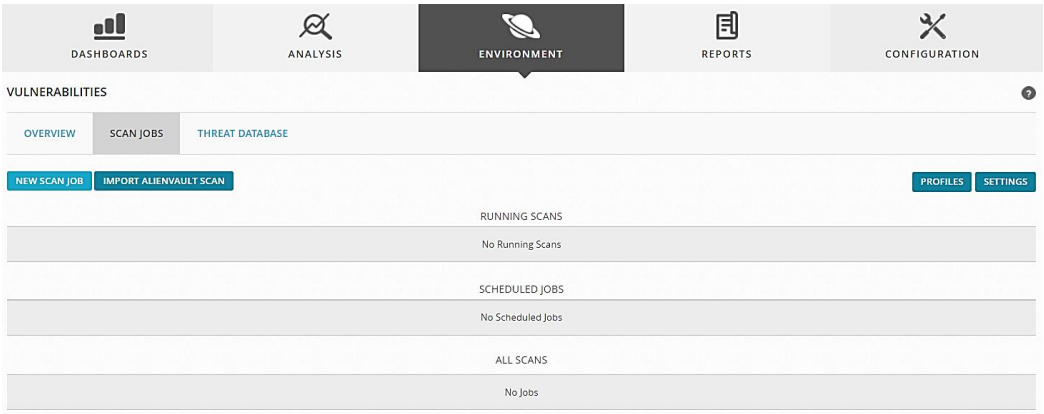


Figura 127: Interfaz web OSSIM AlienVault – Trabajos de escaneo

Fuente: El Autor

Para realizar un nuevo trabajo de escaneo se escoge la opción ‘New scan jobs’ dentro de la pestaña ‘Scan jobs’ para realizar las configuraciones correspondientes. Entre los parámetros que deberán ser ingresados son: ‘Job name’ (Nombre del trabajo), el Sensor (Sensor) que por defecto aparecerá que se configuró previamente, el ‘Profile’ (Perfil), el ‘Schedule method’ (Método de programación), el modo ‘Advanced’ (Avanzado) para especificar credenciales si se requiere, y los activos que se incluyan para el proceso de ‘scanning’ (escaneo).

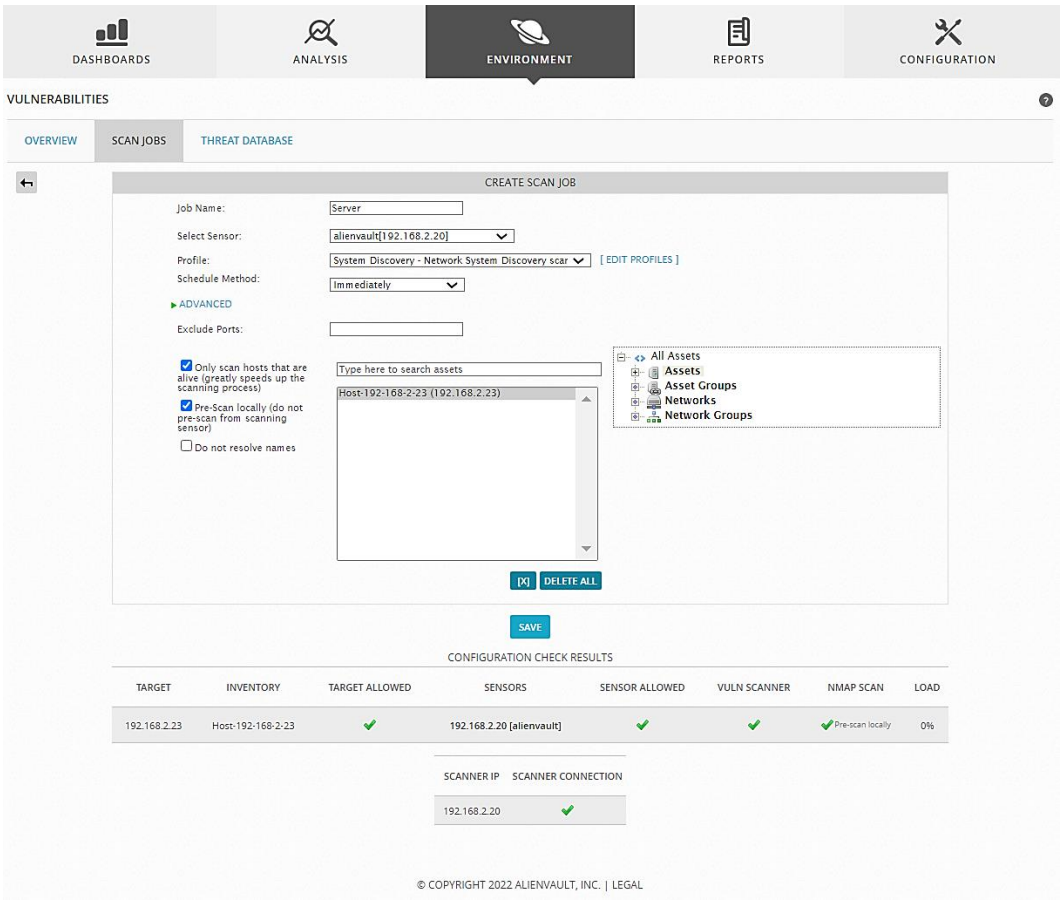


Figura 128: Interfaz web OSSIM AlienVault – Creación del trabajo de escaneo

Fuente: El Autor

Se guardan los cambios realizados con la opción ‘Save’ (Guardar) para que sea incluido el nuevo trabajo de escaneo, que se puede visualizar dentro de la pestaña ‘Scan jobs’. La ejecución del trabajo de escaneo será automática.

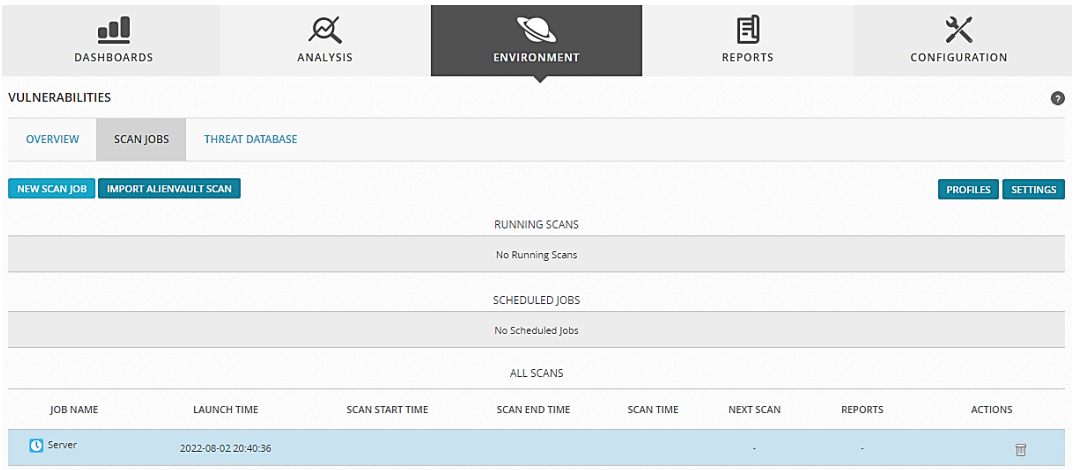


Figura 129: Interfaz web OSSIM AlienVault – Trabajo de escaneo programado

Fuente: El Autor

Al programarse el nuevo trabajo de escaneo, se tendrá a la espera el inicio del proceso, y se indica algunos parámetros de ejecución. Aunque al iniciar la ejecución del escaneo, aparecen opciones de verificación de reporte, eliminación de reporte, o exportación del reporte; además del tiempo de lanzamiento, tiempo de inicio del escaneo, tiempo de finalización del escaneo, duración del escaneo, y las acciones.

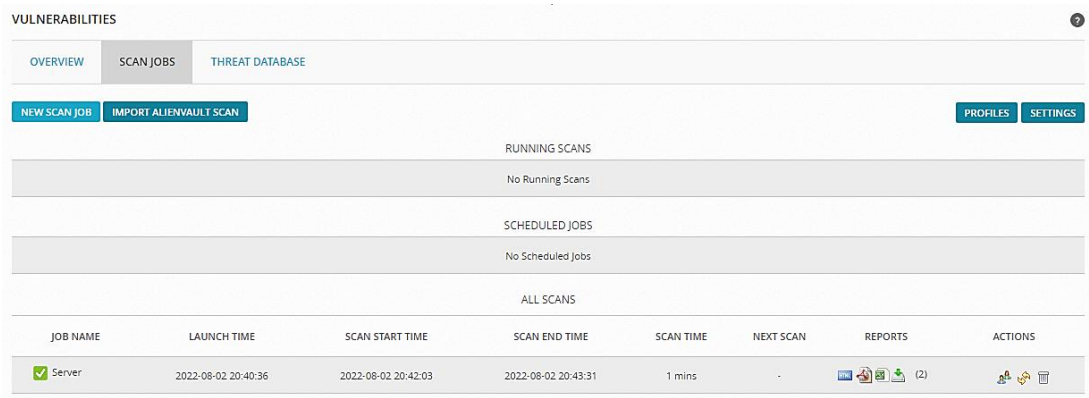


Figura 130: Interfaz web OSSIM AlienVault – Habilitación del trabajo de escaneo

Fuente: El Autor

El trabajo de escaneo programado mostrará un resumen de resultados preliminares referentes a la detección inicial de vulnerabilidades, incluyendo el reporte por puertos. En el reporte se puede evidenciar un diagrama de pastel con el estado general de vulnerabilidades, donde el tipo de vulnerabilidad es representado por categorías y colores.

- Vulnerabilidades críticas (Critical)
- Vulnerabilidades altas (High)
- Vulnerabilidades medias (Medium)
- Vulnerabilidades bajas (Low)
- Vulnerabilidades informativas (Info)

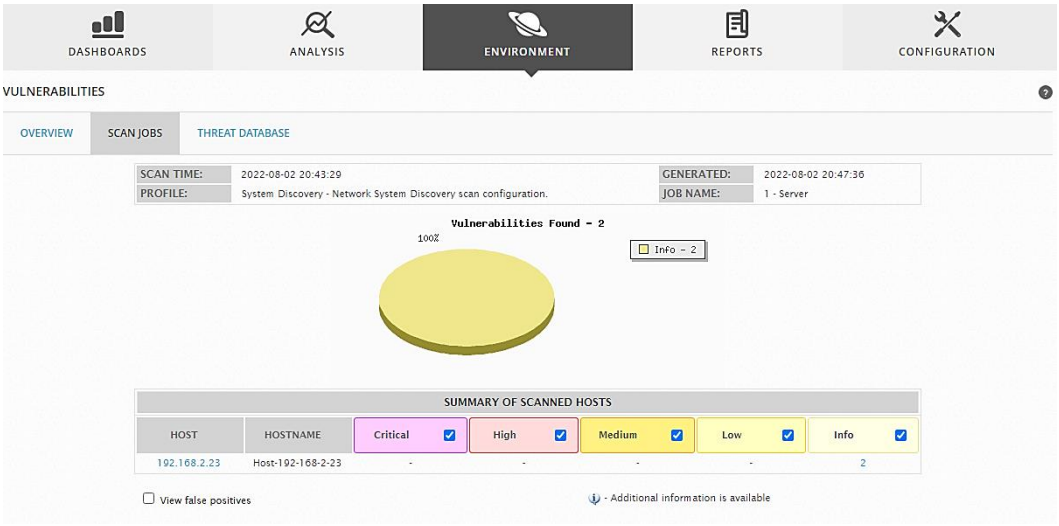


Figura 131: Interfaz web OSSIM AlienVault – Resultados preliminares de escaneo I

Fuente: El Autor

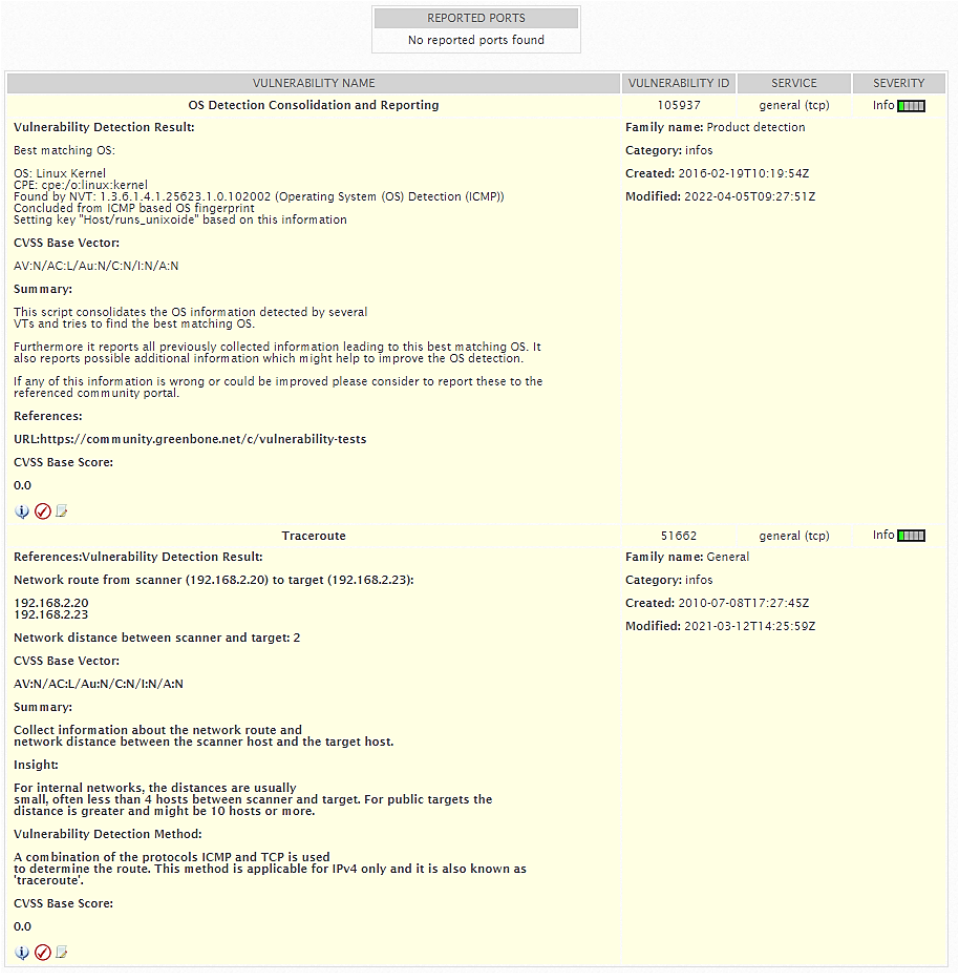


Figura 132: Interfaz web OSSIM AlienVault – Resultados preliminares de escaneo II

Fuente: El Autor

De acuerdo al proceso de 'scanning', el diagrama de tipo pastel muestra por el grado de severidad las vulnerabilidades encontradas de acuerdo al activo analizado (host).

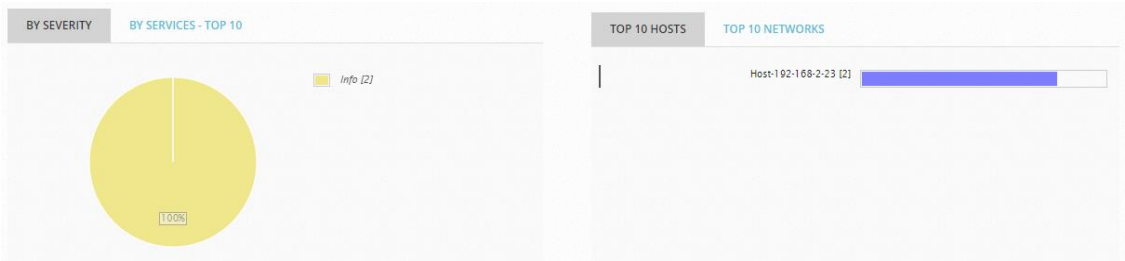


Figura 133: Interfaz web OSSIM AlienVault – Diagrama de severidad del activo

Fuente: El Autor

La categorización de colores conforme a lo analizado en el proceso de ‘scanning’ se establece de la siguiente manera:

- CRIT (Morado): vulnerabilidades críticas
- HIGH (Rojo): vulnerabilidades altas
- MEDI (Amarillo): vulnerabilidades medias
- LOW (Azul): vulnerabilidades bajas
- INFO (Verde): vulnerabilidades de información

Se tiene el resumen detallado de las vulnerabilidades encontradas de un determinado activo con las opciones de exportación de informes en los siguientes formatos: ‘.html’, ‘pdf’, y ‘.xlsx’ respectivamente.

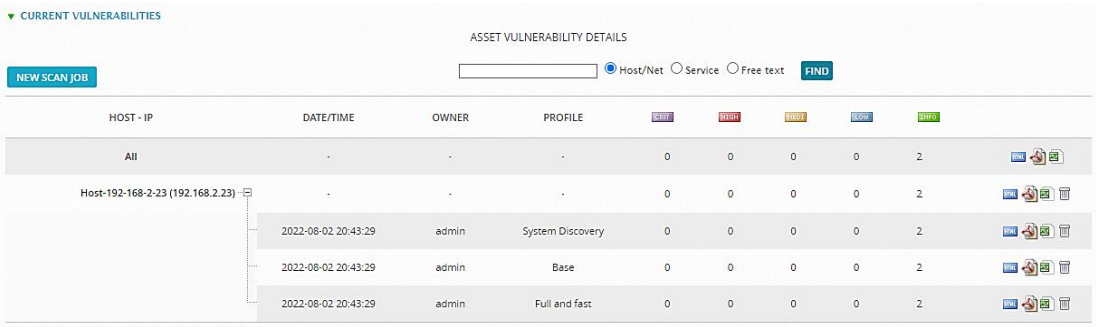


Figura 134: Interfaz web OSSIM AlienVault – Detalles de vulnerabilidad de activo

Fuente: El Autor

También se tendrá el resumen histórico de los procesos de escaneo de un determinado activo (host).

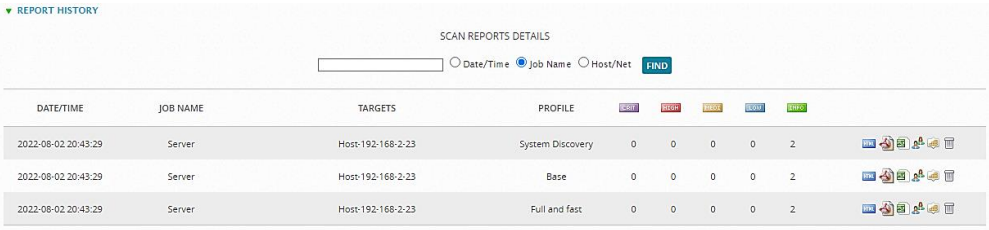


Figura 135: Interfaz web OSSIM AlienVault – Detalles de los informes de escaneo

Fuente: El Autor

Para programar un trabajo de escaneo y que se ejecute a un determinado tiempo, se ingresa a la pestaña ‘Scan Jobs’ de la sección ‘Vulnerabilities’ en la opción ‘New scan job’ donde se ingresarán los datos de programación del nuevo trabajo de ‘scanning’ para un determinado activo de la red, y se guardarán los cambios. La programación será para llevar a cabo un proceso de ‘scanning’ diario del activo requerido.

