UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN SISTEMAS INFORMÁTICOS

TEMA: IMPLEMENTACIÓN DE UN SIEM PARA EL COMANDO DE CIBERDEFENSA UTILIZANDO HERRAMIENTAS DE CÓDIGO ABIERTO BAJO EL ESTÁNDAR ISO 27032

AUTOR: JUMBO VIVANCO PEDRO LUIS

TUTOR: ING. CARRIÓN JUMBO JOE LUIS, PhD.

QUITO- ECUADOR

AÑO: 2019

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: “IMPLEMENTACIÓN DE UN SIEM PARA EL COMANDO DE CIBERDEFENSA UTILIZANDO HERRAMIENTAS DE CÓDIGO ABIERTO BAJO EL ESTÁNDAR ISO 27032”, ha sido desarrollado por el señor Pedro Luis Jumbo Vivanco con C.C. No. 1721344099 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

_____

Pedro Luis Jumbo Vivanco

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación **"IMPLEMENTACIÓN DE UN SIEM PARA EL COMANDO DE CIBERDEFENSA UTILIZANDO HERRAMIENTAS DE CÓDIGO ABIERTO BAJO EL ESTÁNDAR ISO 27032"**, presentado por Pedro Luis Jumbo Vivanco, estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D.M., 12 de marzo de 2019

TUTOR

Ing. Joe Carrión Jumbo, PhD.

AGRADECIMIENTOS

En primer lugar, quisiera agradecer a mis padres que me han ayudado y apoyado en cada etapa de mi vida, ellos conocen de la dedicación con la que hago las cosas y el esfuerzo que le pongo a cada objetivo que me propongo. Agradezco la elaboración de este trabajo a varios compañeros de trabajo que me han colaborado con su valioso tiempo durante el desarrollo de la investigación.

Un agradecimiento especial a mi profesor y tutor, Ing. Joe Carrión, por tomarse de su valioso tiempo para orientar con sus consejos y conocimiento a la elaboración de este trabajo, realmente ha sido una experiencia gratificante haber trabajado bajo su dirección.

Así mismo, deseo expresar mi reconocimiento a todos mis profesores ya que tienen la paciencia para impartir sus conocimientos, han sido una motivación constante para seguir estudiando y ser un mejor profesional.

A todos mis amigos y futuros colegas por todo el apoyo recibido para la finalización de este trabajo con su apoyo moral se ha logrado llegar hasta este objetivo.

A la Universidad Tecnológica Israel por ser la sede de todo el conocimiento adquirido en estos años y brindarme las oportunidades de crecer académicamente.

DEDICATORIA

Este trabajo está dedicado a:

A mis padres Luis Bolívar y Ninfa Aida quienes me han enseñado el sentido de la responsabilidad, ellos me han enseñado que el mejor conocimiento que se puede tener es el que se aprende por sí mismo y que las metas se logran una a una con esfuerzo y dedicación.

A mis hermanos Marjorie Elizabeth, Luis Bolívar y Victoria Nathaly por su apoyo moral durante todo este proceso y a toda mi familia porque con sus consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Finalmente quiero dedicar esta tesis a todas mis amigos y amigas de la universidad, por apoyarnos en todas las circunstancias y en todos los momentos compartidos dentro y fuera de aulas, por ser un grupo cohesionado, divertido y que siempre supimos salir adelante, al llegar a finalizar esta etapa me siento orgulloso de haber sido parte de ustedes y espero que próximamente nos volvamos a encontrar y que todos cumplamos ésta y más metas.

TABLA DE CONTENIDOS

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

Este trabajo de tesis fue realizado para el Comando de Ciberdefensa de las FF.AA., bajo las directrices del estándar ISO 27032 que orienta en la mejora de la seguridad de las redes de sistemas.

Se inició realizando un levantamiento de información que permitió evaluar los riesgos de la red, a partir de esta evaluación se determinó los puntos vulnerables en la misma. Las especificaciones técnicas requeridas por el sistema SIEM implementado fueron evaluadas de acuerdo con las características basadas en la norma ISO 25000 de Evaluación de Calidad del Software.

Con la implementación se comprobó la hipótesis planteada que determina que el sistema SIEM permite la detección automática y respuesta oportuna de las amenazas tecnológicas en tiempo real.

Palabras clave: SIEM, PDCA, ISO 27032, ISO 25000, Magerit, riesgos, seguridad de la información.

ABSTRACT

This thesis work was made for the Cyber Defense Command of the Armed Forces, under the guidelines of the ISO 27032 standard that guides in the improvement of the security of the systems networks.

It was started by carrying out an information survey that made it possible to evaluate the risks of the network, based on this evaluation, the vulnerabilities in the network were determined. The technical specifications required by the implemented SIEM system were evaluated in accordance with the characteristics based on the ISO 25000 standard for Software Quality Assessment.

With the implementation, the hypothesis that determines that the SIEM system allows automatic detection and timely response of technological threats in real time was verified.

Key Words: SIEM, PDCA, ISO 27032, ISO 25000, Magerit, information security.

INTRODUCCIÓN

El ciberespacio es un entorno complejo que resulta de la interacción de personas, software y servicios en Internet, respaldado por dispositivos de tecnología de la información y las comunicaciones (TIC) distribuidos en todo el mundo y redes conectadas. Sin embargo, hay problemas de seguridad que no están cubiertos por las mejores prácticas actuales de seguridad de la información, seguridad de Internet, seguridad de la red y seguridad de las TIC, ya que existen brechas entre estos dominios, así como una falta de comunicación entre las organizaciones y los proveedores en el ciberespacio. Esto se debe a que los dispositivos y las redes conectadas al ciberespacio tienen múltiples propietarios, cada uno con sus propios intereses comerciales, operativos y regulatorios. Los objetivos diferentes por cada organización o proveedores en el ciberespacio han dado como resultado un estado de seguridad fragmentado para el aprovechamiento de vulnerabilidades.

Las sofisticadas amenazas cibernéticas se han convertido en un adversario importante en el ciberespacio de las Fuerzas Armadas, debido a que las tecnologías de defensa son cada vez más vulneradas. Las Fuerzas Armadas de la mayoría de los países han reconocido al quinto dominio como el ciberespacio y las amenazas existentes en el mismo.

Las amenazas tecnológicas ponen en riesgo las operaciones militares y es por eso que las unidades de tecnologías y comunicaciones de las Fuerzas Armadas ponen énfasis en aplicar medidas de contingencia en las redes militares y de esta manera prevenir la pérdida o atentado a la seguridad de la información ya que esto ocasiona un grave peligro, debido a que se maneja información sensible de personal militar y medios tecnológicos desplegados en operaciones propias de Fuerzas Armadas.

ANTECEDENTES DE LA SITUACIÓN OBJETO DE ESTUDIO

Mediante acuerdo Ministerial 281 del 12 de septiembre del 2010, en el Art. 7, El Comando de Ciberdefensa, se conforma como un Comando del Comando Conjunto de las FF.AA., integrado por personal técnico y operativo civil y militar; y tendrá la misión

de operar con las capacidades de defensa, exploración y respuesta en el espacio cibernético, para proteger y defender la infraestructura crítica de FF.AA. e información estratégica del Estado.

El Comando de Ciberdefensa cuenta con tres procesos principales: Defensa, Exploración y Respuesta, los que permiten proteger la infraestructura crítica digital en el ámbito de las FF.AA. y sus unidades adscritas. El proceso que se pretende sistematizar es Defensa, ya que tiene la misión de proteger la infraestructura e información digital y detectar cualquier evento o anomalía presente en las redes de datos del Comando de Ciberdefensa, con el fin de neutralizarlas y mitigar su impacto, para de esta manera cumplir con el Plan de Ciberdefensa descrito en el estatuto del Comando Conjunto de las FF.AA.

Las Directrices contempladas en el estatuto de procesos del Comando Conjunto para el Comando de Ciberdefensa son las siguientes:

- El Comando de Ciberdefensa efectuará operaciones de Defensa y Exploración en el Ciberespacio en forma permanente, protegiendo la infraestructura crítica tecnológica de FF.AA. y otras asignadas, degradando o neutralizando la infraestructura crítica tecnológica del adversario con orden, a fin de contribuir al cumplimiento de la misión del Comando Conjunto de las FF.AA.

- Las operaciones de Defensa, Exploración y Respuesta permitirán que la infraestructura esté segura y se pueda alertar a tiempo a posibles ciberataques de nivel global sea de estados o grupos antagónicos.

PLANTEAMIENTO DEL PROBLEMA

En el Comando de Ciberdefensa denominado más adelante con las siglas COCIBER[1] se mantiene instalada una solución de marca Checkpoint que se encargaba del monitoreo permanente de la red y de la seguridad de sus dispositivos, actualmente dicha solución ya no cuenta con soporte y actualizaciones de seguridad debido a la expiración del contrato con la empresa proveedora, esto ha ocasionado que varios eventos de seguridad pasen desapercibidos en la red. Según el administrador de la red, varios de estos eventos ya han sido mitigados o neutralizados, pero a pesar de ello se siguen

[1] COCIBER: Comando de Ciberdefensa

produciendo intentos de violaciones a la seguridad. Desde enero hasta diciembre de 2018 se han tratado 42 eventos que han puesto en riesgo la seguridad de la información, las estadísticas se muestran en las siguientes figuras.

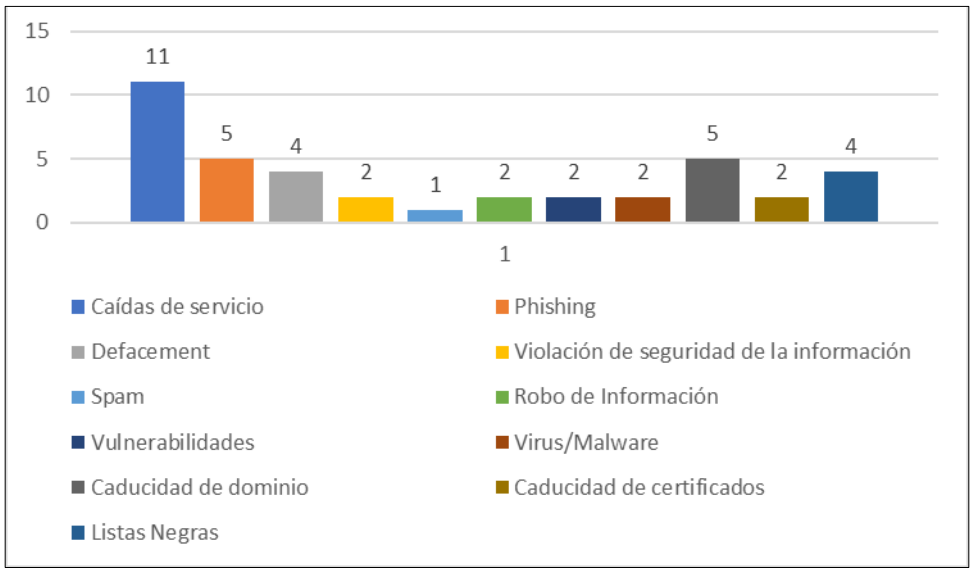


Figura 1. Incidentes Comando de Ciberdefensa 2018

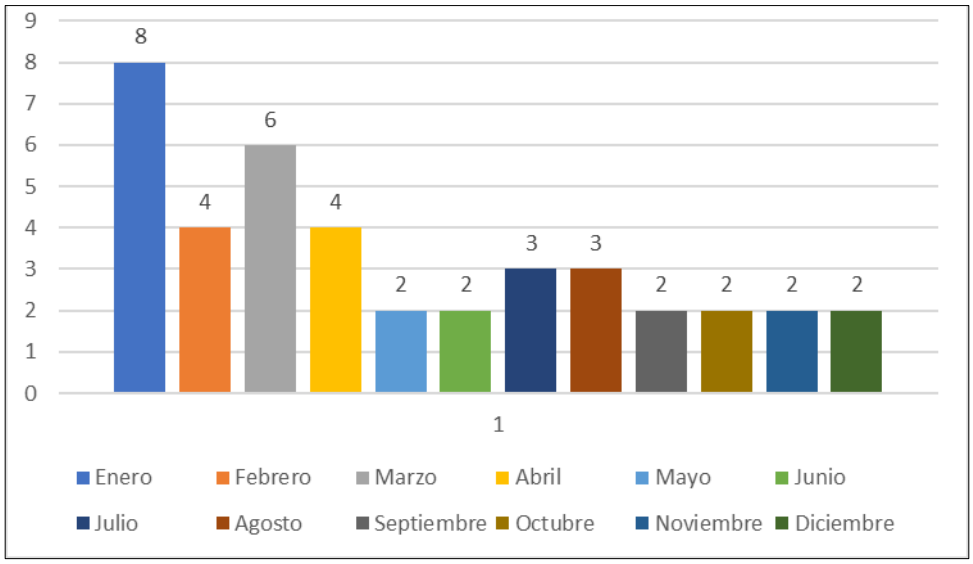


Figura 2. Incidentes Comando de Ciberdefensa 2018

Debido a que los eventos e incidentes de seguridad han sido mitigados después de haberse materializado, el COCIBER ha manifestado la necesidad de implementar un sistema de seguridad que permita la detección de eventos e incidentes de seguridad en la red en tiempo real, y de esta forma evitar intrusiones en la red, que sirva para tomar las medidas preventivas y correctivas en la red e informar oportunamente al mando.

Hay que considerar que si el COCIBER no implementa un sistema para la administración de incidentes de seguridad en la red no será capaz de reaccionar

efectivamente ante las amenazas constantes que atentan a su seguridad y la materialización de una amenaza constituirá un grave riesgo a la información, continuará expuesto a vulnerabilidades y propenso exponencialmente a nuevos ataques.

JUSTIFICACIÓN

Actualmente las organizaciones ya sean de tipo pública o privada realizan lo posible para hacer que las grandes cantidades de registros de sus sistemas sean más comprensibles y fáciles de manejar. Por ejemplo, en el caso de intrusiones de seguridad internas o externas, deberían contar con un sistema que registre todas estas intrusiones para determinar qué sucedió y asegurar las brechas de seguridad o corregir las vulnerabilidades explotadas, por eso es importante tener un sistema SIEM donde todos los eventos e incidentes se almacenen y analicen de acuerdo con los criterios específicos de la organización. Los cortafuegos o los sistemas de seguridad perimetrales ya no son suficientes para prevenir a las instituciones de los ataques informáticos y es ahí donde los sistemas SIEM desarrollan una función importante, que es identificar las posibles actividades maliciosas y tener la capacidad de normalizar y correlacionar los datos de registros de múltiples fuentes y agentes instalados en la red.

El SIEM permitirá visualizar con detalladamente el tráfico de la red del COCIBER y las vulnerabilidades existentes en la misma o en los dispositivos conectados, una vez analizadas las vulnerabilidades, éstas serán priorizadas y correlacionadas, a fin de determinar el nivel de riesgo e impacto que tienen en el COCIBER.

El COCIBER es la unidad encargada de almacenar y proteger la información obtenida de los sistemas de TI de varias unidades militares de FF.AA. por lo que cualquier robo o pérdida de ésta pondría en riesgo la seguridad de las operaciones y del personal. Para el funcionamiento correcto del sistema SIEM en el COCIBER se deberá contar con un sistema de gestión de eventos e incidentes en la red, para así aplicar las configuraciones y políticas adecuadas que permitirán la correlación y priorización de los eventos generados. Una vez que el sistema SIEM entre en funcionamiento se categorizan los eventos e incidentes y se generan los reportes, determinando el nivel de riesgo encontrado lo que daría paso a la gestión de incidentes, misma que sería otro caso de estudio.

OBJETIVOS

GENERAL

Implementar un SIEM para la detección y mitigación de eventos e incidentes de seguridad en el Comando de Ciberdefensa de las FF.AA.

OBJETIVOS ESPECÍFICOS

- Realizar un análisis de riesgos de la red del Comando de Ciberdefensa para determinar los tipos y valoración de los dispositivos.
- Realizar un análisis comparativo de los sistemas SIEM de libre distribución en base al estándar ISO 25000 para seleccionar la mejor opción.
- Implementar el Sistema de gestión de eventos y seguridad de la información.

DESCRIPCIÓN DE LOS CAPÍTULOS

En el capítulo uno se describe los conceptos teóricos de los sistemas SIEM, las tecnologías que serán utilizadas y la terminología para el desarrollo del proyecto. Además de establecer los objetivos a los que se pretende llegar con la implementación de un SIEM.

En el capítulo dos se describe el tipo de investigación realizada que permite obtener la mayor cantidad posible de información que ayude a la implementación de un sistema SIEM, además de describir las técnicas utilizadas y el análisis realizado para determinar el entorno de instalación.

En el capítulo tres se expondrá la propuesta del proyecto, en esta sección se explicará la relación que tienen las metodologías a utilizar con la implementación del SIEM, además de ellos se exponen los requerimientos técnicos de hardware, software y personal que serán necesarios para el SIEM.

En el capítulo cuatro se encuentra la sección de la implementación y es ahí donde se aplica todas las actividades mencionadas anteriormente, desde el análisis de riesgos realizado hasta la implementación se realizó utilizando metodologías y normas que aseguran un buen sistema de gestión de incidentes.

CAPÍTULO 1

FUNDAMENTACIÓN TEÓRICA

1.1 ESTADO DEL ARTE

Los sistemas SIEM tienen como objetivo monitorear los eventos relacionados con la seguridad de los activos[2] de TI[3] de la empresa, incluida la red de datos, los sistemas de defensa perimetral, dispositivos de prevención de intrusos, servidores de aplicaciones, bases de datos y cuentas de usuario. Cada activo puede ser monitoreado usando una variedad de sensores y mantener el registro. El SIEM recibe información de eventos de los sensores y los archivos de registro y activas alertas que indican posibles comportamientos maliciosos, tanto en el perímetro de la red como en la empresa. Cuando se activa una alerta, el personal administrador de la red determina si se produjo una actividad de rutina y es simplemente inofensiva, o si los eventos indican una gran probabilidad de actividad maliciosa en la que habrá que actuar. En este último caso, la alerta se envía al equipo que coordina la respuesta a incidentes y las actividades forenses con los encargados de servidores y aplicaciones involucradas. En casos extremos, el equipo también debe coordinar con los recursos humanos internos, los ejecutivos legales y la aplicación de la ley.

La efectividad de un SIEM depende también de las capacidades analíticas y forenses de los técnicos o personal administrador, de la reacción que presentan frente a las amenazas y de su conocimiento en redes y sistemas para evitar que la información sea alterada o vulnerada.

Existe similitud del presente proyecto con otros realizados anteriormente que pueden servir como guía, ya sea, realizando el análisis de vulnerabilidades, evaluación para la

[2] Activo: cualquier cosa que tenga valor para las personas o la organización: software, información, equipos informáticos, servicios, entre otros.

[3] Tecnologías de la Información: aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos.

selección de la herramienta SIEM o en la implementación. Al final se realiza una tabla donde se comparan los proyectos mencionados y el actual:

Implementación de un Security Information and Event Management –Siem– En el Comando de la Armada Nacional.

Este sistema SIEM fue implementado en la Dirección de Tecnologías de la Información y las Comunicaciones del Comando de la Armada Nacional de Colombia, en la fase inicial realiza el levantamiento de plataformas y activos tecnológicos para luego realizar una selección de una herramienta SIEM de código libre y de bajo costo, la implementación ha servido para tomar decisiones más ágiles y certeras para la mitigación de los riesgos presentados por estos ataques en la entidad.

Análisis y selección de una herramienta para administración y obtención de información de eventos críticos de seguridad informática para la infraestructura del Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL

El trabajo es un caso de estudio que tenía la finalidad de comparar y seleccionar un sistema de seguridad de la información y gestión de eventos - SIEM, para esto se implementó dos sistemas de software licenciado (con versiones demo) y una herramienta de software libre con el fin de analizar los datos de fuentes críticas en seguridad de la información y con esto determinar cuál es la herramienta que tiene el mejor desempeño, bondades y que se acople de la mejor manera a la infraestructura del Ministerio de Telecomunicaciones y de la Sociedad de la Información.

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.

Este trabajo de grado presenta un análisis de la seguridad de la infraestructura de red y de los servidores en una empresa privada, el enfoque principal es de mantener centralizado todos los eventos “logs” que son generados por los diferentes servidores y equipos de red en una sola consola de administración y realizar un análisis detallado de cada evento, así mismo como obtener reportes personalizados de las vulnerabilidades existentes en los hosts que corren bajo el sistema operativo Windows, de ataques

ocasionados y del estado de la red en general.

Security Information and Event Management Tools and Insider Threat Detection

El trabajo fue realizado para una maestría de la ciencia en sistemas y ciberoperaciones, proporciona información de antecedentes sobre los componentes y la funcionalidad de las herramientas de SIEM, resume los casos históricos de amenazas internas para determinar motivaciones comunes, proporciona una visión general de las investigaciones de seguridad militar y las acciones administrativas para determinar las fuentes candidatas para la correlación de SIEM, y proporciona una descripción general de Métodos de exfiltración de datos por parte de maliciosos. En el ámbito militar se puede usar un SIEM para identificar y prevenir posibles amenazas internas al correlacionar las actividades de la red de un individuo con la investigación de antecedentes y la información de acción administrativa.

A continuación, se presentan las diferencias que se encuentran en trabajos anteriores y como el proyecto actual los complementa:

Tabla 1.0.1. Diferencias del proyecto actual con proyectos anteriores

PROYECTO	**FASES REALIZADAS**		
	ANÁLISIS DE RIESGOS	SELECCIÓN DE UN SIEM	IMPLEMENTACIÓN
Implementación de un Security Information and Event Management –SIEM– en el Comando de la Armada Nacional.		X	X
Análisis y selección de una herramienta para administración y obtención de información de eventos críticos de seguridad informática para la infraestructura del Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL		X	
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	X		X
Security Information and Event Management Tools and Insider Threat Detection	X	X	
IMPLEMENTACIÓN DE UN SIEM PARA EL COMANDO DE CIBERDEFENSA UTILIZANDO HERRAMIENTAS DE CÓDIGO ABIERTO BAJO EL ESTÁNDAR ISO 27032.	**X**	**X**	**X**

Fuente: Autor

1.2 LÓGICA DEL NEGOCIO

El COCIBER es un Comando del Comando Conjunto de las FF.AA. que tiene la misión de operar con las capacidades de defensa, exploración y respuesta en el espacio cibernético, para proteger y defender la infraestructura crítica de Fuerzas Armadas e información estratégica del Estado, sus procesos se muestran en la figura 1.3.

Figura 1.1 Representación Gráfica del Resultado de la Observación
Fuente: COCIBER

El SIEM será implementado para el proceso de Defensa del COCIBER el mismo que tiene el propósito de: "efectuar operaciones de Defensa en forma permanente de la infraestructura crítica digital de FF.AA. y unidades adscritas", algunas de sus actividades son:

- Configurar herramientas para realizar el monitoreo de redes y páginas web.
- Realizar el Monitoreo de disponibilidad confidencialidad e integridad de Servicios intranet y extranet de infraestructura crítica digital de FF.AA. y unidades adscritas.
- Informes periódicos de Monitoreo.
- Analizar la base de conocimientos para tratar incidentes.
- **Gestión de Incidentes**

Dentro del proceso de gestión de incidentes se debe tener en cuenta que una parte fundamental es la detección y análisis de incidentes, este aspecto se realiza de forma manual y mediante la detección de alguna firma detectada por el antivirus. El SIEM permite que esta detección se realice de forma automática ya que toma múltiples eventos

aislados que pueden convertirse en un solo incidente de seguridad relevante, para ello se toman parámetros, tales como:

- Dirección IP de origen y destino
- Tipo de ataque
- Tipo de malware instalado en sistemas comprometidos
- La hora en que comenzó o terminó la actividad.
- Vulnerabilidad encontrada.

El sistema SIEM es adecuado para el proceso de Defensa ya que proporcionará visión y claridad sobre las actividades en la red, lo que beneficia a la toma de decisiones del mando.

1.3 HERRAMIENTAS TÉCNICAS

1.3.1 Sistemas de Gestión de Eventos y Seguridad de la Información (SIEM)

Los sistemas SIEM son utilizados para analizar eventos de seguridad informática en tiempo real y para recolectar y almacenar trazas de seguridad, permitiendo el análisis forense de incidentes y el cumplimiento de lo establecido en las regulaciones existentes. Estos sistemas poseen dos funciones principales (Baluja García & Porvén Rubier, 2013):

- Gestión de información de seguridad (SIM): esta función está relacionada con la gestión de trazas y el reporte del cumplimiento de regulaciones. Mediante esta funcionalidad se garantiza la recolección, reportes y análisis de trazas de seguridad.
- Gestión de eventos de seguridad (SEM): esta función está relacionada con la monitorización de eventos en tiempo real y la gestión de incidentes de seguridad informática. Mediante esta funcionalidad se procesan en tiempo real las trazas recolectadas (Baluja García & Porvén Rubier, 2013).

De acuerdo con la investigación realizada por el cuadrante Gartner, los SIEM suelen ser empleados por corporaciones para su uso contra amenazas internas y externas, para monitorear las actividades de los usuarios, los servidores de monitoreo y las bases de datos, y para cumplir con las normas y regulaciones (Nicolett & Kavanagh, 2011).

¿Cómo ayuda un SIEM con la evaluación y mitigación de riesgos?

Un SIEM brinda la capacidad de identificar activos críticos y establecer políticas para actuar cuando esos activos tengan vulnerabilidades o estén sujetos a ataques. Un

SIEM generará alarmas basadas en el riesgo asociado con cualquier evento de seguridad detectado.

La importancia dada a cualquier evento de seguridad dado depende de tres factores:

- El valor del activo asociado al evento.
- La amenaza representada por el evento.
- La probabilidad de que ocurra el evento.

Estos factores son los componentes básicos de la definición tradicional de riesgo: una medida del impacto potencial de una amenaza en sus activos y la probabilidad de que se lleve a cabo una amenaza.

Cada evento generado en el SIEM se debe evaluar en relación con su riesgo asociado; en otras palabras, en proporción a los activos en riesgo, la amenaza representada por el evento y la probabilidad de que la amenaza sea real. En resumen, un sistema SIEM brinda la capacidad de identificar todos los eventos de alto riesgo, algunos de los cuales darán como resultado alarmas, y permitirán priorizar adecuadamente una respuesta (Alienvault, Documentation Alienvault Appliance, 2019).

La administración de registros es el componente más simple de un sistema SIEM, pero puede convertirse en una tarea complicada a medida que se incluyen varias fuentes de información y se habilitan niveles más altos de funcionalidad, como filtrado, correlación e informes (Miller, Harris, Harper, VanDyke, & Blask, 2011).

1.3.2 CICLO PDCA

PDCA (Plan, Do, Check, Act) o en español Planear, Hacer, Verificar y Actuar. Se basa en la idea de la mejora continua, este modelo fue desarrollado para ayudar a mejorar los procesos de las organizaciones y una de las ideas clave de los expertos en utilizar este modelo es que no se puede mejorar una organización en un solo paso (ISOTools, 2018).

Cada organización tiene un proceso complejo con muchas actividades diferentes que son interdependientes, en este método todas las personas que laboran en la institución son responsables por el funcionamiento correcto de cada proceso.

Para aplicar el modelo PDCA, primero se debe asegurar de que la seguridad de la información se considera una actividad recurrente y no como un proyecto. Por este motivo, el primer paso recomendado para la seguridad de la información es crear un

equipo permanente de seguridad de la información. Una vez que el equipo está en su lugar, recomendamos que el equipo implemente PDCA de la siguiente manera:

Se programa una reunión regular del equipo de seguridad de la información a intervalos fijos (mensual o trimestral). Tener reuniones regulares (tanto con el equipo como con la gerencia), esto ayuda a obtener una mejora continua.

La reunión del equipo de seguridad de la información debe tener una agenda basada en PDCA. Por lo tanto, un primer paso podría ser mirar hacia atrás en las métricas y los comentarios sobre las decisiones de las últimas reuniones (Verificación o Estudio), tomar decisiones sobre los cambios anteriores y luego decidir sobre nuevas acciones o controles a implementar (ICT Institute, 2018).

La fase de verificación es utilizada para determinar si los cambios implantados están dando resultados. Por ejemplo, realizar cualquier reunión, capacitación o taller para comprender el conocimiento inicial y terminar con un formulario de comentarios donde las personas pueden proporcionar comentarios y sugerencias sobre la capacitación de las actividades implementadas.

Cuando se discuten nuevos controles para implementar, el equipo de seguridad debe entender que la medición de la efectividad es necesaria para mejorar. Una forma de hacerlo es implementando primero controles que generaron nuevos datos, como el registro, antes de implementar controles que restringen a los usuarios.

Es importante que no se ejecuten demasiados experimentos, la idea detrás de PDCA es que se realicen experimentos uno tras otro ya que, si se ejecuta varios experimentos, existe el riesgo de que dos experimentos tengan un impacto en la misma métrica. Si esto sucede, no sabrá cuál de los experimentos funcionó y tendrá que rehacer los experimentos. Los buenos equipos de seguridad de la información se toman su tiempo y hacen solo unos pocos cambios cada mes o trimestre (ASQ, 2018).

El método PDCA generalmente se incluye en el documento de política de seguridad de la información y se explica brevemente en las capacitaciones de seguridad de la información.

El modelo PDCA puede aplicarse siempre que se considera realizar un cambio en la seguridad de la información, en el COCIBER se decidió instalar un nuevo sistema de gestión de eventos y seguridad de la información, que permita identificar y detectar

eventos que comprometan la seguridad de los activos y que permita asegurar la disponibilidad, integridad y confiabilidad de la información.

A continuación, se presenta un resumen general de la importancia que tiene este modelo en el proyecto actual:

Fase de Planeación: antes de realizar los cambios en la red del COCIBER se debe saber cuál es el valor actual antes de la mejora y cuál es el objetivo o valor esperado después del cambio, para este proyecto se verificará si el SIEM permitirá la detección oportuna de eventos e incidentes en la red del COCIBER. Se tiene el número de eventos e incidentes detectados por el COCIBER en el transcurso de un año detectados de forma manual, con el SIEM se pretende que esta detección sea automática.

Fase de Hacer: una vez que se obtiene las métricas o valores previos, se realizarán los cambios que se tienen como objetivo. En el caso de este proyecto se pretende realizar un análisis de riesgos bajo una metodología seleccionada para determinar la criticidad que tienen los activos que componen la red y así determinar si existen vulnerabilidades. Luego de esta fase se desarrollará un análisis de los mejores sistemas SIEM de código abierto (Open Source) existentes en la actualidad para implementarlo en los puntos críticos del COCIBER.

Fase de Verificación (o estudio): una vez obtenida la evaluación de riesgos y con la selección de un sistema que cumpla con los requerimientos, se procederá a verificar si el sistema SIEM implementado permite la mejora en el monitoreo de red y si el funcionamiento está cumpliendo con las expectativas requeridas por el COCIBER.

Fase de Actuación: si las acciones realizadas con anterioridad permiten determinar que el sistema SIEM es exitoso hay que continuarlo realizando, para ello se deberá volver a actualizar cada fase y las actividades que conlleva un nuevo ciclo de este proceso.

1.3.3 Norma ISO/IEC 27032

La Norma ISO/IEC 27032:2012 "Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" ofrece unas líneas generales de orientación para fortalecer el estado de la Ciberseguridad en una empresa, utilizando los puntos técnicos y estratégicos más importantes para esa actividad y los que están relacionados con:

- La Seguridad en la Redes

- Seguridad en Internet
- Seguridad de la información
- Seguridad de las Aplicaciones

La Norma ISO/IEC 27032 pretende garantizar la seguridad en los intercambios de información en la red para lograr hacer frente de una manera más efectiva al cibercrimen (Instituto Ecuatoriano de Normalización, 2014).

Como tal, la primera área de enfoque de esta Norma Internacional es abordar los problemas de seguridad del Ciberespacio o Ciberseguridad que se concentran en cerrar las brechas entre los diferentes dominios de seguridad en el Ciberespacio. En particular, esta Norma Internacional proporciona orientación técnica para abordar los riesgos comunes de Ciberseguridad, que incluyen:

- ataques de ingeniería social;
- piratería
- la proliferación de software malicioso ("malware");
- spyware y
- otro software potencialmente no deseado (INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS, 2010).

La guía técnica proporciona controles para abordar estos riesgos, incluidos los controles para:

- prepararse para los ataques de malware, delincuentes individuales u organizaciones delictivas en Internet;
- detección y seguimiento de ataques; y
- respuesta a ataques (Instituto Ecuatoriano de Normalización, 2014).

La segunda área de enfoque de esta Norma Internacional es la colaboración, ya que existe la necesidad de un intercambio eficiente y efectivo de información, coordinación y manejo de incidentes entre las partes interesadas en el ciberespacio. Esta colaboración debe ser realizada de manera segura y confiable que proteja la privacidad de los individuos interesados. Muchas de estas partes interesadas pueden residir en diferentes ubicaciones geográficas y zonas horarias, y es probable que estén regidas por diferentes requisitos reglamentarios. Las partes interesadas incluyen a los consumidores, que pueden ser varios tipos de organizaciones o individuos y proveedores, que incluyen proveedores

de servicios (Ministerio de Tecnologías de la Información y las Comunicaciones - Colombia, 2016).

Por lo tanto, esta norma internacional también proporciona un marco para el intercambio de información, coordinación y manejo de incidentes.

El marco incluye elementos clave de las consideraciones para establecer la confianza, los procesos necesarios para la colaboración y el intercambio de información, así como requisitos técnicos para la integración de sistemas y la interoperabilidad entre diferentes partes interesadas.

Dado el alcance de esta Norma Internacional, los controles provistos están necesariamente en un nivel alto. Las normas de especificación técnica detallada y las pautas aplicables a cada área se mencionan en esta Norma Internacional para obtener más información.

1.3.4 Evaluación de riesgos

Consiste en asegurar adecuadamente la infraestructura del COCIBER, la evaluación de riesgos ayudará a determinar la importancia de los activos dentro de la red, las vulnerabilidades de dichos activos en relación con amenazas de explotación específicas y la probabilidad de que ocurran eventos de seguridad contra esos activos. Después de completar estos análisis, se puede diseñar políticas de seguridad en respuesta a los valores de los activos y los riesgos de explotación que plantean las diversas amenazas y vulnerabilidades.

Las políticas de seguridad se centran en cómo proteger mejor los activos más críticos y en riesgo. Por ejemplo, si un recurso de red es crítico y la probabilidad de un ataque contra él es alta, se debe concentrar esfuerzos en crear políticas de seguridad que controlen dichos ataques y desarrollar planes de respuesta para ellos.

1.3.5 Metodología MAGERIT

Magerit es una metodología creada y desarrollada por el Ministerio de Administración Pública de España y que está disponible abiertamente en español e inglés. La primera versión (v.1) del método se publicó en 1997, mientras que la segunda realización se produjo varios años más tarde en 2005, la tercera versión fue actualizada en el año 2012. Magerit permite involucrar análisis cualitativos y cuantitativos. La evaluación de impacto se basa en activos críticos y toma en cuenta la probabilidad, la

vulnerabilidad (activo crítico) y el impacto (amenaza, activo) (Administración Pública de España, 2012).

1.3.6 Norma ISO/IEC 25000

La calidad del software es de gran importancia en la evaluación de un sistema SIEM principalmente debido a las funciones críticas que desarrollará en la red del COCIBER. Para garantizar la calidad del sistema SIEM es necesario realizar evaluaciones de las soluciones Open Source existentes en el mercado digital. Se utilizará esta norma ya que tiene como propósito principal la evaluación idónea de cada parámetro requerido para la selección adecuada de un sistema.

La familia de normas ISO/IEC 25000, conocida como SQuaRE (Requisitos y evaluación de la calidad del producto de software), permite satisfacer la necesidad de evaluar la calidad relacionada de los sistemas SIEM existentes. El objetivo de la norma ISO/IEC 25000 es crear un marco común dentro del cual las normas ISO/IEC 9126 e ISO/IEC 14598 se conviertan en la piedra angular de esta área de ingeniería de software. ISO/IEC 25000 se divide en varias partes: destacamos ISO/IEC 25040 que define el proceso de evaluación de la calidad del producto de software e ISO/IEC 25010 que determina las características y subcaracterísticas del producto de software que se pueden evaluar (Marcos, Arroyo, Garzás, & Mario, 2008).

1.3.7 Tecnologías de Virtualización

Las tecnologías de virtualización permiten que varias máquinas virtuales, con sistemas operativos heterogéneos, se ejecuten en paralelo y de forma aislada en la misma máquina física. Al emular un sistema de hardware completo, desde el procesador a la tarjeta de red, cada máquina virtual puede compartir un conjunto común de hardware sin saber que este hardware también puede ser usado por otra máquina virtual al mismo tiempo. El sistema operativo que se ejecuta en la máquina virtual ve un conjunto de hardware consistente y normalizado, independientemente de los componentes físicos reales del hardware (Campbell, S., Jeronimo, M., 2006).

1.3.8 Hipervisor ESXi

El hipervisor VMware ESXi utilizado en este proyecto es una técnica de virtualización completa que utiliza el hipervisor con alto rendimiento y es ampliamente aceptado en todas las industrias. El hipervisor requiere la instalación de todos los controladores de hardware y software asociado. Implementa versiones ocultas de

estructuras del sistema como las tablas de paginación y mantiene la coherencia con las tablas virtuales al capturar cada instrucción que intenta actualizar estas estructuras. Las páginas virtuales se asignan a páginas físicas a lo largo de la tabla de paginación del sistema operativo invitado. El hipervisor luego traduce la página física a la página de la máquina, que finalmente es la página correcta en la memoria física. Esto ayuda al ESXi a administrar la memoria general y mejorar el rendimiento general del sistema (VMware, 10).

Componentes

La arquitectura de VMware ESXi comprende el sistema operativo subyacente, llamado VMkernel, y los procesos que se ejecutan sobre él. VMkernel proporciona medios para ejecutar todos los procesos en el sistema, incluidas las aplicaciones de administración y los agentes, así como las máquinas virtuales. Tiene el control de todos los dispositivos de hardware en el servidor y administra los recursos para las aplicaciones (VMware, Inc, 2017). Los principales procesos que se ejecutan sobre VMkernel son:

- Interfaz de usuario de consola directa (DCUI): la interfaz de administración y configuración de bajo nivel, accesible a través de la consola del servidor, utilizada principalmente para la configuración básica inicial.
- El monitor de la máquina virtual, que es el proceso que proporciona el entorno de ejecución para una máquina virtual, así como un proceso auxiliar conocido como VMX[4]. Cada máquina virtual en ejecución tiene su propio proceso VMM[5] y VMX.
- Varios agentes utilizados para habilitar la administración de infraestructura de VMware de alto nivel desde aplicaciones remotas.
- El sistema del Modelo de información común (CIM): CIM es la interfaz que permite la administración a nivel de hardware desde aplicaciones remotas a través de un conjunto de API estándar (Chaubal, 2014).

[4] VMX es el archivo de configuración principal para una máquina virtual. Cuando crea una nueva máquina virtual y responde preguntas sobre el sistema operativo, el tamaño de los discos y las redes, esas respuestas se almacenan en este archivo

[5] Virtual Machine Monitor (VMM) es una tecnología que está compuesta por una capa de software que permite utilizar, al mismo tiempo, diferentes sistemas operativos o máquinas virtuales.

1.4 ALTERNATIVAS DE SOLUCIÓN

1.4.1 Gestión de incidentes informáticos en la nube

La computación en la nube ofrece muchos beneficios, como ahorro de costos, servicios a pedido, escalabilidad, redundancia y elasticidad, y beneficios de seguridad, también. Además, el concepto de computación en la nube ofrece varios beneficios para la continuidad del negocio: elimina el tiempo de inactividad, mejora la gestión de la seguridad de la red y de la información, la recuperación ante desastres con gestión de copias de seguridad y redundancia geográfica. También evita o elimina la interrupción de las operaciones, aumenta la disponibilidad del servicio y mitiga la posibilidad de ataques de Denegación de Servicio[6].

La computación en la nube no es solo una tecnología o un concepto, sino que es el futuro, porque la cantidad de proveedores de servicios en la nube y la cantidad de diversos servicios en la nube están aumentando. No solo las empresas líderes mundiales en TI, sino también las nuevas que ofrecen servicios en la nube (Iaas[7], PaaS[8], SaaS[9]), como Amazon AWS y EC2, Google App Engine, Salesforce's Sales and Service Cloud, Microsoft Azure y Live, IBM SmartCloud, etc. diversos tipos de consumidores: proveedores de servicios en la nube, consumidores en la nube y usuarios finales. El crecimiento de la oferta de varios servicios en la nube aumenta el número de consumidores de servicios en la nube (IBM, 2019).

[6] Un ataque de denegación de servicios, también llamado ataque DDoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
[7] IaaS: Infraestructura como servicio, se refiere a los servicios on-line que proporcionan un alto-nivel de APIs utilizadas para indirecciónar detalles a bajo nivel de infraestructura como recursos de informática física, ubicación, dato partitioning, scaling, seguridad, copia de seguridad entre otros.
[8] PaaS: Plataforma como servicio (PaaS) es un entorno de desarrollo e implementación completo en la nube, con recursos que permiten entregar todo, desde aplicaciones sencillas basadas en la nube hasta aplicaciones empresariales sofisticadas habilitadas para la nube.
[9] SaaS: Software como un Servicio, es un modelo de distribución de software donde el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de información y comunicación, a los que se accede vía Internet desde un cliente.

CAPÍTULO 2

MARCO METODOLÓGICO

En el presente capítulo se da a conocer los métodos y herramientas de investigación para el análisis del problema de la gestión de eventos e incidentes en la red del Comando de Ciberdefensa. Para contribuir con la implementación del sistema SIEM se hará uso de las técnicas de observación y recolección de información para identificar amenazas, vulnerabilidades y controles implementados en la red.

4.5 TIPO DE INVESTIGACIÓN

El enfoque de la investigación es deductivo ya que se inició consultando información general de varias fuentes investigadas (teorías y metodologías) acerca de los sistemas SIEM, luego de esto se plantea una hipótesis general o teórica en la misma que no se cuantifica las variables, sino que será basada través de la observación en la fase de evaluación para seleccionar un sistema SIEM. Las características del enfoque deductivo son:

- El razonamiento deductivo funciona de lo más general a lo más específico.
- Se denomina informalmente un enfoque "de arriba hacia abajo".
- La conclusión se deduce lógicamente de las premisas (hechos disponibles).

Dadas las características anteriores el enfoque se usaría para comprobar la hipótesis que con el sistema SIEM mejorará la detección y gestión de incidentes y eventos de seguridad en la red del COCIBER.

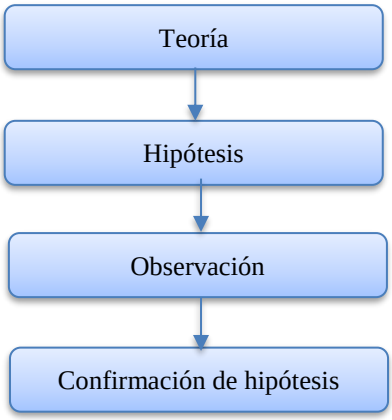


Figura 2.3. Modelo de enfoque deductivo
Fuente: (Baral, 2010)

4.6 RECOPILACIÓN DE INFORMACIÓN

La técnica de observación fue aplicada en el desarrollo de este proyecto ya que permite visualizar y analizar el problema en el sitio donde se desarrollará el proyecto. Para ello se programó una visita a las instalaciones del COCIBER y con ayuda del administrador de red todos los hechos fueron analizados para la posterior elaboración de un cuestionario, ver anexo A.

En la actualidad los cuestionarios son fundamentales para determinar el estado de la seguridad de la información de una organización porque cuenta con preguntas técnicas dirigidas a personal con conocimientos requeridos y que sirve para obtener respuestas rápidas. Este cuestionario se dirigió específicamente al administrador de la red y consta de preguntas cerradas que permiten obtener datos acerca de los activos y controles de seguridad establecidos en la red con mayor facilidad y rapidez, el mismo que se encuentra en el Anexo B.

4.6.1 TÉCNICAS DE RECOPILACIÓN DE INFORMACIÓN

Como se dijo anteriormente se utilizó la técnica de observación para conocer el estado de la infraestructura actual, esta técnica de observación directa implica verificar en forma visual y física los componentes de la red, la forma de detección de eventos e incidentes y riesgos asociados.

Con la técnica de observación se identificó que existen varios procedimientos de controles establecidos que permiten reducir los riesgos, con esta técnica se identificó las vulnerabilidades y amenazas existentes.

El cuestionario fue elaborado a partir de las observaciones realizadas y se toman en cuenta los controles de seguridad existentes, el mismo consta de 18 preguntas que

fueron realizadas al administrador de la red con la autorización verbal del comandante del COCIBER, las preguntas tienen la finalidad de determinar dos aspectos:

• Estado de la red: determinar si existe un inventario de activos, si existe clasificación o valoración de los mismos.

• Controles y seguridad: permite conocer cuáles son los controles o seguridades existentes en la red y si se encuentran funcionando de manera eficiente, esto ayuda a determinar las vulnerabilidades existentes.

Las preguntas realizadas se presentan a continuación en la tabla 2.2 y se reitera que son de tipo cerradas:

PREGUNTAS	SI	NO
ESTADO DE ACTIVOS Y TOPOLOGÍA DE LA RED		
1. ¿Se dispone de un diagrama de la topología de la red?	X	
2. ¿Se dispone de un inventario de activos?		X
3. ¿El inventario es suficientemente detallado y está estructurado adecuadamente?		X
CONTROLES Y SEGURIDAD DE LA RED		
4. ¿Se dispone de un catálogo de amenazas?	X	
5. ¿Cuenta con dispositivos de seguridad perimetral?	X	
6. ¿Se verifica regularmente el correcto funcionamiento de los dispositivos de seguridad perimetral?		X
7. ¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?		X
8. ¿Se registran las actividades de los administradores y usuarios de sistema?		X
9. ¿Cuenta con equipos desatendidos?	X	
10. ¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	X	
11. ¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?		X
12. ¿Cree usted que se incorporan controles adecuados y suficientes para proteger la red?		X
13. ¿Cuenta con un sistema de seguridad esencial para proteger los activos de información?		X
14. ¿La red del COCIBER es supervisada y evaluada constantemente?		X
15. ¿Existen políticas y procedimientos asociados a controles antimalware?	X	
16. ¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado?		X
17. ¿Se actualiza el software antivirus de forma automática?	X	
18. ¿Se generan alertas tras una detección en tiempo real?		X
19. ¿El personal técnico y el administrador de la red tienen la capacidad de reaccionar de forma rápida y apropiada en caso de detectar un incidente en tiempo real?	X	

Tabla 2.2. Dispositivos de seguridad

Fuente: Autor

4.6.2 TABULACIÓN DE RESULTADOS

Los resultados obtenidos del cuestionario aplicado se detallan a continuación:

ASPECTO DE ESTADO DE ACTIVOS Y TOPOLOGÍA DE LA RED

PREGUNTA 1. ¿Se dispone de un diagrama de la topología de la red?

RESPUESTA: SI

ANÁLISIS: el diagrama permite obtener visibilidad acerca de la ubicación de los activos en la red y servirá para determinar la ubicación de los sensores pertenecientes al SIEM. Según la información obtenida de la topología de la red se determina que no existen

dispositivos que sirvan como sensores para el análisis de la red o sus activos, ver figura 2.5.

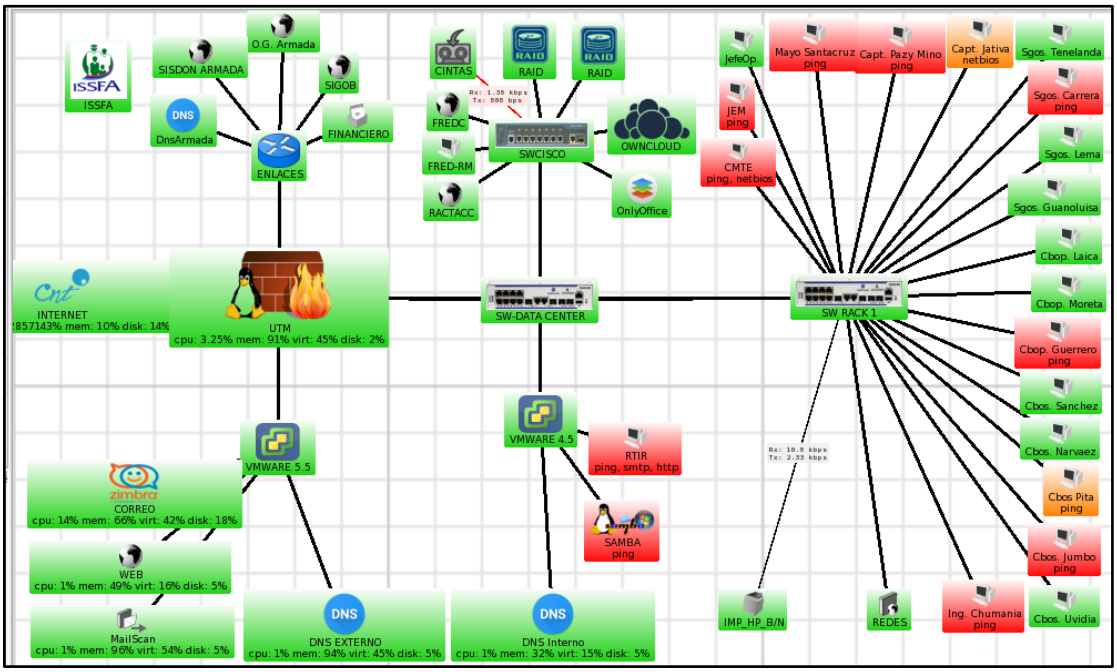


Figura 2.4. Topología actual de la red

Fuente: COCIBER

PREGUNTA 2. ¿Se dispone de un inventario de activos?

RESPUESTA: NO

ANÁLISIS: se debe realizar el levantamiento de los activos de la red, esto será fundamental debido a que se pretende a realizar un análisis de riesgos, además que se pretende conocer cuál es la criticidad que tiene cada activo dentro de la red.

PREGUNTA 3. ¿El inventario es suficientemente detallado y está estructurado adecuadamente?

RESPUESTA: NO

ANÁLISIS: al no existir un inventario de los activos de la red no se puede saber con exactitud cuáles son los dispositivos o sistemas que se encuentran desatendidos y/o vulnerables.

ASPECTO DE CONTROLES Y SEGURIDAD DE LA RED:

PREGUNTA 4. ¿Se dispone de un catálogo de amenazas?

RESPUESTA: SI

ANÁLISIS: el catálogo de amenazas es la lista que ha elaborado el COCIBER y que considera que podrían causar daños a la seguridad de la información o sus activos. El

COCIBER ha considerado únicamente amenazas tecnológicas, y se visualizan en la siguiente tabla.

Tabla 2.3. Amenazas tecnológicas

No.	Nombre de la amenaza
1	Malware
2	Intrusiones a los sistemas
3	Denegación de servicios
4	Anomalías en la red
5	Defacement
6	Hackers
7	Malware en dispositivos móviles
8	Ingeniería Social
9	Fuga de información
10	Abuso de privilegios
11	Phishing
12	Estafas

Fuente: Autor

PREGUNTA 5. ¿Cuenta con dispositivos de seguridad perimetral?

RESPUESTA: SI

ANÁLISIS: los dispositivos de seguridad perimetral permiten establecer seguridades a nivel del borde de la red y su función es no permitir conexiones entrantes o salientes de redes desconocidas, almacenan registros de eventos que serán de utilidad para la correlación en el SIEM, se visualizan en la siguiente tabla:

Tabla 2.4. Dispositivos de seguridad

No.	Nombre
1	Firewall
2	Proxy
3	UTM[10]
4	Antivirus

Fuente: Autor

PREGUNTA 6. ¿Se verifica regularmente el correcto funcionamiento de los dispositivos de seguridad perimetral?

RESPUESTA: NO

[10] UTM: Gestión unificada de amenazas, que comúnmente se abrevia como UTM, es un término de seguridad de la información que se refiere a una sola solución de seguridad.

ANÁLISIS: permite determinar si el administrador de red realiza las actualizaciones, revisiones de vulnerabilidades, fallos o correcciones en los sistemas de seguridad, esta actividad será automatizada con el sistema SIEM a implementarse.

PREGUNTA 7. ¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?

RESPUESTA: NO

ANÁLISIS: La monitorización de activos es una tarea compleja y que requiere de mucho tiempo, pero con el SIEM se verá beneficiada por el software que facilita el descubrimiento, evaluación y gestión del inventario de hardware y software, el cumplimiento de licencias y contribuye a la eliminación segura de amenazas.

PREGUNTA 8. ¿Se registran las actividades de los administradores y usuarios de sistema?

RESPUESTA: NO

ANÁLISIS: el sistema SIEM brinda beneficios de registrar las sesiones de usuarios privilegiados en las computadoras de la red, además que permite reducir significativamente los incidentes de violación de datos, los tiempos de investigación forense de incidentes de TI y los costos de lograr y mantener el cumplimiento normativo.

PREGUNTA 9. ¿Cuenta con equipos desatendidos?

RESPUESTA: SI

ANÁLISIS: los sistemas desatendidos pueden ser la causa por la cual los hackers exploten una vulnerabilidad y puedan acceder a los sistemas del COCIBER, los sistemas desatendidos se encuentran detallados en la Tabla 2.5.

Tabla 2.5. Sistemas desatendidos

SISTEMA	S.O.	Conectado a la
OTRS	Linux	SI
RTIR	Linux	SI
Estación de	Windows	SI
Servidor	Linux	NO

Fuente: Autor

PREGUNTA 10. ¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?

RESPUESTA: SI

ANÁLISIS: se realizan las actualizaciones correspondientes a dispositivos o servicios al momento de detectar vulnerabilidades y que sea utilizado en Fuerzas Armadas. El COCIBER recibe frecuentemente las vulnerabilidades CVE´s del sitio

https://cve.mitre.org ya que cuenta con suscripción al mismo, el administrador menciona verbalmente que el procedimiento en términos generales es el siguiente:

- El personal de guardia deberá revisar diariamente vulnerabilidades recibidas de MITRE en el correo electrónico asignado al COCIBER.
- Si la vulnerabilidad aplica a algún producto o servicio que sea utilizado en el COCIBER se aplica la actualización o parche inmediato.
- Se envía un mensaje militar a todas las unidades de Fuerzas Armadas indicando la vulnerabilidad existente y las recomendaciones para corregirla.

PREGUNTA 11. ¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?

RESPUESTA: NO

ANÁLISIS: El administrador manifiesta que sigue ciertos lineamientos de seguridad, pero los mismos no se encuentran alineados o cumplen con un estándar como ISO 27001 o NIST, en el proyecto se utilizará el estándar ISO 27032 que proporciona pautas con respecto a la protección de los procesos de seguridad de la información. Además, proporciona a los técnicos la capacidad de desarrollar un marco de políticas en el que identifica los procesos más vulnerables a los ataques cibernéticos; y eso es considerado para asegurar que el COCIBER y los usuarios no estén en riesgo.

PREGUNTA 12. ¿Cree usted que se incorporan controles adecuados y suficientes para proteger la red?

RESPUESTA: NO

ANÁLISIS: El administrador menciona que no existen controles suficientes, los sensores a implementar en la red COCIBER permiten las funciones de descubrimiento y monitoreo de todos los activos en la red, manteniendo información detallada sobre la configuración de cada dispositivo y aplicación; y enviando los datos la base de datos de activos utilizada por el SIEM para identificar amenazas.

PREGUNTA 13. ¿Cuenta con un sistema de seguridad esencial para proteger los activos de información?

RESPUESTA: NO

ANÁLISIS: el COCIBER no cuenta con un sistema SIEM, brindando la oportunidad de implementarlo. El sistema SIEM recopila y agrega datos de registro generados a través de la red, desde sistemas y aplicaciones a dispositivos de red y de seguridad, como firewalls y filtros antivirus.

PREGUNTA 14. ¿La red del COCIBER es supervisada y evaluada constantemente?

RESPUESTA: NO

ANÁLISIS: el sistema SIEM permitirá que se generen gráficos estadísticos de los eventos generados en la red, así como también amenazas críticas, lo que permitirá mejorar la seguridad de los activos e información.

PREGUNTA 15. ¿Existen políticas y procedimientos asociados a controles antimalware?

RESPUESTA: SI

ANÁLISIS: el administrador tiene conocimiento del procedimiento ante un malware detectado, este procedimiento es necesario debido a que en el momento que el sistema SIEM detecte un evento que atente a la seguridad es necesaria la oportuna intervención del administrador a fin de evitar que el malware se propague hacia otros equipos o redes, el procedimiento se encuentra en el Anexo C.

PREGUNTA 16. ¿Se utilizan listas blancas o negras para controlar el tráfico autorizado y no autorizado?

RESPUESTA: NO

ANÁLISIS: La supervisión del tráfico de red es una tarea difícil y exigente pero muy importante de los administradores de red. Con la implementación del SIEM se pretende que el administrador sea proactivo en lugar de reactivo, el administrador debe monitorear el tráfico y bloquear el tráfico desde direcciones que considere sospechosas.

PREGUNTA 17. ¿Se actualiza el software antivirus de forma automática?

RESPUESTA: SI

ANÁLISIS: el administrador menciona que la Unidad de Tecnologías mantiene un agente instalado en los computadores de la organización que actualiza el antivirus, es importante actualizar constantemente el software antivirus en una computadora porque regularmente aparecen nuevos virus. Las actualizaciones de antivirus contienen los últimos archivos necesarios para combatir nuevo software malicioso y contribuyen así a proteger las computadoras y red.

PREGUNTA 18. ¿Se generan alertas tras una detección en tiempo real?