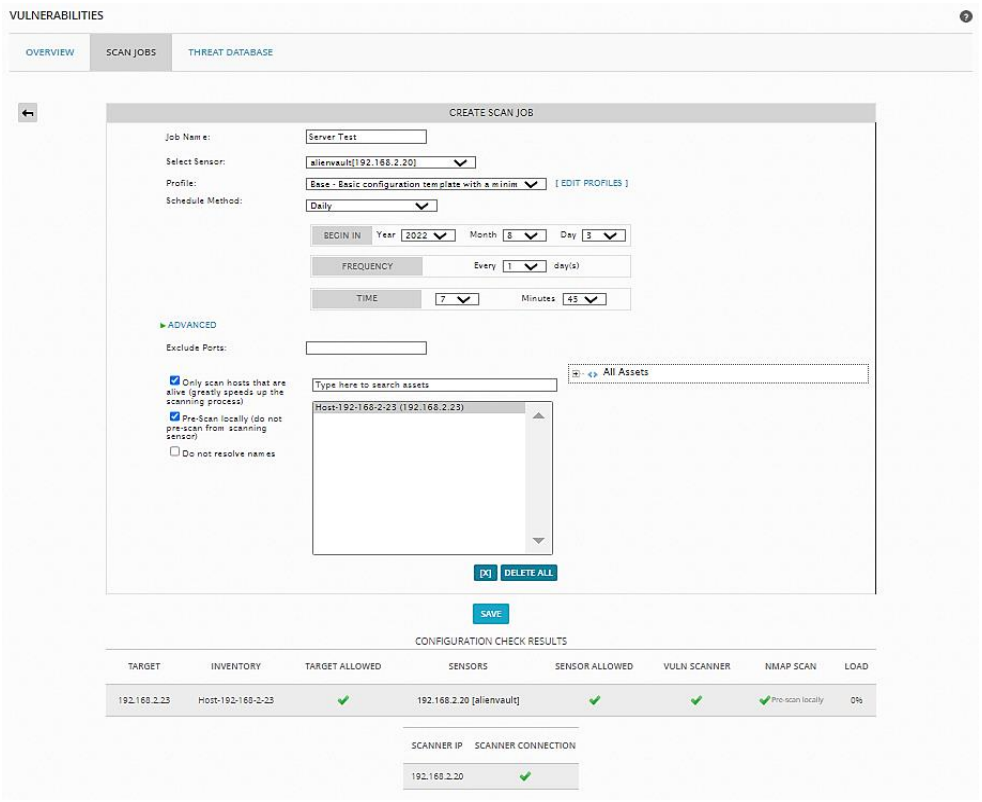


Figura 136: Interfaz web OSSIM AlienVault – Programación de trabajo de escaneo

Fuente: El Autor

Al guardarse los cambios, se puede evidenciar en el panel de despliegue de ‘Scan jobs’ con un estado habilitado de ejecución programada.

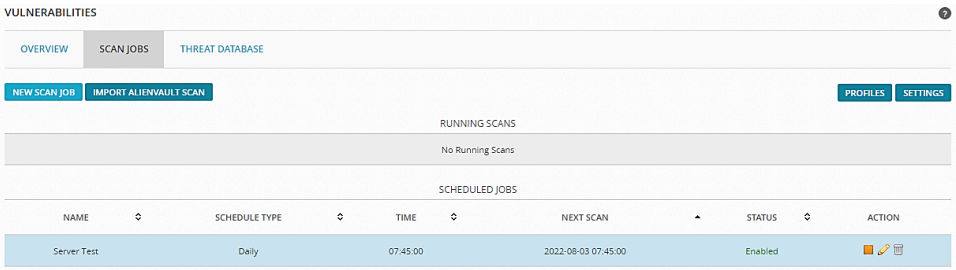


Figura 137: Interfaz web OSSIM AlienVault – Programación automática de trabajos

Fuente: El Autor

4.8 Gestión de riesgo

La herramienta SIEM, gestiona el riesgo al que está expuesto cada uno de los activos de la red de la organización o entidad en base al inventario general de activos mediante un IDS (Intrusion Detection System) o Sistema de detección de intrusos, aunque no realiza el bloqueo de tráfico anómalo que sea recibido, con lo que, el sistema permite alertar posibles eventos de riesgo. En la interfaz web de OSSIM AlienVault se accede al apartado de ’Analysis’ en la opción de ‘Security events (SIEM)’.

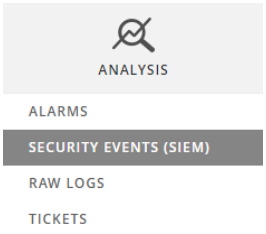


Figura 138: Interfaz web OSSIM AlienVault – Acceso a eventos de seguridad

Fuente: El Autor

Al ingresar se despliega un listado de incidencias relacionadas a la seguridad donde se podrá verificar la información de diversos eventos que han sido detectados por OSSIM AlienVault, dichos eventos permiten conocer parámetros de nombre del evento, fecha del evento, el origen, el destino y el nivel de riesgo correspondiente. Los eventos pueden mostrarse por horas, día, semana, mes o un determinado rango de tiempo.

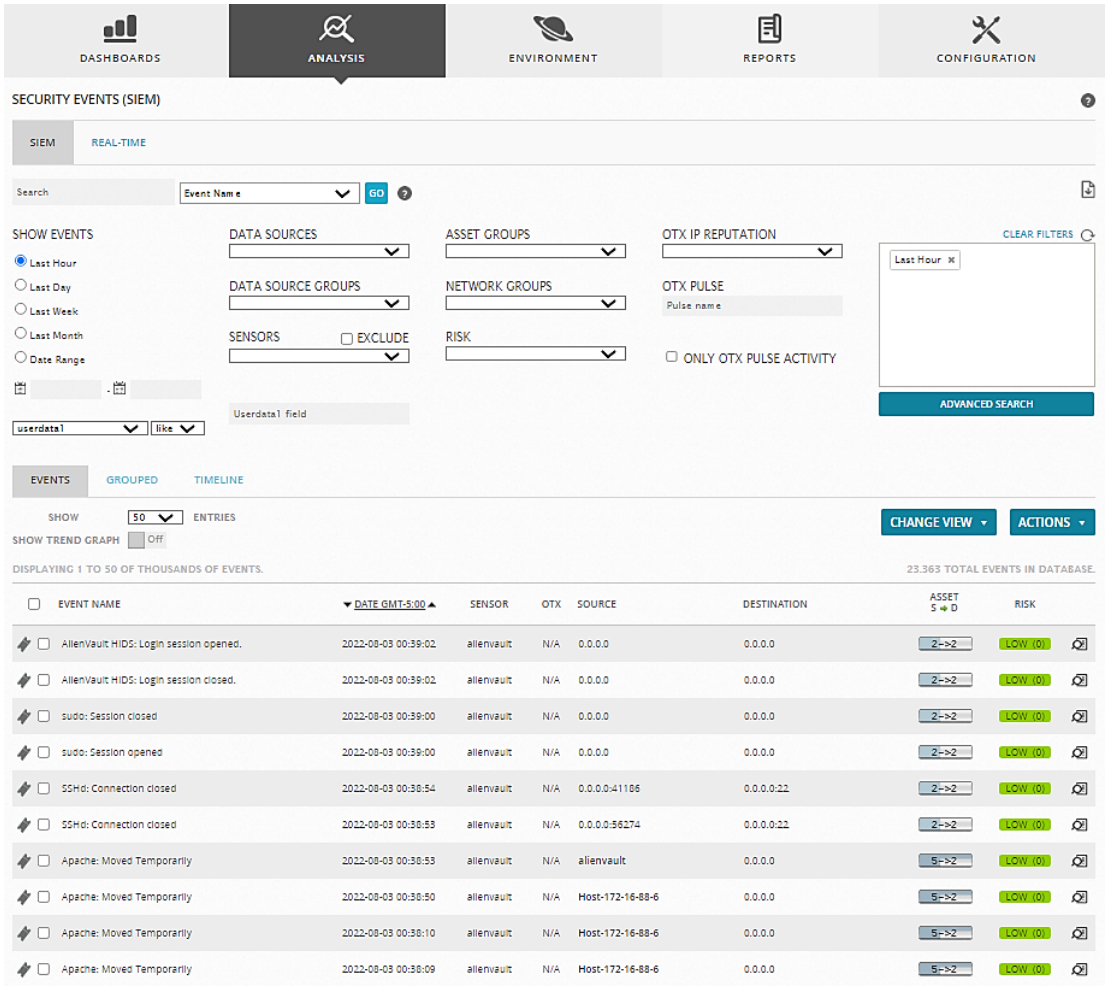


Figura 139: Interfaz web OSSIM AlienVault – Eventos de seguridad SIEM

Fuente: El Autor

La información recabada por OSSIM AlienVault puede analizarse en relación con el tráfico generado. Como una prueba de tráfico anómalo relacionado a una autenticación fallida y poder evidenciar el comportamiento de la herramienta. Se abrirá una consola de

comandos donde se ejecutará un comando para efectuar una conexión ‘ssh’ con un usuario inexistente y validar si el evento fue registrado en el SIEM.

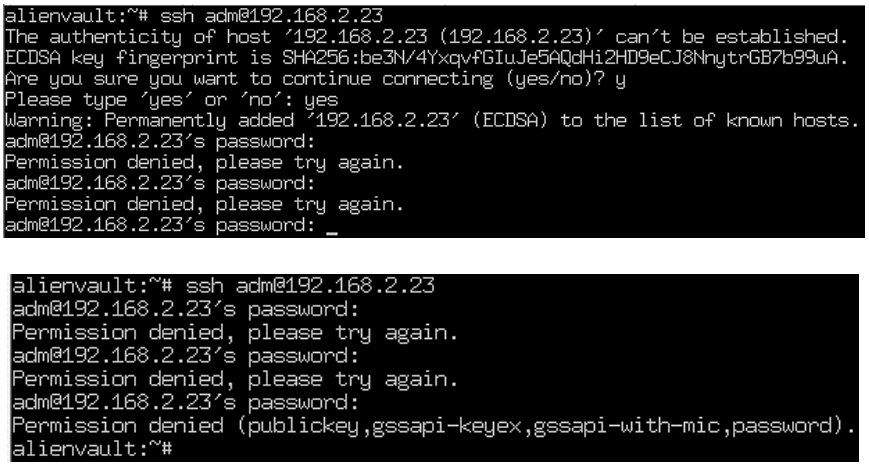


Figura 140: Interfaz web OSSIM AlienVault – Conexión ssh a un activo de red

Fuente: El Autor

En la pestaña ‘Real time’ de la sección ‘Security events (SIEM)’, se podrá visualizar en tiempo real la captura de tráfico, indicando los intentos de conexión fallida de un usuario inexistente dentro de un activo de la red.

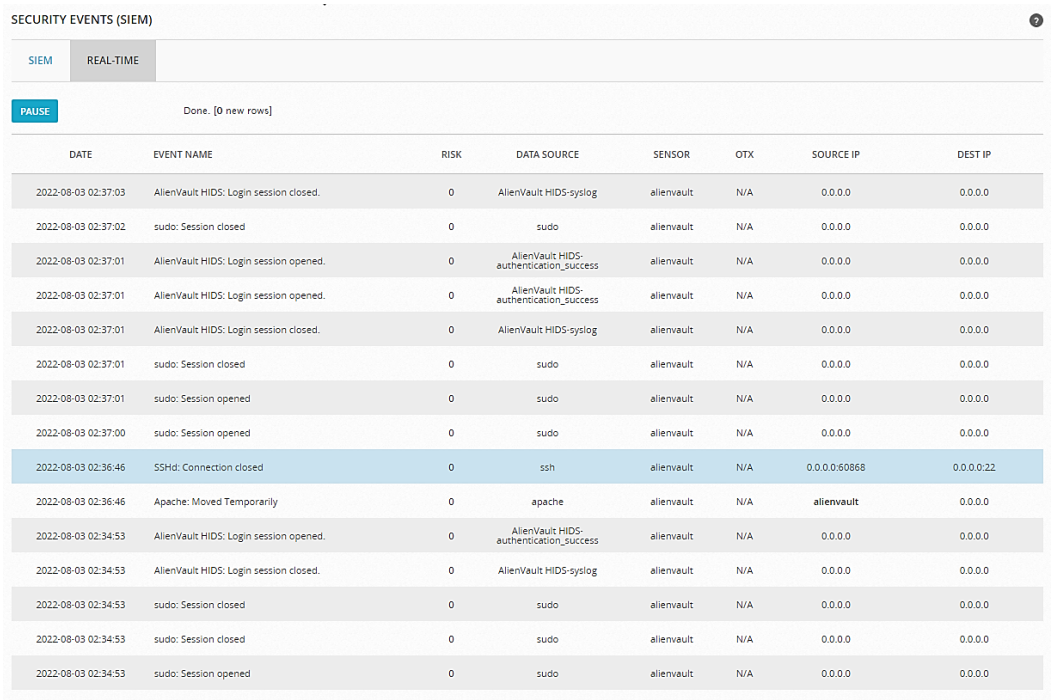


Figura 141: Interfaz web OSSIM AlienVault – Lista de eventos en tiempo real

Fuente: El Autor

Al ingresar en el evento suscitado por autenticación se puede verificar el detalle del evento con información relevante que comprende la fecha, la dirección IP, el ID del tipo de evento, el protocolo, la categoría, el origen de datos, tipo de producto, e información adicional. También se muestra la prioridad, fiabilidad y riesgo analizado.

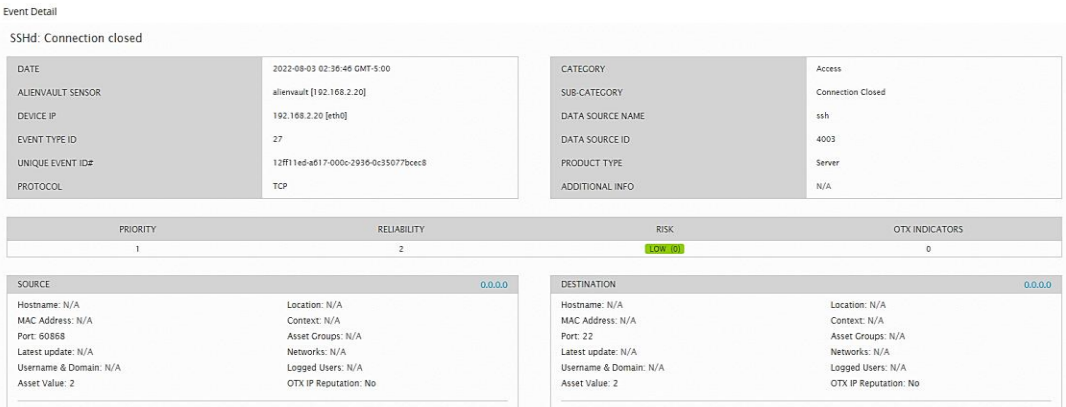


Figura 142: Interfaz web OSSIM AlienVault – Detalle del evento suscitado

Fuente: El Autor

Dentro de la pantalla de la pestaña ‘SIEM’, se puede incluir algún tipo de filtrado según las necesidades de la organización e información de cada uno de los eventos suscitados; y en la opción ‘Grouped’ se puede visualizar los eventos agrupados por tipo de evento.

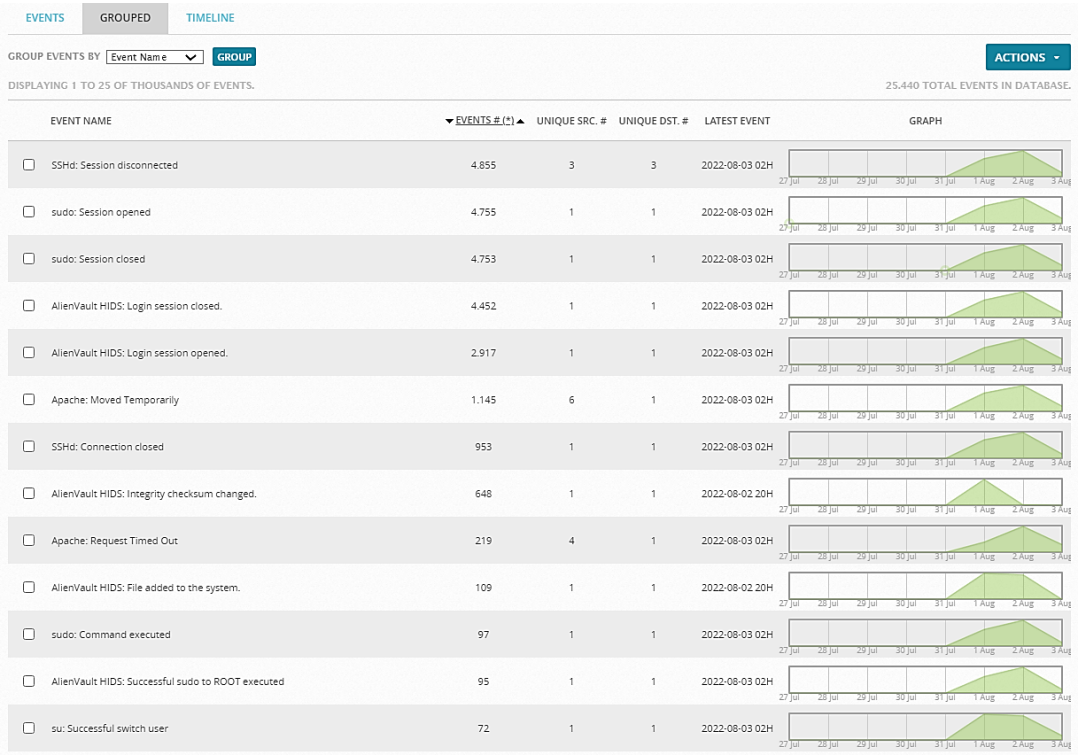


Figura 143: Interfaz web OSSIM AlienVault – Agrupación de eventos

Fuente: El Autor

La siguiente opción es ‘Timeline’, donde se puede determinar la resolución de línea de tiempo sobre la ocurrencia de los eventos suscitados.