RESPUESTA: NO

ANÁLISIS: el administrador ha manifestado que las detecciones identificadas no han sido a tiempo, esto brinda que el sistema SIEM garantice obtener datos de las alertas generadas como direcciones IP, estados de autenticación, puertos o códigos de error,

siempre se debe tomar esos datos para conocer el potencial de la amenaza en curso y tomar las acciones adecuadas en la mitigación del incidente.

PREGUNTA 19. ¿El personal técnico y el administrador de la red tienen la capacidad de reaccionar de forma rápida y apropiada en caso de detectar un incidente en tiempo real?

RESPUESTA: SI

ANÁLISIS: durante un incidente de seguridad, el personal técnico y el administrador de la red deben afrontar varias incógnitas y estar frente a actividades a veces hasta desconocidas. En ese entorno tan agitado, es posible que el personal no siga los procedimientos adecuados de respuesta a los incidentes para limitar efectivamente el daño. Es importante porque un incidente de seguridad puede ser una situación de alta presión, y el personal encargado debe concentrarse de inmediato en las tareas críticas. El SIEM mejorará la capacitación y la experiencia del personal técnico ya que la detección se realiza en tiempo real y ayudará tomar rápidamente pasos de respuesta durante un incidente de seguridad y evitar impactos innecesarios o daños a la reputación.

4.7 HIPÓTESIS

La hipótesis planteada es de tipo general o teórica y se comprobará a través de las observaciones realizadas y se determinará si la implementación de un SIEM en el COCIBER mejorará la detección eventos e incidentes en la red y en tiempo real, lo que permitirá una respuesta eficaz y oportuna frente a cualquier anomalía o intento de violación de la seguridad

CAPÍTULO 3

PROPUESTA

Este capítulo incluye el modelo propuesto para la implementación del SIEM y describe cómo realizar el análisis de riesgo basado en la metodología Magerit. El SIEM está basado en los lineamientos descritos en la norma ISO/IEC 27032, Protección de los activos en el Ciberespacio que incluye las actividades de identificar, proteger, detectar, responder y recuperarse frente a cualquier desastre.

Para la selección del sistema SIEM se dispone de la norma ISO/IEC 25000 Calidad de Software que asegura que el sistema implementado cumplirá con los requisitos de calidad adecuados para el COCIBER.

4.8 DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

Según la información obtenida del cuestionario se puede visualizar que no existen sensores que contribuyan a mantener la seguridad de los activos (figura 6), un sensor es un dispositivo que recopila datos del tráfico que circula en la red y lo envía a un sistema central que analiza y correlaciona esos datos. Además, según las observaciones realizadas el COCIBER cuenta con dispositivos de seguridad perimetral pero que no están siendo verificados y actualizados con regularidad, este problema se produce por no verificar el procedimiento existente en las funciones que debe cumplir el administrador de red, al momento de realizarse un relevo de funciones.

El análisis de los eventos (logs) de los dispositivos perimetrales o de seguridad implementados es importante ya que sirve para encontrar indicios de usuarios o aplicaciones maliciosas, estos eventos serán de ayuda para el administrador ya que así se enfocará en los dispositivos que requieren de mantenimiento y/o actualización y lograría cumplir con los procedimientos de seguridad aplicados a los dispositivos.

El COCIBER no cuenta actualmente con un sistema de gestión de incidentes y seguridad de la información, por lo que, para implementarlo se deberá hacer un correcto proceso de mejora continua con el modelo PDCA. A continuación, se muestra un gráfico descriptivo de la forma que se lleva el proceso de detección de incidentes actualmente, todo el proceso es realizado de forma manual.

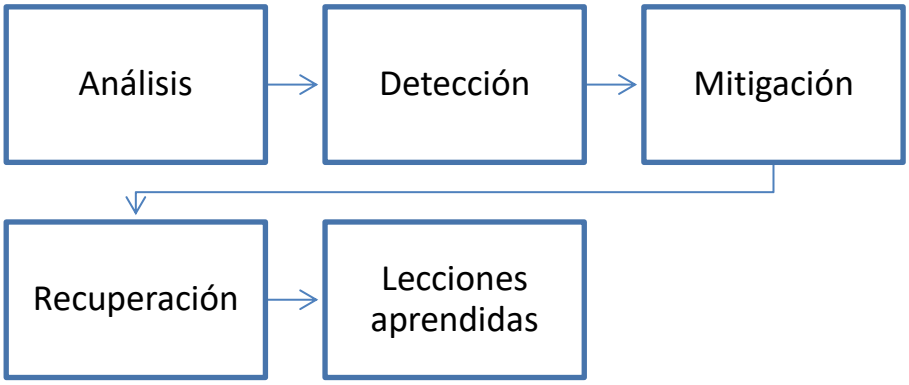


Figura 3.5. Proceso de detección de incidentes

Fuente: Autor

4.8.1 FACTIBILIDAD TÉCNICA

El proyecto es factible técnicamente debido a que la infraestructura del COCIBER presta las condiciones adecuadas para la implementación de un SIEM, el detalle de cada una de las características técnicas en la cual se implementará el sistema se encuentra en el capítulo de implementación de este proyecto, pero a continuación se presenta una breve descripción de hardware y software necesario.

Tabla 3.6. Requerimientos técnicos hardware

Harware	
Marca	HP
Modelo	ProLiant ML110 G6
CPU	Intel(R) Xeon(R) CPU X3430 @ 2.40GHz
Memoria	8 GB
Disco Duro	500 GB

Fuente: Autor

Tabla 3.7. Requerimientos técnicos software

Software	
Marca	VMWare
Producto	ESXi 6.5

Fuente: Autor

4.8.2 FACTIBILIDAD OPERACIONAL

El proyecto es factible operacionalmente debido a que el personal encargado del SIEM cuenta con capacitaciones en sistemas Linux, además de trabajar varios años en infraestructura de redes en varias unidades de las Fuerzas Armadas. Dentro de la administración del SIEM se contará con varios perfiles de usuarios

los mismos que han sido designados para determinar la responsabilidad de cada actividad.

Los perfiles de los usuarios que tendrán acceso al sistema SIEM deberán cumplir con los siguientes conocimientos mínimos:

- Conocimientos fundamentales de seguridades informáticas.
- Conocimientos básicos en Sistemas operativos Linux.
- Conocimientos en Sistemas operativos Windows.

• Interpretar los logs generados por los diferentes eventos en los sistemas operativos.

- Conocimientos básicos del modelo TCP/IP.
- Conocimientos básicos de Redes LAN/WAN.
- Conocimientos de seguridades en redes de Datos.
- Interpretar gráficos estadísticos y realizar reportes.

Además de los conocimientos previamente descritos se deberán establecer los siguientes roles recomendados por Alienvault, pero que han sido ampliados por el COCIBER:

Tabla 3.8. Requisitos operaciones y roles para un SIEM

Actividades operativas del SIEM	**Rol**	**Disponibilidad**	**Tiempo de Respuesta**	**Tiempo de resolución**
Soporte técnico Respuesta a llamadas de problemas causadas por mal funcionamiento del sistema SIEM, falla del dispositivo o software, etc.	Administrador	8/5	4h	≤ 48h
Administración de la infraestructura del SIEM (por ejemplo): - ver estado y monitorear mensajes de administración; - agregar y mantener usuarios y permisos de SIEM; - mantener el estado de los componentes y la base de datos de SIEM eficazmente; - realizar actualizaciones y parches regulares (seguridad y corrección de errores); - realizar procedimientos regulares de archivo, copia de seguridad y recuperación del sistema; - controlar el estado de los agentes instalados y demás dispositivos que lo integran;	Administrador	8/5	N/A	N/A

- diseñar, desarrollar y mantener la infraestructura de flujo de trabajo SIEM (conectores inteligentes y flexibles) para fuentes existentes y nuevas; etc.				
Monitoreo continuo, mantenimiento y mejora del contenido SIEM, estándar y personalizado, (por ejemplo): - supervisar el rendimiento, mantener y ajustar las correlaciones, casos de uso, reglas, filtros, monitores de datos, listas activas y listas de sesiones; - desarrollar y publicar artículos de la base de conocimiento; - desarrollar perfiles de Descubrimiento de Patrones; etc.	Operador	8/5	N/A	N/A
Desarrollo de nuevos contenidos SIEM: - Desarrollar y probar nuevos contenidos de correlación y casos de uso utilizando filtros, reglas, monitores de datos, listas activas y listas de sesiones. - Desarrollar y probar nuevas herramientas de monitoreo utilizando canales activos, paneles de control, informes y tendencias; etc.	Operador	8/5	N/A	N/A
Servicios SOC, (por ejemplo): - ver canales activos y paneles de control; - crear anotaciones, crear y actualizar tickets de incidentes de seguridad; - Investigar incidentes de seguridad utilizando canales, gráficos de eventos, informes, registros; - describir incidentes, síntomas, recomendar respuestas y consulte los posibles artículos de la Base de conocimientos; etc.	Analista	8/5	N/A	N/A
Servicios SOC, alertas críticas: - reenviando cualquier alerta crítica, como por su ocurrencia.	Operador	24/7	N/A	N/A
Informes: Informes periódicos y bajo demanda.	Analista	8/5	N/A	N/A

Fuente: Autor

4.8.3 FACTIBILIDAD ECONÓMICA

El proyecto es factible económicamente ya que el sistema a implementarse está basado en fuentes abiertas, a excepción del software de virtualización ESXi pero el mismo cuenta con licencia y será facilitado por el COCIBER:

Costos de software:

Tabla 3.9. Costos de Software

Software	Costo
Servidor SIEM	Open Source
Agentes	Open Source
Bases de Datos	Open Source
Software de virtualización nivel 0 (ESXI)	Licenciado

Fuente: Autor

Costos de hardware:

Tabla 3.10. Costos de Hardware

Hardware	Costo
Servidor Hp ProLiant ML110 G6	$1.000,00
Almacenamiento Disco	$400,00
Tarjeta de red 1Gb/s	$100,00
Memoria RAM 8gb	$400,00
4 CPUs x Intel(R) Xeon(R) CPU X3430 @ 2.40GHz	$150,00
TOTAL	**$2.100,00**

Fuente: Autor

Todo el hardware necesario para la implementación del SIEM será proporcionado por el COCIBER, por lo que no se requiere realizar algún gasto adicional a la implementación ya que el COCIBER ya tiene disponible todo el hardware y software, tal como se explica en el capítulo de Implementación.

4.9 MODELO O ESTÁNDAR POR APLICAR

En esta sección se procederá a describir todas las metodologías y Normas ISO aplicadas en la implementación del sistema SIEM, se procura que la propuesta realice un adecuado uso y cumplimiento de las directrices establecidas en cada norma y al final se obtenga un sistema eficiente al servicio de los procesos del COCIBER.

A continuación, se presenta las normas y metodologías a utilizarse para la implementación de un SIEM:

4.9.1 Norma ISO/IEC 27032:2012 "Tecnología de la información - Técnicas de seguridad - Directrices para la Ciberseguridad"

Con las directrices de esta norma internacional se pretende enfatizar la importancia que tienen los activos en el ciberespacio y la protección adecuada que debe asignarle el COCIBER en los aspectos de seguridad de la información, seguridad de red, tráfico desde Internet y protección de la infraestructura. La norma ISO 27032 establece que el sistema

SIEM debe responder como control a los problemas de ciberseguridad, con la implementación del SIEM el COCIBER tendrá la capacidad de estar preparado para detectar, monitorear y responder a los ataques producidos en la red.

La norma también cuenta con las guías para identificar, analizar y evaluar los riesgos asociados a la ciberseguridad, técnicas, métodos y controles se pueden implementar para ayudar a mitigar los riesgos de seguridad de la información; es por ello que se realizará uso de la metodología Magerit que se encuentra expuesta más adelante.

Por último, esta norma nos permite utilizar la metodología PDCA como mejora continua ya que contempla las fases de planificación, implementación, mantenimiento y evaluación de la seguridad de la información

4.9.2 Modelo PDCA (Plan, Do, Check, Act)

El ciclo PDCA o llamado también de Deming es un modelo de mejoramiento continuo, la implementación de este modelo en el proyecto no garantizará la totalidad de la seguridad de la red, pero servirá para que los riesgos de seguridad de la información del COCIBER sean conocidos, asumidos, gestionados y minimizados eficientemente, cumpliendo con la mejora continua que representa este ciclo.

Para visualizar de una forma gráfica cada fase del modelo PDCA propuesto en este proyecto se ha realizado un gráfico donde se visualiza las fases que contempla la implementación:

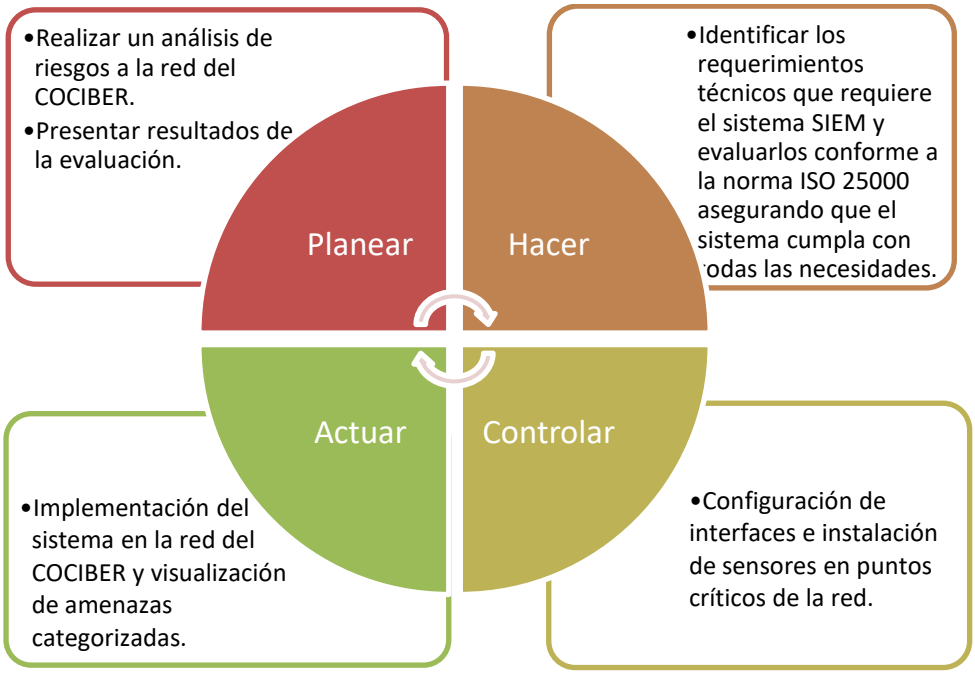


Figura 3.6. Fases del ciclo PDCA para el COCIBER

Fuente: Autor

Las actividades propuestas por cada fase del ciclo de Deming serán las siguientes:

FASE DE PLANIFICAR: se realizará un análisis de riesgos de la red del Comando de Ciberdefensa, realizando un levantamiento de información para cuantificar y valorizar los activos conforme a su nivel de criticidad. Esta información recolectada será muy valiosa para la realización de las matrices de evaluación y riesgos.

El modelo de análisis de riesgos propuesto servirá para determinar la evaluación de seguridad de la red. Existen muchas metodologías existentes pero se selecciona la metodología Magerit debido a que es de libre acceso y no es auditable (https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar/metodologia.html), las fases propuestas se visualizan en la figura 3.7:

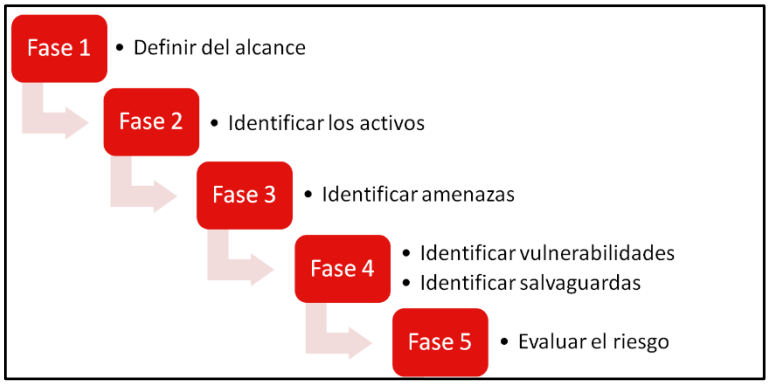


Figura 3.7. Fases del análisis de Riesgos

Fuente: Magerit V. 3.0

Las fases descritas anteriormente serán las que se realizarán en el COCIBER y las actividades de cada una se describen a continuación:

Fase 1. Definición del alcance

En esta fase se describe cuáles serán los límites de esta evaluación, es decir, cuáles activos, sistemas, dispositivos y personal serán evaluados. Se debe tener cuidado en esta fase ya que, a mayor alcance, mayor será el tiempo que se debe destinar a la evaluación.

Fase 2. Identificación de activos

La identificación de los activos se registrará conforme a la siguiente tabla:

Tabla 3.11. Identificación de activos

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de Finanzas	Analista Redes	Servidor Físico	Datacenter 1	SI

Fuente: Elaboración propia

Fase 3. Identificar las amenazas

Para esta fase se procederá a tomar las amenazas contempladas en el catálogo del COCIBER que se encuentra expuesta en la tabla 2 y se solicitará una reunión con el administrador de red para agregar las amenazas expuestas en la Metodología de riesgos Magerit, esto debido a que el COCIBER solo contempla amenazas tecnológicas, se tomará en cuenta también las amenazas de tipo industrial o por desastres naturales.

Fase 4. Identificar vulnerabilidades y salvaguardas

El cuestionario realizado como recopilación de información permite identificar cuál es el procedimiento que el COCIBER realiza frente a vulnerabilidades expuestas, además de eso, se solicitará los procedimientos de seguridad que tienen para asegurar la información en caso de la materialización de una amenaza.

Fase 5. Evaluación del riesgo

La evaluación del cálculo de riesgo se realizará con criterios cualitativos o cuantitativos, para realizar esta evaluación se deberán considerar los activos identificados anteriormente y asociarlos a las amenazas a los que se pueden encontrar expuestos, luego de eso se tomará en cuenta las vulnerabilidades (si existen) y las salvaguardas que permite mitigar el riesgo, para la evaluación se podrá hacer uso de las siguientes tablas:

Descripción de probabilidad

Tabla 3.12. Tabla para el cálculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	**1**	Ocurre una vez al año
Media	**2**	Ocurre una vez al mes
Alta	**3**	Ocurre una vez cada semana

Fuente: Magerit V. 3.0

- **Ocurre una vez al año:** se refiere a eventos que no tienen probabilidad de suceder o han sucedido una vez al año.
- **Ocurre una vez al mes:** son eventos que han sucedido y que pueden repetirse en el transcurso del año.
- **Ocurre una vez cada semana:** son eventos que se producen frecuentemente y que requieren de atención.

Descripción de impacto

Tabla 3.13. Tabla para el cálculo del impacto

Cualitativo	Cuantitativo	Descripción
Bajo	**1**	No tiene consecuencias relevantes
Medio	**2**	Tiene consecuencias reseñables
Alto	**3**	Tiene consecuencias graves para la organización

Fuente: Magerit V. 3.0

- **No tiene consecuencias relevantes:** la materialización de un evento no produce daños o no tienen relevancia.
- **Tiene consecuencias reseñables:** la materialización de un evento causa daños que pueden considerarse serios para el COCIBER.
- **Tiene consecuencias graves para la organización:** la materialización de un evento causa la pérdida de información, deterioro de imagen o cualquier tipo de incidente grave.

Más adelante, en la Implementación se propone la fórmula que servirá para la evaluación de cada activo que se interconecta a la red del COCIBER, de acuerdo con las categorías que se encuentren los activos se procederá a realizar una evaluación por categorías para determinar en qué parte de la topología de la red se instalarán los sensores del SIEM.

Aceptación del riesgo

Tabla 3.14. Criterios de aceptación del riesgo

CRITERIOS DE ACEPTACIÓN DEL RIESGO	
RANGO	**DESCRIPCIÓN**
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a su tratamiento.

Fuente: Autor

- **La organización considera el riesgo poco reseñable:** la organización solo debe tomar medidas preventivas para mitigar las amenazas.
- **La organización considera el riesgo reseñable y debe proceder a su tratamiento:** se considera que se deben tomar medidas correctivas o de control para asegurar la información.

FASE DE HACER: en esta fase se procederá a realizar un estudio de los sistemas SIEM en base a la norma ISO 25000 para determinar el mejor sistema que se adapte

a la red para luego proceder a la configuración e instalación de los componentes del sistema.

La norma ISO/IEC 25000 describe qué hacer, pero no especifica cómo, en otras palabras, no detalla el procedimiento a realizar para las métricas de evaluación que se utilizarán, ni describe cómo agrupar estas métricas. Por lo que el sistema SIEM a implementarse se han alineado de acuerdo a los conceptos dados en esta norma y a la documentación oficial de cada sistema Open Source evaluado. Además de la documentación oficial existen trabajos relacionados donde se han evaluado varios parámetros que requiere un sistema SIEM, dichos trabajos se encuentran en el capítulo de Fundamentación Teórica.

Los parámetros de evaluación del sistema SIEM no se muestran en el presente capítulo, debido a que se explican detalladamente en el capítulo de implementación. Dentro de los sistemas SIEM evaluados están:

- **OSSIM:** Open Source Security Information Management por sus siglas (OSSIM) es una colección de herramientas bajo licencia GPL, fue diseñado para ayudar a los administradores de red en la seguridad de las redes, detección de intrusos y prevención. Es un sistema de código abierto y gestión de eventos (SIEM), que cuenta con la recopilación, normalización y correlación de eventos. Fue elaborado por ingenieros de seguridad debido a la falta de productos de código abierto disponibles, y tiene como objetivo específico abordar la realidad a la que se enfrentan muchos profesionales de la seguridad. OSSIM aprovecha la potencia de Open Threat Exchange [11](OTX) al permitir a los usuarios contribuir y recibir información en tiempo real sobre hosts maliciosos. (Alienvault, OSSIM: The Open Source SIEM, 2019).
- **ELK:** es el acrónimo de tres proyectos de código abierto: Elasticsearch, Logstash y Kibana. Elasticsearch es un motor de búsqueda y análisis. Logstash es un canal de procesamiento de datos del lado del servidor que ingiere datos de múltiples fuentes simultáneamente, los transforma y luego los envía a un servidor como Elasticsearch. Kibana permite a los usuarios visualizar datos con tablas y gráficos en Elasticsearch (Elastic Stack, 2019) .

[11] Open Threat Exchange es una de las plataformas de seguridad informática, con más de 80,000 participantes en 140 países que comparten diariamente más de 19 millones de amenazas potenciales. Es de uso gratuito.

- **Apache Metron:** Apache Metron proporciona un marco de análisis de seguridad avanzado y escalable construido con la Comunidad Hadoop que evoluciona del Proyecto Cisco OpenSOC. Un marco de aplicación de seguridad cibernética que proporciona a las organizaciones la capacidad de detectar anomalías cibernéticas y permitir a las organizaciones responder rápidamente a las anomalías identificadas. Apache Metron integra una variedad de tecnologías de big data de código abierto para ofrecer una herramienta centralizada para el monitoreo y análisis de seguridad. Proporciona capacidades para la agregación de registros, indexación de captura de paquetes completos, almacenamiento, análisis de comportamiento avanzado y enriquecimiento de datos, al tiempo que aplica la información de inteligencia de amenazas más actual a la telemetría de seguridad dentro de una única plataforma (Apache Metron, 2019).

Fase de Controlar: en esta fase se procederá a la instalación y configuración de sensores en puntos críticos que fueron evaluados en el análisis de riesgos, se deberá realizar un diagrama de la red con los sensores agregados y además de documentar todo el procedimiento realizado para la instalación, desde el software de virtualización ESXi hasta el sistema central.

Fase de Actuar: en esta fase se identificarán las funcionalidades que reporte el sistema SIEM y servirán para la comprobación de la hipótesis planteada en este proyecto. La hipótesis indica que el SIEM mejorará la detección eventos e incidentes en la red y en tiempo real, lo que permitirá una respuesta eficaz y oportuna frente a cualquier anomalía o intento de violación de la seguridad, para esta comprobación se extraerán los reportes del sistema y se adjuntarán al proyecto

CAPÍTULO 4

IMPLEMENTACIÓN

En el presente capítulo se demuestra la implementación del sistema SIEM basado en el ciclo Deming o PDCA, aquí se expone todas las actividades realizadas y las características técnicas de los equipos y software en el que se implementó el sistema.

4.1 APLICACIÓN DEL MODELO, ESTÁNDAR O METODOLOGÍA

Como se explicó en capítulos anteriores se hará uso del ciclo de Deming (PDCA) y a continuación se mostrará las actividades realizadas en cada fase.

4.1.1 Fase de planificación (P)

En esta fase de desarrolló una evaluación de riesgos que tenía como objetivo analizar y determinar el riesgo inherente en la red COCIBER. Para esta evaluación se aplicó la metodología Magerit v. 3.0, este tipo de metodología nos da los lineamientos para realizar un análisis sin necesariamente estar certificados, como observación general, ninguna metodología de análisis de riesgos muestra un procedimiento detallado de cómo hacer paso a paso un análisis de riesgos, por lo que en este proyecto se ha intentado hacer un análisis adecuado y aproximado a la realidad de la seguridad de la red. Las actividades que constan en la metodología seleccionada son las siguientes:

Tabla 4.15. Evaluación de riesgo

Fases de evaluación del riesgo	
Definición del alcance	Se explica cuáles serán las actividades que se realizarán en el análisis
Inventario de activos	Se identifican todos los activos conectadas a la red.
Identificación y selección de las amenazas	Se identificaron las amenazas a los que se encuentra expuesto el COCIBER.
Identificar las vulnerabilidades y salvaguardas	Se identificaron las amenazas y protocolos para asegurar la información.
Evaluación del riesgo	Se evalúa y determina el nivel de riesgo de la red.

Fuente: Autor

- **Definición del alcance:** El alcance de este análisis de riesgos es limitado ya que solo se enfoca a los activos de información que componen la red del COCIBER por los que no se ha tomado en cuenta al recurso humano u operarios, además de no tomar en cuenta la categoría de dispositivos móviles debido a que existe una política para el uso de los mismos en el COCIBER.

  Este análisis forma parte de la implementación de un SIEM y sirve para determinar cuáles son los activos con mayor criticidad y de acuerdo a la evaluación obtenida se establecerán los sensores en puntos estratégicos de la red.

- **Inventario de activos:** el inventario de activos fue realizado para determinar el número de dispositivos que se conectan a la red de datos. Este inventario permite visualizar todos los activos que poseen información importante sobre el COCIBER.

  En la siguiente tabla se visualiza el detalle del inventario de activos de la red, se indica que por razones de espacio solamente se muestran los campos de código, tipo de dispositivos, responsables, si es físico o lógico y si es crítico para la red del COCIBER, para la visualización de todos los campos se verifican en el anexo D.

Tabla 4.16. Inventario de activos de la red COCIBER

Categoría	ID	Nombre	Responsable	Tipo	¿Crítico?
COMPUTADORES DE ESCRITORIO Y PORTÁTILES	PC-01	PC	Usuario técnico	Físico	SI
	PC-02	PC	Usuario técnico	Físico	SI
	PC-03	PC	Usuario técnico	Físico	SI
	PC-04	PC	Usuario técnico	Físico	SI
	PC-05	PC	Usuario técnico	Físico	SI
	PC-06	PC	Usuario técnico	Físico	SI
	PC-07	PC	Usuario técnico	Físico	SI
	PC-08	PC	Usuario técnico	Físico	SI
	PC-09	PC	Usuario técnico	Físico	SI
	PC-10	PC	Usuario técnico	Físico	SI
	PC-11	PC	Usuario técnico	Físico	SI
	PC-12	PC	Usuario administrativo	Físico	SI
	LAP-01	Laptop	Usuario técnico	Físico	SI
	LAP-02	Laptop	Usuario técnico	Físico	SI

	LAP-03	Laptop	Usuario técnico	Físico	SI
	LAP-04	Laptop	Usuario técnico	Físico	SI
	LAP-05	Laptop	Usuario técnico	Físico	SI
	LAP-06	Laptop	Usuario técnico	Físico	SI
	LAP-07	Laptop	Servidor público	Físico	SI
	LAP-08	Laptop	Administrador de Redes	Físico	SI
	LAP-09	Laptop	Administrador de Redes	Físico	SI
	LAP-10	Laptop	Director	Físico	SI
	LAP-11	Laptop	Subdirector	Físico	SI
	LAP-12	Laptop	Jefe administrativo	Físico	SI
	LAP-13	Laptop	Jefe de personal	Físico	SI
	LAP-14	Laptop	Jefe Defensa	Físico	SI
	LAP-15	Laptop	Jefe Exploración	Físico	SI
	LAP-16	Laptop	Jefe Respuesta	Físico	SI
SEGURIDAD PERIMETRAL	SEG-01	UTM	Administrador de Redes	Físico	SI
EQUIPOS DE COMUNICACIONES	COM-01	Switch	Administrador de Redes	Físico	SI
	COM-02	Switch	Administrador de Redes	Físico	SI
	COM-03	Switch	Administrador de Redes	Físico	SI
	COM-04	Switch	Administrador de Redes	Físico	SI
	COM-05	Switch	Administrador de Redes	Físico	SI
	COM-06	Router	Administrador de Redes	Físico	SI
SERVICIOS Y APLICACIONES	SA-01	Plataformas de virtualización	Administrador de Redes	Físico	SI
	SA-02	Plataformas de virtualización	Administrador de Redes	Físico	SI
	SA-03	Servicio DNS	Administrador de Redes	Virtual	SI
	SA-04	Servicio DNS	Administrador de Redes	Virtual	NO
	SA-05	Servidor de Correo	Administrador de Redes	Virtual	SI
	SA-06	Página Web	Administrador de Redes	Virtual	SI
	SA-07	Antispam	Administrador de Redes	Virtual	NO
	SA-08	Gestor de Tickets	Administrador de Redes	Virtual	NO
	SA-09	Servidor de archivos	Administrador de Redes	Virtual	NO
	SA-10	Only Office	Administrador de Redes	Virtual	NO
	SA-11	Owncloud	Administrador de Redes	Virtual	SI
	SA-12	Disco de almacenamiento 01 (RAID)	Usuario técnico forense	Físico	SI

	SA-13	Disco de almacenamiento 02 (RAID)	Usuario técnico forense	Físico	SI
	SA-14	Disco de almacenamiento	Usuario técnico forense	Físico	SI
	SA-15	Equipo FRED	Usuario técnico forense	Físico	SI
	SA-16	RACTACC	Usuario técnico forense	Físico	SI
EQUIPOS UPS Y ENFRIAMIENTO	AE-01	Equipo UPS	Administrador de Redes	Físico	SI
	AE-02	Equipo UPS	Administrador de Redes	Físico	SI
	AE-03	Equipo UPS	Administrador de Redes	Físico	SI
	AE-04	Aire acondicionado	Administrador de Redes	Físico	SI
SISTEMAS SEGURIDAD FÍSICA	SF-01	Equipo biométrico	Administrador de Redes	Físico	SI
	SF-02	Equipo biométrico	Administrador de Redes	Físico	SI
	SF-03	Equipo biométrico	Administrador de Redes	Físico	SI
	SF-04	Cámaras de seguridad	Administrador de Redes	Físico	SI
	SF-05	Cámaras de seguridad	Administrador de Redes	Físico	SI

Fuente: Autor

- **Identificación y selección de las amenazas:** las amenazas fueron filtradas de la metodología Magerit, debido a que existen amenazas que no tienen riesgo de materializarse. El listado se realizó con la ayuda proporcionada del administrador de red, ver anexo G (Acta de reunión). Las amenazas seleccionadas son las siguientes:

Tabla 4.17. Catálogo de amenazas

No.	Tipo	Nomenclatura	Amenaza
1	[N] Desastres Naturales	N1	Fuego
2		N2	Daños por agua
3		N*	Desastres naturales
4	[I] De origen industrial	I1	Corte del suministro eléctrico
5		I2	Condiciones inadecuadas de temperatura o humedad
6		I3	Fallo de servicios de comunicaciones
7		I4	Interrupción de otros servicios y suministros esenciales
8		I*	Otros desastres industriales
9		E1	Errores de los usuarios
10		E2	Errores del administrador

11	[E] Errores y fallos no intencionados	E3	Errores de configuración
12		E4	Degradación de los soportes de almacenamiento de la información
13		E5	Errores de mantenimiento / actualización de programas (software)
14		E6	Errores de mantenimiento / actualización de equipos (hardware)
15		E7	Caída del sistema por sobrecarga
16		E8	Pérdida de equipos
17		E9	Indisponibilidad del personal
18	[A]Ataques intencionados	A1	Robo físico
19		A2	Denegación de servicio
20		A3	Robo de información
22		A5	Extorsión
23		A6	Ingeniería social
24		A7	Fuga de información
25		A8	Introducción de falsa información
26		A9	Interceptación de información (escucha)
27		A10	Accesos no autorizados
28		A11	Abuso de privilegios
29		A12	Alteración deliberada de la información
30		A13	Corrupción de la información
31		A14	Destrucción de información
32		A15	Difusión de software dañino

Fuente: Autor

- **Identificar las vulnerabilidades y salvaguardas:** en el COCIBER se cuenta con procedimientos de gestión de incidentes y eventos de seguridad, entre las políticas y procedimientos principales se mencionan los siguientes y se pueden verificar en el anexo H:
    - De gestión de incidentes y seguridad
    - Tratamiento de la información
    - Protección de datos en diferentes medios
    - Intercambio de información
    - Respaldo de la información
    - Uso aceptable de medios
    - Comunicaciones
    - Educación y entrenamiento
    - Uso de dispositivos móviles.

Los procedimientos existentes para respuesta a incidentes son:

- Infección por gusanos
- Intrusiones en sistemas Windows, Linux
- Ataques de DoS
- Actividad maliciosa en la red
- Ataques a sitios web
- Infección de malware en PC´s y dispositivos móviles
- Ingeniería social
- Fuga de información
- Abuso de privilegios
- Estafas
- Infracción de marca registrada

Además de los procedimientos descritos se cuenta también con un procedimiento ante vulnerabilidades nuevas, este procedimiento fue indicado verbalmente y se encuentra en la sección de tabulación de resultados del capítulo Marco Metodológico.

Se pueden visualizar las políticas y procedimientos con los que cuenta el COCIBER en el anexo G.

- **Evaluación del riesgo:** con la evaluación se identifica cuál es el nivel de riesgo inherente existente, lo que sirve para la aplicación de los controles que es el sistema SIEM mejorando la detección de incidentes y ayudando con la comprobación de la hipótesis planteada en este proyecto.

  Se ha tomado como referencia la valoración **cuantitativa** para determinar la probabilidad y el impacto de que una amenaza ponga en grave riesgo a la seguridad de la información.

Tabla 4.18. Probabilidad de materialización de amenazas

Cuantitativo	Descripción
1	Ocurre una vez al año
2	Ocurre una vez al mes
3	Ocurre una vez cada semana

Fuente: Autor

Tabla 4.19. Impacto o consecuencias

Cuantitativo	Descripción
1	No tiene consecuencias relevantes
2	Tiene consecuencias reseñables
3	Tiene consecuencias graves para la organización

Fuente: Autor

La descripción de impacto y probabilidades ya fueron expuestas en el capítulo de Propuesta, y así mismo se utilizará la fórmula propuesta a continuación que sirve para determinar el nivel de riesgo:

Fórmula 4.1. Fórmula de cálculo

$$RIESGO=PROBABILIDAD * AMENAZAS$$

Fuente: Autor

En la siguiente tabla se definen los criterios de aceptación del riesgo:

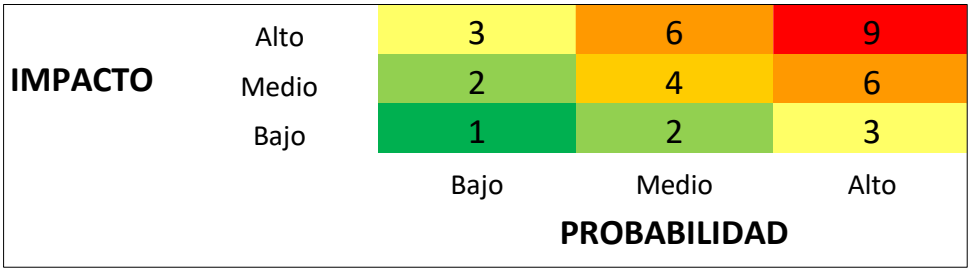
Tabla 20. Criterios de aceptación del riesgo

RANGO	DESCRIPCIÓN
Riesgo <= 4	La organización considera el riesgo poco reseñable.
Riesgo > 4	La organización considera el riesgo reseñable y debe proceder a su tratamiento.

Fuente: Autor

Con los criterios y valoraciones definidas se realizó el análisis que determinó el nivel de riesgo en las diferentes categorías del inventario de los activos, el nivel corresponde a un color que puede ser visualizado en la siguiente figura.

Figura 4.8. Nivel de riesgo



Fuente: Autor

Una vez expuestos todos criterios y valoraciones se procedió a la clasificación y evaluación de los activos en distintas categorías, a continuación, se muestra una descripción de cada categoría que se ha evaluado:

- COMPUTADORES: son todos los dispositivos para uso laboral del personal de directores, técnicos y administrativos del COCIBER.
- DISPOSITIVOS DE SEGURIDAD PERIMETRAL: son todos los dispositivos que mantienen la función de evitar intrusiones de red, en el COCIBER existe el UTM que se compone de un firewall, antivirus, antispam, IDS y un router.
- EQUIPOS DE COMUNICACIONES: son todos los dispositivos que se interconectan y configuran para el acceso a la red de todos los activos, aquí se encuentran los enrutadores y conmutadores (routers y switches).
- SERVICIOS Y APLICACIONES: comprende a los servicios que se encuentran en la red COCIBER, varios de estos son parte fundamental de los procesos, debido a que en los mismos se gestiona mucha información como: respaldos, software licenciado e información reservada.
- SEGURIDAD FÍSICA: son todos los dispositivos utilizados para la seguridad física, tales como: biométricos, cámaras de seguridad, entre otros.

La evaluación del riesgo en el COCIBER nos permite identificar los siguientes niveles de riesgos encontrados en las categorías indicadas anteriormente:

Tabla 21. Nivel de riesgo

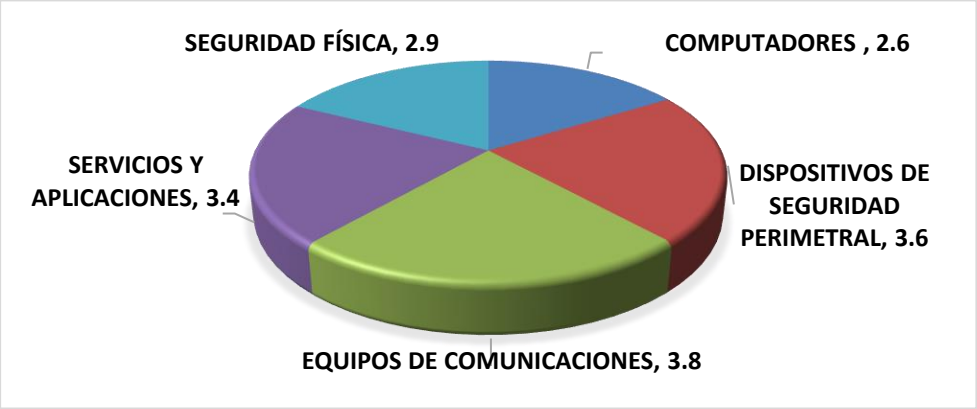
CATEGORÍAS	NIVEL DE RIESGO	DESCRIPCIÓN
COMPUTADORES	2,6	MEDIO
DISPOSITIVOS DE SEGURIDAD PERIMETRAL	3,6	ALTO
EQUIPOS DE COMUNICACIONES	3,8	ALTO
SERVICIOS Y APLICACIONES	3,4	MEDIO
SEGURIDAD FÍSICA	2,9	BAJO

Fuente: Autor

La matriz de riesgos en su totalidad se encuentra en el Anexo F del proyecto, en la misma se detallan las amenazas que se pueden dar en cualquiera de los activos o servicios de la red y que suponen un peligro para la seguridad. En esta sección se expondrá únicamente los resultados obtenidos del cálculo del riesgo que permite

identificar en que categoría de los activos de información se deberán implementar los sensores del sistema SIEM como medida de tratamiento de riesgo. En la siguiente figura se detalla el riesgo inherente:

Figura 4.9. Riesgo Inherente



Fuente: Autor

Según los resultados que se obtienen del análisis de riesgos realizado al COCIBER podemos mencionar el resumen del análisis de cada categoría:

CATEGORÍA 1: Computadores - nivel de riesgo 2.6% (Riesgo Medio): se considera que existe un riesgo **MEDIO** de producirse amenazas en la categoría de Computadoras, a pesar de que se demuestra en los anexos que los activos de esta categoría se encuentran con contraseñas y discos cifrados, así como también en el caso de las portátiles no pueden ser llevadas fuera de la unidad.

CATEGORÍA 2: Dispositivos de seguridad perimetral - nivel de riesgo 3.6% (Riesgo Alto): se considera que existe un riesgo **ALTO** de producirse amenazas en la categoría de Dispositivos de Seguridad perimetral que comprende al UTM (firewall, antivirus, IDS, Router, Antispam) y precisamente, el problema de este proyecto se centra en esta sección debido a que los equipos no han sido correctamente actualizados y configurados por lo que varias amenazas han ingresado a la red interna, estas amenazas se encuentran detalladas en la primera sección de este proyecto. Todas las amenazas que se han materializado no fueron detectadas por estos equipos por lo que su intrusión causó un peligro a la información de varios usuarios.

CATEGORÍA 3: Equipos de comunicaciones - nivel de riesgo 3.8% (Riesgo Alto): se considera que existe un riesgo **ALTO** de producirse amenazas en la categoría de Equipos de Comunicaciones porque la seguridad perimetral no ha sido bien gestionada en los últimos meses por lo que estos dispositivos que interconectan a todos los usuarios han permitido todo tipo de tráfico sin ser analizados a través de la red.

CATEGORÍA 4: Servicios y aplicaciones - nivel de riesgo 3.4% (Riesgo Medio): se considera que existe un riesgo **MEDIO** de producirse amenazas en la categoría de Servicio y aplicaciones, a pesar de que la mayoría de estos servicios se encuentran instalados en un centro de datos estratégico con las seguridades físicas respectivas. Es importante colocar un sensor en este segmento de red, ya que la pérdida o intrusión a la información de esta categoría pondría en grave riesgo la seguridad de las unidades y personal, debido a que existe información reservada de vulnerabilidades e incidentes de las unidades de las FF.AA., así como también los sistemas y respaldos necesarios para las operaciones del COCIBER.

CATEGORÍA 5: Seguridad Física - nivel de riesgo 2.9% (Riesgo Bajo): se considera que existe un riesgo **BAJO** de producirse amenazas en la categoría de Seguridad Física, debido a que existen dispositivos biométricos y cámaras de seguridad, el sistema biométrico se encuentra registrado únicamente para personal autorizado al centro de datos. A pesar de que el riesgo es bajo en esta categoría no hay que descartar tomar medidas alternas ya que siempre habrá riesgo de desastres naturales que ponen en peligro las instalaciones.

4.1.2 Fase de Hacer (D)

En esta fase del modelo PDCA se realizó la evaluación de un sistema SIEM que permitió una adecuada selección para la implementación. Aquí se realizó la evaluación en base a la norma ISO 25000 y los sistemas Open Source seleccionados para la comparación fueron: OSSIM, ELK y Apache Metron descritos en el capítulo anterior.

Antes de iniciar la evaluación de los sistemas se debe tomar en cuenta que al ser sistemas Open Source se pueden adaptar y modificar libremente y de acuerdo a los

requerimientos de cada usuario, sin embargo, para el desarrollo de este proyecto se descarga un sistema que cumpla con la mayoría de los requerimientos. Además de la evaluación del SIEM con la norma ISO 25000, se pretende corroborar la evaluación y selección de sistemas SIEM expuestos en trabajos de grado anteriores y que se encuentran en la Fundamentación Teórica de este proyecto, en la que se analiza las características técnicas y operativas.

Las características evaluadas fueron obtenidas de la documentación expuesta en las páginas web oficiales de cada sistema:

- Software OSSIM: https://www.alienvault.com/documentation/
- Software ELK: https://www.elastic.co/guide/index.html
- Software Apache Metron: http://metron.apache.org/documentation/

La norma ISO 25000 evalúa ocho (08) características para un adecuado modelo de calidad, que pueden ser visualizadas en la figura 12 y la descripción detallada a continuación:

Figura 4.10. Características ISO 25000

Fuente: Portal ISO 25000

Característica 1: Adecuación Funcional

Representa la capacidad del producto software para proporcionar funciones que satisfacen las necesidades declaradas e implícitas, cuando el producto se usa en las condiciones especificadas (ISO, 2014), las características incluidas en el SIEM se analizan en la siguiente tabla:

Tabla 4.22. Evaluación de la adecuación funcional

Subcaracterística	Requerimientos	OSSIM	ELK	Apache Metron
	Recolección y análisis de los logs	X	X	X

Completitud funcional	Correlación de logs	**X**		**X**
	Integración con otras herramientas	**X**	**X**	**X**
	Análisis de vulnerabilidades	**X**		
Corrección funcional	Determinar los niveles de seguridad de los eventos detectados	**X**		
	Inventario y descubrimiento de activos	**X**	**X**	**X**
	Determinar los dispositivos que más eventos han generado	**X**	**X**	**X**
Pertinencia funcional	Creación de usuarios	**X**	**X**	**X**
	Administración de niveles de usuario	**X**		**X**
	El sistema registrará las actividades del sistema	**X**	**X**	**X**

Fuente: Autor

En esta característica evaluada se selecciona a OSSIM por ser el sistema que cumple con todos los requerimientos de la adecuación funcional.

Característica 2: Eficiencia de desempeño

Esta característica representa el desempeño relativo a la cantidad de recursos utilizados bajo determinadas condiciones (ISO, 2014).

Tabla 4.23. Evaluación de eficiencia de desempeño

Subcaracterística	Requerimientos	OSSIM	ELK	Apache Metron
Comportamiento temporal	Detección en tiempo real de eventos	**X**	**X**	**X**
	Emisión de alertas en tiempo real	**X**	**X**	**X**
Utilización de recursos	Funcionar con un mínimo de 4 GB de memoria RAM	**X**	**X**	**X**
	Funcionar con un disco de almacenamiento de mínimo 100 GB	**X**	**X**	**X**
	Funcionará con un procesador de 3.0 GHz	**X**	**X**	**X**
	El S.O. deberá ser de Arquitectura de 64 bits	**X**	**X**	**X**
Capacidad	Deberá soportar como mínimo 10 usuarios de administración	**X**	**X**	**X**
	Deberá soportar como mínimo la integración de 100 dispositivos en la red	**X**	**X**	**X**
	Deberá ser capaz de funcionar en ambientes físicos o virtuales	**X**	**X**	**X**

Fuente: Autor

Todos los sistemas SIEM evaluados cumplen con la característica de eficiencia de desempeño requerida para la implementación en el SIEM.

Característica 3: Compatibilidad

Es la capacidad de dos o más sistemas o componentes para intercambiar información y/o llevar a cabo sus funciones requeridas cuando comparten el mismo entorno hardware o software (ISO, 2014).

Tabla 4.24. Evaluación de la compatibilidad

Subcaracterística	Requerimientos	OSSIM	ELK	Apache Metron
Interoperabilidad	Integración de sensores de otros fabricantes	**X**	**X**	**X**
	Instalación sobre cualquier sistema operativo			

Fuente: Autor

Las tres (03) soluciones de seguridad SIEM cumplen con integrarse a sensores o agentes de otros fabricantes, pero no todos son compatibles con todos los sistemas operativos, ya que éstos se instalan únicamente bajo versiones Linux.

Característica 4: Usabilidad

Es la capacidad del producto software para ser entendido, aprendido, usado y resultar atractivo para el usuario, cuando se usa bajo determinadas condiciones (ISO, 2014):

Tabla 4.25. Evaluación de la característica de Usabilidad

Subcaracterística	Requerimientos	OSSIM	ELK	Apache Metron
Capacidad de adecuación	Acceso por entorno web	**X**	**X**	**X**
	Ingreso a la interfaz desde cualquier navegador	**X**	**X**	**X**
	Todos los módulos deben realizarse en distintos menús	**X**	**X**	**X**
Capacidad para ser usado	Monitorización de eventos desde la interfaz	**X**	**X**	**X**
	Monitorización de los recursos del sistema	**X**		
	Permitirá la creación de políticas	**X**	**X**	**X**
	Permitirá la valoración de activos	**X**		
	Permitirá la valoración de amenazas	**X**		
	Permitir generación de reportes	**X**	**X**	**X**
	Permitir generación de reportes personalizados	**X**		
Protección contra errores de usuario	Validar la entrada de datos de los usuarios a la interfaz	**X**	**X**	**X**
Estética de la interfaz	La interfaz deberá ser de fácil uso para el operario	**X**	**X**	**X**

Fuente: Autor

De acuerdo a la evaluación de usabilidad de los sistemas SIEM el sistema seleccionado en esta característica es el OSSIM.

Característica 5: Fiabilidad

Es la capacidad de un sistema o componente para desempeñar las funciones especificadas, cuando se usa bajo unas condiciones y periodo de tiempo determinados (ISO, 2014):

Tabla 4.26. Evaluación en base a la Fiabilidad

Subcaracterística	Requerimientos	OSSIM	ELK	Apache Metron
Madurez	Evitar fallos en situaciones normales	**X**	**X**	**X**
Disponibilidad	Deberá ser capaz de trabajar 24/7	**X**	**X**	**X**
Tolerancia a fallos	El sistema funcionará y mostrará un aviso en caso de fallo de software	**X**		
Capacidad de recuperación	El sistema deberá guardar la integridad de los datos obtenidos	**X**	**X**	**X**

Fuente: Autor

De acuerdo con la evaluación obtenida se selecciona al sistema OSSIM, por ser el único sistema SIEM que muestra notificaciones en el navegador al momento de producirse un fallo de software.

Característica 6: Seguridad

Es la capacidad de protección de la información y los datos de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos (ISO, 2014):

Tabla 4.27. Evaluación de la seguridad

Subcaracterística	Requerimientos	OSSIM	ELK	Apache Metron
Confidencialidad	La consola de comandos deberá ser de acceso único al administrador	**X**	**X**	**X**
	La interfaz web será usada únicamente por personal técnico asignado	**X**	**X**	**X**
	La consola y la interfaz web deben poseer credenciales de acceso	**X**	**X**	**X**
	Las comunicaciones deben ser cifradas para evitar cualquier robo de información	**X**	**X**	
Integridad	Las contraseñas deben caducar después de un límite de tiempo	**X**		
	Registrar los usuarios que ingresan al sistema	**X**	**X**	**X**
	Permitir una cantidad de intentos para acceder al sistema	**X**	**X**	**X**
	Validar entradas de ataques de tipo SQL injection, XSS, DoS, entre otros	**X**	**X**	**X**
No repudio	El sistema almacena las actividades de cada usuario	**X**	**X**	**X**
Autenticidad	Identificación de direcciones IP, desde la cual se ingresa al sistema	**X**	**X**	**X**
	Identificación de S.O., desde la cual se ingresa al sistema	**X**	**X**	**X**

Fuente: Autor

En esta característica OSSIM vuelve a ser seleccionado debido a que los otros sistemas SIEM no cumplen con todos los parámetros de seguridad requeridos.

Característica 7: Mantenibilidad

Esta característica representa la capacidad del producto software para ser modificado efectiva y eficientemente, debido a necesidades evolutivas, correctivas o perfectivas (ISO, 2014):

Tabla 4.28. Evaluación con respecto a la Mantenibilidad

Subcaracterística	Requerimientos	OSSIM	ELK	Apache Metron
Modularidad	Los módulos que se integren no deben tener conflictos con componentes adicionales	**X**		
Capacidad para ser modificado	El sistema debe permitir la modificación/eliminación de configuraciones del sistema	**X**	**X**	**X**
	Modificación/eliminación de componentes del sistema	**X**	**X**	**X**
Capacidad para ser probado	Comprobación en el sistema de cambios realizados	**X**	**X**	**X**

Fuente: Autor

Debido a que el sistema SIEM es Open Source cumple con las características de Mantenibilidad, es decir, se pueden agregar o quitar funcionalidades en el sistema de acuerdo con el nivel de conocimiento de los administradores o técnicos.

Característica 8: Portabilidad

Esta característica representa la capacidad del producto software para ser modificado efectiva y eficientemente, debido a necesidades evolutivas, correctivas o perfectivas (ISO, 2014):

Tabla 4.29. Evaluación de la Portabilidad

Subcaracterística	Requerimientos	OSSIM	ELK	Apache Metron
Adaptabilidad	El sistema debe ser capaz de adaptarse a los componentes actuales de la red	**X**	**X**	**X**
Capacidad para ser instalado	El sistema podrá instalarse y desinstalarse en cualquier momento	**X**	**X**	**X**
Capacidad para ser reemplazado	El sistema no tendrá conflictos para reemplazarse por un sistema del mismo propósito	**X**	**X**	**X**

Fuente: Autor

Esta característica de evaluación se cumple en todos los sistemas evaluados ya que se aplica nuevamente los principios de Open Source, en la cual un software puede ser descargado, modificado, distribuido o eliminado.

Conclusiones de la evaluación

- Los sistemas de libre distribución (Open Source) pueden ser modificados y adaptados como convenga a los requerimientos de cada administrador, pero en este caso se implementará el sistema con sus funcionalidades originales.
- Esta selección ha evaluado de manera eficiente las características de los sistemas SIEM en base a la Norma ISO 25000, un estándar reconocido. En trabajos anteriores y descritos en el marco metodológico de este proyecto únicamente se evalúan ciertas funcionalidades y precios, pero sin basarse a alguna metodología o norma reconocida.
- El sistema que cumple con la mayoría de las características técnicas y operativas es el **OSSIM**, por lo tanto, es el sistema seleccionado para implementarse en la red COCIBER.

4.1.3 Fase de Control (C)

A continuación, se demuestra las actividades realizadas para la instalación y configuración de sensores en los distintos puntos de la red COCIBER. La implementación consiste en documentar desde la instalación a partir de la descarga y su creación dentro del entorno virtualizado. En la siguiente figura se incluye la topología de la red y la ubicación de los sensores instalados:

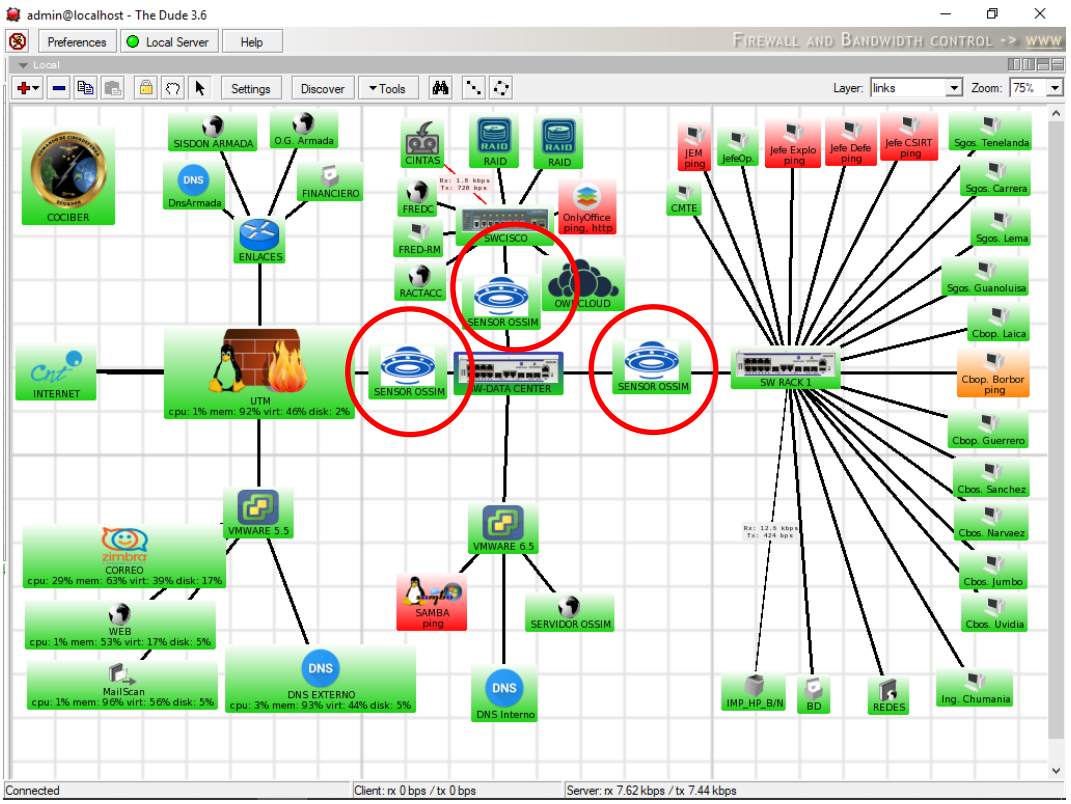


Figura 4.11. Diagrama actual de la red con los sensores OSSIM

Fuente: COCIBER

4.1.4 Fase de Actuar (A)

Para esta fase se ha tomado como referencia la visualización de reportes que ha emitido el sistema acerca de las amenazas y eventos detectados hasta la fecha. Los reportes que emite el sistema pueden ser verificados por las siguientes categorías:

- Reporte de alarmas
- Reporte de activos
- Reporte de registros
- Reporte de eventos de seguridad
- Reporte de operaciones de seguridad
- Reporte de Tickets
- Reporte de actividad de los usuarios
- Reportes personalizados

Todos estos reportes pueden ser visualizados en el Anexo I.