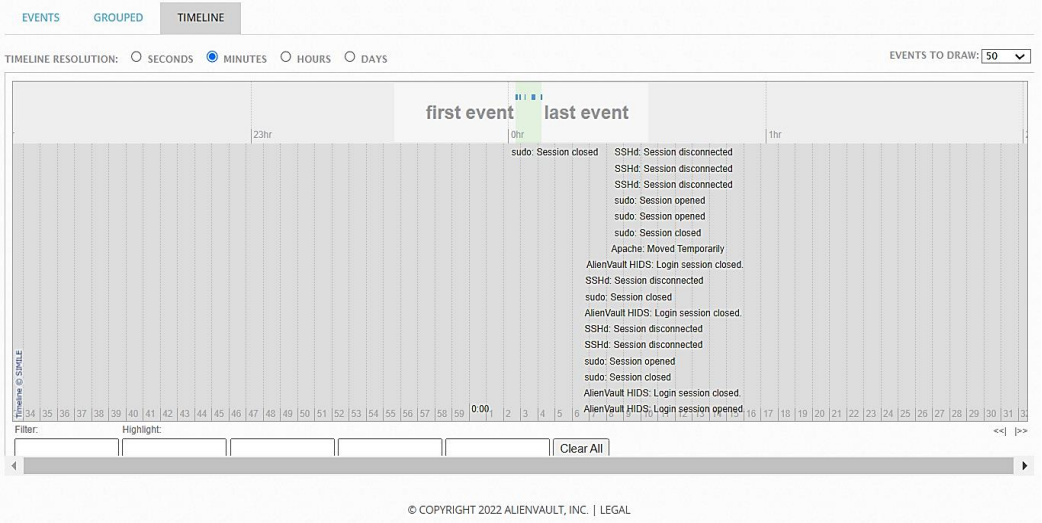


Figura 144: Interfaz web OSSIM AlienVault – Línea de tiempo de eventos

Fuente: El Autor

Para aplicar el filtrado de un activo específico de la red dentro de la opción ‘SIEM’, correspondiente a ‘Security events (SIEM)’, se ingresa la dirección IP de origen y el tiempo para verificar la cantidad de eventos que han ocurrido en dicho activo (host). Lo cual, se muestra el listado general de eventos e incidentes con un nivel de riesgo bajo (LOW), que pueden ser exportados.

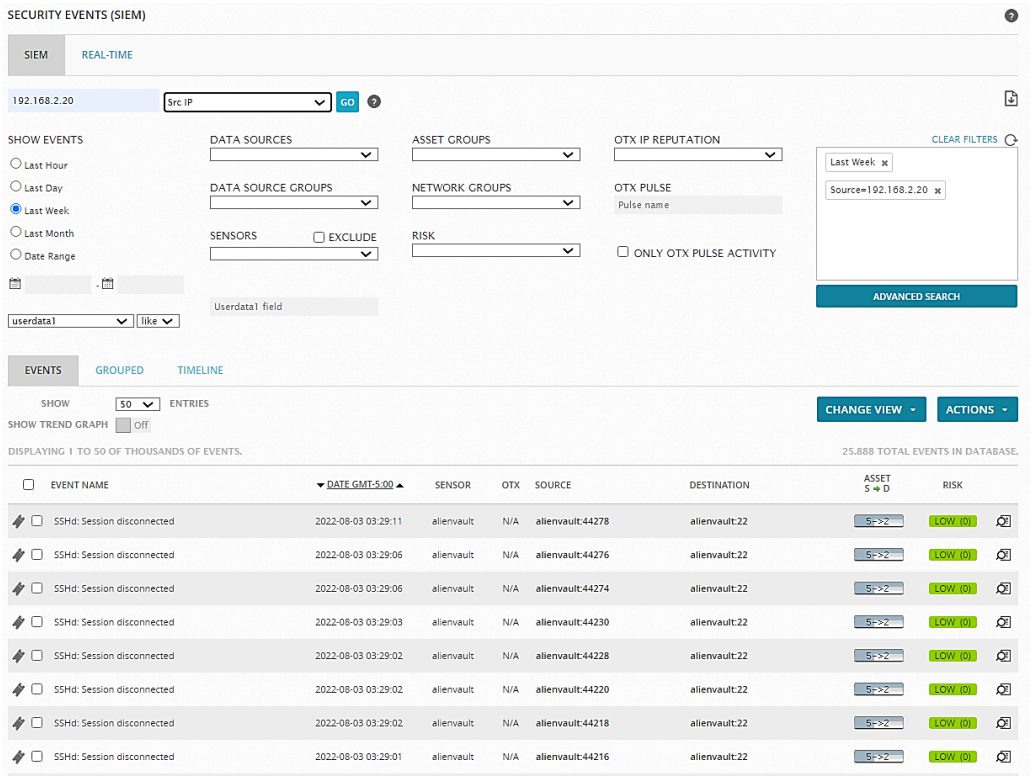


Figura 145: Interfaz web OSSIM AlienVault – Eventos filtrados de un activo

Fuente: El Autor

4.9 Open Threat Exchange

El intercambio de amenazas abiertas, en relación a la valoración de las direcciones IP y la determinación de la red a la cual pertenece; se ingresa al apartado ‘Dashboard’ en la opción ‘Open Threat Exchange’.

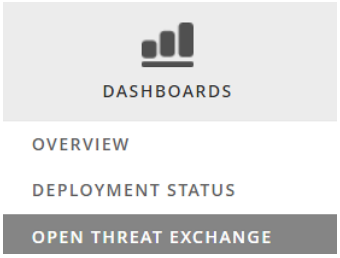


Figura 146: Interfaz web OSSIM AlienVault – Open Threat Exchange

Fuente: El Autor

Se abre la pantalla de configuración, donde se solicita el 'OTX Key' (Clave OTX), a partir de la creación de una cuenta en caso de no contar con una.

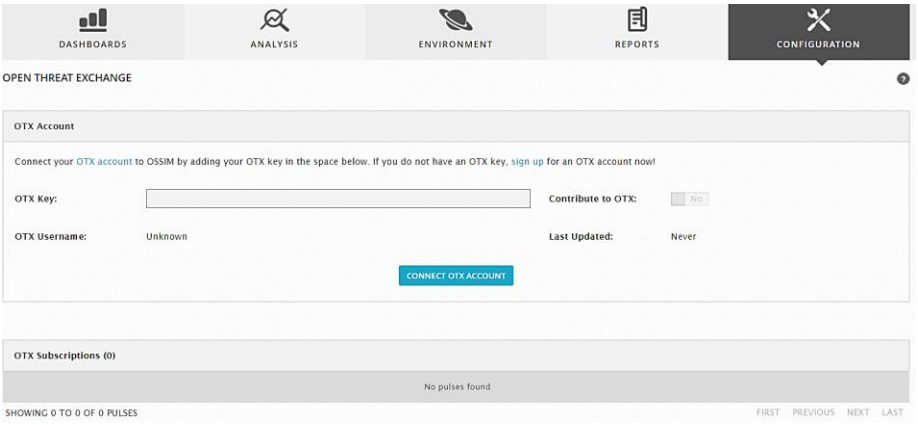


Figura 147: Interfaz web OSSIM AlienVault – OTX Key (clave)

Fuente: El Autor

El siguiente paso es conectarse a una cuenta OTX, en la opción 'Connect OTX account', aunque en el caso de haber creado una cuenta, se deberá iniciar sesión donde se podrá acceder a la información general y propia de la cuenta.

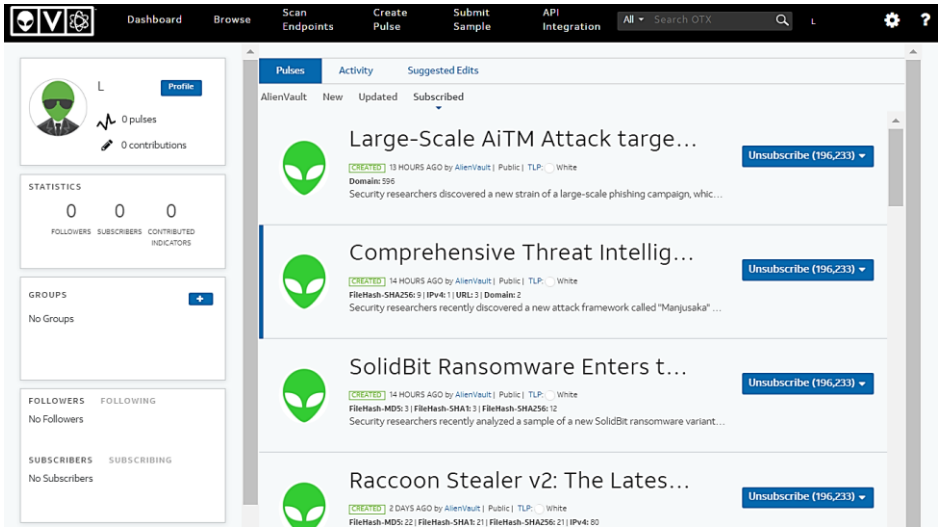


Figura 148: Interfaz web OSSIM AlienVault – Cuenta OTX

Fuente: El Autor

Se ingresa a la opción ‘API Integration’, donde se podrá obtener la clave OTX requerido por la interfaz web de OSSIM AlienVault.

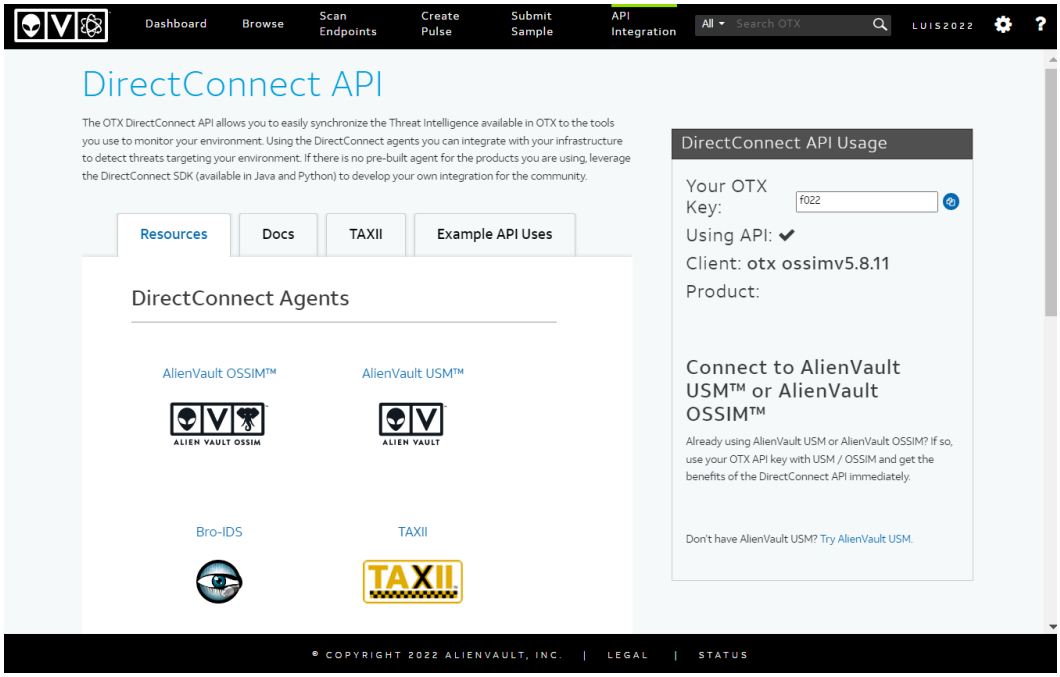


Figura 149: Interfaz web OSSIM AlienVault – API Integration clave OTX

Fuente: El Autor

La clave se ingresa en ‘Open Threat Exchange’ del apartado ‘Dashboards’, que al momento de conectarse se espera a que la clave OTX ingresada se autentique y se valide en el sistema. Al terminar el proceso de autenticación aparecerá un mensaje de conexión satisfactoria y con acceso a OTX.

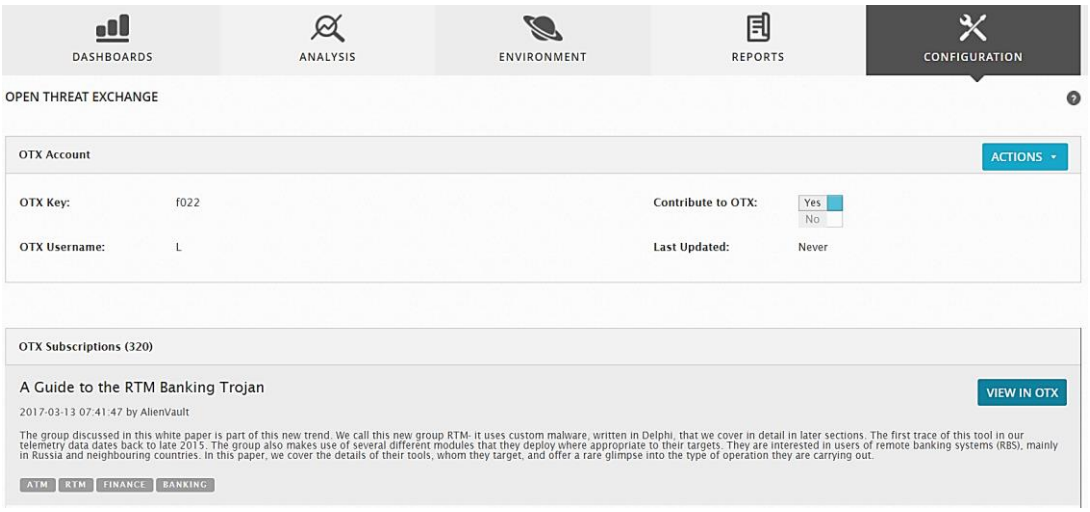


Figura 150: Interfaz web OSSIM AlienVault – Validación e ingreso de clave OTX

Fuente: El Autor

Con lo cual, se puede acceder a la opción ‘Open Threat Exchange’ en 'Dashboards’, donde se puede encontrar información de la reputación de direcciones IP, además de indicadores, actualizaciones, números de alarmas y número de eventos, etc. Dentro de la pestaña ‘Source’ de ‘IP Reputation’ (Reputación IP), se podrá verificar información de eventos SIEM o los datos de reputación de todos los servidores reportados a nivel mundial. Y si hubiera algún evento en el que coincida la dirección IP referenciada en OTX, se realizará una evaluación y se mostrará dentro del listado de vulnerabilidades de OSSIM AlienVault.

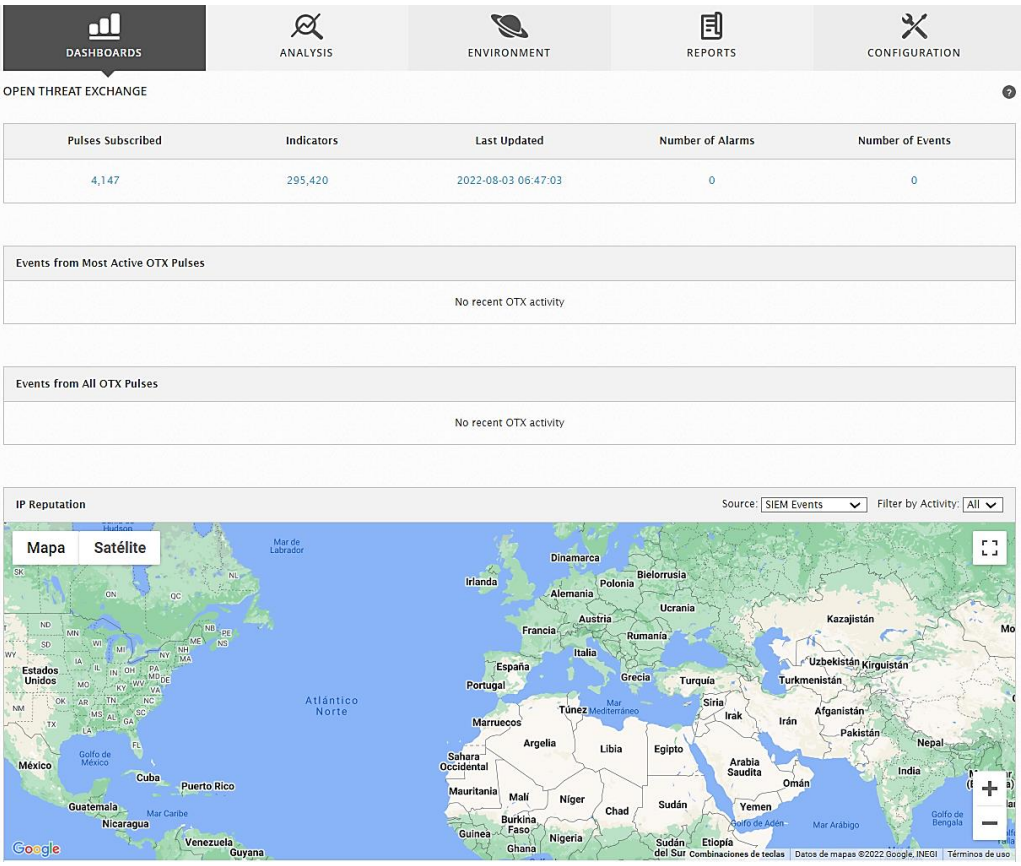


Figura 151: Interfaz web OSSIM AlienVault – Open Threat Exchange

Fuente: El Autor

4.10 Gestión de alarmas y eventos

De inicio, se tiene un ‘banner’ en la pantalla principal de OSSIM AlienVault que indica un resumen sobre las alarmas que se encuentran activas o que aún no están resueltas.

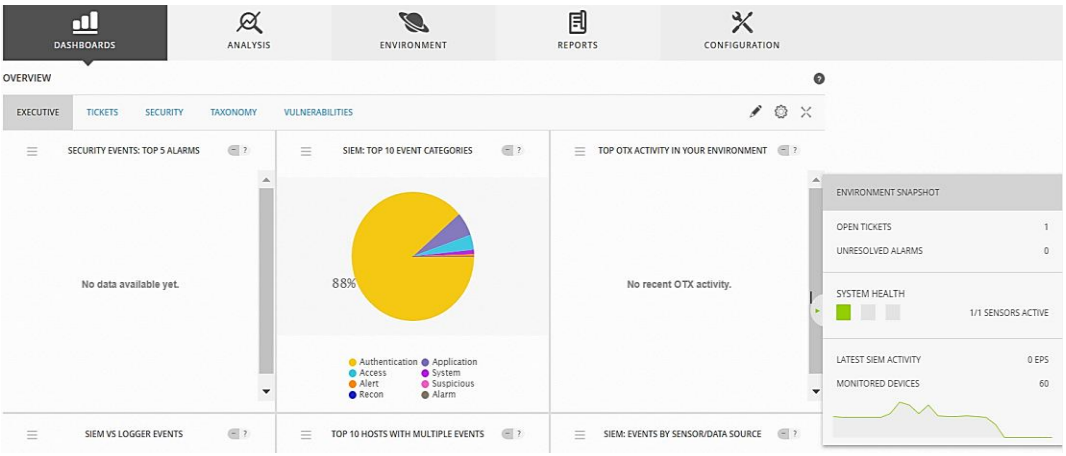


Figura 152: Interfaz web OSSIM AlienVault – Banner de alarmas

Fuente: El Autor

Para acceder a las configuraciones propias de las alarmas se ingresa al apartado ‘Analysis’ en la opción ‘Alarms’ (Alarmas).

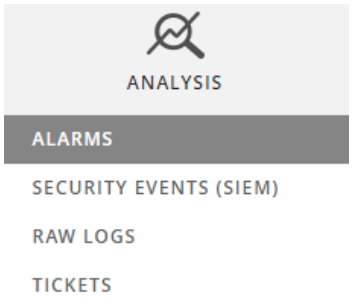


Figura 153: Interfaz web OSSIM AlienVault – Opción de alarmas

Fuente: El Autor

Al ingresar se puede apreciar la información con todas las alarmas generadas.

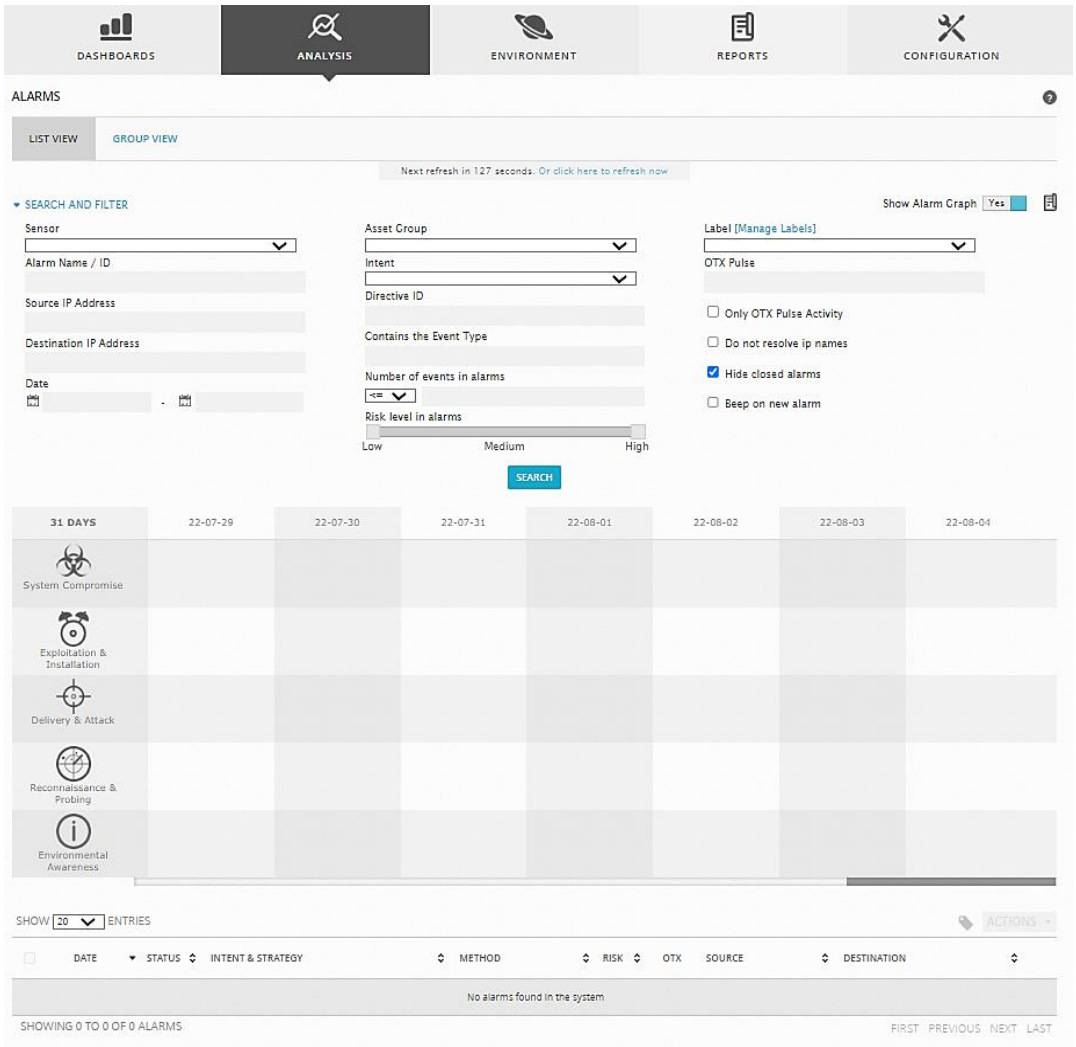


Figura 154: Interfaz web OSSIM AlienVault – Vista de la lista de alarmas

Fuente: El Autor

También se puede revisar el listado de alarmas de manera agrupada en la opción ‘Group view’ (Vista agrupada), aunque inicialmente no se mostrará ninguna alarma debido a las configuraciones que deben realizarse.

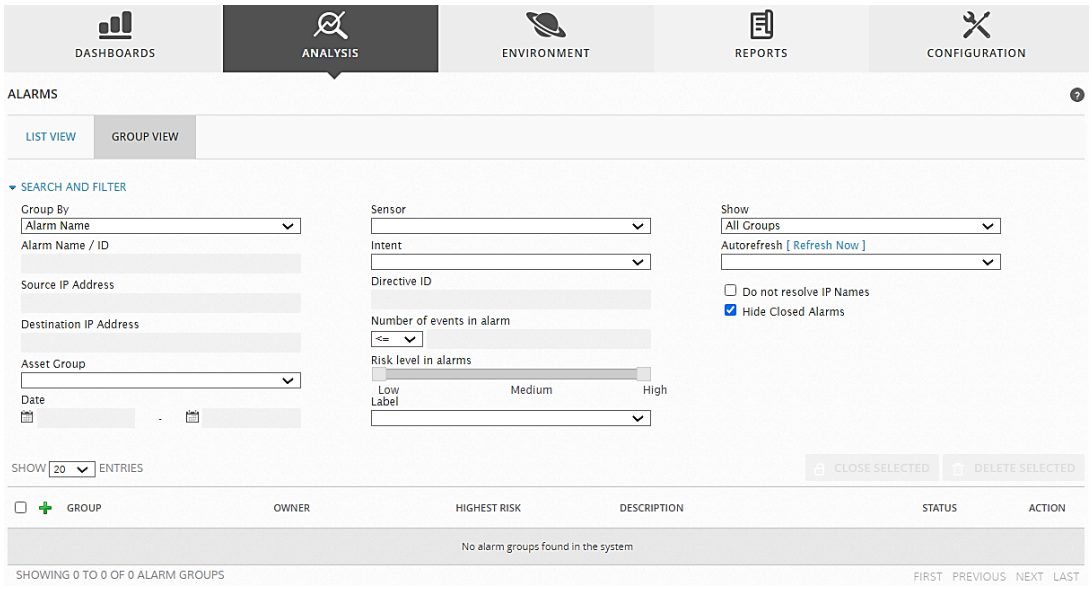


Figura 155: Interfaz web OSSIM AlienVault – Vista agrupada de la lista de alarmas

Fuente: El Autor

En la opción 'List view', se puede programar alarmas dentro de los parámetros de configuración de 'Search and filter', en función de un determinado activo de red de la organización que permita gestionar cuando haya algún tipo de evento con probabilidades de alto riesgo.

4.11 Administración de tickets

La generación de tickets tiene base sobre las alarmas y eventos reportados dentro de OSSIM AlienVault, y se asocia a la gestión de vulnerabilidades, dado que al haber alguna detección de vulnerabilidades se podrá generar un ticket para ser asignado a un operador dentro del SIEM. Se ingresa al apartado 'Analysis' en la opción 'Security events (SIEM)', el mismo que permite visualizar el listado de eventos ocurridos.

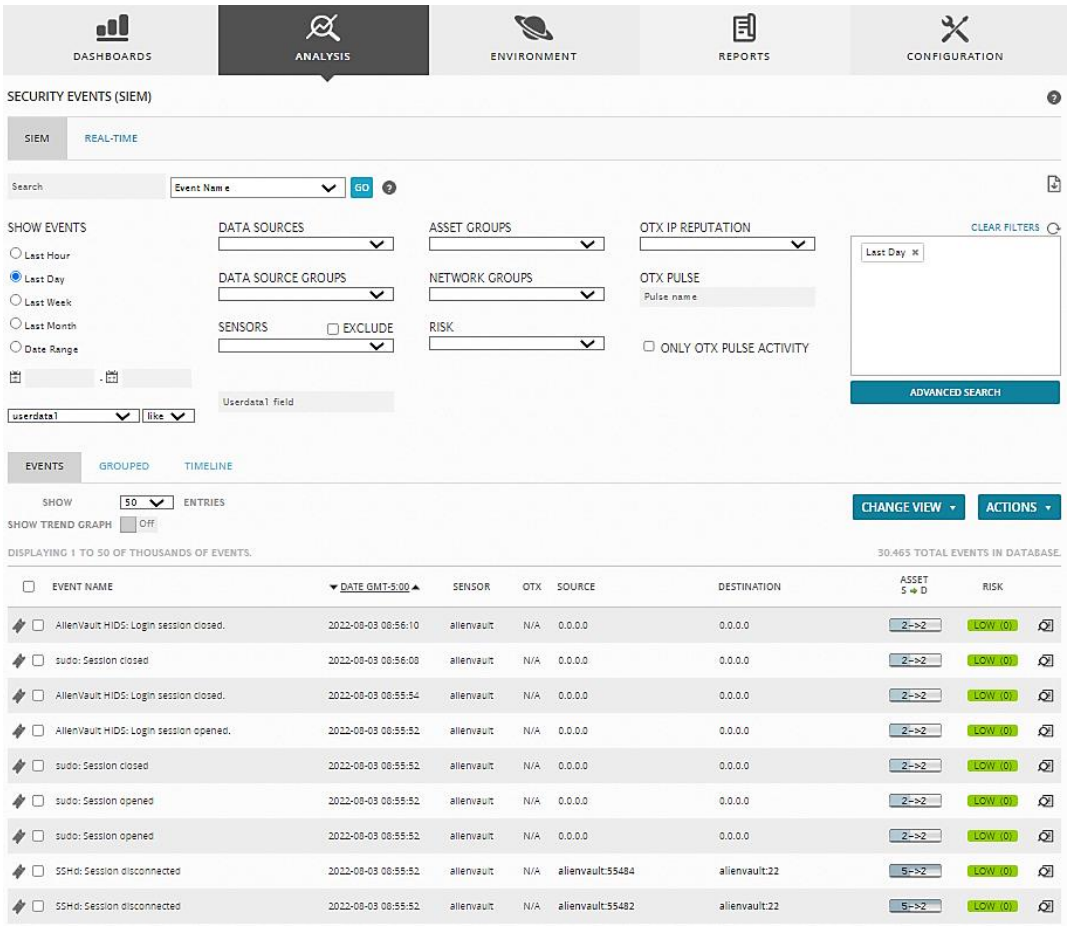


Figura 156: Interfaz web OSSIM AlienVault – Listado de eventos ocurridos

Fuente: El Autor

Al seleccionar un determinado evento mediante el botón de generación de ticket, se abrirá una ventana para ingresar los datos de título, usuario, prioridad, tipo, y se guardan los cambios realizados.

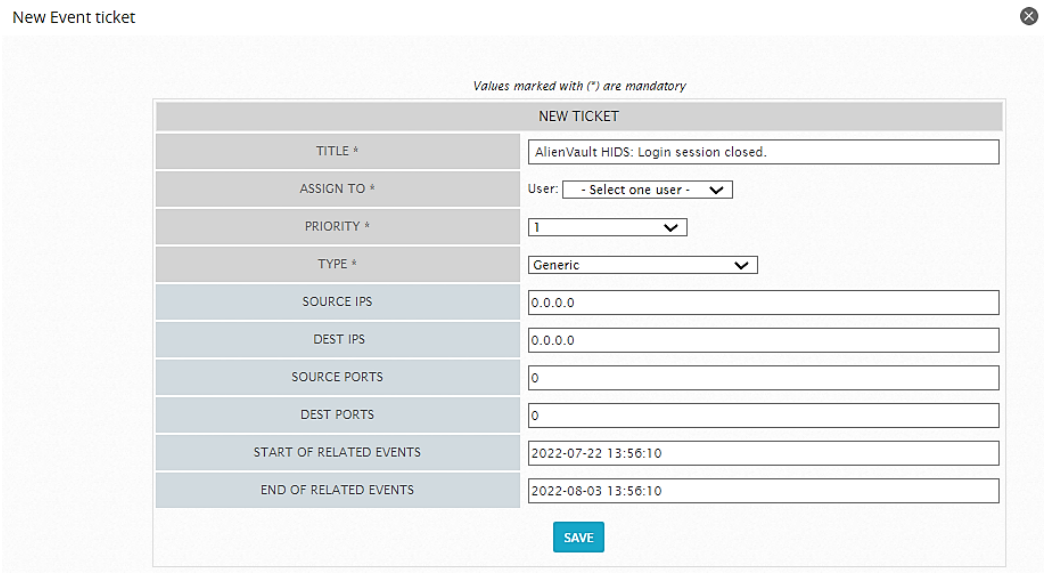


Figura 157: Interfaz web OSSIM AlienVault – Creación de nuevo ticket

Fuente: El Autor

Al guardarse los cambios del nuevo ticket, será incluido en la lista de tickets con un estado ‘Open’ (Abierto); es decir, que debe ser cerrado posteriormente.

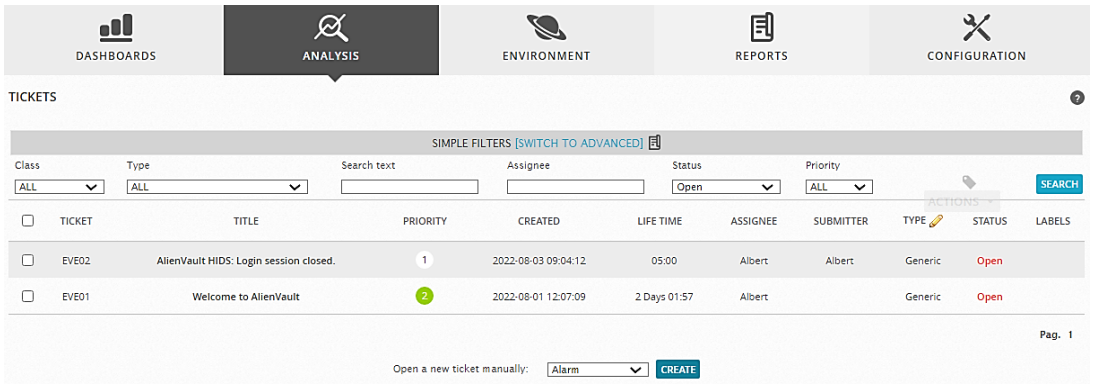


Figura 158: Interfaz web OSSIM AlienVault – Esquema de tickets creados

Fuente: El Autor

En el apartado ‘Analysis’ en la opción ‘Tickets’ se tendrá acceso a todo el listado de boletos creados dentro de OSSIM AlienVault.

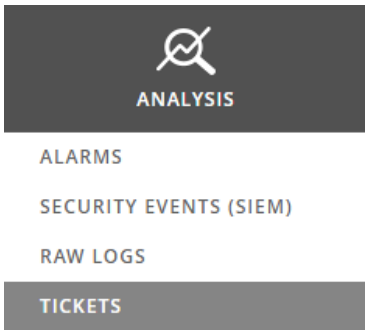


Figura 159: Interfaz web OSSIM AlienVault – Tickets

Fuente: El Autor

Al tener acceso a la opción de boletos, se visualizará cada uno de los tickets que se encuentran abiertos, también se puede revisar cada uno a detalle seleccionando uno de ellos.

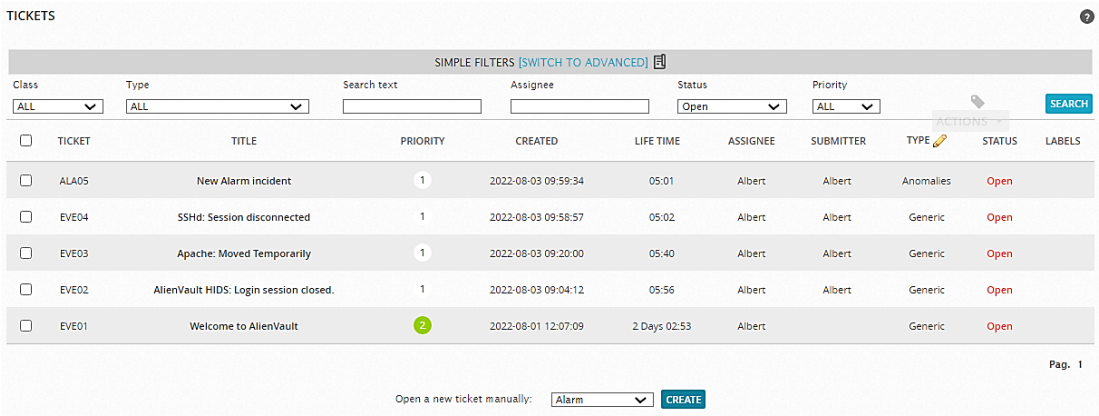


Figura 160: Interfaz web OSSIM AlienVault – Tickets

Fuente: El Autor

Seleccionar uno de los tickets del listado, se tiene el detalle para observar y conocer la información referida a dicho boleto.

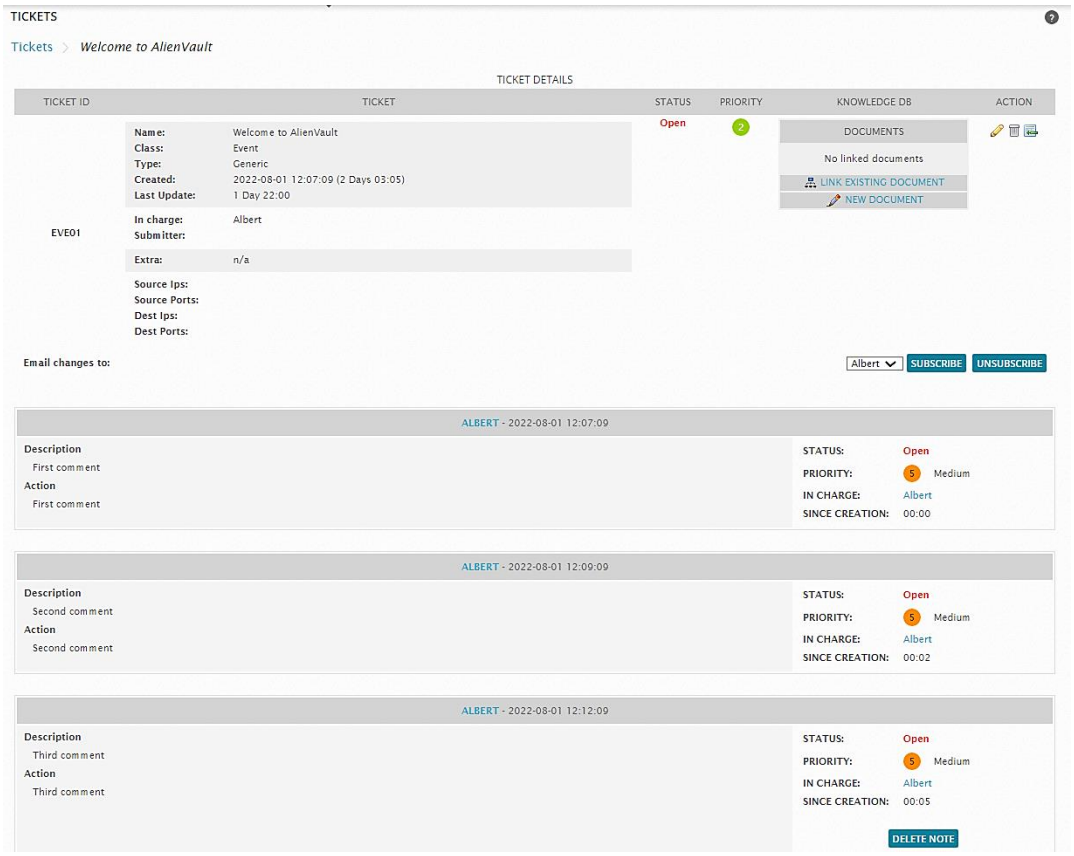


Figura 161: Interfaz web OSSIM AlienVault – Detalle de ticket

Fuente: El Autor

De tomar alguna acción relativa al ticket analizado, se puede concluir cerrando el estado del mismo, en la opción ‘Status’ indicando el estado ‘Closed’ (Cerrado) y se guardan los cambios con la opción ‘Save ticket’.