4.2 DISEÑO

A partir del análisis de riesgos obtenido se configuraron dos sensores adicionales en la red del COCIBER, los mismos están distribuidos en las diferentes redes VLAN segmentadas del COCIBER, tal como se puede apreciar en la figura 13.

El sistema OSSIM seleccionado como plataforma SIEM se instalará en un servidor que cuenta con las siguientes características de hardware y software:

Tabla 4.30. Características Técnicas del hardware

Hardware	
Fabricante	HP
Modelo	Proliant ML 110 G6
CPU	4 CPUs x Intel(R) Xeon(R) CPU X3430 @ 2.40GHz
Memoria	8 GB
Almacenamiento	500 GB

Fuente: Autor

Tabla 4.31. Hipervisor ESXi

VMware vSphere 6 Enterprise Plus	
Clave:	JV425-XXX-XXX-XXX-XXX
Fecha de caducidad:	Nunca
Características:	Versión full

Fuente: Autor

4.2.1 Configuración de características técnicas

El sistema SIEM se instalará dentro del hipervisor ESXi de VMWare, el COCIBER cuenta con la licencia respectiva de este producto, como se aprecia en la tabla 27. Una de las ventajas de este hipervisor es que se accede a la consola de administración mediante ambiente web (por seguridad no se mostrarán las direcciones IP), ver figura 14.

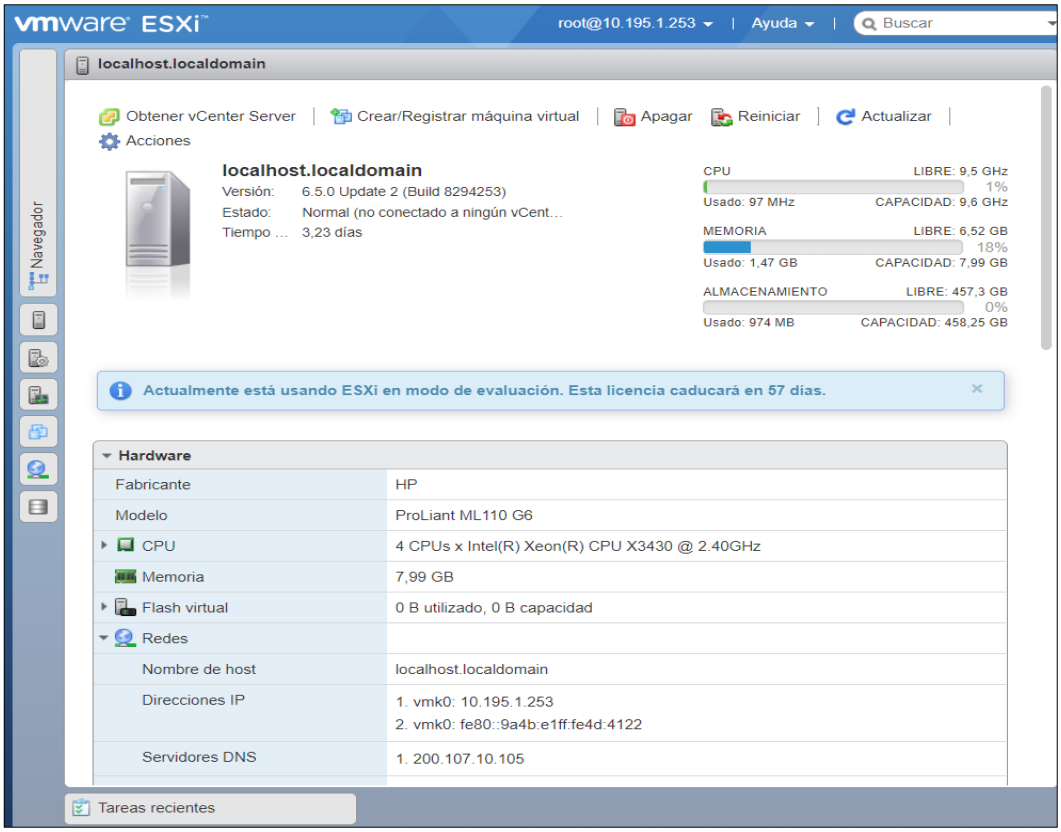


Figura 4.12. Diagrama actual de la red con los sensores OSSIM

Fuente: COCIBER

Para verificar la instalación del sistema OSSIM, véase el anexo I.

Una vez finalizada la instalación se encuentran algunas opciones y alarmas, donde podremos revisar los eventos generados por el sistema o eventos de seguridad donde encontramos todos los registros que han llegado al sistema, podemos hacer filtros sobre ellos y exportarlos en formato csv o pdf, o bien ver cómo llegan en tiempo real, y en la opción de tickets donde se puede encontrar los que se han generado en el sistema automáticamente, su usuario encargado y su estado actual, ver las siguientes figuras:

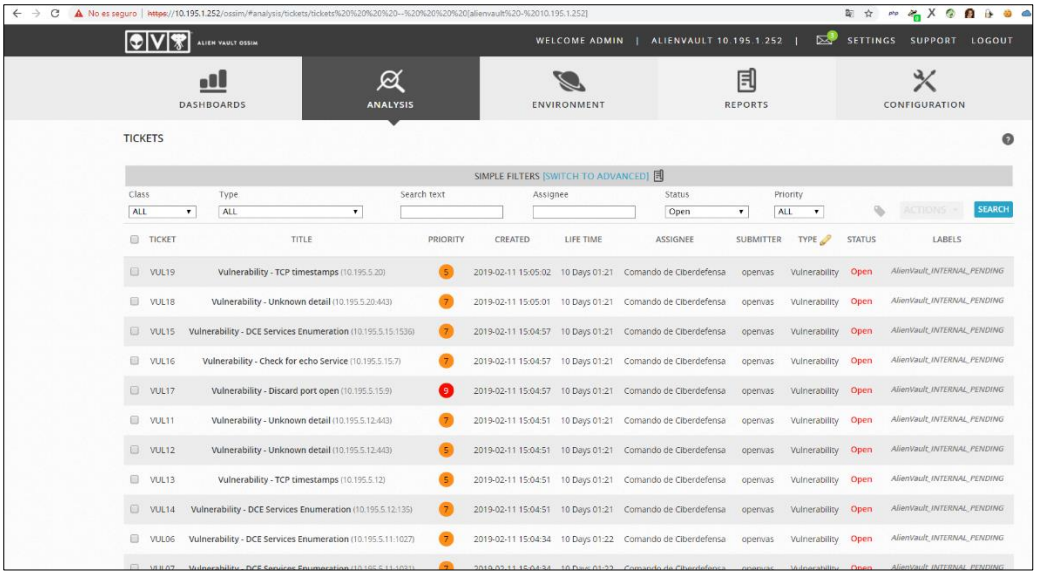


Figura 4.13. Vista de eventos del sistema

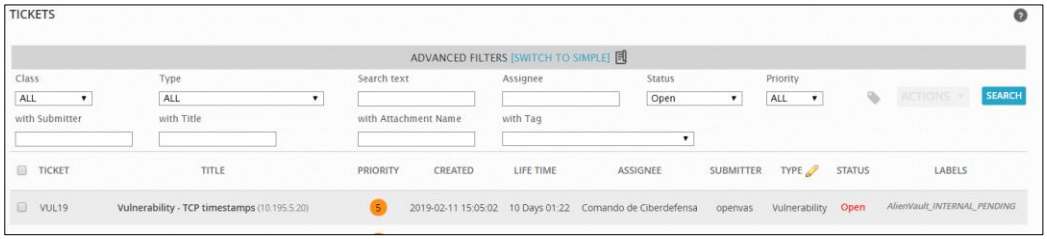


Figura 4.14. Filtros

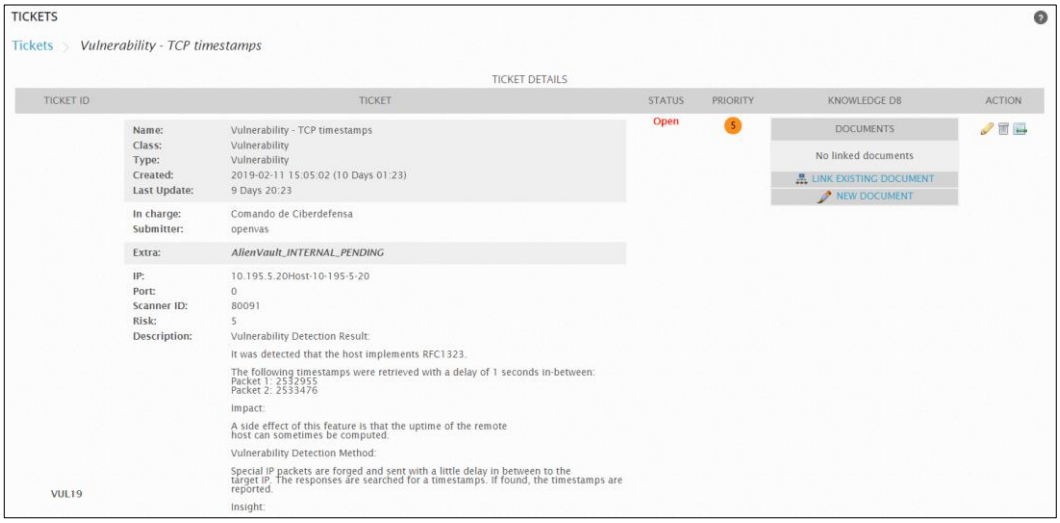


Figura 4.15. Vista detallada de cada evento

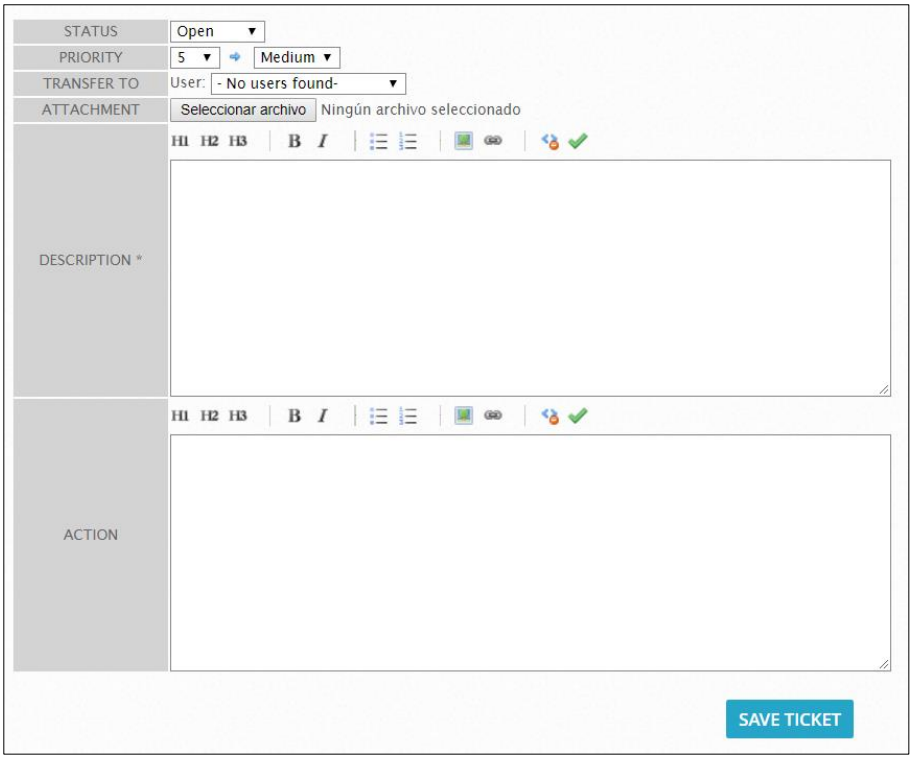


Figura 4.16. Asignación de usuarios

4.2.2 Acceso a la configuración por consola de OSSIM

El sistema OSSIM puede ser modificado o personalizado de acuerdo con las configuraciones de cada administrador. Se puede acceder a la consola de configuración de OSSIM de una de las siguientes maneras:

- **Administración local:** mediante el uso de un monitor, teclado y ratón conectados directamente al hardware de instalación de OSSIM.
- **Administración virtual:** los usuarios de dispositivos virtuales acceden a la consola a través de un cliente SSH como Bitvise.

Para simplificar el procedimiento, las siguientes figuras hacen referencia a la interfaz de usuario (IU) del cliente Bitvise SSH como un medio para explicar cómo acceder a la consola del sistema.

- Iniciar Bitvise SSH y, en el campo Nombre de host (o dirección IP), escriba la dirección IP del dispositivo.
- Verificar que SSH está seleccionado.
- Seleccionar Abrir.

En la ventana de consola que aparece ingrese las credenciales de usuario que usó en la instalación del sistema y luego presione la tecla **Enter**, ver la siguiente figura.

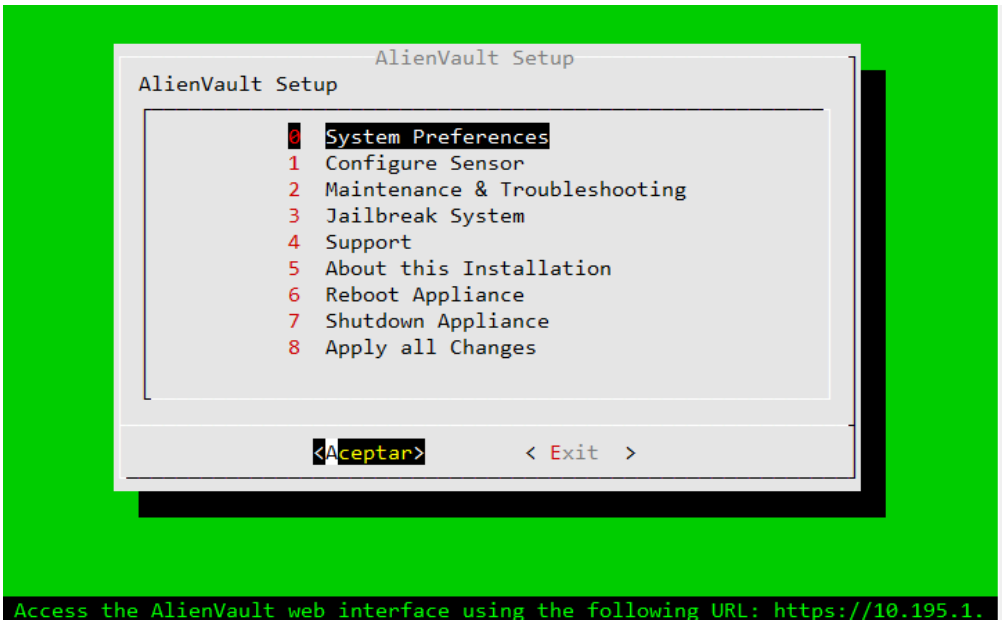


Figura 17. Acceso a la consola

Aparece la pantalla de inicio del sistema, a continuación, se describe la configuración que se puede hacer en cada una de las opciones que aparece:

- **Preferencias del sistema:** en este módulo se puede configurar todo el sistema, como configurar la red, nombre del sistema, cambio de contraseñas y configuración de archivos de OSSIM e incluso agregar mejoras al sistema.
- **Configuración del sensor:** en este módulo se configuran las redes que se desean monitorear, así como también los agentes que envíen los datos hacia el servidor.
- **Mantenimiento y solución de problemas:** OSSIM no ofrece una herramienta para realizar copias de seguridad o restaurar todo el sistema de forma colectiva. Sin embargo, se puede hacer una copia de seguridad o restaurar sus datos y las configuraciones del sistema por separado. También puede restaurar el dispositivo de hardware de USM Appliance a su estado de fábrica si es necesario (Alienvault, USM Appliance Deployment Guide, 2019).
- **Consola:** brinda el acceso a la línea de comandos del OSSIM, esto es fundamental ya que más abajo se visualiza cuáles son los archivos existentes a los cuales se ingresará para la creación o modificación de reglas.

- **Soporte:** este menú ofrece ayuda remota, generalmente es utilizado para las versiones de pago del sistema OSSIM.
- **Información de la instalación OSSIM:** este menú brinda información acerca de la instalación del sistema, como la fecha de instalación, versión y el ID del sistema.
- **Reinicio:** Reinicia el sistema.
- **Apagado:** Apaga el sistema.
- **Aplicar cambios realizados:** una vez que haya realizado alguna modificación o eliminación de funcionalidades se deberán guardar obligatoriamente los cambios para OSSIM empiece a trabajar con los cambios realizados.

4.3 COMPROBACIÓN DE HIPÓTESIS

La hipótesis planteada es de tipo general o teórica en la cual la comprobación se puede realizar a través de las observaciones realizadas con el sistema OSSIM.

Para las observaciones se tomaron en cuenta los reportes emitidos por el sistema y en la cual se deduce que la implementación del SIEM en el COCIBER **SÍ** mejora la detección de eventos e incidentes de seguridad en la red y en tiempo real, esto permite una respuesta eficaz y oportuna frente a cualquier anomalía o intento de violación de la seguridad de la información.

A continuación, se demuestra en las siguientes figuras los reportes realizados con OSSIM y el proceso de gestión automatizada que el sistema realiza, facilitando de esta manera el trabajo del administrador, ver Anexo I para visualizar más detalles.

Reporte de alarmas: muestra un reporte acerca de las amenazas existentes en la red, clasificadas según su prioridad, además muestra datos como direcciones IP de origen del atacante.

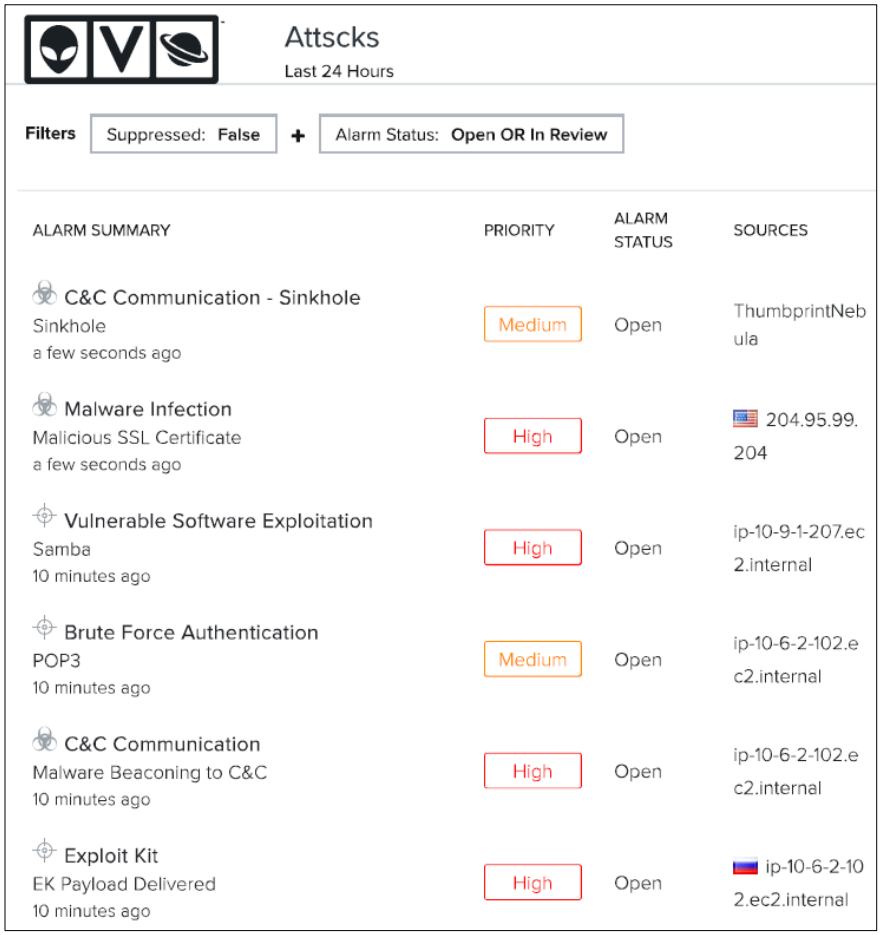


Figura 4.18. Reporte de alarmas

Reporte de eventos: muestra un reporte del tráfico en tiempo real de red, además de eso muestra un gráfico estadístico de los usuarios que generan más actividad en la red.

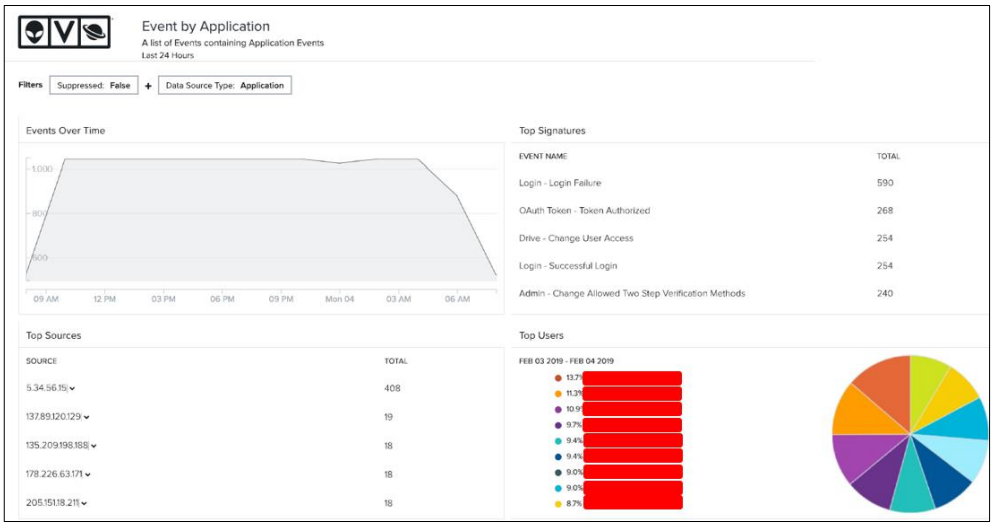
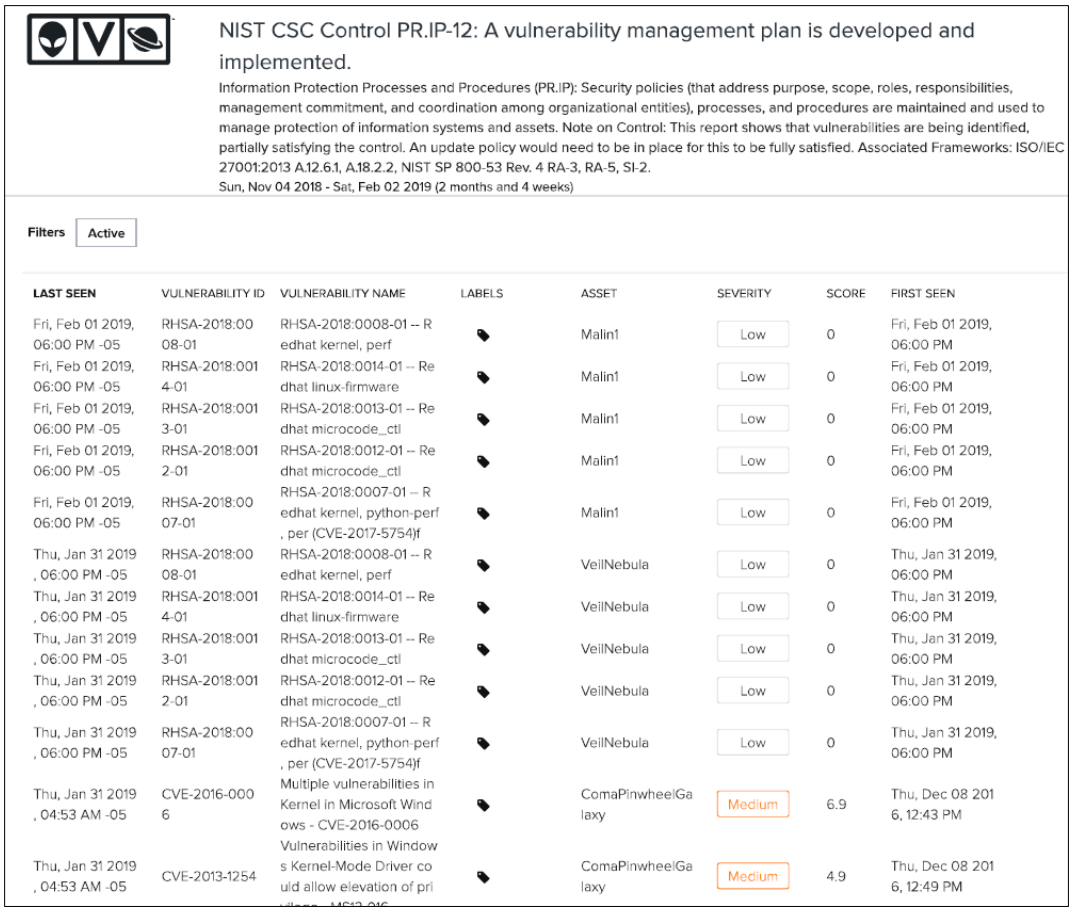


Figura 4.19. Reporte de eventos

Reporte de vulnerabilidades: gracias al componente de identificación de activos, permite al sistema realizar un análisis de vulnerabilidades a los activos presentes en la red, esto es fundamental ya que se gestionará automáticamente el tratamiento de vulnerabilidades realizado por el personal de guardia.



NIST CSC Control PR.IP-12: A vulnerability management plan is developed and implemented.

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. Note on Control: This report shows that vulnerabilities are being identified, partially satisfying the control. An update policy would need to be in place for this to be fully satisfied. Associated Frameworks: ISO/IEC 27001:2013 A.12.6.1, A.18.2.2, NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2.

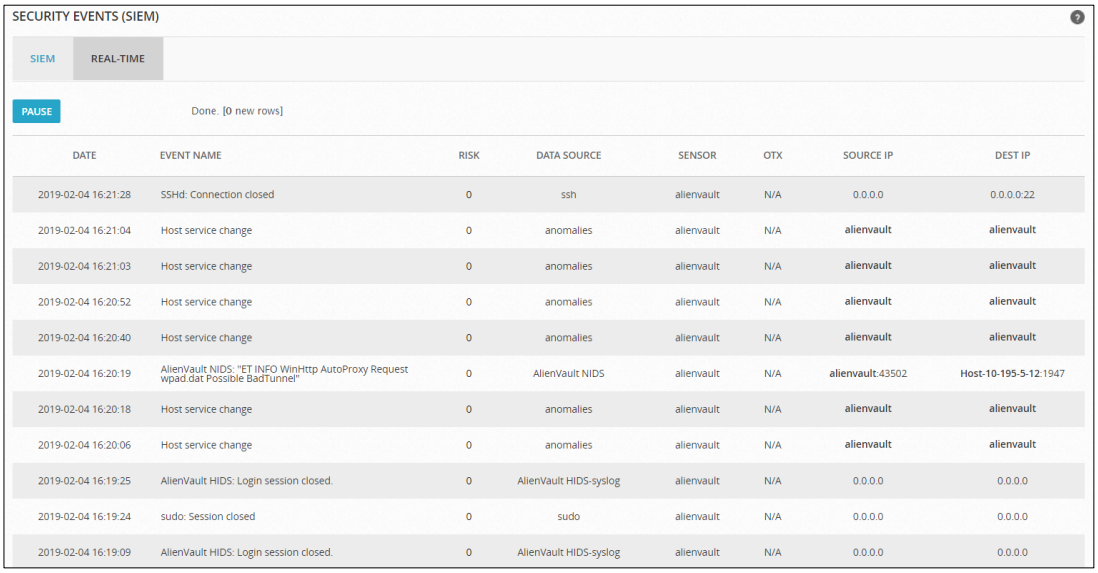
Sun, Nov 04 2018 - Sat, Feb 02 2019 (2 months and 4 weeks)

Filters Active

LAST SEEN	VULNERABILITY ID	VULNERABILITY NAME	LABELS	ASSET	SEVERITY	SCORE	FIRST SEEN
Fri, Feb 01 2019, 06:00 PM -05	RHSA-2018:0008-01	RHSA-2018:0008-01 -- Redhat kernel, perf		Malin1	Low	0	Fri, Feb 01 2019, 06:00 PM
Fri, Feb 01 2019, 06:00 PM -05	RHSA-2018:0014-01	RHSA-2018:0014-01 -- Redhat linux-firmware		Malin1	Low	0	Fri, Feb 01 2019, 06:00 PM
Fri, Feb 01 2019, 06:00 PM -05	RHSA-2018:0013-01	RHSA-2018:0013-01 -- Redhat microcode_ctl		Malin1	Low	0	Fri, Feb 01 2019, 06:00 PM
Fri, Feb 01 2019, 06:00 PM -05	RHSA-2018:0012-01	RHSA-2018:0012-01 -- Redhat microcode_ctl		Malin1	Low	0	Fri, Feb 01 2019, 06:00 PM
Fri, Feb 01 2019, 06:00 PM -05	RHSA-2018:0007-01	RHSA-2018:0007-01 -- Redhat kernel, python-perf, per (CVE-2017-5754)f		Malin1	Low	0	Fri, Feb 01 2019, 06:00 PM
Thu, Jan 31 2019, 06:00 PM -05	RHSA-2018:0008-01	RHSA-2018:0008-01 -- Redhat kernel, perf		VeilNebula	Low	0	Thu, Jan 31 2019, 06:00 PM
Thu, Jan 31 2019, 06:00 PM -05	RHSA-2018:0014-01	RHSA-2018:0014-01 -- Redhat linux-firmware		VeilNebula	Low	0	Thu, Jan 31 2019, 06:00 PM
Thu, Jan 31 2019, 06:00 PM -05	RHSA-2018:0013-01	RHSA-2018:0013-01 -- Redhat microcode_ctl		VeilNebula	Low	0	Thu, Jan 31 2019, 06:00 PM
Thu, Jan 31 2019, 06:00 PM -05	RHSA-2018:0012-01	RHSA-2018:0012-01 -- Redhat microcode_ctl		VeilNebula	Low	0	Thu, Jan 31 2019, 06:00 PM
Thu, Jan 31 2019, 06:00 PM -05	RHSA-2018:0007-01	RHSA-2018:0007-01 -- Redhat kernel, python-perf, per (CVE-2017-5754)f		VeilNebula	Low	0	Thu, Jan 31 2019, 06:00 PM
Thu, Jan 31 2019, 04:53 AM -05	CVE-2016-0006	Multiple vulnerabilities in Kernel in Microsoft Windows - CVE-2016-0006		ComaPinwheelGalaxy	Medium	6.9	Thu, Dec 08 2016, 12:43 PM
Thu, Jan 31 2019, 04:53 AM -05	CVE-2013-1254	Vulnerabilities in Windows Kernel-Mode Driver could allow elevation of pri		ComaPinwheelGalaxy	Medium	4.9	Thu, Dec 08 2016, 12:49 PM

Figura 4.20. Reporte de vulnerabilidades

Reporte de eventos en tiempo real: este reporte sirve para monitorear la red en tiempo real, en caso de producirse una amenaza el sistema dará una notificación.