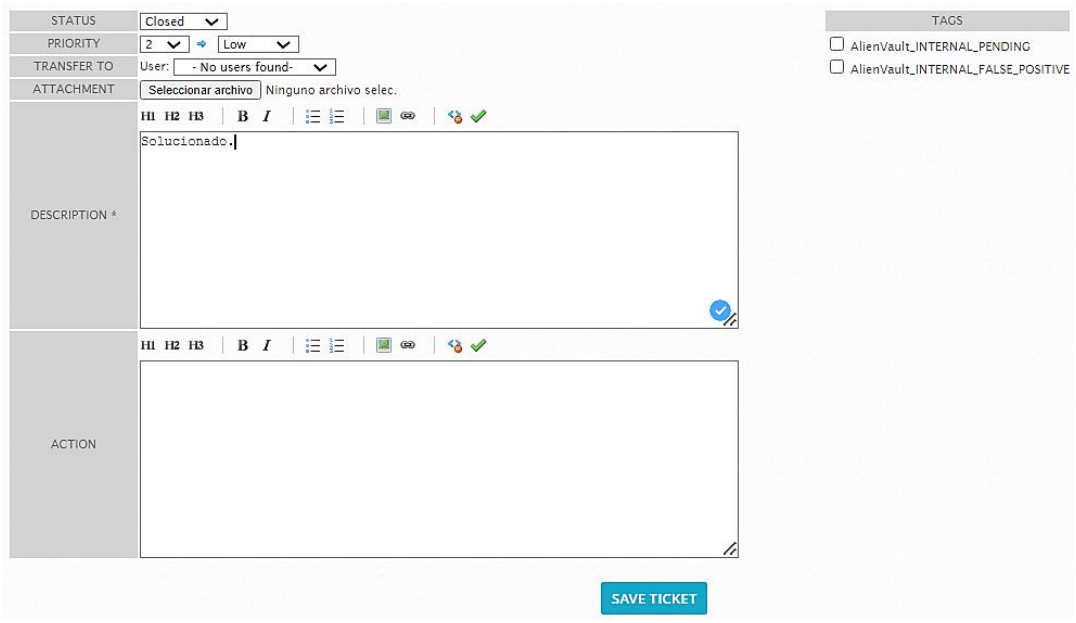


Figura 162: Interfaz web OSSIM AlienVault – Configuraciones del ticket

Fuente: El Autor

Se actualizará el listado de los tickets existentes, y se podrá verificar que uno de los tickets ya se encuentra con estado de 'Closed' (Cerrado).

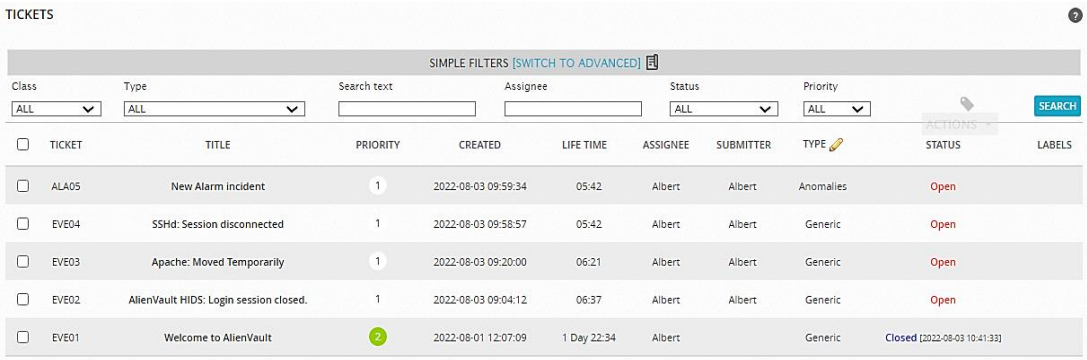


Figura 163: Interfaz web OSSIM AlienVault – Actualización del estado del ticket

Fuente: El Autor

4.12 Flujo de red

Para el ingreso a los detalles del flujo de la red, ubicar la opción ‘Netflow’ dentro del apartado ‘Environment’. NetFlow es un protocolo diseñado y publicado por Cisco Systems que permite registrar y transmitir información sobre los flujos de red que sean registrados.

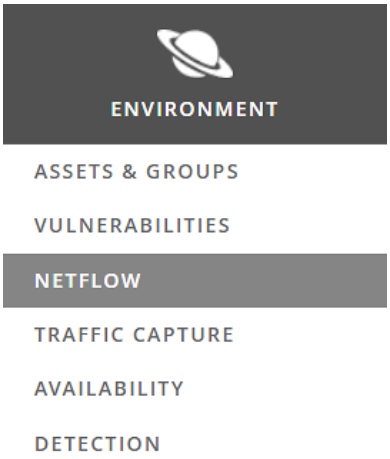


Figura 164: Interfaz web OSSIM AlienVault – Flujo de red

Fuente: El Autor

En la opción de flujo de red, se tendrá información en tiempo real con opción de elegir alternativas de tiempo, visualizar los gráficos de flujo de red, tráfico de red, paquetes de red para los protocolos TCP, UDP, ICMP, y otros.

Figura 165: Interfaz web OSSIM AlienVault – Detalles del flujo de red

Fuente: El Autor

En la pestaña ‘Overview’ (Resumen), se podrá observar el resumen del flujo de red que ha sido generado por la herramienta.

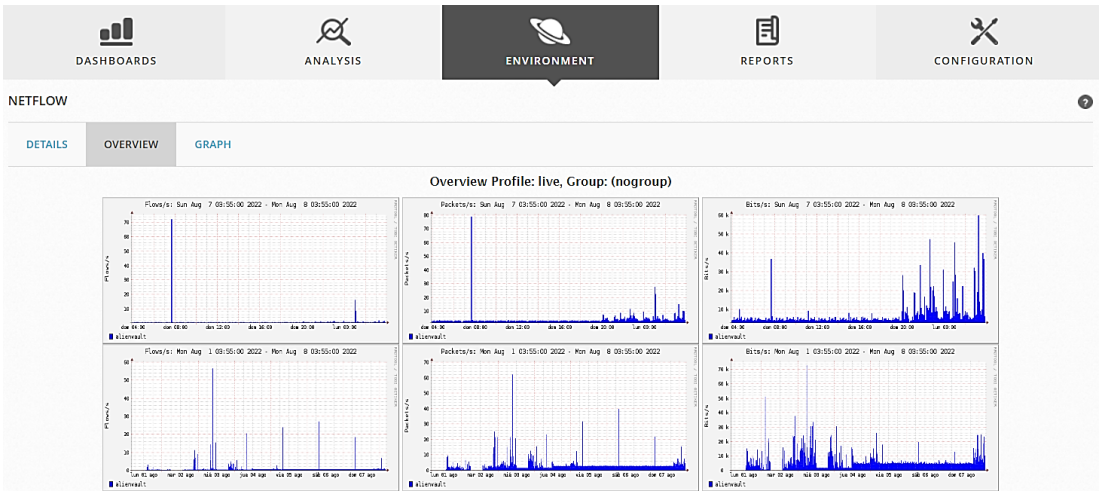


Figura 166: Interfaz web OSSIM AlienVault – Resumen de flujo de red

Fuente: El Autor

En la pestaña ‘Graph’ (Gráfico), se tiene los gráficos por flujo, paquetes y tráfico de la red generado.

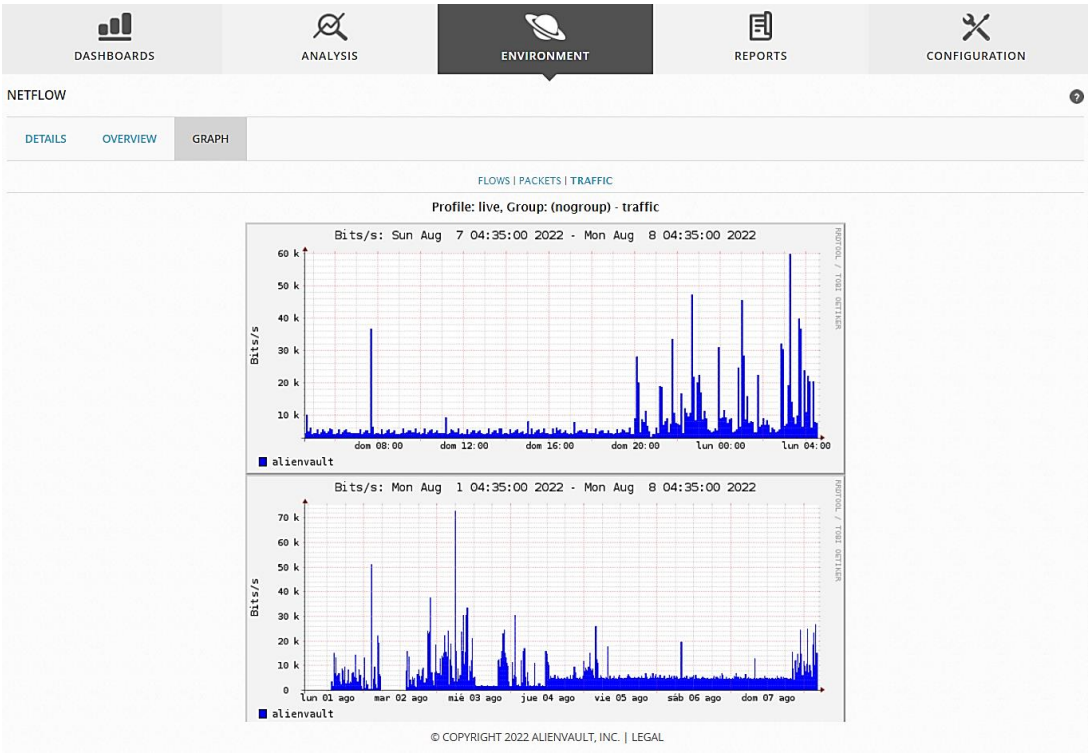


Figura 167: Interfaz web OSSIM AlienVault – Gráficos de flujo de red

Fuente: El Autor

Después de haber configurado diferentes módulos del SIEM, la pantalla principal de OSSIM AlienVault presenta nuevos cambios en la visión general de los procesos.

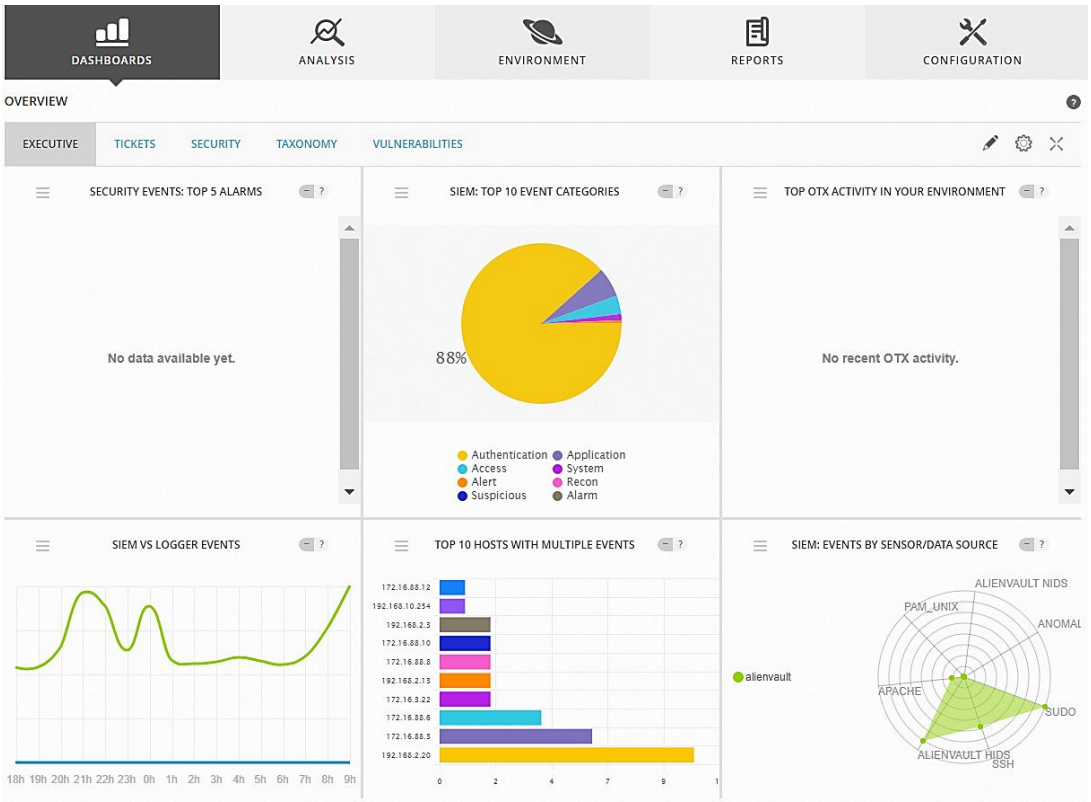


Figura 168: Interfaz web OSSIM AlienVault – Visión general del SIEM

Fuente: El Autor

Adicionalmente, en el apartado ‘Dashboards’, en la opción ‘Deployment Status’ (Estado de implementación), se puede añadir la ubicación del sensor de OSSIM AlienVault escogiendo ‘Add Location’.

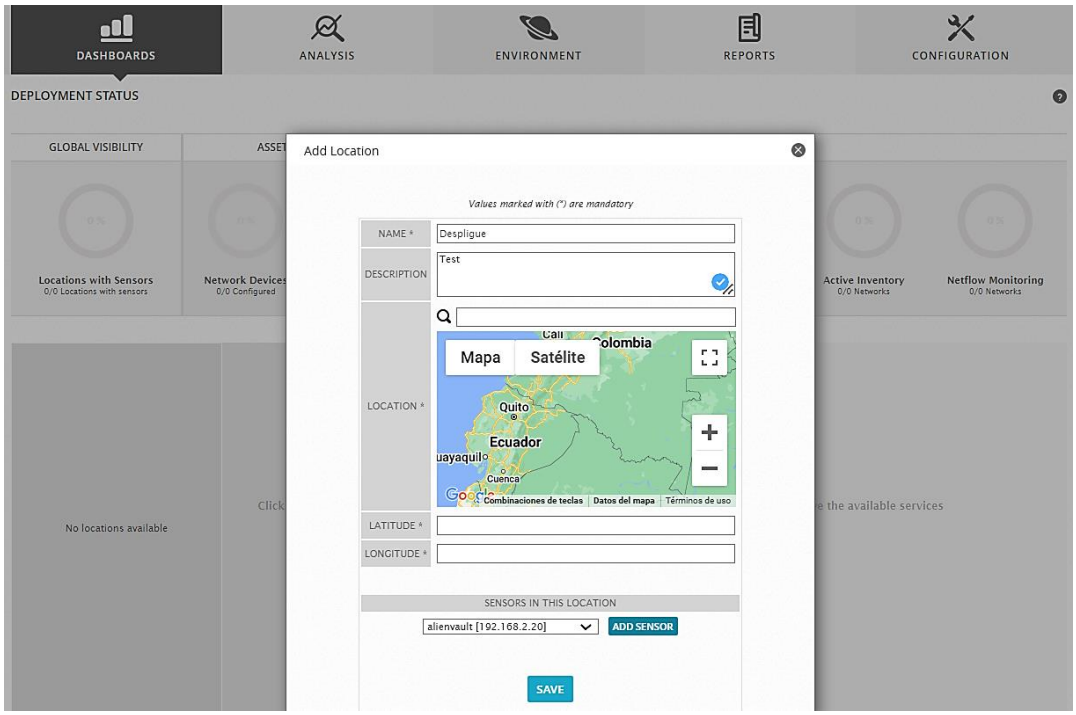


Figura 169: Interfaz web OSSIM AlienVault – ubicación

Fuente: El Autor

Al guardar los datos ingresados de ubicación, el sistema actualizará automáticamente e incluirá al sensor especificado de OSSIM AlienVault en el cuadro estadístico.

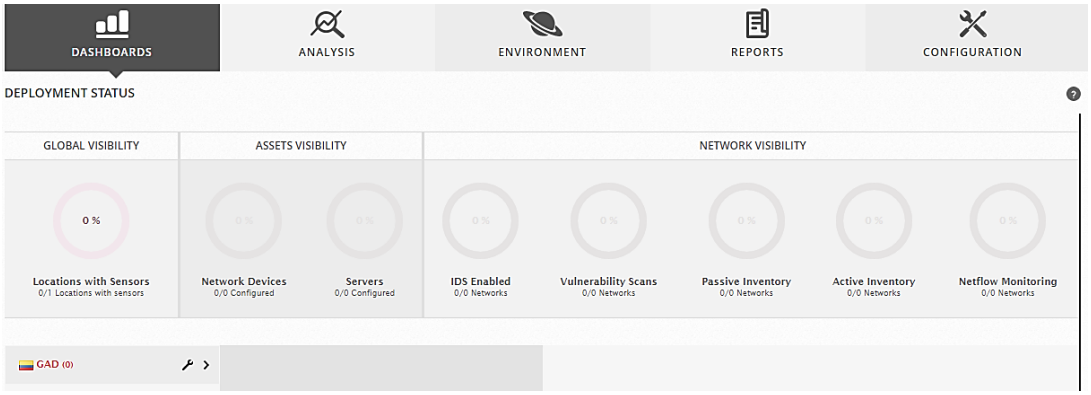


Figura 170: Interfaz web OSSIM AlienVault – Estado de implementación

Fuente: El Autor

Adicionalmente, se propone el planteamiento de una política de seguridad que complemente la gestión de la implementación de la herramienta SIEM. Pese a la existencia de un reglamento de uso de la tecnología y recursos de información, la política de seguridad inicial pretende establecer una guía con directrices de uso, previa aprobación de la dirección del departamento de TIC, para que los usuarios de la entidad gubernamental conozcan y acepten el cumplimiento del mismo, a fin de precautelar los activos de información.

El cumplimiento de la política de seguridad debe tener un carácter obligatorio para todo el personal de la entidad, independientemente del área a la que pertenezca o función que desempeñe. La política de seguridad debe tener un enfoque que se ajuste a las necesidades de la entidad, tomando en consideración los criterios de la norma ISO/IEC 27002 en relación a controles organizativos. (Watkins, 2020)

A continuación, se describe la propuesta de la política de seguridad.

Política de Seguridad

- Política:

  Estructura de seguridad de la entidad gubernamental

- Descripción de la Política:

La política y cada uno de sus criterios o artículos deberán revisarse para realizar cambios en caso de ser necesario con la debida documentación, a través de solicitudes u oficios dirigidos a la autoridad máxima de la entidad.

La entidad, contará o creará un equipo de seguridad responsable de la gestión y respuesta a incidentes de seguridad. También se establecerá un comité de revisión y apoyo de políticas de seguridad que sea integrada por el jefe del departamento de TIC, una autoridad máxima Administrativa, y el jefe de Recursos Humanos para la elaboración de políticas posteriores.

La política propuesta inicial se ajustará a la estructura y estrategias que maneje la entidad gubernamental posibilitando la conformación de un equipo de seguridad para la administración del sistema de gestión de eventos e incidentes de seguridad implementado o que se vaya a implementar.

- Objetivo:

Establecer la estructura de seguridad que será acogida por la entidad para la continuidad de la operatividad de los servicios, sistemas de información, equipos e infraestructura de TIC que utilizan.

- Criterios de implementación de la política de seguridad:

  - Aprobación previa de la prefectura.

- Definición de la jerarquía organizacional del equipo de seguridad y del comité de apoyo en la entidad.
- Definición del coordinador del equipo de seguridad para el manejo de la seguridad de la información y del sistema de gestión de eventos e incidentes.
- Definición de las funciones técnicas de los integrantes del equipo de seguridad.
- Revisión de la política de seguridad al menos 3 veces al año mediante una evaluación de resultados.

– Alcance:

La política de seguridad va dirigida al departamento de TIC, prefectura, administración, y recursos humanos de la entidad gubernamental, debido a la inexistencia y falta de un equipo de seguridad que gestione, administre, y controle el uso de los activos de información e infraestructura de red.

– Responsabilidades:

- Especificación de las funciones estratégicas.
- Soporte al departamento de TIC de la entidad.
- Supervisión del equipo de seguridad.
- Definición de las actividades y procedimientos de protección.
- Gestión y autorización de accesos a los activos de información.
- Análisis, monitoreo, control, registro y respuesta ante ciber amenazas.
- Clasificación y priorización de eventos e incidentes de seguridad.

- Recopilación de eventos e incidentes de seguridad.
- Coordinación, asignación, organización y colaboración del equipo de seguridad y comité de apoyo.
- Elaboración de la documentación y material técnico de referencia.
- Gestión, control y administración de la infraestructura de red de la entidad.
- Administración del sistema de gestión de eventos e información de seguridad.
- Gestión de sistemas de gestión de seguridad de la información.
- Asistencia en la respuesta ante incidentes de seguridad.

La política propuesta pretende contribuir a la creación de un equipo para la estructura de seguridad de la entidad gubernamental para la gestión, control y administración del sistema SIEM, o de futuras implementaciones, incluyendo la elaboración de nuevas políticas bajo el modelo referencial de la norma ISO/IEC 27001 / 27002 en conjunto con la integración de la documentación provista por el MINTEL, el cual establece: el Plan Nacional de Gobierno Electrónico, la Estrategia Nacional de Ciberseguridad, la Política Nacional de Ciberseguridad, y los Acuerdos Ministeriales respectivos.

CAPÍTULO V

RESULTADOS

5.1 Implementación OSSIM AlienVault

Como parte de la propuesta de solución de implementación del SIEM, se puede evidenciar en el diagrama general de red de la entidad gubernamental; que la disposición de la herramienta dentro de los nodos de la red se distribuye en los principales puntos críticos para efectuar el monitoreo, prevención, detección y mitigación de posibles amenazas de seguridad que puedan ocasionar algún tipo de impacto en los activos de información.

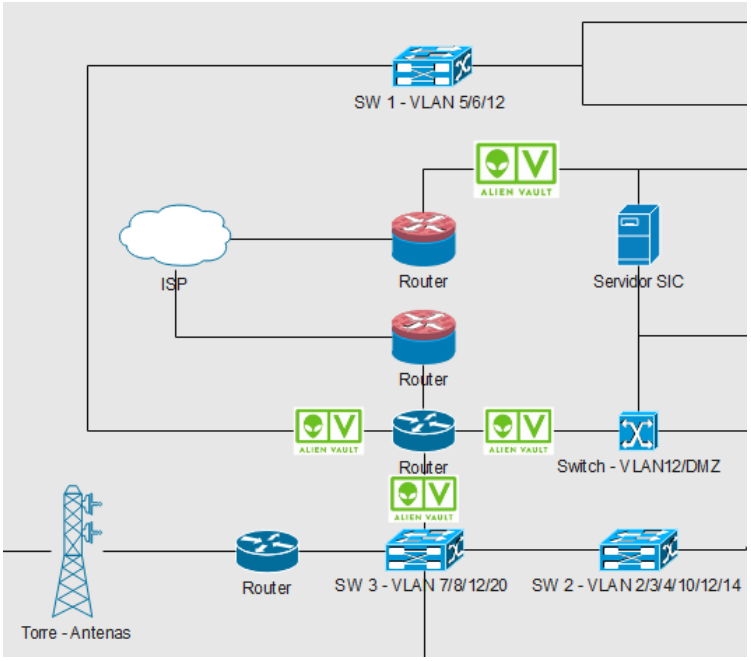


Figura 171: Implementación OSSIM AlienVault – Disposición del SIEM en la red

Fuente: El Autor

Debido a la falta de políticas y controles de seguridad, la red de la entidad gubernamental se ha visto expuesta a posibles riesgos de seguridad; sin embargo, a través de la implementación del SIEM, se ha podido alcanzar un control de los distintos segmentos de red, obteniendo cuadros estadísticos de los resultados de monitoreo y detección de vulnerabilidades en algunos activos y equipos de información de acuerdo a los acontecimientos que fueron registrados, procesados, y almacenados.

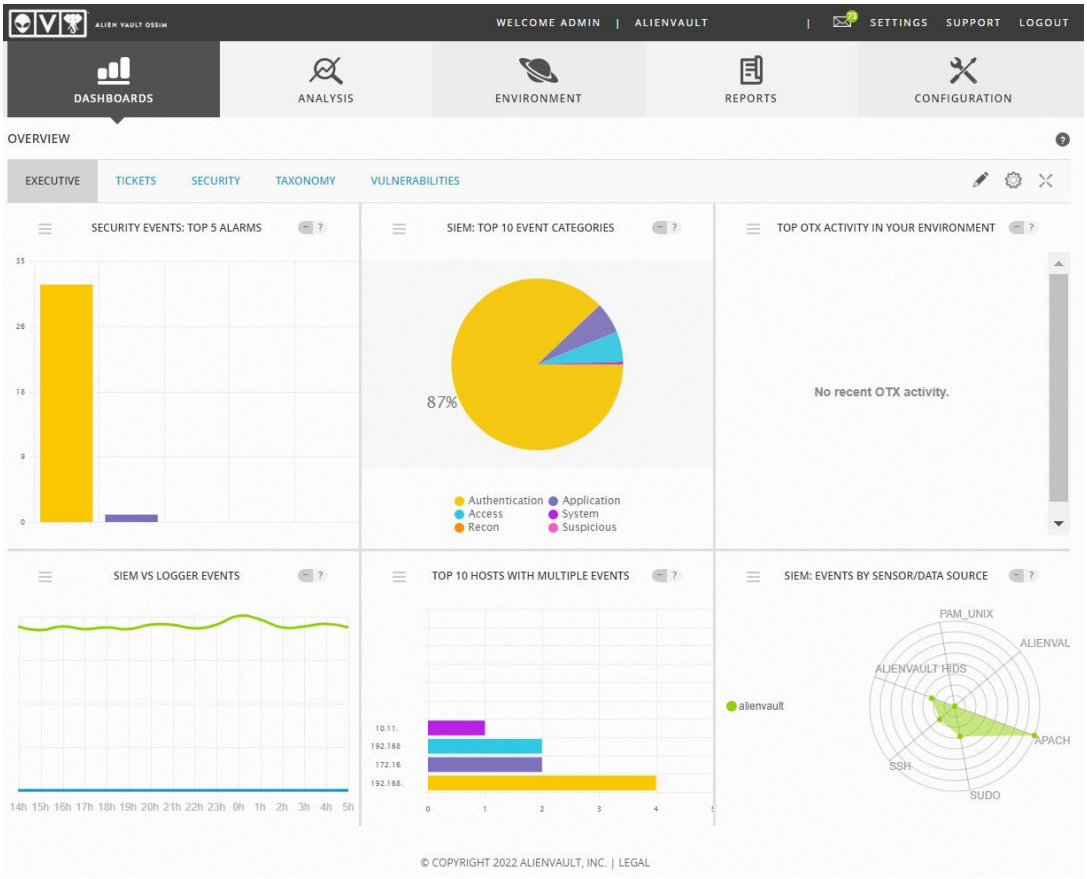


Figura 172: Implementación OSSIM AlienVault – Resumen estadístico del SIEM

Fuente: El Autor

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Una vez realizada la implementación del sistema de gestión de información y eventos de seguridad para la prevención y detección de incidentes o amenazas de seguridad, se vuelve muy importante conocer previamente la situación en la que se encuentra la infraestructura tecnológica de la entidad, con lo cual, se pueden tomar medidas que se ajusten a los requerimientos tecnológicos; y al ser una herramienta SIEM de código abierto posibilita a que el factor económico que conlleva su aplicación sea prácticamente nulo o sin costo. Otro factor en el que incurre OSSIM AlienVault como solución SIEM es que permitió agregar una herramienta complementaria de gestión de seguridad que anteriormente era inexistente, cubriendo necesidades que ni siquiera se habían tomado en cuenta como las vulnerabilidades propias de los diferentes sistemas y activos de información de la entidad, o posibles anomalías; favoreciendo una administración de seguridad de la red más eficiente y efectivo, siendo capaz de incorporar la correlación de eventos en función del registro de logs y de una búsqueda de patrones que sugieran un posible ataque cibernético.
- La implementación de una herramienta de gestión de incidentes, eventos, amenazas proporciona una serie de beneficios en procesos de monitoreo, protección y control de los activos de información e infraestructura tecnológica

de la red de una organización, debido a los mecanismos de detección, identificación, mitigación, y protección que pueden ser aplicados en una organización, entidad, o empresa, con el fin de garantizar y conservar la confidencialidad, integridad y disponibilidad de la información.

- Uno de los beneficios de las plataformas de gestión SIEM como OSSIM AlienVault es la integración de diferentes herramientas que permiten una centralización de la administración de los activos, y con ello contar con diferentes servicios activos para el monitoreo de la red.
- La cantidad de información de los eventos de seguridad que se recopila al efectuarse la gestión de riesgos mediante procesos de escaneo, se convierte en una acción de gran importancia debido al grado de riesgo al que pueden estar expuestos cada uno de los activos de red de la organización; sean equipos de comunicaciones, dispositivos, servidores o equipos en el que el sensor con el que dispone OSSIM AlienVault debe configurarse como 'mirror' para asegurar que todo el tráfico que pasa por el switch Core (conmutador núcleo) sea monitoreado y se verifique por el SIEM para su administración. Todos los eventos registrados serán recopilados por OSSIM AlienVault y con ello, determinar si existe algún agente, código o ataque malicioso para tomar acciones correctivas o preventivas basándose en el inventario de activos gestionado.

6.2 Recomendaciones

- Previo a una implementación de un sistema de gestión para la seguridad de la información, es preciso contar con toda la información necesaria referente a la documentación que describa antecedentes suscitados o informes de rendimiento de las condiciones tecnológicas de la entidad para de esa manera establecer un diagnóstico inicial que permita identificar cada una de las falencias existentes en una determinada infraestructura tecnológica de comunicaciones de red, y a la vez detectar vulnerabilidades que representen un riesgo para la entidad gubernamental.
- La implementación de la herramienta OSSIM AlienVault debe ir en conjunto con la aplicación de controles y políticas de seguridad previamente aprobadas por el área de TIC, que ayuden a la gestión, monitoreo, concientización, resolución, corrección, prevención de incidentes, e identificación de amenazas y vulnerabilidades que puedan presentarse en la infraestructura general de la red de la organización.
- Al llevar a cabo las configuraciones iniciales de OSSIM AlienVault es recomendable contar con 2 interfaces de red, una para la administración, y otra para la recolección de la información.
- Si hubiera algún error al momento de efectuar el escaneo rápido de nuevos activos, se recomienda ejecutar directamente en el servidor el comando ‘ossim-reconfig -c -v -d’.
- Se recomienda que antes de que un servidor, aplicativo, portal, sistema, página web o cualquier plataforma tenga salida a un entorno de producción, se debe realizar un ‘scanning’ y ‘test’ de vulnerabilidades de manera periódica para

determinar posibles vulnerabilidades que dejen a la red de la organización expuesta a riesgos de seguridad.

- Es recomendable no dejar pendientes los tickets que se encuentren abiertos y tratar de cerrarlos para generar una base de datos con los registros de los eventos o incidentes suscitados.
- Se recomienda tomar en cuenta que un SIEM constituye una herramienta complementaria de seguridad para prevenir y detectar anomalías e incidentes de seguridad, pero su dependencia no debe ser en su totalidad, ya que la responsabilidad de gestión está en los análisis que puedan efectuar los encargados de TI.

BIBLIOGRAFÍA

1. Alexandra, B. M. (2019). *Monitoreo y gestión de seguridad sobre la infraestructura de red mediante la implementación de una herramienta OSSIM aplicando al sector de la mediana empresa.* Guayaquil: UG.
2. Ángel Bravo, Á. V. (2015). *Implantación de una herramienta OSSIM para el monitoreo y gestión de la seguridad de la red y plataformas Windows y Linux aplicado a empresas medianas.* Guayaquil: ESPOL.
3. Anne Kohnke, K. S. (2014). *Implementing Cybersecurity.* Florida: CRC Press.
4. Asencio, L. D. (2015). *Análisis de la herramienta OSSIM AlienVault de correlación de eventos para la seguridad de la red.* Guayaquil: UG.
5. AT&T. (2021). *AlienVault - Quick Start Guide.* Estados Unidos: AT&T.
6. AT&T. (2022). *cybersecurity.att.com.* Obtenido de https://cybersecurity.att.com/products/ossim/download
7. Auditscripts. (2022). *auditscripts.com.* Obtenido de https://www.auditscripts.com/?attachment_id=4011
8. Campos, M. A. (2020). *Implementación de un security information and event management (SIEM) para detectar vulnerabilidades y amenazas expuestas en las plataformas informáticas y redes de una entidad financiera.* Lima: UTP.
9. Chang, J. E. (2020). *Análisis de ataques cibernéticos hacia el Ecuador.* Guayas: Revista Científica Aristas - Coordinación de investigación, desarrollo tecnológico e innovación.

10. Christopher Wahl, S. P. (2014). *Networking for VMware Administrators.* Indiana, United States: VMware Press.

11. CIC. (02 de 08 de 2021). *cic.es.* Obtenido de https://www.cic.es/seguridad-de-la-informacion-y-ciberseguridad-es-lo-mismo/

12. CIS. (2021). *CIS Critical Security Controls V8.* CIS Controls.

13. CIS. (2022). *cisecurity.org.* Obtenido de https://www.cisecurity.org/controls/v8

14. CIS. (2022). *cisecurity.org.* Obtenido de https://www.cisecurity.org/controls

15. Comercio, E. (29 de 07 de 2021). *elcomercio.* Obtenido de https://www.elcomercio.com/tendencias/tecnologia/ecuador-ciberataques-america-latina-hacker.html

16. Corporation, O. (2022). *virtualbox.org.* Obtenido de https://www.virtualbox.org

17. David Carasso, S. C. (2012). *Exploring Splunk.* New York: Splunk Inc.

18. David R. Miller, S. H. (2011). *Security Information and Event Management Implementation.* USA: Mc Graw Hill - Network Pro Library.

19. Delgado, A. E. (2008). *Decereto Oficial No. 1014.* San Francisco de Quito: Registro Oficial.

20. Elastic. (2022). *elastic.co.* Obtenido de https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html

21. España, D. L. (2016). *Evaluación del Sistema de Gestión de Seguridad de la Información del Gobierno Autónomo Descentralizado de la Provincia de Esmeraldas (GADPE).* Esmeraldas: PUCE.

22. Ferruzola Gómez, E. C., & Arévalo Gamboa, L. M. (2021). *Análisis de los sistemas centralizados de seguridad informáticaa través de la herramienta Alienvault Ossim* . Babahoyo: Ecuadorian Science Journal -GDEON.

23. finid, S. a. (19 de 05 de 2020). *digitalocean.com*. Obtenido de https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-postfix-as-a-send-only-smtp-server-on-ubuntu-18-04-es

24. GADPS. (2022). *sucumbios.gob.ec*. Obtenido de https://www.sucumbios.gob.ec/

25. García, G. Á.-P. (2004). *Seguridad informática para empresas y particulares*. Madrid - España: Mc Graw Hill.

26. Gartner. (2022). *Security Information and Event Management (SIEM) Reviews and Ratings.* U.S.A.: Peer Insights.

27. Gorka Sadowski, K. K. (2020). *Critical Capabilities for Security Information and Event Management.* U.S.A.: Gartner, Inc.

28. Graylog. (2021). *Graylog Documentation.* Houston: Graylog, Inc.

29. Greenbone. (2022). *Manual Greenbone Enterprise Appliance with Greenbone OS 21.04.* Germany: Greenbone Networks GmbH.

30. Gustavo González Granadillo, S. G. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, 28.

31. Hammond, B. (16 de 02 de 2022). *fosslinux.com*. Obtenido de https://www.fosslinux.com/49953/how-to-install-and-configure-postfix-on-debian.htm

32. IEC, I. /. (2018). *ISO/IEC 27000 International Standard.* Ginebra - Suiza: 5th Edition - ISO / ICE.

33. Institute, L. (03 de 03 de 2021). *Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información.* Obtenido de https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion

34. ISACA. (2015). *Cybersecurity Fundamentals Study Guide.* USA: ISACA.

35. ISO/IEC. (2022). *International Standard ISO/IEC 27002.* Suiza: ISO/IEC - 3th Edition.

36. James C. Van Horne, J. M. (2010). *Fundamentos de Administración Financiera.* México: Pearson.

37. Jaramillo, L. E. (2022). *Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19.* Guayaquil: UCSG.

38. Kelly Kavanagh, T. B. (2020). *Magic Quadrant for Security Information and Event Management.* U.S.A.: Gartner, Inc.

39. Lima, F. d. (2018). *Implementación modular de un sistema de centralización y correlación de eventos de seguridad de la información (SIEM).* Puebla: BUAP.

40. Lorenzo, J. M. (2011). *AlienVault.* California - USA: AlienVault LC.

41. Maldonado, N. M. (2021). *Estado de la Ciberseguridad en las empresas del sector público del Ecuador: Una revisión sistemática* . Guayaquil: UPS.