SECURITY EVENTS (SIEM)

SIEM | REAL-TIME

PAUSE — Done. [0 new rows]

DATE	EVENT NAME	RISK	DATA SOURCE	SENSOR	OTX	SOURCE IP	DEST IP
2019-02-04 16:21:28	SSHd: Connection closed	0	ssh	alienvault	N/A	0.0.0.0	0.0.0.0:22
2019-02-04 16:21:04	Host service change	0	anomalies	alienvault	N/A	alienvault	alienvault
2019-02-04 16:21:03	Host service change	0	anomalies	alienvault	N/A	alienvault	alienvault
2019-02-04 16:20:52	Host service change	0	anomalies	alienvault	N/A	alienvault	alienvault
2019-02-04 16:20:40	Host service change	0	anomalies	alienvault	N/A	alienvault	alienvault
2019-02-04 16:20:19	AlienVault NIDS: "ET INFO WinHttp AutoProxy Request wpad.dat Possible BadTunnel"	0	AlienVault NIDS	alienvault	N/A	alienvault:43502	Host-10-195-5-12:1947
2019-02-04 16:20:18	Host service change	0	anomalies	alienvault	N/A	alienvault	alienvault
2019-02-04 16:20:06	Host service change	0	anomalies	alienvault	N/A	alienvault	alienvault
2019-02-04 16:19:25	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	alienvault	N/A	0.0.0.0	0.0.0.0
2019-02-04 16:19:24	sudo: Session closed	0	sudo	alienvault	N/A	0.0.0.0	0.0.0.0
2019-02-04 16:19:09	AlienVault HIDS: Login session closed.	0	AlienVault HIDS-syslog	alienvault	N/A	0.0.0.0	0.0.0.0

Figura 4.21. Reporte de eventos en tiempo real

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La metodología PDCA fue utilizada en este proyecto porque permite el desarrollo, implementación, mantenimiento y mejora continua de las seguridades existentes en el COCIBER, a través de sus fases se utilizaron algunas metodologías o normas de ISO para asegurar que el SIEM implementado fue analizado y evaluado correctamente.
- A pesar de existir procedimientos de seguridad se ha observado que el usuario administrador no realiza una verificación minuciosa de las actividades que debe cumplir en el COCIBER acerca de los dispositivos de seguridad perimetrales.
- Existen procedimientos que no se verifican correctamente al momento de realizar el relevo de funciones cuando los administradores de red salen con el pase de la unidad.
- La evaluación de riesgos permitió determinar la importancia de los activos dentro de la red del COCIBER, a través de la evaluación se conoció que sistemas se encuentran con mayor exposición a amenazas y en qué puntos de la red se aplicaron los sensores.
- La norma ISO 25000 fue utilizada para el análisis y evaluación de sistemas SIEM Open Source, a través de sus lineamientos se evaluó las características técnicas y operativas que requería el SIEM implementado en el COCIBER.
- Se realizó la implementación del sistema SIEM en las instalaciones del COCIBER para la gestión de eventos y contribución a los controles establecidos en la norma ISO 27032 para la mejora de la seguridad de la información.

RECOMENDACIONES

- Realizar un informe de revisión de procedimientos de seguridad en el COCIBER para controlar que los administradores de red entrantes y salientes cumplan con todas las actividades y evitar brechas de seguridad.
- Realizar el análisis de la evaluación de riesgos una vez cada tres meses, ya que de esta manera se identifica a los activos que se encuentren con vulnerabilidades dentro de la red o sistemas que sean vulnerables a nuevas amenazas.
- Realizar actualizaciones frecuentes del sistema OSSIM instalado en la red del COCIBER para permitir la mejora de seguridades y funcionalidades. El administrador del sistema debe gestionar adecuadamente todos los eventos detectados en el sistema y dar tratamiento a los mismos, así se cumpliría con las directrices establecidas en la norma ISO 27032.
- Continuar con procesos de mejora continua PDCA en los demás procesos del COCIBER ya que a través de estos se logra asegurar la información almacenada en los activos, además que servirá al COCIBER en caso de que requiera certificarse en alguna norma como ISO 27001.
- Evaluar el sistema OSSIM y otros sistemas de seguridad que se implementen con las metodologías ISO 25000 para asegurar la calidad del software. En lo posible se deben realizar mediciones de la efectividad de la herramienta.

REFERENCIAS BIBLIOGRÁFICAS

Administración Pública de España. (2012). *Magerit, Metodología de análisis y gestión de riesgos de los sistemas de información.*

Aguilera, M. A. (2013). *Repositoria PUCE.* Obtenido de Desarrollo de un sistema web de control de citas, para un hospital del día: http://repositorio.puce.edu.ec/bitstream/handle/22000/9534/DESARROLLO%20DE%20UN%20SISTEMA%20WEB%20DE%20CONTROL%20DE%20CITAS%2C%20%20PARA%20UN%20HOSPITAL%20DEL%20D%C3%8DA%20%282%29.pdf?sequence=1&isAllowed=y

Alava, I. A., & Avelino, J. (Diciembre de 2016). *Propuesta Tecnologica de un aplicativo para Gestionar y Auditar los servicios automotrices que realiza el personal de la empresa Tecnicentro RONNSALT.* Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/16904/1/PROPUESTA%20TECNOL%C3%93GICA%20DE%20UN%20APLICATIVO%20PARA%20GESTIONAR%20Y%20AUDITAR%20LOS%20SERVICIOS%20AUTOMOTRICES.pdf

Alienvault. (Enero de 2019). *Documentation Alienvault Appliance.* Obtenido de Documentation Alienvault Appliance: https://www.alienvault.com/documentation/usm-appliance/system-overview/about-usm-solution.htm

Alienvault. (21 de 01 de 2019). *OSSIM: The Open Source SIEM*. Obtenido de OSSIM: The Open Source SIEM: https://www.alienvault.com/products/ossim

Alienvault. (14 de 01 de 2019). *USM Appliance Deployment Guide.* Obtenido de USM Appliance Deployment Guide: https://www.alienvault.com/documentation/resources/pdf/usm-appliance-deployment-guide.pdf

Apache Metron. (21 de 01 de 2019). *Apache Metron*. Obtenido de Apache Metron: http://metron.apache.org/

Arcos, M. (2014). Obtenido de DISEÑO Y CONSTRUCCIÓN DE UNA APLICACIÓN WEB: http://repositorio.uisrael.edu.ec/bitstream/47000/926/1/UISRAEL%20-%20EC%20-%20SIS%20-%20378.242%20-%20200.pdf

ASQ. (10 de 12 de 2018). *What is the Plan-Do-Check-Act (PDCA) Cycle?* Obtenido de PDCA Cycle: https://asq.org/quality-resources/pdca-cycle

Baluja García, W., & Porvén Rubier, J. (2013). Gestión automatizada integrada de controles de seguridad. *Revista de Ingeniería Electrónica, Automática y Comuniaciones, XXXIV*.

Baral, H. R. (21 de 05 de 2010). A protocol for Network Security Assessment Methodology. *AASA (Analysis, Assess, Security and Awareness)*, 59. Chelmsford, United Kingdom.

Bravo, C. (03 de marzo de 2015). *¿Qué es un Mock Up?* Obtenido de http://estudioka.es/que-es-un-mock-up/

Campbell, S., Jeronimo, M. (2006). An introduction to virtualization. *Applied Virtualization*, 1-2. Obtenido de Applied Virtualization.

Cevallos, K. (6 de mayo de 2015).). *Metodología de Desarrollo Ágil: XP y Scrum.* . Obtenido de https://ingsotfwarekarlacevallos.wordpress.com/2015/05/08/metodologia-de-desarrollo-agil-xp-y-scrum/

Chaubal, C. (2014). VMware White Paper. *The Architecture of VMware ESXi*, 3.

Elastic Stack. (21 de 01 de 2019). *ELK Stack: Elastic Search, Logstash y Kibana*. Obtenido de ELK Stack: Elastic Search, Logstash y Kibana: https://www.elastic.co/elk-stack

Freire, M. (marzo de 2018). *Representante de la Clinica Dental House*. Obtenido de C. Freire, Entrevistadores

Gallo, C. D. (2012). *DESARROLLO E IMPLEMENTACION DE LOS MODULOS DE COTIZACION Y VISUALIZACION DE PAGOS, Y SUB-MODULO DE ODONTOGRAMA PARA LA GESTION DE CONSULTA EXTERNA ODONTOLOGICA MEDIANTE SIIS EN MODALIDAD SAAS.* Obtenido de https://docplayer.es/4118660-Cristhian-david-gallo-medina.html

Guerrero, N. (21 de junio de 2017). *Modelo vista controlador en PHP*. Obtenido de http://programaenlinea.net/modelo-vista-controlador-en-php/

Heredia, E. (2015). *Repositorio ESPE.* Obtenido de Diseño de un Sistema de Gestion Documental-Digital para el Archivo de Historia Clinicas: https://repositorio.espe.edu.ec/bitstream/21000/10999/1/T-ESPE-049012.pdf

Hernandez, R. (Diciembre de 2007). Obtenido de Propuesta de metodología para el Desarrolo de páginas y sitios web: https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/11078/Propuesta%20de%20metodolog%C3%ADa%20para%20el%20desarrollo%20de%20p%C3%A1ginas%20y%20sitios%20web.pdf?sequence=1

IBM. (01 de 02 de 2019). *Cloud computing: A complete guide*. Obtenido de What is cloud computing?: https://www.ibm.com/cloud/learn/cloud-computing

ICT Institute. (12 de 12 de 2018). *Information security and PDCA (Plan-Do-Check-Act)*. Obtenido de ICT Institute | Information Security : https://ictinstitute.nl/pdca-plan-do-check-act/

Instituto Ecuatoriano de Normalización, I. (2014). N. T. E. IEC 27032. *N. T. E. IEC 27032*.

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. (Diciembre de 2010). *CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO.* Obtenido de CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL

CIBERESPACIO: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

ISO, I. O. (03 de 2014). *IEC 25000 Software and system engineering–Software product Quality Requirements and Evaluation (SQuaRE)–Guide to SQuaRE*. Obtenido de iso/iec 25000: https://www.iso.org/standard/64764.html

ISOTools. (26 de 12 de 2018). *¿En qué consiste el ciclo PHVA de mejora continua?* Obtenido de Ciclo PHVA: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/

Marcos, J., Arroyo, A., Garzás, J., & Mario, P. (2008). *La norma ISO/IEC 25000 y el proyecto KEMIS para su automatización con software libre.* Recuperado el 24 de 11 de 2018, de Revista Española de Innovación, Calidad e Ingeniería del Software: https://www.redalyc.org/html/922/92218339013/

Miller, D. R., Harris, S., Harper, A. A., VanDyke, S., & Blask, C. (2011). SIEM Concepts: Components for Small and Medium-size Businesses. En *Security Information and Event Management (SIEM) Implementation* (págs. 55-56). Florida: McGraw Hill.

Ministerio de Tecnologías de la Información y las Comunicaciones - Colombia. (22 de enero de 2016). *POLITICA NACIONAL DE SEGURIDAD DIGITAL.* Obtenido de POLITICA NACIONAL DE SEGURIDAD DIGITAL: https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf

Moreno, J. (15 de marzo de 2013). *PHP: WampServer Definicion, Instalación y configuración*. Obtenido de https://codegeando.blogspot.com/

Nicolett, M., & Kavanagh, K. M. (2011). *Critical capabilities for security information and event management technology.* Stamford: Gartner Inc.

Perez, A. (2007). *Desarrollo de herramientas web de gestión docente.* Obtenido de http://repositorio.upct.es/bitstream/handle/10317/179/pfc2475.pdf

Ramos, D. E. (marzo de 2010). *Analisis de diseño e implementacion de un sistema de flujo de trabajo que permita el manejo y control de planes, politicas, seguridades de la unidad de informatica aplicando servicio Ecuatoriano SECAP.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/4484/1/UPS-ST000411.pdf

Renau, T., & Salinas, P. (2000). *LA SEGURIDAD DE LA INFORMACIÓN EN LAS HISTORIAS CLÍNICAS INFORMATIZADAS.* Obtenido de http://www.sedom.es/wp-content/themes/sedom/pdf/4e14387fbe5e42_seguridad.pdf

Torres, D. R. (26 de February de 2017). Obtenido de Comparativa entre XP y SCRUM: http://davidrtmetodosagiles.blogspot.com/2017/02/comparativa-entre-xp-y-scrum.html

Universidad del Pais Vasco. (2016). Obtenido de Servicio de Odontología General: https://www.ehu.eus/es/web/clinica.odontologica/odontologia-orokorreko-zerbitzua

VMware. (24 de 11 de 10). *ESXi*. Obtenido de vSphere ESXi Hypervisor: https://www.vmware.com/latam/products/esxi-and-esx.html

VMware, Inc. (17 de 1 de 2017). *Administrar máquinas virtuales de vSphere.* Obtenido de Documentación oficial VMWare: https://docs.vmware.com/es/VMware-vSphere/6.0/vsphere-esxi-vcenter-server-601-virtual-machine-admin-guide.pdf

ANEXOS

ANEXO A. ACTA DE REUNIÓN PARA RECOPILACIÓN DE INFORMACIÓN

	COMANDO DE CIBERDEFENSA ACTA DE REUNIÓN	Página 1 de 1

Acta No.	02	***Fecha***	06	11	2018	***H.I.***	10:00	***H.F.***	12:30
Asunto	RECOPILACIÓN DE INFORMACIÓN PARA DESARROLLO DE PROYECTO								
Lugar	QUITO, COCIBER			***Elaborada por***		SGOS. GUANOLUISA M.			

Asistentes		
Nombre	**Rol**	**Firma**
Capt. Juan Játiva	Oficial de Seguridad	
Sgos. Guanoluisa Milton	Administrador red del COCIBER	
CBOS-IF Jumbo Pedro	Solicitante	

Temas Tratados
• Con la autorización del señor Oficial de seguridad del COCIBER se procede a realizar una guía al señor CBOS-IF Pedro Jumbo a las instalaciones del COCIBER, la misma que servirá para la observación y recopilación de información acerca de: o Activos conectados a la red o Sistemas y servicios o Información almacenada o Dispositivos de seguridad o Políticas y procedimientos establecidos o Gestión de incidentes o Controles adicionales

Compromisos Adquiridos		
Actividad	***Fecha***	***Responsable***
El solicitante se compromete a: • Resguardar y proteger la información levantada sobre la red del COCIBER. • No divulgar la información levantada a terceros sin la autorización del COCIBER. • Utilizar la información del COCIBER solo para los fines acordados.	Viernes, 09 de noviembre de 2018	CBOS-IF Pedro Jumbo

ANEXO B. CUESTIONARIO REALIZADO

UNIVERSIDAD TECNOLÓGICA ISRAEL

CUESTIONARIO REALIZADO AL ADMINISTRADOR DE RED COCIBER

El presente cuestionario consta de 23 preguntas y es realizado para el administrador de redes del COCIBER, servirá para determinar información relativa a la ubicación, estado y riesgos de los activos de información.

PREGUNTAS	SI	NO
ESTADO DE ACTIVOS Y TOPOLOGÍA DE LA RED		
1. ¿Se dispone de un diagrama de la topología de la red?	X	
2. ¿Se dispone de un inventario de activos?		X
3. ¿El inventario es suficientemente detallado y está estructurado adecuadamente?		X
CONTROLES Y SEGURIDAD DE LA RED		
4. ¿Se dispone de un catálogo de amenazas?	X	
5. ¿Cuenta con dispositivos de seguridad perimetral?	X	
6. ¿Se verifica regularmente el correcto funcionamiento de los dispositivos de seguridad perimetral?		X
7. ¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?		X
8. ¿Se registran las actividades de los administradores y usuarios de sistema?		X
9. ¿Cuenta con equipos desatendidos?	X	
10. ¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	X	
11. ¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?		X
12. ¿Cree usted que se incorporan controles adecuados y suficientes para proteger la red?		X
13. ¿Cuenta con un sistema de seguridad esencial para proteger los activos de información?		X
14. ¿La red del COCIBER es supervisada y evaluada constantemente?		X
15. ¿Existen políticas y procedimientos asociados a controles antimalware?	X	
16. ¿Se utilizan listas blancas o negras para controlar el uso de software autorizado y no autorizado?		X
17. ¿Se actualiza el software antivirus de forma automática?	X	
18. ¿Se generan alertas tras una detección en tiempo real?		X
19. ¿El personal técnico y el administrador de la red tienen la capacidad de reaccionar de forma rápida y apropiada en caso de detectar un incidente en tiempo real?	X	

Sgos. De Com. Guanoluisa Milton
Administrador de Red COCIBER

ANEXO C. PROCEDIMIENTO DE DETECCIÓN DE MALWARE

Preparación/Registro 1

- Una vez detectado el incidente, el Analista Forense debe accesar los sistemas que detectan eventos ilícitos posibles.
- Para ello, debe realizar un Clon (ya sea del equipo, disco duro, medio de almacenamiento, archivos logs, etc.) que le permita realizar el análisis forense respectivo.
- El análisis de la evidencia, debe ser en una máquina/servidor desconectada de la red. Lo que hace seguro el trabajo para el analista forense.
- Es necesario, contar con el conocimiento de los servicios que corren usualmente en la máquina, equipo, dispositivo, etc. En caso contrario, se debe solicitar ayuda a un experto, si lo considera necesario.
- Nota: *El analista, deberá tener un archivo con la descripción de la actividad usual de puertos, para así tener un punto de comparación con el estado actual.*

Identificación/Clasificación 2

Signos generales de la presencia de malware en el escritorio

Al reconocer varios indicios pueden insinuar que el sistema estaría comprometido por malware:

- El antivirus levanta una alerta o no puede actualizar sus firmas o deja de correr o no corre ni siquiera manualmente;
- Actividad inusual en el disco duro, lo que hace operaciones grandes en momentos no esperados.
- Equipo inusualmente lento.
- Actividad inusual de red: conexión a Internet es muy lenta la mayor parte del tiempo de navegación.
- El equipo se reinicia sin motivo.
- Algunas aplicaciones se cierran o cuelgan de manera inesperada.
- Aparecen ventanas emergentes durante la navegación en la web. (a veces incluso sin estar navegando)
- La dirección IP (si es estática) está consignada en una o más listas negras de Internet.
- Las personas se quejan de que han recibido un correo electrónico o mensaje instantáneo, mientras que usted no lo hizo.

Las acciones mencionadas a continuación, utilizan las herramientas de Windows por defecto. Los usuarios autorizados pueden utilizar las utilidades de *sysinternals* de "troubleshooting" para realizar estas tareas.

Cuentas inusuales

Buscar patrones de cuentas inusuales y desconocidas, especialmente en el grupo Administradores: *C:\> lusrmgr.msc*

Archivos inusuales

Buscar patrones de archivos inusuales de gran tamaño en el soporte de almacenamiento (mayor a 10 MB).

Buscar patrones de archivos inusuales añadidos recientemente en carpetas del sistema, especialmente C:\WINDOWS\system32.

O archivos con el atributo "oculto": *C:\> dir /S /A:H*

Entradas inusuales en el "Registry"

Buscar en el Registry del Windows, la existencia de programas inusuales que arrancan el momento que se inicia el equipo, especialmente en:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

Procesos inusuales y Servicios

Búsqueda de patrones de entradas inusuales/desconocidas entre los procesos en funcionamiento, especialmente entre los procesos con nombre de usuario "SYSTEM" y "administrador": *C:\> taskmgr.exe*
(tlisk o tasklist, según la versión de Windows)

Búsqueda de patrones de servicios de red inusuales/inesperados instalado e iniciados: *C:\> services.msc C:\> net start*
Nota: Es necesario un buen conocimiento de los servicios habituales.

Actividad inusual de red

Comprobar si hay recursos compartidos de archivos y verificar cada uno está vinculado a una actividad normal: *C:\> net view \ \ 127.0.0.1*

Observar las sesiones abiertas en la máquina: *C:\> net session*

Observar las acciones que la máquina ha abierto con otros sistemas: *C:\> net use*

Verificar que no haya conexiones NetBIOS sospechosas: *C:\> netstat -S*

Buscar cualquier actividad sospechosa en puertos TCP / IP del sistema: *C:\> netstat -na 5* (-na 5 significa actualizar cada 5 seg.)

Usar -o en Windows XP/2003 para ver el dueño de cada proceso: *C:\> netstat -nao 5*

Utilizar un sniffer (Wireshark, tcpdump, etc.) y ver si existen intentos de conexiones inusuales hacia o desde sistemas remotos. Si no se presencia actividad sospechosa, usar un sniffer mientras navega por algunos sitios web sensibles (sitio web de bancos, por ejemplo) y vea si hay actividad particular en la red.

Nota: Se necesita tener un buen conocimiento de la actividad legítima de la red.

Tareas automáticas inusuales

Buscar entradas inusuales en la lista de las tareas programadas: *C:\> at*
En Windows 2003/XP: *C:\> schtasks*

También puede ver los directorios de usuario de inicio automático:
C:\Documents and Settings*usuario*\Start Menu\Programs\ Startup
C:\WINNT\Profiles*usuario*\Start Menu\Programs\Startup

Las entradas de registro inusuales

Buscar entradas inusuales en archivos de registro: *C:\> eventvwr.msc*

Buscar eventos como los siguientes:

- "Event log service was stopped" "Windows File Protection is not active"
- "The protected System file <nombre> was not restored to its original"
- "Telnet Service has started successfully"

Buscar actividad sospechosa en los archivos de registro del firewall.

Análisis/Contención 3

Se debe realizar una investigación forense adicional en el sistema mientras está apagado. El caso ideal, es hacer un clon, es decir una copia bit a bit del disco duro que contiene el sistema, y luego analizar la copia utilizando herramientas forenses como EnCase o X-Ways.

Resolución 4

- Reiniciar desde un CD "Live" y haga una copia de seguridad de todos los datos importantes.
- Borrar los binarios y las entradas relacionadas en el "Registry" Buscar las mejores prácticas para eliminar el malware. Por lo general, se pueden encontrar en sitios web de compañías antivirus.
- Ejecutar una búsqueda por medio del antivirus.

Recuperación 5

Si es posible reinstalar el sistema operativo y las aplicaciones.

Restaurar los datos del usuario desde una copia de respaldo confiable.

En caso de que el equipo no se haya reinstalado completamente:

Restaurar los archivos que podrían haber sido dañados por el malware, especialmente los archivos de sistema.

Cierre/Repercusiones 6

Informe

Se debe redactar un informe de resolución de crisis, el cual debe ser distribuido entre todos los actores involucrados en el manejo de incidencia.

El Informe debe contener los siguientes temas:

- Causa inicial de la infección;
- Acciones a realizar;
- Líneas de tiempo de los eventos adicionales;
- Medidas realizadas
- Impacto;
- Costo del incidente

Seguimiento:

Se debe definir las acciones para el mejoramiento de los procedimientos del manejo de infecciones de gusanos.

Las acciones realizadas, son para la mejora continua basándose en la experiencia y en el conocimiento que cada una de ellas entrega.

PROTOCOLO 7 Detección de Malware en Windows

Extracto PRI.

"*Protocolo de Respuesta a Incidentes*" (PRI), es un resumen para los administradores de incidentes de seguridad informática de CSIRT de Fuerzas Armadas.

Objetivo PRI: Manejo de Intercambio o divulgación de información Secreta-Confidencial.

Usuario del PRI:

- Encargado Administrativo
- Analista de Seguridad de la Información
- Analista T.I
- Oficial de Seguridad física
- Auditor
- Abogado
- Comunicaciones.
- Perito informático.

Pasos del manejo de incidentes

Se definen 6 pasos para manejar los incidentes de seguridad:

- Preparación/Registro: Alistarse para manejar el incidente.
- Identificación/Clasificación: Detectar e identificar el incidente.
- Análisis/ Contención: Limitar el impacto del incidente.
- Resolución: Dar solución a la amenaza.
- Recuperación: En caso que sea necesario recuperar una etapa normal.
- Cierre/Repercusiones: Informar y mejorar el proceso anterior.

Control de Docto.