42. Marchionni, E. A. (2011). *Administrador de servidores.* Buenos Aires - Argentina: 1ra edición.

43. Metron, A. (14 de 05 de 2019). *https://metron.apache.org/*. Obtenido de https://metron.apache.org/current-book/index.html

44. MINTEL. (2018 - 2021). *Plan Nacional de Gobierno Electrónico.* Quito: Subsecretaría de Gobierno Electrónico.

45. MINTEL. (2019). *Acuerdo Ministerial 025-2019.* Distrito Metropolitano de Quito: Registro Oficial.

46. MINTEL. (15 de 04 de 2019). *telecomunicaciones.gob.ec.* Obtenido de https://www.telecomunicaciones.gob.ec/mas-de-40-millones-de-ataques-al-ecuador-neutralizados-desde-el-retiro-del-asilo-a-julian-assange/

47. MINTEL. (2021). *ACUERDO MINISTERIAL 006-2021*. Distrito Metropolitano de Quito: Registro Oficial.

48. MINTEL. (2021). *Política Nacional de Ciberseguridad - Anexo.* Distrito Metropolitano de Quito: Registro Oficial.

49. MINTEL. (2022). *ACUERDO N° MINTEL-MINTEL-2022-0022*. Quito: Registro Oficial.

50. MINTEL. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador.* Quito: Registro Oficial.

51. Mozilla. (2021). *MozDef Documentation.* San Francisco: Mozilla.

52. NIST, J. T. (2021). *Security and Privacy Controls for Federal Information Systems and Organizations.* U.S.A.: NIST Special Publication. Obtenido de Security and Privacy Controls for Federal Information Systems and

53. Oficial, R. (31 de 12 de 2019). *CODIGO ORGANICO DE ORGANIZACION TERRITORIAL,*. Obtenido de https://www.cpccs.gob.ec/wp-content/uploads/2020/01/cootad.pdf

54. OSS, P. (2022). *prelude-siem.org.* Obtenido de https://www.prelude-siem.org/projects/prelude/wiki/InstallingPreludeRequirement

55. Poveda, A. F. (2015). *Propuesta de mejoramiento de la herramienta OSSIM SIEM (Open Source), para obtener los niveles óptimos de gestión en la administración de la seguridad, en una red implementada en cloud computing.* Quito: UPS.

56. Pranav Shukla, S. K. (2019). *Learning Elastic Stack.* Birmingham: Packt Publishing - 2nd Edition .

57. Project, O. (2020). *OSSEC HIDS Documentation.* Virginia: OSSEC.

58. Project, T. S. (2020). *SNORT - Users Manual.* Estados Unidos: SANS Institute.

59. Sagan, Q. . (2022). *quadrantsec.com.* Obtenido de https://quadrantsec.com/sagan_log_analysis_engine/

60. Sanchez, U. A. (2021). *Diseño, despliegue e Inteligencia de una herramienta SIEM.* Bilbao: UPV/EHU.

61. Sanders, S. O.-C. (2022). *Security Onion Documentation.* U.S.A.: Security Onion Solutions, LLC.

62. Santos, J. C. (2006). *Seguridad Informática.* Madrid: Ra-Ma.

63. SIEMonster. (2019). *SIEMonster System Administrator's Guide.* New York City: SIEMONSTER.

64. Skovfoged, H. (2022). *conscia.com.* Obtenido de https://conscia.com/blog/cis-controls-version-8/

65. SURICATA. (2022). *suricata.readthedocs.io.* Obtenido de https://suricata.readthedocs.io/en/latest/quickstart.html

66. Urbina, G. B. (2016). *Introducción a la Seguridad Informática.* MÉXICO: GRUPO EDITORIAL PATRIA - PRIMERA EDICIÓN.

67. Valarezo, C. J. (2018). *Implementación de un sistema de gestión centralizada de seguridad de información y eventos a través del software Open Source OSSIM.* Guayaquil: ESPOL.

68. Vieites, Á. G. (2014). *Enciclopedia de la Seguridad Informática.* 2da edición - Alfaomega Ra-Ma.

69. Villacreses, A. A. (2022). *Plan de fortalecimiento ante ataques informáticos del hospital de especialidades Portoviejo basados en sistemas de correlación de log.* Calceta: ESPAMMFL.

70. Walter Baluja García, C. C. (2012). *OSSIM, una alternativa para la integración de la gestión de seguridad en la red.* La Havana: CUJAE.

71. WATKINS, A. C. (2019). *Information Security Risk Management for ISO 27001 / ISO 27002.* United Kingdom: IT Governance Publishing Ltd - 3rd Edition.

72. Watkins, A. C. (2020). *IT Governance - An international guide to data security and ISO27001/ISO27002.* U.S.A.: Kogan Page Limited - 7th Edition.

73. Wazuh. (2022). *documentation.wazuh.com.* Obtenido de https://documentation.wazuh.com/current/user-manual/

74. Wojciech Kocjan, P. B. (2016). *Learning Nagios.* Brimingham, UK: Packt Publishing - Third Edition.

75. Zamora, J. M. (2019). *Monitoreo y gestión de seguridad sobre la infraestructura de red mediante la implementación de una herramienta OSSIM aplicando al sector de la mediana empresa.* Guayaquil: UG.

ANEXOS

7.3 Anexo 1 – Acuerdo

ACUERDO DE CONFIDENCIALIDAD

A efectos de proteger la confidencialidad de la información, se hace necesario la firma de un acuerdo que garantice y establezca la confianza entre las partes, de acuerdo a la normativa vigente.

Intervienen en la celebración del presente "ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN", por una parte, el Ing. Luis Alberto Muñoz Alvarez con cédula de ciudadanía Nro. 1722945688, en mi calidad de estudiante para efectos del presente instrumento en representación de la Universidad Internacional SEK; y por otro lado el Ing. Dario Eugenio García Gaibor con cédula de ciudadanía Nro. 2100555966, en mi calidad de Jefe de TICS perteneciente al GADPS, para efectos del presente instrumento en calidad de Receptor de la Información quienes libre y voluntariamente celebran el presente acuerdo.

Ambas partes intercambiarán y crearán información, y reconocen recíprocamente su capacidad para dar cumplimiento al presente instrumento, por lo que suscriben el presente Acuerdo de Confidencialidad, con base a las siguientes cláusulas que se detallan a continuación:

Primera. - Antecedentes:

El artículo 226 de la Constitución de la República del Ecuador prevé que: "Las instituciones del Estado, sus organismos y dependencias, y las servidoras o servidores públicos, tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución";

En virtud de lo establecido en el numeral 19 del artículo 66 de la Norma Suprema se dispone: "Se reconoce y garantizará a las personas: (...) El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos

1

7.4 Anexo 2 – Abreviaturas

- CIDR: Classless Inter-Domain Routing, Enrutamiento entre Dominios sin Clases
- CIS: Center for Internet Security, Centro de Seguridad en Internet
- CIS: Critical Security Controls, Controles Críticos de Seguridad
- DNS: Domain Name System, Sistema de Nombres de Dominio
- EISP: Enterprise Information Security Policy, Política de Seguridad de la Información Empresarial
- HIDS: Host-based Intrusion Detection System, Sistema de Detección de Intrusos en un Host
- ICMP: Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet
- ID: Identifier Device, Identificador de dispositivo
- IDS: Intrusion Detection System, Sistema de Detección de Intrusiones
- IP: Internet Protocol, Protocolo de Internet
- ISP: Internet Service Provider, Proveedor de servicios de Internet
- ISSP: Issue-Specific Security Policy, Políticas de Seguridad de Asuntos Específicos
- OSSIM: Open Source Security Information Management, Gestión de Información de Seguridad de Código Abierto
- OTX: Open Threat Exchange, Intercambio de Amenazas Abiertas
- RAM: Random Access Memory, Memoria de Acceso Aleatorio
- SANS: SysAdmin, Audit, Networking and Security Institute, Instituto de Auditoría, Redes y Seguridad SysAdmin
- SEM: Security Event Management, Gestión de Eventos de Seguridad

- SGSI: Information Security Management System, Sistema de Gestión de la Seguridad de la Información
- SIEM: Security Information and Event Management, Gestión de Información y Eventos de Seguridad
- SIM: Security Information Management, Gestión de Información de Seguridad
- SOC: Security Operations Center, Centro de Operaciones de Seguridad
- SysSP: System-Specific Policy, Políticas de Seguridad de Sistemas Específicos
- TCP: Transmission Control Protocol, Protocolo de Control de Transmisión
- TIC: Tecnologías de la Información y la Comunicación
- UDP: User Datagram Protocol, Protocolo de Datagramas de Usuario
- UEBA: User and Event Behavioral Analytics, Análisis de comportamiento de usuarios y eventos
- USM: Unified Security Management, Sistema de Gestión de Seguridad Unificada
- VLAN: Virtual Local Area Network, Red de Área Local Virtual
- VPN: Virtual Private Network, Red Privada Virtual

7.5 Anexo 3 – Formulario de encuesta

Encuesta General de Seguridad

1. ¿Cuál es el tipo de asignación de direcciones IP a los equipos informáticos para el acceso a la red de la entidad?

- ◯ Asignación de dirección IP dinámica
- ◯ Asignación de dirección IP estática
- ◯ Otro tipo de asignación
- ◯ Ninguna asignación

2. ¿Cuál es el modo de autenticación del personal de TIC para acceder a la información alojada en los servidores de la entidad?

- ◯ Autenticación de doble factor
- ◯ Autenticación por identificador y contraseña
- ◯ Autenticación por identificador
- ◯ Autenticación por contraseña
- ◯ Sin autenticación

3. ¿Qué activos tecnológicos se encuentran protegidos en la entidad?

- ◯ Móviles personales
- ◯ Portátiles personales
- ◯ Equipos de comunicaciones de red de la entidad
- ◯ Equipos informáticos de la entidad
- ◯ Ningún activo está protegido

4. ¿Qué tipo de registros de activos posee la entidad?

- ◯ Bitácoras
- ◯ Inventario
- ◯ Listas
- ◯ Ninguna

5. ¿Qué mecanismo de seguridad existe para el acceso a los sistemas de información de la entidad?

- ◯ Autenticación por identificador y contraseña
- ◯ Autenticación con llaves públicas y privadas
- ◯ Autenticación de doble factor
- ◯ Ningún tipo de autenticación

6. ¿La información de la entidad en qué medios es almacenada?

- ◯ Discos duros
- ◯ Discos de estado sólido
- ◯ Almacenamiento en la nube
- ◯ Ninguno

7. ¿Qué seguridad tienen los sistemas informáticos que utilizan los usuarios de la entidad?

- ◯ Software antivirus
- ◯ Otros
- ◯ Ninguna

8. ¿La red de comunicaciones de la entidad tiene algún sistema de gestión de seguridad y protección ante eventos e incidentes de riesgo?

- ◯ Sistema de monitoreo de red
- ◯ Sistema de gestión de eventos e información
- ◯ Restricciones y reglas del cortafuegos
- ◯ Ninguna

9. ¿Qué tipo de sistema existe para el acceso físico y lógico hacia el Centro de Datos y Cuartos Máquinas de la entidad?

- ◯ Sistema de autenticación biométrica
- ◯ Sistema de reconocimiento facial
- ◯ Sistema de acceso informático
- ◯ Ninguno

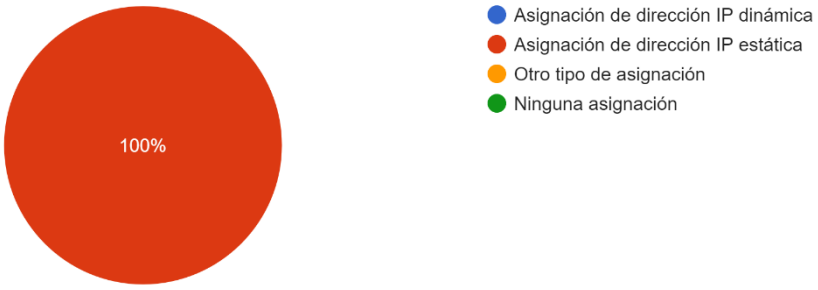
10. ¿Qué activos de información autorizados son ingresados o retirados de la entidad?

- ◯ Documentos físicos
- ◯ Dispositivos extraíbles
- ◯ Equipos informáticos
- ◯ Equipos de comunicaciones
- ◯ Ninguno

7.6 Anexo 4 – Resultados de encuesta general

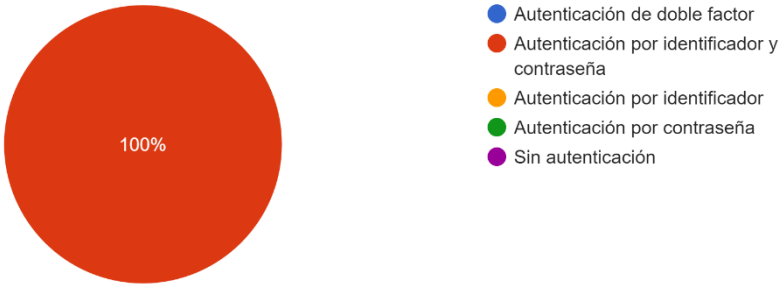
1. ¿Cuál es el tipo de asignación de direcciones IP a los equipos informáticos para el acceso a la red de la entidad?

2 respuestas



2. ¿Cuál es el modo de autenticación del personal de TIC para acceder a la información alojada en los servidores de la entidad?

2 respuestas

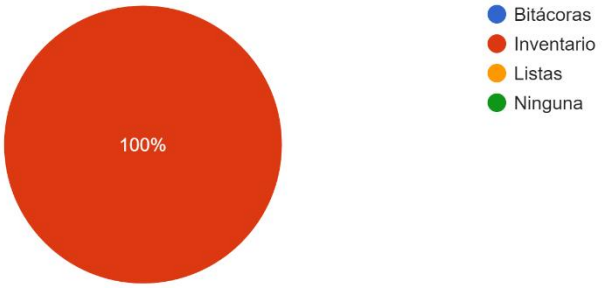


3. ¿Qué activos tecnológicos se encuentran protegidos en la entidad?

2 respuestas

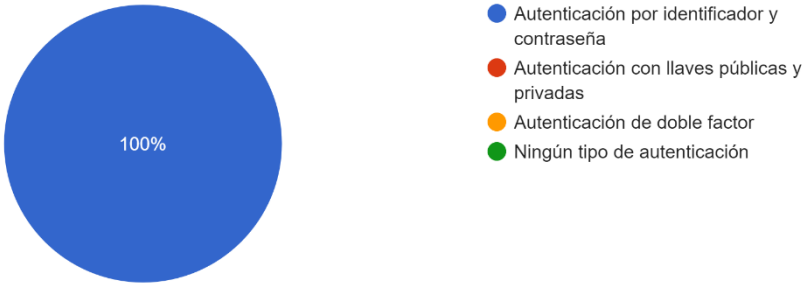
4. ¿Qué tipo de registros de activos posee la entidad?

2 respuestas



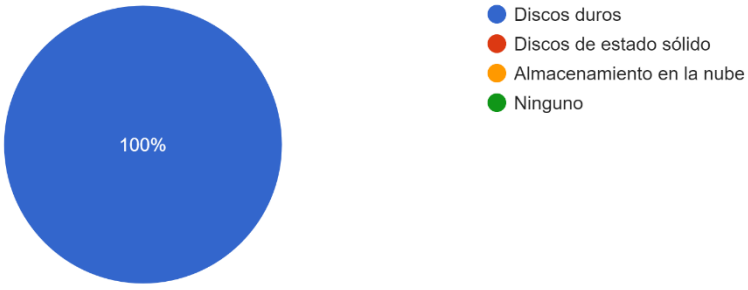
5. ¿Qué mecanismo de seguridad existe para el acceso a los sistemas de información de la entidad?

2 respuestas



6. ¿La información de la entidad en qué medios es almacenada?

2 respuestas

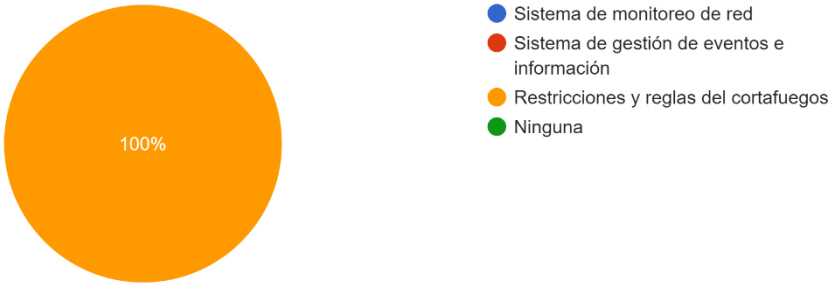


7. ¿Qué seguridad tienen los sistemas informáticos que utilizan los usuarios de la entidad?

2 respuestas

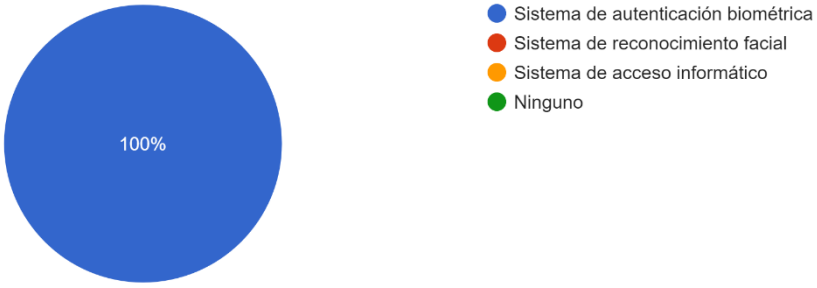
8. ¿La red de comunicaciones de la entidad tiene algún sistema de gestión de seguridad y protección ante eventos e incidentes de riesgo?

2 respuestas



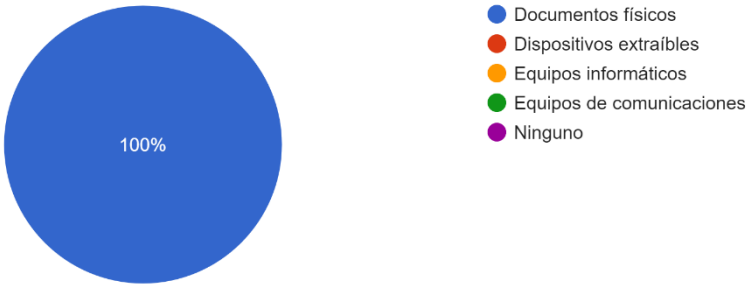
9. ¿Qué tipo de sistema existe para el acceso físico y lógico hacia el Centro de Datos y Cuartos Máquinas de la entidad?

2 respuestas



10. ¿Qué activos de información autorizados son ingresados o retirados de la entidad?

3 respuestas



7.7 Anexo 5 – Formulario de encuesta 2

Encuesta General de Seguridad 2

1. ¿Desde la creación de la entidad, el número de usuarios se ha incrementado por cada departamento?

- ◯ Si
- ◯ No

2. ¿En la entidad se han realizado adaptaciones e incremento de nuevos nodos de red?

- ◯ Si
- ◯ No

3. ¿La entidad cuenta con una nómina actualizada de funcionarios por cada departamento?

- ◯ Si
- ◯ No

4. ¿La entidad dispone de sistemas automatizados de procesos por cada departamento?

- ◯ Si
- ◯ No

5. ¿El departamento de TIC ha implementado un esquema de seguridad de las Bases de Datos de la entidad?

- ◯ Si
- ◯ No

6. ¿El departamento de informática de la entidad ha implementado políticas de seguridad para la gestión de la información?

- ◯ Si
- ◯ No

7. ¿El personal de la entidad tiene conocimiento de las políticas de seguridad existentes?

- ◯ Si
- ◯ No

8. ¿En cada departamento de la entidad se cuenta con políticas de seguridad específicas del área?

- ◯ Si
- ◯ No

9. ¿Los funcionarios de la entidad tienen conocimiento sobre los activos y recursos de información existentes?

- ◯ Si
- ◯ No

10. ¿Los funcionarios de la entidad tienen conocimiento de las responsabilidades sobre el uso de recursos y activos de información que tienen a su cargo?

- ◯ Si
- ◯ No

11. ¿La entidad dispone de un control de acceso para que solo el personal del departamento de TIC pueda acceder a los activos, recursos, sistemas y equipos de información?

- ◯ Si
- ◯ No

12. ¿La entidad ha establecido controles de usuario restrictivos de acuerdo a cada perfil?

- ◯ Si
- ◯ No

13. ¿En la entidad se realiza el mantenimiento preventivo y correctivo de los activos y equipos de información al menos 2 veces por año?

- ◯ Si
- ◯ No

14. ¿En la entidad se realiza el mantenimiento preventivo y correctivo del cableado estructurado por cada departamento?

- ◯ Si
- ◯ No

15. ¿El departamento de TIC de la entidad tiene un esquema de procedimientos cuando se presenta algún fallo o anomalía en los activos, sistemas o equipos de información?

- ◯ Si
- ◯ No

16. ¿El departamento de TIC realiza el monitoreo de los sistemas y red de la entidad?

- ◯ Si
- ◯ No

17. ¿La entidad cuenta con un inventario de activos y equipos de información?

- ◯ Si
- ◯ No

18. ¿El departamento de TIC de la entidad tiene personal especializado en seguridad de la información?

- ◯ Si
- ◯ No

19. ¿El departamento de TIC realiza el respaldo de información generado en la entidad?

- ◯ Si
- ◯ No

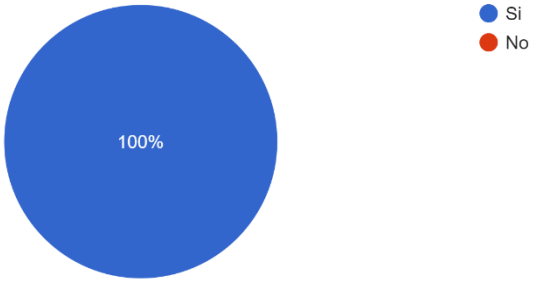
20. ¿La entidad ha implementado políticas de renovación de equipos, dispositivos y cableado de la infraestructura de red?

- ◯ Si
- ◯ No

7.8 Anexo 6 – Resultados de encuesta general 2

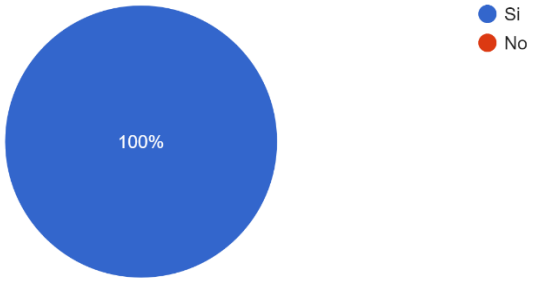
1. ¿Desde la creación de la entidad, el número de usuarios se ha incrementado por cada departamento?

3 respuestas



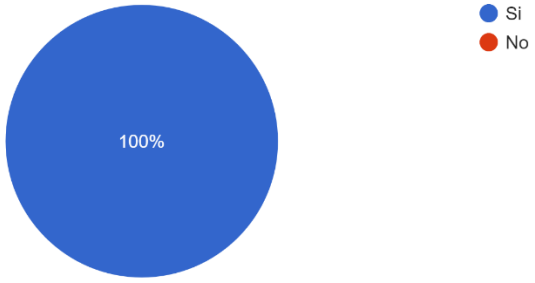
2. ¿En la entidad se han realizado adaptaciones e incremento de nuevos nodos de red?

3 respuestas



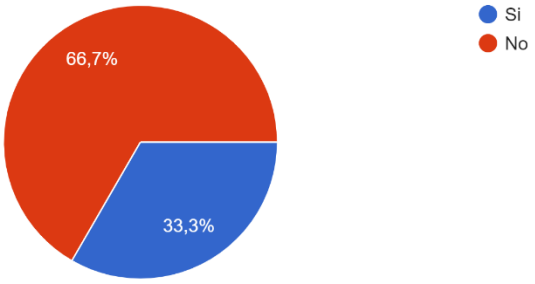
3. ¿La entidad cuenta con una nómina actualizada de funcionarios por cada departamento?

3 respuestas



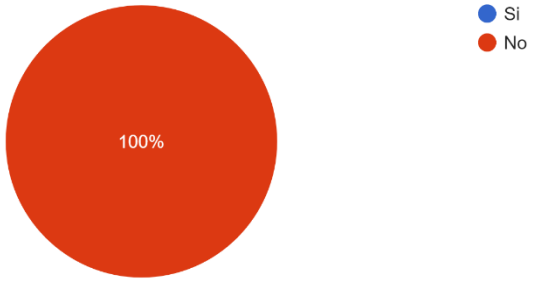
4. ¿La entidad dispone de sistemas automatizados de procesos por cada departamento?

3 respuestas



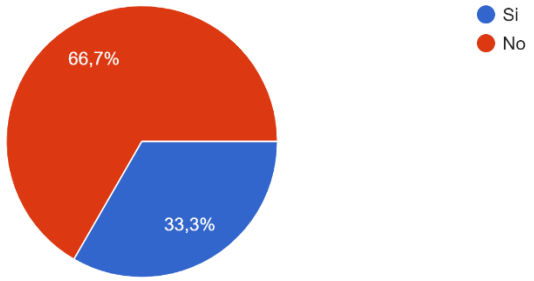
5. ¿El departamento de TIC ha implementado un esquema de seguridad de las Bases de Datos de la entidad?

3 respuestas



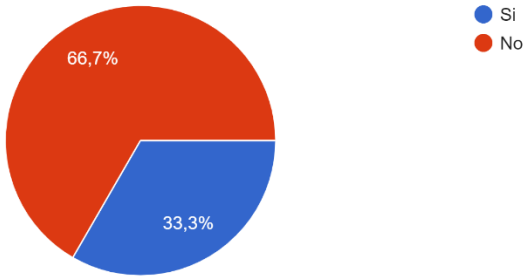
6. ¿El departamento de informática de la entidad ha implementado políticas de seguridad para la gestión de la información?

3 respuestas



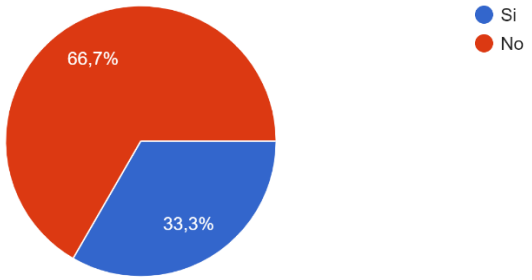
7. ¿El personal de la entidad tiene conocimiento de las políticas de seguridad existentes?

3 respuestas



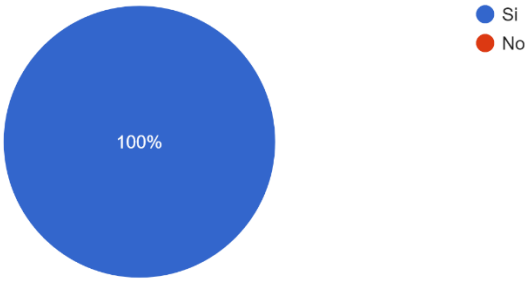
8. ¿En cada departamento de la entidad se cuenta con políticas de seguridad específicas del área?

3 respuestas



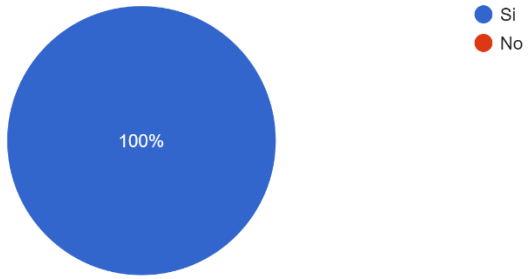
9. ¿Los funcionarios de la entidad tienen conocimiento sobre los activos y recursos de información existentes?

3 respuestas



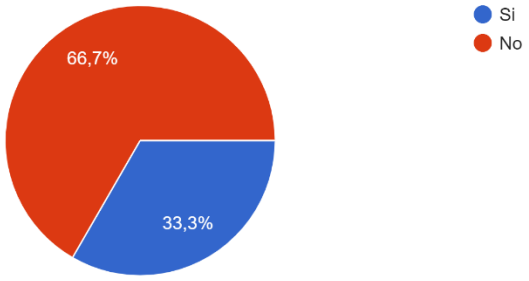
10. ¿Los funcionarios de la entidad tienen conocimiento de las responsabilidades sobre el uso de recursos y activos de información que tienen a su cargo?

3 respuestas



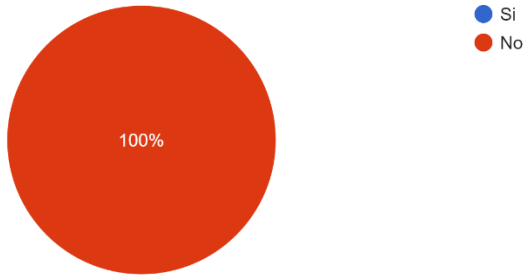
11. ¿La entidad dispone de un control de acceso para que solo el personal del departamento de TIC pueda acceder a los activos, recursos, sistemas y equipos de información?

3 respuestas



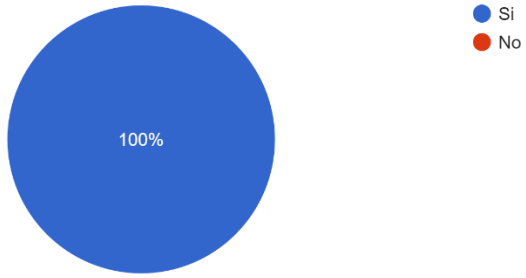
12. ¿La entidad ha establecido controles de usuario restrictivos de acuerdo a cada perfil?

3 respuestas



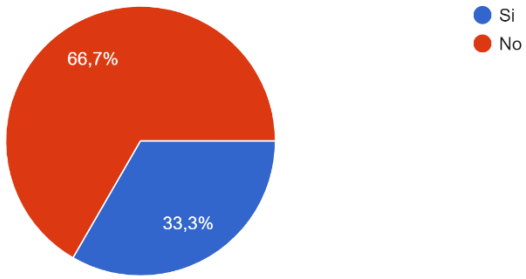
13. ¿En la entidad se realiza el mantenimiento preventivo y correctivo de los activos y equipos de información al menos 2 veces por año?

3 respuestas



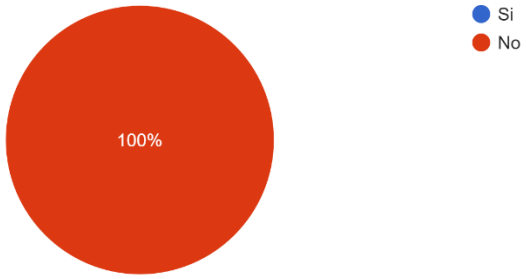
14. ¿En la entidad se realiza el mantenimiento preventivo y correctivo del cableado estructurado por cada departamento?

3 respuestas



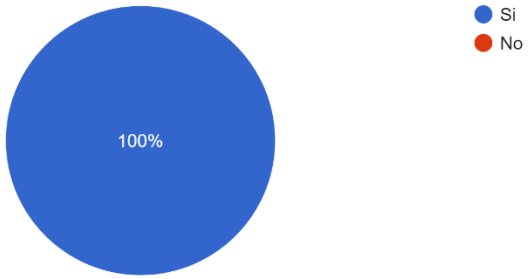
15. ¿El departamento de TIC de la entidad tiene un esquema de procedimientos cuando se presenta algún fallo o anomalía en los activos, sistemas o equipos de información?

3 respuestas



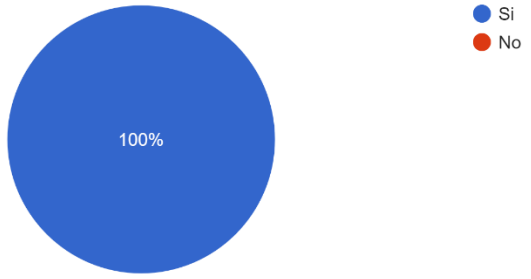
16. ¿El departamento de TIC realiza el monitoreo de los sistemas y red de la entidad?

3 respuestas



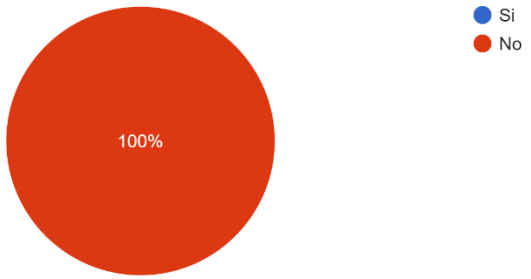
17. ¿La entidad cuenta con un inventario de activos y equipos de información?

3 respuestas



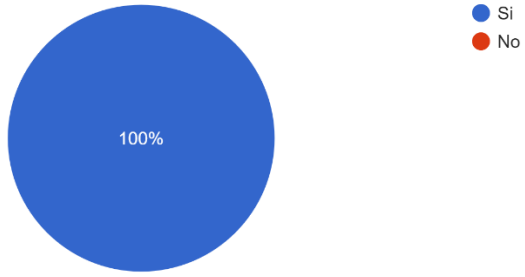
18. ¿El departamento de TIC de la entidad tiene personal especializado en seguridad de la información?

3 respuestas



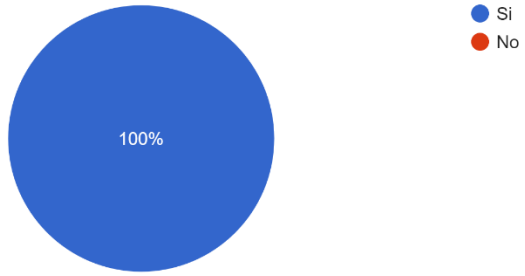
19. ¿El departamento de TIC realiza el respaldo de información generado en la entidad?

3 respuestas



20. ¿La entidad ha implementado políticas de renovación de equipos, dispositivos y cableado de la infraestructura de red?

3 respuestas



7.9 Anexo 7 – Resultados

AuditScripts **Critical Security Controls Executive Assessment Tool (v8.0a)** enclave SECURITY

Riesgo abordado: 11%

Riesgo Aceptado: 89%

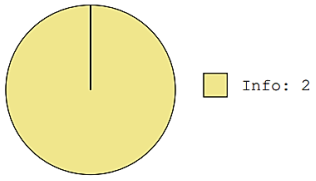
Inventario y Control de Activos	
¿La organización ha mantenido un inventario completo de los activos informáticos que deben protegerse?	**No Implementado**
¿La organización ha implementado herramientas de escaneo para identificar dispositivos conectados a la red?	**Implementado en todos los Sistemas**
Inventario y Control de Activos de Software	
¿La organización ha implementado herramientas de escaneo para identificar las aplicaciones de software instaladas?	**No Implementado**
¿La organización ha implementado una herramienta de lista blanca de software para permitir la ejecución de programas de software autorizados en los sistemas utilizados?	**No Implementado**
Gestión continua de vulnerabilidades	
¿La organización ha implementado herramientas de escaneo para identificar cualquier vulnerabilidad de software en los sistemas utilizados?	**No Implementado**
¿La organización ha implementado un sistema de administración de parches automatizado para actualizar continuamente los sistemas utilizados?	**No Implementado**
Administración de cuentas	
¿La organización ha implementado una herramienta de escaneo para hacer un inventario de usuarios con derechos administrativos elevados en los sistemas utilizados?	**No Implementado**
¿Se ha asegurado la organización de que solo los usuarios con necesidades comerciales obtengan derechos administrativos elevados en los sistemas utilizados?	**Implementado en todos los Sistemas**
Configuración segura de activos y software	
¿La organización ha implementado herramientas de escaneo para identificar cualquier configuración de seguridad mal configurada en los sistemas utilizados?	**No Implementado**
¿La organización ha implementado un sistema de cumplimiento de configuración de seguridad en los sistemas utilizados?	**No Implementado**
Gestión de registros de auditoría	
¿La organización ha habilitado el registro de auditoría completo en cada uno de sus sistemas de información críticos?	**No Implementado**
¿La organización ha agregado de forma centralizada sus registros de auditoría críticos en una plataforma de gestión de eventos e información de seguridad?	**No Implementado**

7.10 Anexo 8 – Reporte

AlienVault: I.T Security Vulnerability Report

Scan time:	-	Generated:	2022-08-02 23:12:52

Total number of vulnerabilities identified on 1 system(s)



Total number of vulnerabilities identified per system

HostIP	HostName	Critical	High	Med	Low	Info
192.168.2.23	Host-192-168-2-23	--	--	--	--	2

7.11 Anexo 9 – Reporte

192.168.2.23	Host-192-168-2-23

OS Detection Consolidation and Reporting

Risk: Info
Application: general
Port: 0
Protocol: tcp
Script ID: 105937

Vulnerability Detection Result:
Best matching OS:
OS: Linux Kernel
CPE: cpe:/o:linux:kernel
Found by NVT: 1.3.6.1.4.1.25623.1.0.102002 (Operating System (OS) Detection (ICMP))
Concluded from ICMP based OS fingerprint
Setting key "Host/runs_unixoide" based on this information

CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:
This script consolidates the OS information detected by several
VTs and tries to find the best matching OS.
Furthermore it reports all previously collected information leading to this best matching OS. It
also reports possible additional information which might help to improve the OS detection.
If any of this information is wrong or could be improved please consider to report these to the
referenced community portal.
References:
URL:https://community.greenbone.net/c/vulnerability-tests

CVSS Base Score:
0.0

Family name:
Product detection

Category:
infos

Created:
2016-02-19T10:19:54Z

Modified:
2022-04-05T09:27:51Z

7.12 Anexo 10 – Reporte

Traceroute

Risk: Info
Application: general
Port: 0
Protocol: tcp
Script ID: 51662

Vulnerability Detection Result:
Network route from scanner (192.168.2.20) to target (192.168.2.23):
192.168.2.20
192.168.2.23
Network distance between scanner and target: 2

CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N

Summary:
Collect information about the network route and
network distance between the scanner host and the target host.

Insight:
For internal networks, the distances are usually
small, often less than 4 hosts between scanner and target. For public targets the
distance is greater and might be 10 hosts or more.

Vulnerability Detection Method:
A combination of the protocols ICMP and TCP is used
to determine the route. This method is applicable for IPv4 only and it is also known as
'traceroute'.

CVSS Base Score:
0.0

Family name:
General

Category:
infos

Created:
2010-07-08T17:27:45Z

Modified:
2021-03-12T14:25:59Z

7.13 Anexo 11 – Manual