Creación PRI: CSIRT de Fuerzas Armadas/ V1.1
email: incidente@ccffaa.mil.ec
web: **Pendiente**.
Fono: Red Mode Nº26938, Número civil: 022284801.Twitter: **Pendiente.**

ANEXO D. INVENTARIO DE ACTIVOS

INVENTARIO DE ACTIVOS DE LA RED COCIBER

	ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico	Observaciones
COMPUTADORES DE ESCRITORIO Y PORTÁTILES	PC-01	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-02	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-03	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-04	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-05	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-06	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-07	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-08	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-09	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-10	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-11	PC	Computador asignado al personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	PC-12	PC	Computador asignado al personal administrativo	Usuario administrativo	Físico	Dpto. Administrativo	SI	
	LAP-01	Laptop	Laptop asignado a personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	LAP-02	Laptop	Laptop asignado a personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	LAP-03	Laptop	Laptop asignado a personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	LAP-04	Laptop	Laptop asignado a personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	LAP-05	Laptop	Laptop asignado a personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	LAP-06	Laptop	Laptop asignado a personal técnico	Usuario técnico	Físico	Sala de operaciones	SI	
	LAP-07	Laptop	Laptop asignado a personal técnico	Servidor público	Físico	Sala de operaciones	SI	
	LAP-08	Laptop	Laptop asignado a personal técnico	Administrador de Redes	Físico	Sala de operaciones	SI	
	LAP-09	Laptop	Laptop asignado a personal técnico	Administrador de Redes	Físico	Sala de operaciones	SI	
	LAP-10	Laptop	Laptop asignado a personal técnico	Director	Físico	Oficina del Sr. Comandante	SI	
	LAP-11	Laptop	Laptop asignada a Jefes de área	Subdirector	Físico	Oficina del Sr. Jefe Estado Mayor	SI	
	LAP-12	Laptop	Laptop asignada a Jefes de área	Jefe administrativo	Físico	Sala de operaciones	SI	
	LAP-13	Laptop	Laptop asignada a Jefes de área	Jefe de personal	Físico	Sala de operaciones	SI	
	LAP-14	Laptop	Laptop asignada a Jefes de área	Jefe Defensa	Físico	Sala de operaciones	SI	
	LAP-15	Laptop	Laptop asignada a Jefes de área	Jefe Exploración	Físico	Sala de operaciones	SI	
	LAP-16	Laptop	Laptop asignada a Jefes de área	Jefe Respuesta	Físico	Sala de operaciones	SI	
EQUIPOS DE SEGURIDAD PERIMETRAL	SEG-01	UTM	Este equipo se compone de: Firewall, Antivirus, Antispam, IDS, Antispyware y enrutador.	Administrador de Redes	Físico	Centro de datos	SI	
EQUIPOS DE COMUNICACIONES	COM-01	Switch	Red LAN	Administrador de Redes	Físico	Centro de datos	SI	
	COM-02	Switch	Red Servidores	Administrador de Redes	Físico	Centro de datos	SI	
	COM-03	Switch	Red de Almacenamiento	Administrador de Redes	Físico	Centro de datos	SI	
	COM-04	Switch	Red de Almacenamiento	Administrador de Redes	Físico	Centro de datos	SI	
	COM-05	Switch	DMZ	Administrador de Redes	Físico	Centro de datos	SI	
	COM-06	Router	Equipo conectado hacia Red Grutel que provee internet	Administrador de Redes	Físico	Centro de datos	SI	
SERVICIOS Y APLICACIONES	SA-01	Plataformas de virtualización	VM Ware v. 4.5 sin soporte actualmente	Administrador de Redes	Físico	Centro de datos	SI	Actualmente sin licencia
	SA-02	Plataformas de virtualización	VM Ware v. 5.5 sin soporte actualmente	Administrador de Redes	Físico	Centro de datos	SI	Actualmente sin licencia
	SA-03	Servicio DNS	Servidor DNS externo	Administrador de Redes	Virtual	Centro de datos	SI	Cuenta con respaldo
	SA-04	Servicio DNS	Servidor DNS interno	Administrador de Redes	Virtual	Centro de datos	NO	No está expuesto a red WAN y se tiene respaldo
	SA-05	Servidor de Correo	Servidor de correo Zimbra	Administrador de Redes	Virtual	Centro de datos	SI	Actualmente sin registros de dominio en NIC https://190.152.214.132
	SA-06	Página Web	Servidor WEB	Administrador de Redes	Virtual	Centro de datos	SI	Actualmente sin registros de dominio en NIC http://190.152.214.131
	SA-07	Antispam	Solución antispam para el correo	Administrador de Redes	Virtual	Centro de datos	NO	Existe antispam en el UTM
	SA-08	Gestor de Tickets	Servidor RTIR de Gestión de Tickets	Administrador de Redes	Virtual	Centro de datos	NO	Actualmente sin funcionamiento
	SA-09	Servidor de archivos	Servidor SAMBA	Administrador de Redes	Virtual	Centro de datos	NO	Actualmente sin funcionamiento
	SA-10	Only Office	Complemento para el servidor de archivos OwnCloud	Administrador de Redes	Virtual	Centro de datos	NO	Se puede editar usando cualquier editor de texto, presentaciones, etc.
	SA-11	Owncloud	Servidor de archivos	Administrador de Redes	Virtual	Centro de datos	SI	
	SA-12	Disco de almacenamiento 01 (RAID)	Discos de almacenamiento 30 TB	Usuario técnico forense	Físico	Centro de datos	SI	
	SA-13	Disco de almacenamiento 02 (RAID)	Discos de almacenamiento 30 TB	Usuario técnico forense	Físico	Centro de datos	SI	
	SA-14	Disco de almacenamiento	Discos de respaldo de información forense	Usuario técnico forense	Físico	Centro de datos	SI	
	SA-15	Equipo FRED	Hardware para análisis forense	Usuario técnico forense	Físico	Centro de datos	SI	Actualmente sin licencia
	SA-16	RACTACC	Equipo acelerador para descifrar claves	Usuario técnico forense	Físico	Centro de datos	SI	Actualmente sin licencia
EQUIPOS UPS Y ENFRIAMIENTO	AE-01	Equipo UPS	Sistema de alimentación ininterrumpida para equipos forenses	Administrador de Redes	Físico	Centro de datos	SI	
	AE-02	Equipo UPS	Sistema de alimentación ininterrumpida para equipos forenses	Administrador de Redes	Físico	Centro de datos	SI	
	AE-03	Equipo UPS	Sistema de alimentación ininterrumpida para racks	Administrador de Redes	Físico	Centro de datos	SI	
	AE-04	Aire acondicionado	Sistema de enfriamiento para el centro de datos	Administrador de Redes	Físico	Centro de datos	SI	
SISTEMAS SEGURIDAD FÍSICA	SF-01	Equipo biométrico	Lector de huellas de acceso al COCIBER	Administrador de Redes	Físico	Acceso al COCIBER	SI	
	SF-02	Equipo biométrico	Lector de huellas de acceso a la sala de operaciones	Administrador de Redes	Físico	Acceso a sala operaciones	SI	
	SF-03	Equipo biométrico	Lector de huellas de acceso al centro de datos	Administrador de Redes	Físico	Acceso al Centro de datos	SI	
	SF-04	Cámaras de seguridad	Cámara de seguridad de acceso al COCIBER	Administrador de Redes	Físico	Acceso al COCIBER	SI	
	SF-05	Cámaras de seguridad	Cámara de seguridad acceso centro de datos	Administrador de Redes	Físico	Acceso al Centro de datos	SI	

ANEXO E. CATÁLOGO DE AMENAZAS

CÓDIGO	TIPO	NOMENCLATURA	AMENAZA
1	[N] Desastres Naturales	N1	Fuego
2		N2	Daños por agua
3		N*	Desastres naturales
4	De origen industrial	I1	Corte del suministro eléctrico
5		I2	Condiciones inadecuadas de temperatura o humedad
6		I3	Fallo de servicios de comunicaciones
7		I4	Interrupción de otros servicios y suministros esenciales
8		I*	Otros desastres industriales
9	Errores y fallos no intencionados	E1	Errores de los usuarios
10		E2	Errores del administrador
11		E3	Errores de configuración
12		E4	Degradación de los soportes de almacenamiento de la información
13		E5	Errores de mantenimiento / actualización de programas (software)
14		E6	Errores de mantenimiento / actualización de equipos (hardware)
15		E7	Caída del sistema por sobrecarga
16		E8	Pérdida de equipos
17		E9	Indisponibilidad del personal
18	Ataques intencionados	A1	Robo físico
19		A2	Denegación de servicio
20		A3	Robo de información
22		A5	Extorsión
23		A6	Ingeniería social
24		A7	Fuga de información
25		A8	Introducción de falsa información
26		A9	Interceptación de información (escucha)
27		A10	Accesos no autorizados
28		A11	Abuso de privilegios
29		A12	Alteración deliberada de la información
30		A13	Corrupción de la información
31		A14	Destrucción de información
32		A15	Difusión de software dañino

ANEXO F. EVALUACIÓN DE LOS RIESGOS

CATEGORÍAS		AMENAZAS	PROBABILIDAD	IMPACTO	RIESGO
COMPUTADORES DE ESCRITORIO Y PORTÁTILES	Ordenadores usuarios técnicos	Fuego	1	3	3
		Daños por agua	1	3	3
		Desastres naturales	1	3	3
		Corte del suministro eléctrico	1	2	2
		Fallo de servicios de comunicaciones	1	2	2
		Errores de los usuarios	1	1	1
		Errores del administrador	1	1	1
		Errores de configuración	1	1	1
		Errores de mantenimiento / actualización de programas (software)	1	1	1
		Errores de mantenimiento / actualización de equipos (hardware)	1	2	2
		Caída del sistema por sobrecarga	2	2	4
		Robo de información	1	3	3
		Abuso de privilegios	1	3	3
		Corrupción de la información	1	3	3
		Destrucción de información	1	1	1
		Difusión de software dañino	2	3	6
	Ordenadores usuarios administrativos	Fuego	1	3	3
		Daños por agua	1	3	3
		Desastres naturales	1	3	3
		Corte del suministro eléctrico	1	2	2
		Fallo de servicios de comunicaciones	1	2	2
		Errores de los usuarios	2	2	4
		Errores del administrador	1	2	2
		Errores de configuración	1	2	2
		Degradación de los soportes de almacenamiento de la información	1	3	3
		Errores de mantenimiento / actualización de programas (software)	1	3	3
		Errores de mantenimiento / actualización de equipos (hardware)	1	3	3
		Indisponibilidad del personal	2	3	6
		Robo de información	1	3	3
		Ingeniería social	1	3	3

		Fuga de información	1	3	3
		Accesos no autorizados	2	2	4
		Abuso de privilegios	2	2	4
		Difusión de software dañino	2	3	6
	LAPTOPS	Fuego	1	1	1
		Condiciones inadecuadas de temperatura o humedad	1	1	1
		Fallo de servicios de comunicaciones	1	1	1
		Errores de los usuarios	1	1	1
		Errores del administrador	1	1	1
		Errores de configuración	1	1	1
		Errores de mantenimiento / actualización de programas (software)	1	2	2
		Errores de mantenimiento / actualización de equipos (hardware)	1	2	2
		Caída del sistema por sobrecarga	1	2	2
		Pérdida de equipos	1	3	3
		Robo físico	1	3	3
		Denegación de servicio	1	1	1
		Robo de información	2	2	4
		Extorsión	1	2	2
		Ingeniería social	1	1	1
		Fuga de información	1	2	2
		Interceptación de información (escucha)	1	2	2
		Destrucción de información	2	3	6
		Difusión de software dañino	2	3	6

EQUIPOS DE SEGURIDAD PERIMETRAL	UTM	Fuego	1	3	3
		Desastres naturales	1	3	3
		Corte del suministro eléctrico	1	3	3
		Condiciones inadecuadas de temperatura o humedad	1	3	3
		Fallo de servicios de comunicaciones	1	3	3
		Interrupción de otros servicios y suministros esenciales	1	3	3
		Errores del administrador	2	3	6
		Errores de configuración	2	3	6
		Errores de mantenimiento / actualización de programas (software)	2	3	6
		Caída del sistema por sobrecarga	1	3	3

		Indisponibilidad del personal	1	3	3
		Denegación de servicio	1	3	3
		Interceptación de información (escucha)	1	3	3
		Accesos no autorizados	1	3	3
		Destrucción de información	1	3	3
EQUIPOS DE COMUNICACIONES	Switches	Fuego	1	3	3
		Desastres naturales	1	3	3
		Corte del suministro eléctrico	1	3	3
		Condiciones inadecuadas de temperatura o humedad	1	3	3
		Fallo de servicios de comunicaciones	1	3	3
		Interrupción de otros servicios y suministros esenciales	2	3	6
		Errores del administrador	2	3	6
		Errores de configuración	2	3	6
		Errores de mantenimiento / actualización de programas (software)	2	3	6
		Caída del sistema por sobrecarga	1	3	3
		Indisponibilidad del personal	2	3	6
		Denegación de servicio	1	3	3
		Interceptación de información (escucha)	1	3	3
		Accesos no autorizados	1	3	3
		Destrucción de información	1	3	3
	Router	Fuego	1	3	3
		Corte del suministro eléctrico	1	3	3
		Condiciones inadecuadas de temperatura o humedad	1	3	3
		Fallo de servicios de comunicaciones	1	3	3
		Interrupción de otros servicios y suministros esenciales	2	3	6
		Errores del administrador	1	3	3
		Errores de configuración	1	3	3
		Errores de mantenimiento / actualización de programas (software)	1	3	3
		Caída del sistema por sobrecarga	1	3	3
		Indisponibilidad del personal	2	3	6
		Denegación de servicio	2	3	6
		Robo de información	1	3	3

		Accesos no autorizados	1	3	3
		Abuso de privilegios	1	3	3
		Difusión de software dañino	1	3	3
SERVICIOS Y APLICACIONES	Plataformas de virtualización	Fuego	1	3	3
		Corte del suministro eléctrico	1	3	3
		Condiciones inadecuadas de temperatura o humedad	1	3	3
		Fallo de servicios de comunicaciones	1	3	3
		Interrupción de otros servicios y suministros esenciales	2	3	6
		Otros desastres industriales	1	3	3
		Errores del administrador	2	2	4
		Errores de configuración	1	2	2
		Degradación de los soportes de almacenamiento de la información	2	2	4
		Caída del sistema por sobrecarga	1	2	2
		Indisponibilidad del personal	1	3	3
		Robo de información	1	3	3
		Alteración deliberada de la información	1	2	2
		Corrupción de la información	1	3	3
		Destrucción de información	1	3	3
	Servidores DNS	Errores del administrador	1	3	3
		Errores de configuración	2	3	6
		Errores de mantenimiento / actualización de programas (software)	1	3	3
		Caída del sistema por sobrecarga	1	3	3
		Denegación de servicio	1	3	3
		Interceptación de información (escucha)	1	3	3
		Accesos no autorizados	1	3	3
		Alteración deliberada de la información	1	3	3
		Corrupción de la información	1	3	3
	Servidor de Correo	Errores de los usuarios	1	3	3
		Errores del administrador	1	3	3
		Errores de configuración	2	3	6
		Degradación de los soportes de	1	2	2

		almacenamiento de la información			
		Errores de mantenimiento / actualización de programas (software)	1	2	2
		Caída del sistema por sobrecarga	1	3	3
		Indisponibilidad del personal	2	3	6
		Denegación de servicio	2	3	6
		Robo de información	1	3	3
		Fuga de información	2	3	6
		Introducción de falsa información	1	3	3
		Interceptación de información (escucha)	2	3	6
		Alteración deliberada de la información	1	3	3
		Difusión de software dañino	2	3	6
	Página Web	Errores de los usuarios	1	1	1
		Errores del administrador	2	1	2
		Errores de configuración	2	3	6
		Degradación de los soportes de almacenamiento de la información	1	1	1
		Errores de mantenimiento / actualización de programas (software)	1	1	1
		Caída del sistema por sobrecarga	1	1	1
		Indisponibilidad del personal	1	1	1
		Denegación de servicio	3	3	9
		Robo de información	2	3	6
		Fuga de información	2	3	6
		Introducción de falsa información	2	3	6
		Interceptación de información (escucha)	1	3	3
		Alteración deliberada de la información	2	3	6
		Difusión de software dañino	2	3	6
	Antispam	Errores del administrador	2	3	6
		Errores de mantenimiento / actualización de programas (software)	2	3	6
		Indisponibilidad del personal	1	2	2
	Gestor de Tickets	Errores de los usuarios	1	1	1
		Errores del administrador	2	2	4
		Errores de configuración	2	3	6

		Degradación de los soportes de almacenamiento de la información	1	3	3
		Errores de mantenimiento / actualización de programas (software)	1	3	3
		Caída del sistema por sobrecarga	1	1	1
		Denegación de servicio	1	2	2
		Robo de información	2	3	6
		Introducción de falsa información	2	3	6
		Alteración deliberada de la información	2	3	6
	Servidor de archivos	Errores de los usuarios	2	2	4
		Errores del administrador	2	2	4
		Errores de configuración	2	2	4
		Degradación de los soportes de almacenamiento de la información	1	3	3
		Errores de mantenimiento / actualización de programas (software)	1	3	3
		Errores de mantenimiento / actualización de equipos (hardware)	2	3	6
		Caída del sistema por sobrecarga	1	3	3
		Denegación de servicio	1	1	1
		Robo de información	1	2	2
		Fuga de información	1	3	3
		Introducción de falsa información	1	2	2
		Interceptación de información (escucha)	1	2	2
		Accesos no autorizados	1	3	3
		Abuso de privilegios	1	2	2
		Alteración deliberada de la información	1	3	3
		Corrupción de la información	1	3	3
		Destrucción de información	1	2	2
		Difusión de software dañino	1	3	3
	Owncloud y Only Office	Errores de los usuarios	2	2	4
		Errores del administrador	2	2	4
		Errores de configuración	2	3	6
		Degradación de los soportes de almacenamiento de la información	1	3	3

		Errores de mantenimiento / actualización de programas (software)	1	3	3
		Errores de mantenimiento / actualización de equipos (hardware)	1	3	3
		Caída del sistema por sobrecarga	2	3	6
		Denegación de servicio	1	3	3
		Robo de información	2	3	6
		Fuga de información	2	3	6
		Introducción de falsa información	2	3	6
		Interceptación de información (escucha)	1	3	3
		Accesos no autorizados	1	3	3
		Abuso de privilegios	1	3	3
		Alteración deliberada de la información	1	3	3
		Corrupción de la información	1	3	3
		Destrucción de información	1	3	3
		Difusión de software dañino	1	3	3
	Discos de almacenamiento	Fuego	1	3	3
		Daños por agua	1	3	3
		Desastres naturales	1	3	3
		Corte del suministro eléctrico	1	3	3
		Condiciones inadecuadas de temperatura o humedad	1	3	3
		Fallo de servicios de comunicaciones	1	3	3
		Interrupción de otros servicios y suministros esenciales	1	3	3
		Errores de los usuarios	1	3	3
		Errores del administrador	1	3	3
		Errores de configuración	1	3	3
		Degradación de los soportes de almacenamiento de la información	1	3	3
		Robo físico	1	3	3
		Robo de información	1	2	2
		Fuga de información	1	3	3
		Accesos no autorizados	2	2	4
		Abuso de privilegios	2	2	4
		Alteración deliberada de la información	2	3	6
		Corrupción de la información	1	2	2
		Destrucción de información	1	2	2

	Equipo de Análisis Forense FRED	Fuego	1	2	2
		Daños por agua	1	2	2
		Desastres naturales	1	2	2
		Corte del suministro eléctrico	1	2	2
		Condiciones inadecuadas de temperatura o humedad	1	2	2
		Fallo de servicios de comunicaciones	1	2	2
		Interrupción de otros servicios y suministros esenciales	2	2	4
		Otros desastres industriales	1	2	2
		Errores de los usuarios	1	2	2
		Errores del administrador	1	1	1
		Errores de configuración	1	1	1
		Degradación de los soportes de almacenamiento de la información	2	1	2
		Errores de mantenimiento / actualización de programas (software)	1	2	2
		Errores de mantenimiento / actualización de equipos (hardware)	1	2	2
		Caída del sistema por sobrecarga	1	2	2
		Pérdida de equipos	3	3	9
		Indisponibilidad del personal	2	2	4
SISTEMAS DE SEGURIDAD	Equipos UPS	Fuego	1	3	3
		Daños por agua	1	3	3
		Desastres naturales	1	3	3
		Corte del suministro eléctrico	1	3	3
		Condiciones inadecuadas de temperatura o humedad	1	3	3
		Otros desastres industriales	1	3	3
		Errores de configuración	1	2	2
		Indisponibilidad del personal	2	2	4
	Aire acondicionado	Fuego	1	3	3
		Daños por agua	1	3	3
		Desastres naturales	1	3	3
		Corte del suministro eléctrico	1	3	3
		Condiciones inadecuadas de temperatura o humedad	1	3	3
		Otros desastres industriales	1	3	3
		Errores de configuración	1	2	2

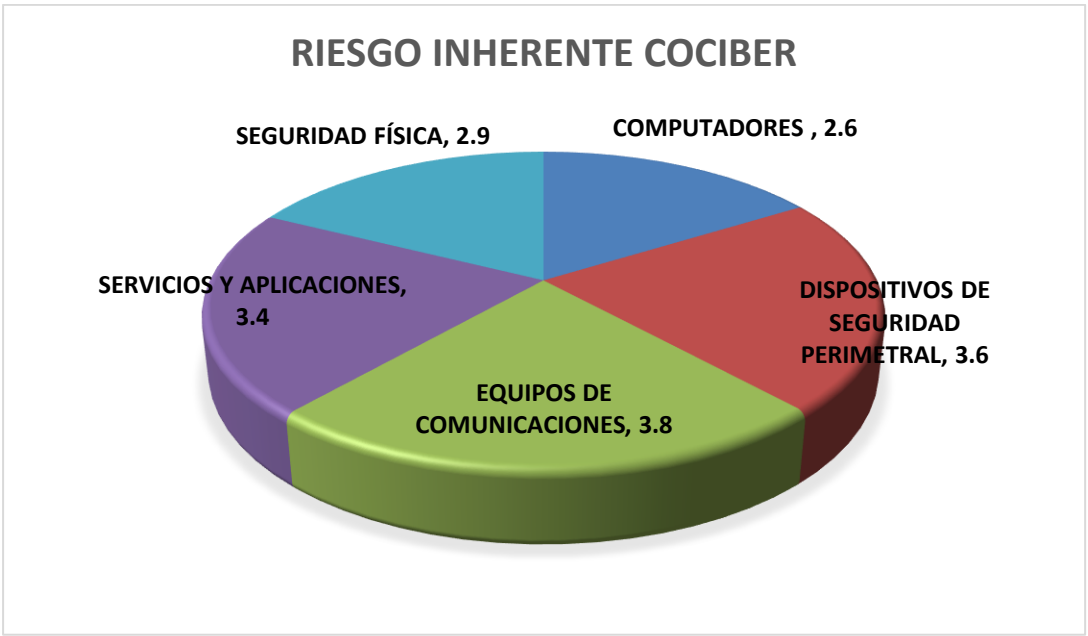
		Indisponibilidad del personal	1	2	2

RESULTADOS DEL ANÁLISIS DE RIESGOS

Tabla de Riesgo

IMPACTO				
	Alto	3	6	9
	Medio	2	4	6
	Bajo	1	2	3
		Bajo	Medio	Alto
		PROBABILIDAD		

RIESGO INHERENTE	
COMPUTADORES	2.6
DISPOSITIVOS DE SEGURIDAD PERIMETRAL	3.6
EQUIPOS DE COMUNICACIONES	3.8
SERVICIOS Y APLICACIONES	3.4
SEGURIDAD FÍSICA	2.9



ANEXO G. ACTA SEGUNDA REUNIÓN

	COMANDO DE CIBERDEFENSA ACTA DE REUNIÓN	Página 1 de 1

Acta No.	02	***Fecha***	21	12	2018	***H.I.***	12:00	***H.F.***	15:30
Asunto	ELABORACIÓN Y SELECCIÓN DE AMENAZAS QUE ATENTAN A LA INFRAESTRUCTURA Y SEGURIDAD DE LA RED COCIBER								
Lugar	QUITO, COCIBER			***Elaborada por***		SGOS. GUANOLUISA M.			

Asistentes		
Nombre	**Rol**	**Firma**
Sgos. Guanoluisa Milton	Administrador red del COCIBER	
CBOS-IF Jumbo Pedro	Solicitante	

Temas Tratados
• Se realizó un análisis y selección de las amenazas existentes en la metodología MAGERIT a los que se encuentra expuesta la seguridad de la información y activos de la red COCIBER, que servirá para realizar un análisis de evaluación de riesgos por parte del solicitante.

Compromisos Adquiridos		
Actividad	***Fecha***	***Responsable***
El solicitante se compromete a: • Resguardar y proteger la información levantada sobre la red del COCIBER. • No divulgar la información levantada a terceros sin la autorización del COCIBER. • Utilizar la información del COCIBER solo para los fines acordados.	Viernes, 21 de diciembre de 2018	CBOS-IF Pedro Jumbo

ANEXO H. ACTA ENTREGA DE INFORMACIÓN

	COMANDO DE CIBERDEFENSA ACTA DE ENTREGA DE INFORMACIÓN	Página 1 de 2

Acta No.	03	***Fecha***	25	01	2019	***H.I.***	14:00	***H.F.***	15:30
Asunto	ENTREGA DE LISTADO DE POLÍTICAS Y PROCEDIMIENTOS IMPLEMENTADOS EN EL COCIBER.								
Lugar	QUITO, COCIBER			***Elaborada por***		MAYO. SANATCRUZ WILLIAM			

	Asistentes	
Nombre	**Rol**	**Firma**
MAYO. Santacruz William	Oficial de Seguridad	
CBOS-IF Jumbo Pedro	Solicitante	

Temas Tratados

- Se recibe por parte del CBOS-IF Pedro Jumbo la solicitud de un listado de políticas y procedimientos implementados en el COCIBER.

- Se entrega únicamente el listado de lo solicitado, no se puede entregar el contenido de los mismos por razones de seguridad.

- Políticas:
  - Manejo de incidentes
  - Tratamiento de la información
  - Uso de dispositivos móviles
  - Protección de datos en diferentes medios
  - Intercambio de información
  - Uso aceptable
  - Comunicaciones
  - Educación y Entrenamiento

- Procedimientos:
  - Gestión de Incidentes por:
    - ✓ Infección por gusanos
    - ✓ Intrusiones en sistemas Windows, Linux
    - ✓ Ataques de DoS
    - ✓ Actividad maliciosa en la red
    - ✓ Ataques a sitios web
    - ✓ Infección de malware en PC´s y dispositivos móviles
    - ✓ Ingeniería social
    - ✓ Fuga de información

	COMANDO DE CIBERDEFENSA ACTA DE ENTREGA DE INFORMACIÓN	Página 2 de 2

- ✓ Abuso de privilegios
- ✓ Estafas
- ✓ Infracción de marca registrada
- Reporte de Incidentes
- Respaldo de la información

Compromisos Adquiridos		
Actividad	***Fecha***	***Responsable***
El solicitante se compromete a: • Resguardar y proteger la información levantada sobre la red del COCIBER. • No divulgar la información levantada a terceros sin la autorización del COCIBER. • Utilizar la información del COCIBER solo para los fines acordados.	Viernes, 21 de diciembre de 2018	CBOS-IF Pedro Jumbo

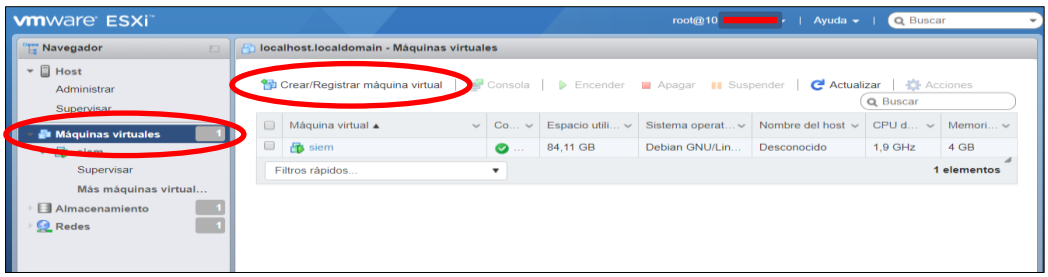
ANEXO I

MANUAL DE INSTALACIÓN OSSIM

Antes de iniciar con la instalación del sistema OSSIM se debe realizar la descarga de la imagen ISO del sitio web oficial de Alienvault: https://www.alienvault.com/products/ossim/download.

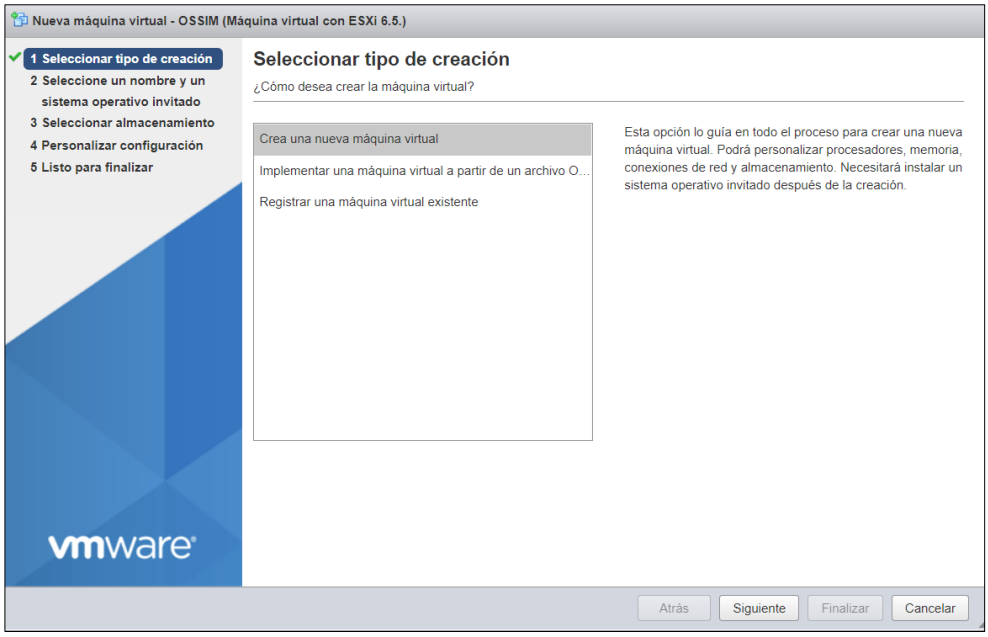
Una vez que ha terminado la descarga de la imagen se procede a crear una nueva máquina virtual en ESXi, los pasos requeridos se muestran a continuación:

- En el menú que se encuentra en el lado derecho se seleccionará la opción de “Máquinas Virtuales” y luego escoge la opción de “Crear/Registrar máquina virtual”, ver figura.



-

- El primer paso será seleccionar el tipo de creación de máquina virtual, existen tres opciones de creación, que se describen a continuación:
    - **Crear una máquina virtual (seleccionada):** esta opción sirve de guía en todo el proceso para crear una nueva máquina virtual. Se puede personalizar procesadores, memoria, conexiones de red y almacenamiento. Se necesitará instalar un sistema operativo invitado después de la creación.
    - **Implementar una máquina virtual a partir de un archivo:** esta opción sirve de guía a través del proceso de creación de una máquina virtual a partir de archivos OVF y VMDK.
    - **Registrar una máquina virtual existente:** esta opción lo guía a través del registro de una máquina virtual que ya existe en un almacén de datos.



- Para el segundo paso se especifica un nombre para el sistema a virtualizar, el tipo de sistema de operativo y la versión. OSSIM es un sistema basado en la distribución Linux Debian 8 “Jesse” (Alienvault, Updating USM Appliance and AlienVault OSSIM® to Version 5.2, 2018).

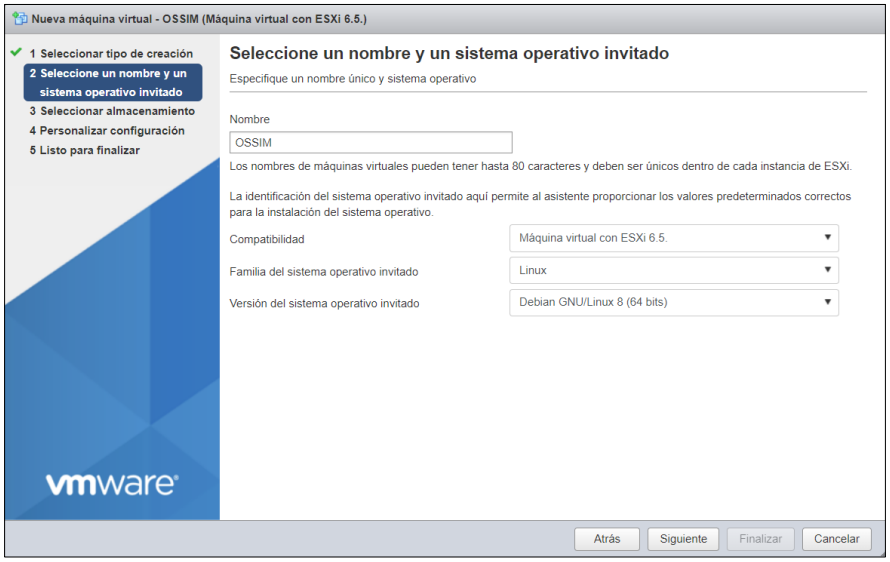
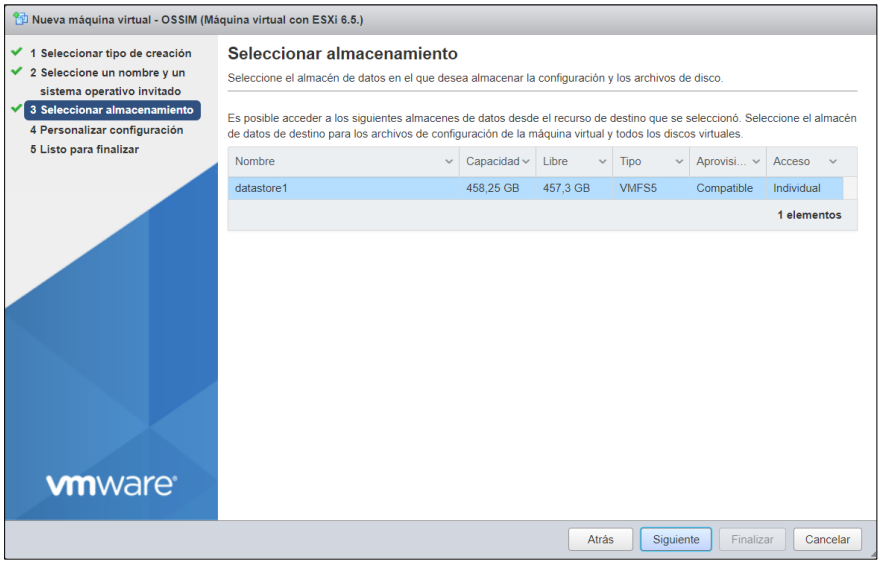
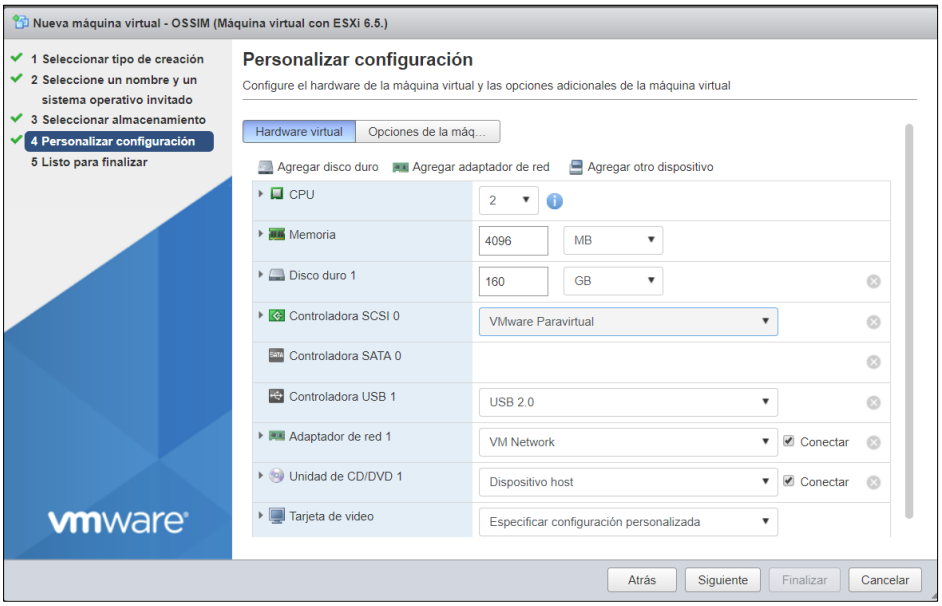


Figura 22. Tipos de creación de máquinas virtuales

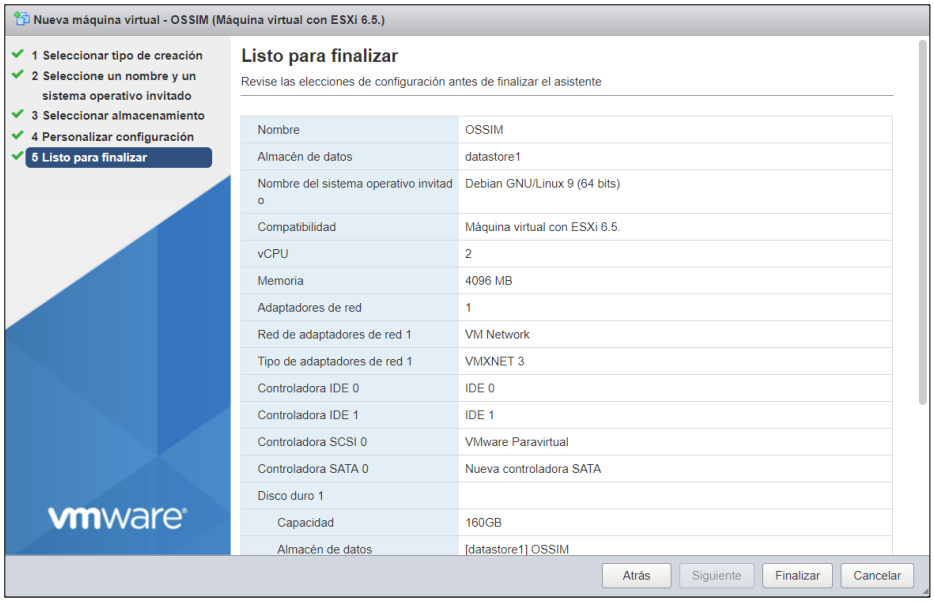
- Para el tercer paso se selecciona el almacén de datos donde se instalará el sistema OSSIM, como ya se especificó anteriormente este servidor solo cuenta con un disco de almacenamiento por lo que se selecciona la única opción disponible que es datastore1, ver figura.



- La personalización del sistema consiste en seleccionar las características técnicas a ser utilizadas, principalmente nos enfocamos en número de procesadores (2), memoria RAM (4 GB), tarjeta de red conectada y el almacenamiento (160 GB).



- El último paso requerido es la revisión de las características con las que el sistema se instalará dentro de ESXi. Si existe alguna modificación se debe pulsar en la tecla atrás o caso contrario pulsar Finalizar.

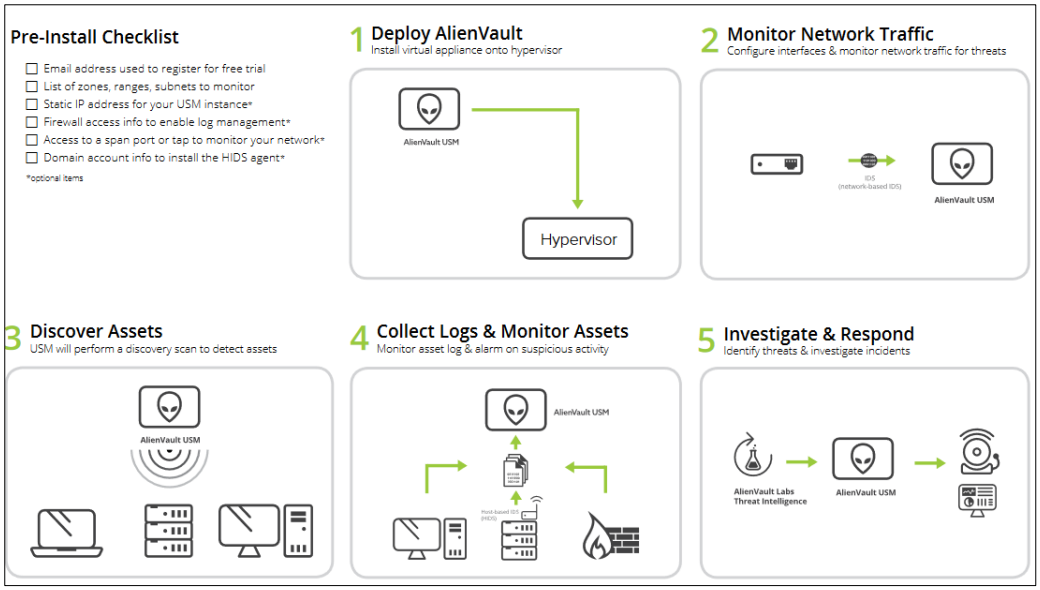


4.3.1 Instalación del sistema OSSIM

Antes de iniciar la instalación se procederá a verificar los siguientes requisitos:

- Una dirección de correo electrónico
- Lista de rangos de redes a ser monitoreadas
- Dirección IP fija para la consola central
- Acceso al UTM para la gestión de logs
- Acceso a los puertos para el monitoreo de red
- Información del dominio para instalar los sistemas de detección de intrusos

A continuación, se describirá la instalación de OSSIM en la red del COCIBER, sin embargo, en el siguiente gráfico se demuestra los prerrequisitos necesarios para el sistema y las actividades que realizará después de finalizar su instalación.



Una vez que se ha finalizado la configuración inicial de características en ESXi que utilizará OSSIM se procede a configurar el orden de arranque del nuevo sistema virtual, para lo cual en el parámetro de “Unidad de CD/DVD” deberá escoger la opción de “Seleccionar imagen de disco” y seleccionar la imagen descargada anteriormente.

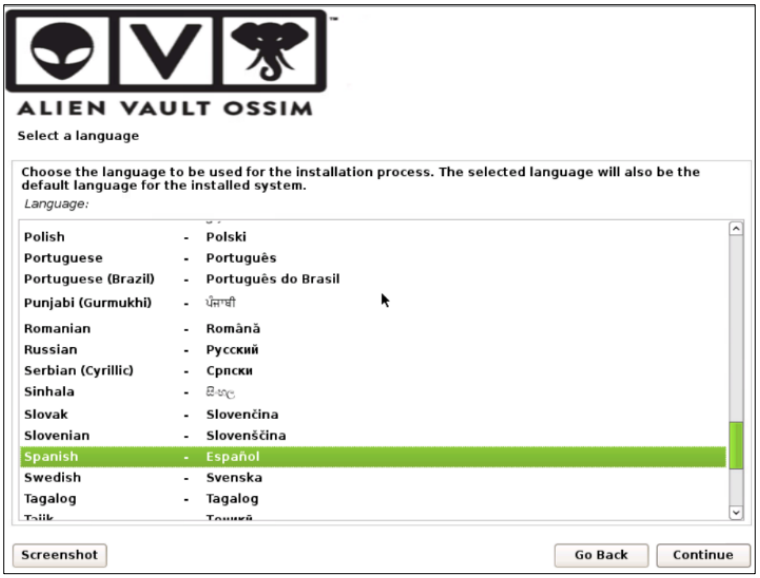
Otra ventaja del sistema OSSIM es que el proceso de instalación es similar al de una distribución Linux que incluso muchos de los pasos de configuración están omitidos debido a que el sistema los realiza automáticamente. El proceso que se detalla a continuación aplica tanto para la instalación del sistema central y el de los sensores.

Servidor central: es el dispositivo que recibirá toda la información recibida en la red, además de ser el encargado de correlacionar y realizar los análisis de amenazas detectadas (Alienvault, OSSIM: The Open Source SIEM, 2019).

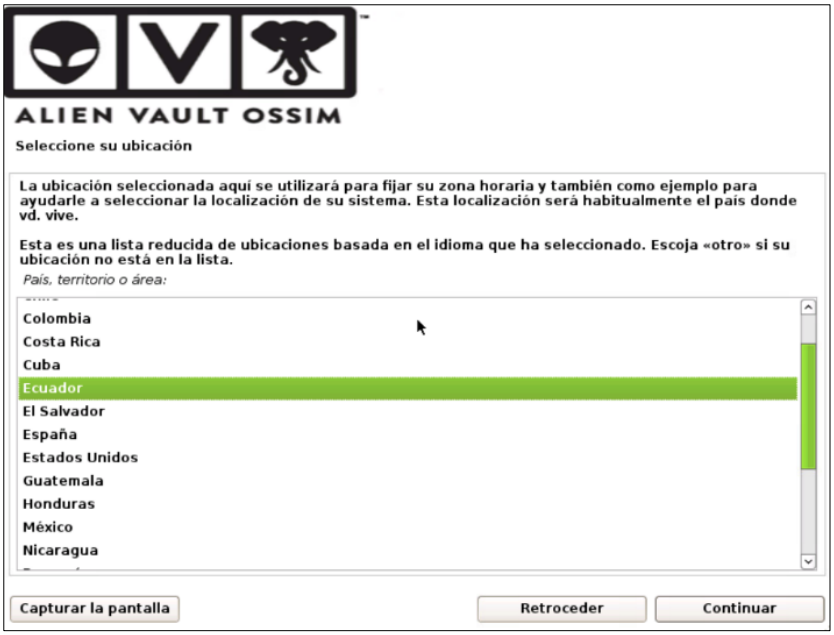
Sensor: es una instalación independiente que envía la información hacia el servidor central, este sensor puede modificarse para que envíe solo información de cierto tipo, por ejemplo, que envíe solo el tráfico UDP de su segmento de red (Alienvault, OSSIM: The Open Source SIEM, 2019).

- El primer paso es seleccionar el tipo de instalación, ver figura:

- Luego seleccionar el tipo de idioma en la que se realiza la instalación.



- El paso siguiente será la selección de la ubicación, que servirá para determinar la hora:



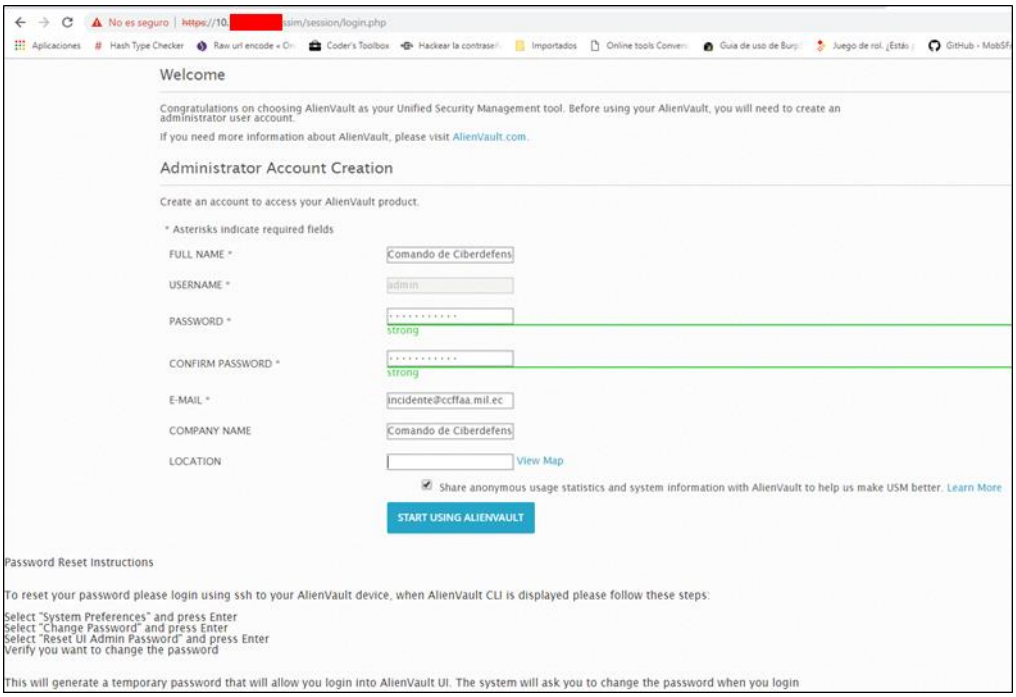
- La siguiente opción es definir la dirección IP solicitada, esta dirección asignada deberá tener acceso a las redes y será la utilizada para la administración vía web de OSSIM. Es recomendable que tenga acceso a internet para que pueda recibir alertas de nuevas amenazas a través de la funcionalidad OTX integrada como uno de sus módulos.

- Configurar la contraseña de administración de la consola.

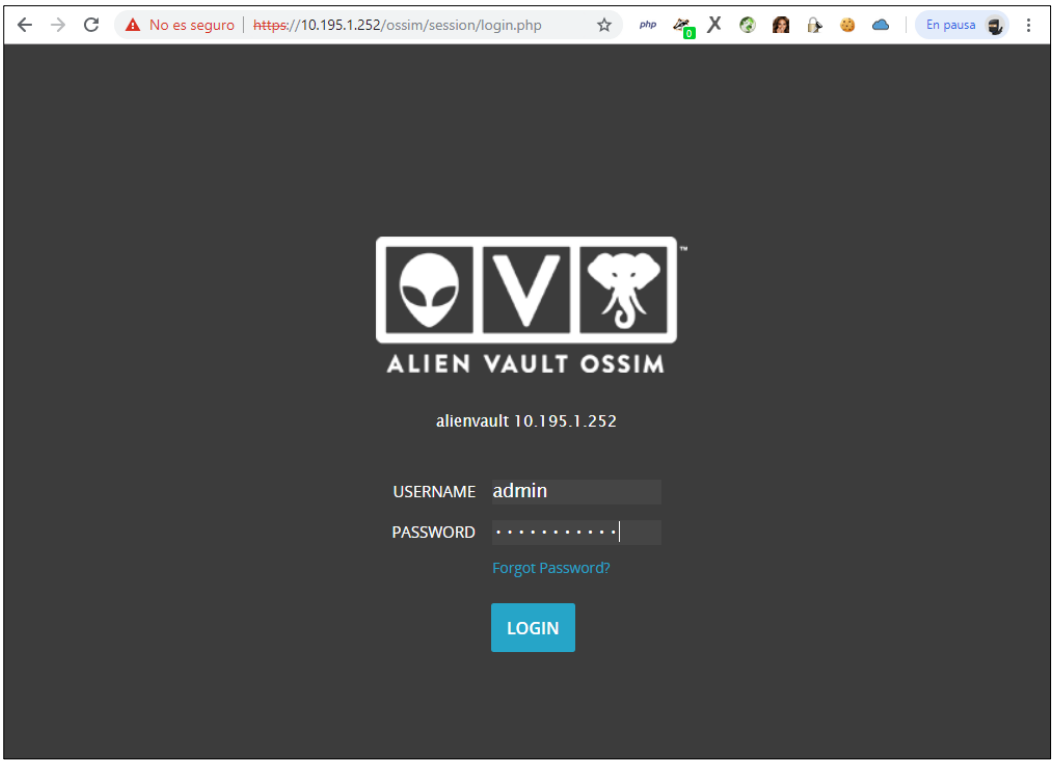
Figura 23. Configuración de contraseña

- El siguiente paso es seleccionar la zona horaria:

- Una vez realizados todos los pasos anteriores se finaliza la instalación y se procede a realizar la configuración básica del sistema, para ello se abre un navegador y se escribe la dirección IP asignada en el proceso de instalación y en la pantalla que aparece de bienvenida se ingresan los datos para la creación de la cuenta del Administrador, tal como se visualiza en la siguiente figura:



Luego de esto el sistema nos redirecciona a una pantalla de autenticación, en la que se debe ingresar el usuario y contraseña que ingresó en la ventana anterior:



Si la autenticación es exitosa el próximo paso es la configuración de la interfaz de red previamente establecida, generalmente con el nombre de eth0.

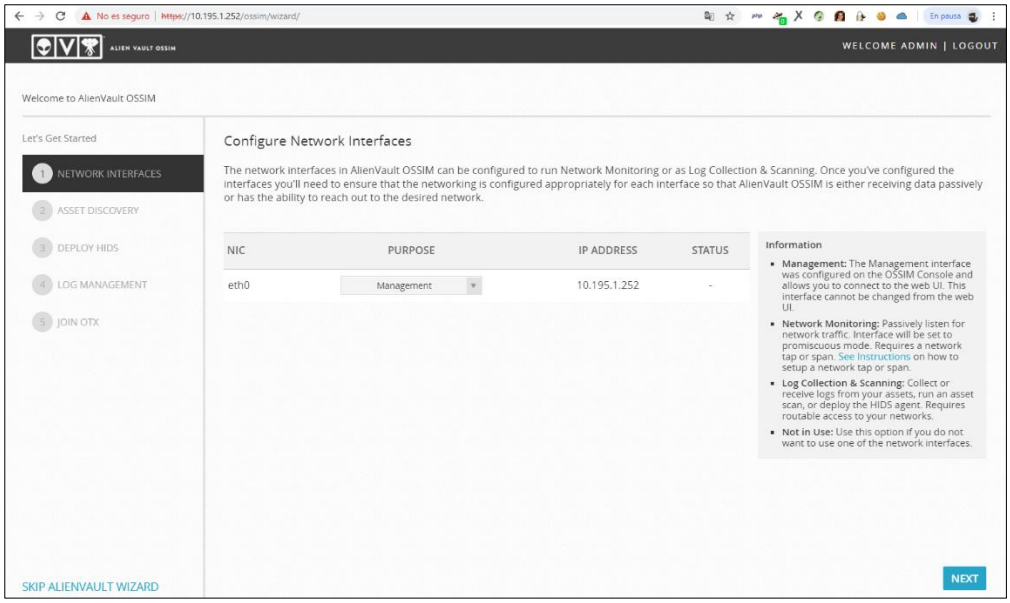
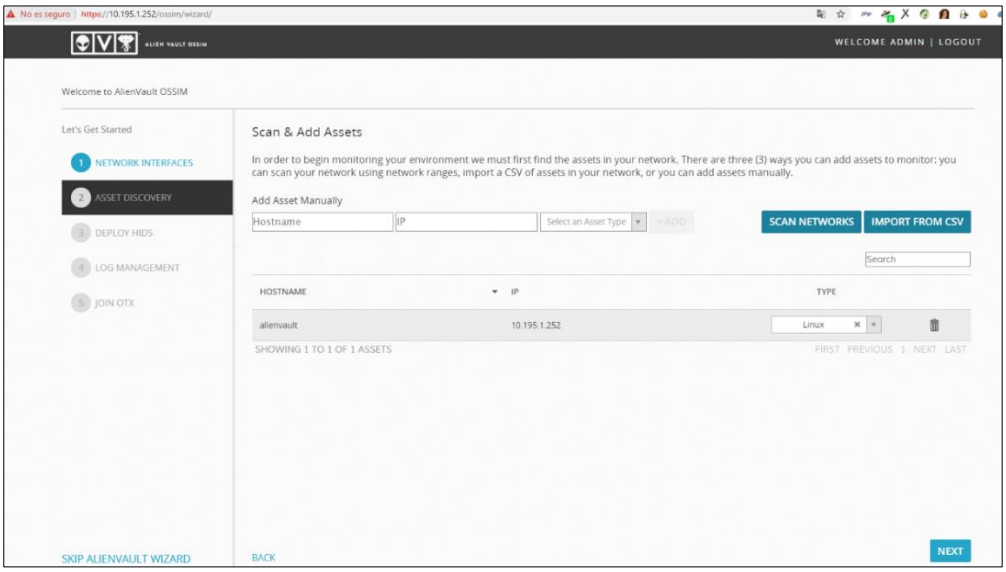


Figura 24. Configuración de interfaces de red

Luego se procederá a ingresar los rangos de red que se prevén monitorear, este paso puede ser omitido o a su vez puede añadir los rangos en los campos del formulario o importarlos desde un archivo con extensión SCV.



El siguiente paso es la configuración es la configuración de los HIDS[12], esta configuración se puede realizar de dos formas:

- A través del asistente de instalación: esta opción admite la implementación en hosts de Windows y la implementación sin agentes en hosts de Linux. Para obtener

[12] HIDS: Sistema de detección de intrusos en un Host, es un componente de OSSIM que realiza análisis de vulnerabilidades

instrucciones, consulte Implementación de HIDS en servidores, en el tema Asistente de introducción.

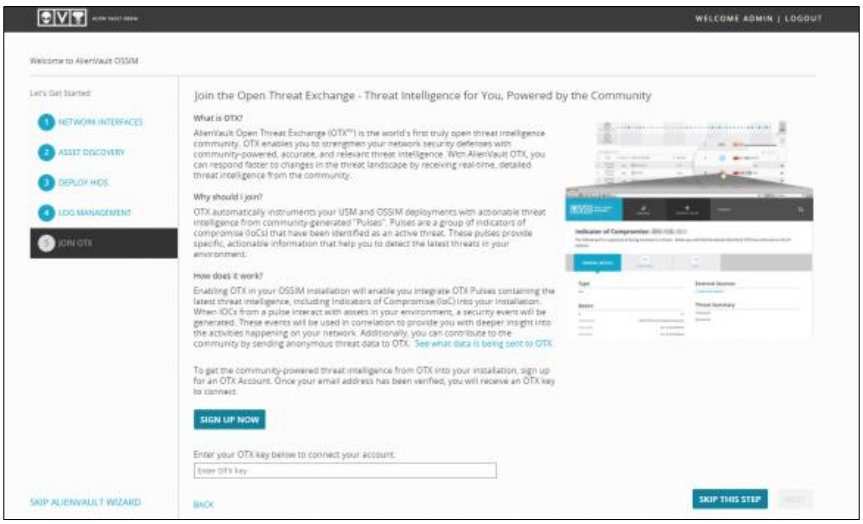
- Desde la vista de lista de activos: esta opción solo admite la implementación en servidores de Microsoft Windows.

Esta fase no se demuestra debido a que se configura automáticamente cuando se realiza un análisis de vulnerabilidades de los dispositivos y además porque al momento de la instalación aún no se contaba con acceso a todas las subredes.

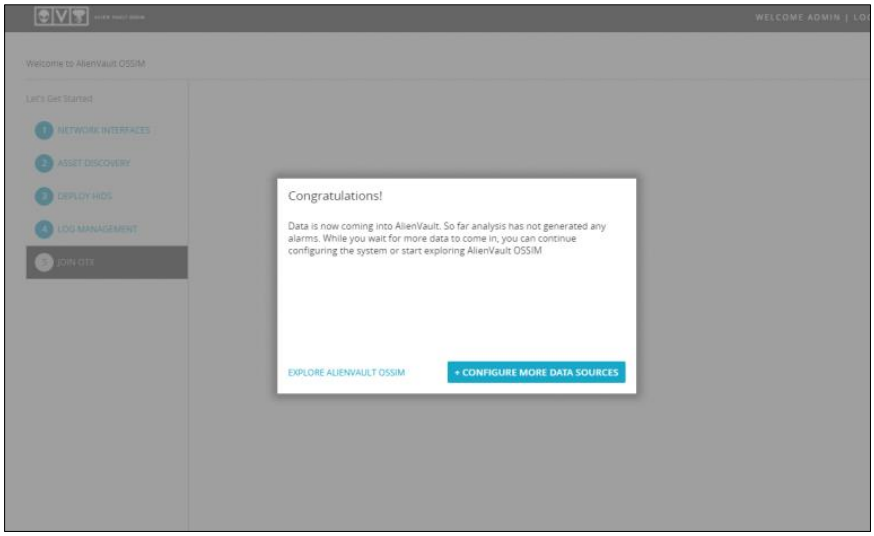
Para el siguiente paso de La Administración de logs es un paso similar al descubrimiento de activos, pero con la capacidad de recopilar datos externos de dispositivos de red, dispositivos de seguridad y sus servidores. Los datos recopilados permiten a OSSIM correlacionar eventos para ver patrones de actividad y emitir alarmas.

El asistente de introducción hace que sea fácil y rápido configurar cada uno de los activos que descubrió o agregó como parte de la tarea de detección de activos con el complemento de recopilación de datos adecuado.

Habilitar la característica OTX en la instalación permitirá compartir automáticamente información anónima sobre amenazas con la comunidad OTX, esta característica permite compartir datos e inteligencia de amenazas entre los productos de OSSIM o Alienvault:



Si se desea agregar más fuentes de datos se deberá pulsar en la opción “CONFIGURE MORE DATA SOURCES”, al finalizar la instalación.



Si se realizó todo el proceso anterior, se mostrará el panel de administración del sistema OSSIM y le mostrará una pantalla como se muestra a continuación: