UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
Ingeniera e Ingeniero de Sistemas

TEMA:
DISEÑO DE UN SECURITY OPERATIONS CENTER (SOC), MEDIANTE LA IMPLEMENTACIÓN DE ROLES DEFINIDOS POR EL INSTITUTO SANS PROPORCIONANDO LAS FUNCIONES DE RECOPILAR Y FILTRAR DATOS, DETECTAR Y CLASIFICAR AMENAZAS, ANALIZAR E INVESTIGAR AMENAZAS Y LA IMPLEMENTACIÓN DE MEDIDAS PREVENTIVAS PARA LA RED DE LA UNIDAD EDUCATIVA SALESIANA MARÍA AUXILIADORA - UESMA, CIUDAD DE ESMERALDAS.

AUTORES:
MARIUXI ALEXANDRA MARQUEZ QUIROZ
BRYAN MARCELO RAMOS MOLINA

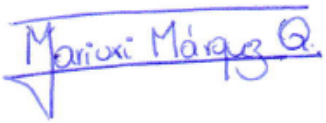
TUTOR:
JOSÉ LUIS AGUAYO MORALES

Quito, agosto del 2020

CESIÓN DE DERECHOS DE AUTOR

Nosotros MARIUXI ALEXANDRA MARQUEZ QUIROZ, con documento de identificación N° 0803600287 y, BRYAN MARCELO RAMOS MOLINA, con documento de identificación N° 1723461008, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: "DISEÑO DE UN SECURITY OPERATIONS CENTER (SOC), MEDIANTE LA IMPLEMENTACIÓN DE ROLES DEFINIDOS POR EL INSTITUTO SANS PROPORCIONANDO LAS FUNCIONES DE RECOPILAR Y FILTRAR DATOS, DETECTAR Y CLASIFICAR AMENAZAS, ANALIZAR E INVESTIGAR AMENAZAS Y LA IMPLEMENTACIÓN DE MEDIDAS PREVENTIVAS PARA LA RED DE LA UNIDAD EDUCATIVA SALESIANA MARÍA AUXILIADORA - UESMA, CIUDAD DE ESMERALDAS", mismo que ha sido desarrollado para optar por el título de INGENIERA E INGENIERO DE SISTEMAS, en la Universidad Politécnica Salesiana, que dando la Universidad faculta da para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.



..……..
Mariuxi Alexandra
Marquez Quiroz
CI: 0803600287

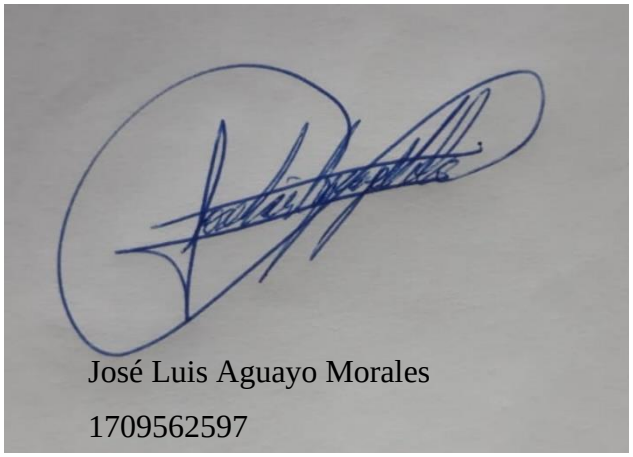
……..
Bryan Marcelo
Ramos Molina
CI:1723461008

Quito, agosto del 2020

DECLARATORIA DE COAUTORIA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico, con el tema: "DISEÑO DE UN SECURITY OPERATIONS CENTER (SOC), MEDIANTE LA IMPLEMENTACIÓN DE ROLES DEFINIDOS POR EL INSTITUTO SANS PROPORCIONANDO LAS FUNCIONES DE RECOPILAR Y FILTRAR DATOS, DETECTAR Y CLASIFICAR AMENAZAS, ANALIZAR E INVESTIGAR AMENAZAS Y LA IMPLEMENTACIÓN DE MEDIDAS PREVENTIVAS PARA LA RED DE LA UNIDAD EDUCATIVA SALESIANA MARÍA AUXILIADORA - UESMA, CIUDAD DE ESMERALDAS", realizado por MARIUXI ALEXANDRA MARQUEZ QUIROZ y BRYAN MARCELO RAMOS MOLINA, obtenido un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, agosto del 2019



José Luis Aguayo Morales
1709562597

UNIDAD EDUCATIVA FISCOMISIONAL
"MARÍA AUXILIADORA"
CÓDIGO AMIE 08H00366
Km 2.5 Vía Atacames – Teléfono: 062766413 – 062765196

CARTA DE AUTORIZACIÓN

09 de septiembre del 2019
Esmeraldas, Ecuador

Señor(a)
Ing. Patsy Malena Prieto MSc.
Directora de la Carrera de Ingeniería de Sistemas
Universidad Politécnica Salesiana, Sede Quito

Presente. -

En calidad de representante legal de la Unidad Educativa Salesiana "María Auxiliadora" - UESMA, Ciudad de Esmeraldas, autorizo y comprometo el apoyo de la institución en lo que sea necesario para el proyecto de titulación a los estudiantes, Srta. Márquez Quiroz Mariuxi Alexandra con C.I: 080360028-7 y el Sr. Ramos Molina Bryan Marcelo con C.I: 172346100-8 de la Carrera de Ingeniería de Sistemas de la Universidad Politécnica Salesiana - Sede Quito bajo el Tema: "Diseño de un Security Operations Center SOC, mediante la implementación de roles definidos por el instituto SANS proporcionando las funciones de recopilar y filtrar datos, detectar y clasificar amenazas, analizar e investigar amenazas y la implementación de medidas preventivas para la red de la Unidad Educativa Salesiana María Auxiliadora - UESMA, Ciudad de Esmeraldas".

Comprendiendo que este trabajo va a ser desarrollado con fines única y exclusivamente académicos por parte de los interesados.

Por la atención al presente anticipo mi más sincero agradecimiento.

Atentamente,

PADRE: PEDRO VIDAL ROCUANT. SdB
DIRECTOR SALESIANO

P. Pedro Vidal Rocuant

COMUNIDAD SALESIANA
ESMERALDAS
ECUADOR
SAN FELIPE NERI

Nombre del Represéntate Legal
Numero de Cedula P 0164 2332.
Firma y Sello

"Educar buenos cristianos y honrados ciudadanos"

DEDICATORIA

A Dios por su bendición en mi vida, a mis queridos padres Flavio y Angela quienes han dado todo para verme cosechar triunfos, ellos que han sido apoyo incondicional y con su ejemplo han formado la persona humilde y honrada que soy, asimismo a mi hermano Edwin por ser siempre tan frontal y optimista conmigo, al que siempre está ahí para darme consejos de motivación que hacen de mi más fuerte, de la misma manera a mis hermanas Angela y Jenniffer quienes han sabido enseñarme que con amor y paciencia todo llega, que los esfuerzos valen la pena, porque el camino se lo hace caminando.

Además, dedico este trabajo de titulación a la Misión Salesiana de Esmeraldas junto al Colegio Fiscomisional Técnico "San Rafael" que con la nueva reforma ministerial es la Unidad Educativa Salesiana "María Auxiliadora" UESMA, ellos quienes aposaron por mí. El inicio de esta gran historia no hubiera sido posible sin su beca estudiantil.

También a la Residencia Universitaria Intercultural Don Bosco por haber sido mi hogar en estos años universitarios, a todos quienes conforman mi querida Residencia, ellos han sido participes de mi proceso, formación personal y profesional.

Y como no escribir líneas de dedicación a la Universidad Politécnica Salesiana, por proteger la identidad de Don Bosco y educar bajo su práctica. Los que han hecho que las preguntas sean respondidas, pero algo mucho mejor, me han enseñado a cuestionarlas. Fue lindo fue haber estudiado con ustedes y para ustedes, tengan por seguro que adquiero mi profesión con mucho respeto y gran admiración.

Finalmente a todos quienes me conocen que han aportado de forma directa o indirecta con sus consejos, ejemplos y motivación para continuar este gran proceso.

Mariuxi Alexandra Marquez Quiroz

DEDICATORIA

Este trabajo está dedicado a mi familia, en especial a mi madre quien siempre se ha esforzado para que tenga lo mejor y para que logre todas las metas que me he propuesto, con su amor, su apoyo y esfuerzo me ha convertido en la persona que soy, gracias por todo eres un pilar muy importante en mi vida, te amo mamá.

Además, se lo dedico a mis hermanos Camila y Maximiliano que pueden ver en mi un ejemplo de perseverancia para alcanzar sus metas y sueños, los amo y saben que siempre pueden contar conmigo. Una mención especial al Sr. Luis Cola por el apoyo que ha brindado en mi familia en el trascurso de todo este tiempo.

De igual manera una especial y sentida dedicatoria a la ingeniera Michaela Salgado quien en el trascurso de mi carrera me supo brindar su cariño y su amor, gracias por todo. También a cada uno de los integrantes de la familia Cueva Sierra quienes me abrieron las puertas de su hogar, con su cariño y apoyo me acompañaron en esta travesía y me brindaron muchas enseñanzas las cuales atesoro con mucho cariño en el corazón.

Por último, pero no menos importantes, dedico este trabajo a todos los ingenieros, compañeros y amigos que conocí durante este tiempo en la Universidad Politécnica Salesiana, de cada uno de ellos guardo experiencias y enseñanzas las cuales nunca olvidare.

Bryan Marcelo Ramos Molina

AGRADECIMIENTO

A la Universidad Politécnica Salesiana por la formación que nos brindaron, han hecho de nosotros jóvenes comprometidos con la carrera y la sociedad.

De igual importancia a nuestro tutor ingeniero José Luis Aguayo Morales que es fuente de inspiración, por guiarnos y caminar con nosotros tanto en el ambiente académico como en este proyecto de titulación. Así mismo este trabajo debe mucho a la colaboración de la Unidad Educativa Salesiana María Auxiliadora-UESMA por la apertura brindada.

Finalmente un agradecimiento profundo a nuestras familias que han sido los pilares fundamentales para la consecución de este logro y nos han acompañado en el transcurso de esta larga travesía.

Mariuxi Alexandra Marquez Quiroz

Bryan Marcelo Ramos Molina

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

La Unidad Educativa Salesiana María Auxiliadora - UESMA solicitó un diseño del Centro de Operaciones de Seguridad (SOC) porque quiere mejorar su nivel de seguridad y habilidades de detección de amenazas cibernéticas.

Se propuso un diseño de un prototipo de SOC basado en los roles de SANS, para que la UESMA pueda recopilar y filtrar datos, para detectar, clasificar, analizar e investigar amenazas.

Se utilizó la metodología "Hoja de ruta para la implementación de proyectos piloto". Para determinar el estado de la infraestructura, se recopilaron datos de red relacionados con sus operaciones de seguridad. El SOC diseñado ayudará a lograr los objetivos de las funciones sustantivas de la UESMA.

El prototipo de SOC se construyó en un entorno de simulación utilizando software VMware y ELK, Cuckoo, Moloch, Zabbix, GLPI, Grafana, PfSense, Windows Server, McAfee. Las pruebas de funcionalidad mostraron que el rendimiento es estable y la prueba de penetración mostró que es robusto a los ataques externos.

Los valores de la implementación y operación del SOC se estimaron que para el primer año son inferiores a $ 300,000 y por operación a partir del segundo año en adelante son inferiores a $ 200,000. Finalmente, en lo legal, se citó un grupo de leyes que, con la evidencia recopilada por el SOC, ayudaría a tomar acciones legales.

ABSTRACT

The Unidad Educativa Salesiana María Auxiliadora - UESMA requested a design of Security Operations Center (SOC) because it wants to improve its security level and detection skills of cyber threats.

It was proposed a design of a SOC prototype based in the SANS roles, that the UESMA will be able to collect and filter data, to detect, classify, analyze and investigate threats.

The methodology “Roadmap for the implementation of pilot projects” was used. To determine the state of the infrastructure, were collected network data related with its security operations. The designed SOC will help to get the goals the UESMA's substantive functions.

The prototype SOC was built in a simulation environment using VMware and ELK, Cuckoo, Moloch, Zabbix, GLPI, Grafana, PfSense, Windows Server, McAfee software. The functionality tests showed that the performance is stable and the penetration test showed that it is robust to external attacks.

The values of the implementation and operation of the SOC was estimated that for the first year are below $ 300,000 and per operation from the second year onwards are under $ 200,000. Finally, in the legal, there were cited a group of laws that with the evidence collected by the SOC, would help to take legal actions.

CAPÍTULO 1 - ESTUDIO DEL PROBLEMA

Introducción

En la era del mundo digital, la mayor parte del entorno esta interconectado con las redes y se consigue acceder a información de cualquier forma, por ello proteger los datos e información en las instituciones educativas es motivo fundamental.

La seguridad de la información ya no es un nivel de preferencia secundario (Denning, 2012). Actualmente, las organizaciones consideran la información como el activo más importante por lo tanto utilizan herramientas informáticas para precautelar su confidencialidad, integridad y disponibilidad.

Las computadoras infectadas con virus, gusanos, troyanos o pirateadas por alguien no es algo nuevo, lo nuevo es la sofisticación, la naturaleza y la sutileza de los ataques (Coopers, 2015). Las amenazas persistentes avanzadas como el ciber espionaje y la denegación de servicio distribuida (DDoS) son algunos de los ataques que pueden causar un gran daño a la organización (Muniz, 2015).

Una institución educativa tiene información valiosa por ejemplo su sistema de calificaciones, contabilidad, facturación electrónica, transferencias y pagos, que deben protegerse contra ataques de acceso ilegítimo, mal uso o denegación de servicio. Teniendo en cuenta esta información, si se usa incorrectamente o se ve comprometida, puede ocasionar un gran daño a la reputación de la institución o exponerla a pérdidas y otros riesgos (Gray, 8 Ways to Defend Higher Education against Cyberattacks, 2014). Por lo tanto, debería existir un centro de operaciones que maneje de forma centralizada la seguridad, que apoye a la institución con la identificación y gestión de las amenazas informáticas sobre sus activos (P. Jacobs, 2013).

El diseño de un centro de operaciones de seguridad (SOC) ayudará a contrarrestar la propagación del incidente en tiempos cortos. Todo esto mediante software de monitoreo

constante y adoptando estándares propuestos por el organismo internacional SANS (SANS™ Institute, 2000 - 2019), es decir evalúa el personal profesional que debe repartirse sobre los cuatro niveles de escalamiento de problemas, esto según un informe que detalla: “Future SOC: SANS 2017 Security Operations Centers Survey” (Technology Institute SANS , 2020). El nivel de categoría 1 vigila los incidentes, realiza informes sobre los mismos y se enfoca en la mitigación de las amenazas detectadas en la red. En cuanto al nivel de categoría 2, entra en detalle a fondo sobre las causas del incidente y proceden a proponer soluciones. Simultáneamente el nivel de categoría 3 evita la propagación de las amenazas sobre la red, establecen nuevas medidas de detección. Y finalmente la categoría 4 el administrador del SOC posee el contacto con la institución e informa los procedimientos del centro de monitoreo (CISCO, 2019).

La investigación se realizó en colaboración con el sector educativo privado de un colegio en la ciudad de esmeraldas con el fin de proteger sus sistemas contra las amenazas informáticas.

El documento tiene la siguiente estructura: Capítulo 1 presenta la recopilación de los datos actuales acerca de la red de la Unidad Educativa Salesiana “María Auxiliadora” UESMA, ciudad de Esmeraldas haciendo énfasis en los dos primeros objetivos del presente proyecto. El Capítulo 2, describe los conceptos fundamentales para diseño del SOC. Por otra parte el Capítulo 3, propone el análisis y diseño del SOC. El Capítulo 4, detalla el análisis sobre los resultados del SOC prototipo en un entorno de simulación de forma técnica, económica y legal.

Por último, las conclusiones validan la propuesta de los objetivos planteados para el proyecto, también, se proponen recomendaciones para posibles mejoras y posteriores estudios.

Antecedentes

El robo de información por internet o redes interconectadas es el ataque más frecuente que cometen delincuentes informáticos (El Telégrafo, 2019). Según estudios de Deloitte sobre la

Seguridad de la Información en Ecuador expresa que: “El 60% de las organizaciones no disponen actualmente de un SOC” (Deloitte Ecuador, 2017) pero que están predispuesto a su adquisición.

Acerca de ataques informáticos, según Centurylink: “En Ecuador y Latinoamérica se reconoce un promedio de 10 a 12 ataques cibernéticos por segundo” (El Telégrafo, 2019). En el año 2019 se obtuvieron cifras con un total de 40 millones de ataques cibernéticos en el país (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2019) con mayor cantidad de incidentes informáticos se destacaron el malware y los errores humanos. Las amenazas y vulnerabilidades de seguridad de TI surgen continuamente.

De la información presentada por el Ministerio de telecomunicaciones y de la sociedad de la información se extraen los siguientes porcentajes: 43% en ataques de malware, 41% errores humanos, 35% no definido su procedencia, 13% abuso de información privilegiada, 8% una intrusión externa,7% accesos no autorizados y finalmente un 4% de violación de seguridad por terceros (Banka, 2017).

Por ejemplo, en ecuador empresas como Telefónica poseen un SOC que protege sistemas y servicios, monitorea constantemente su red, y la de empresas asociadas a la compañía (Telefónica, 2018).

No existe un enfoque único para la seguridad cibernética (Capgemini, 2017). Por ende, el centro de operaciones de seguridad SOC deberá estar conformado por personal especializado, que acompañado de una infraestructura tecnológica avanzada puedan dar soluciones minimizando riesgos y vulnerabilidades a los que está expuesta una institución educativa.

¿Y qué lleva a las instituciones a poner en marcha sus propios SOC? Principalmente el deseo de mantener un control lo más preciso posible sobre sus datos, la gestión de su seguridad y el

proceso de respuesta cuando se produce una incidencia o se detecta un problema (ComputerPro, 2017).

Problema

La Unidad Educativa Salesiana "María Auxiliadora" (UESMA), se encuentra ubicada vía a Atacames Km 2 ½, valle San Rafael sur de la ciudad de Esmeraldas (Flores, 2017), este establecimiento está dividido en 4 bloques, de una y dos plantas las mismas que corresponden a las áreas administrativas, académicas, laboratorios informáticos dirigidos a la básica inferior, superior, bachillerato. Los laboratorios técnicos de electrónica y mecánica para el bachillerato, la Comunidad Salesiana y la Parroquia de la Comunidad las cuales albergan en su seno a 3000 estudiantes en dos secciones, matutina y vespertina (UESMAE, 2019).

Actualmente, la institución educativa afronta problemas para detectar de manera óptima las amenazas que afectan la infraestructura de la institución.

La UESMA cuenta con un departamento de TICS, pero, al no precisar con un analista especializado en operaciones de ciberseguridad en la institución, se tiene problemas al detectar y clasificar de manera correcta los diversos tipos de ataques y el acceso malicioso a los que esta propensa la red, los host y datos (Anchundia, 2000).

Según la entrevista realizada a los técnicos de TICS de la UESMA en el 2019 ver **¡Error! No se encuentra el origen de la referencia.**, actualmente la unidad educativa posee una infraestructura tecnológica propia, teniendo en cuenta que la institución maneja sistemas para: contabilidad, facturación electrónica de calificación y no poseen un centro de operaciones de seguridad. ¿Es posible mejorar procesos actuales gracias a la detección, clasificación, análisis, recopilación y filtrado de los datos de ataques recibidos para prevenir amenazas?

Justificación

La seguridad informática se ha transformado en una de las vitales preocupaciones de las instituciones (Rodríguez, 2016). “Las estadísticas muestran que las instituciones académicas se encuentran entre los tres principales objetivos de los delitos cibernéticos” (Lubna, Baber, & Umar, 2015).

Se necesita un centro que relacione las personas, los procesos y las tecnologías, que ofrezcan técnicas y métodos sobre la situación en la que se encuentra la red para detección, prevención y solución de amenazas (Ciso, 2018). Porque existen ciberdelincuentes atacando a sistemas e información útil, ataques que pueden darse mediante técnicas de denegación de servicios, archivos infectados, gusanos, *ransomware* y muchos más (Ramiro, 2018).

Al obtener información de valor los ciberdelincuentes la usan para su beneficio, pero al añadir un centro de monitoreo de seguridad, este ayudará al departamento de TICS a precautelar los datos de la red de la UESMA. Así mismo el centro permitirá gestionar incidentes de manera efectiva para que el daño sea limitado en tiempo y los costos de recuperación se mantengan al mínimo lo cual muestra la pertinencia de crear este centro.

Objetivo general

Diseñar un Security Operations Center SOC, mediante la implementación de roles definidos por el instituto SANS en la Unidad Educativa Salesiana María Auxiliadora UESMA para recopilar y filtrar datos, detectar y clasificar, analizar e investigar amenazas.

Objetivos específicos

Recopilar los datos de la red de la UESMA relacionados a sus operaciones de seguridad para conocer el estado en el que se encuentra la infraestructura.

Analizar los datos recopilados, en cuanto a seguridad e infraestructura tecnológica de la UESMA, para detectar vulnerabilidades.

Diseñar un SOC siguiendo los roles definidos por el instituto SANS, para que cumpla con sus funciones sustantivas que apoyen a la UESMA.

Analizar los resultados del SOC prototipo en un entorno de simulación de forma técnica, económica y legal.

Estado Inicial

Se presenta la recopilación de los datos actuales acerca de la red de la Unidad Educativa Salesiana “María Auxiliadora”- UESMA, ciudad de Esmeraldas, haciendo énfasis en los dos primeros objetivos del proyecto; recopilar los datos de la red y análisis de estos en cuanto a la seguridad e infraestructura tecnológica de la unidad educativa.

1. Esquema Implementado - UESMA

A continuación, se detallan los componentes de la infraestructura actual de la institución, cabe recalcar que la UESMA cuenta con sus propios equipos lo cuales se ubican en su Data Center.

La UESMA para ofrecer sus servicios cuenta con una infraestructura virtualizada como se muestra en la Figura 1, bajo el sistemas operativo ESXi.

Esquema de Aplicaciones

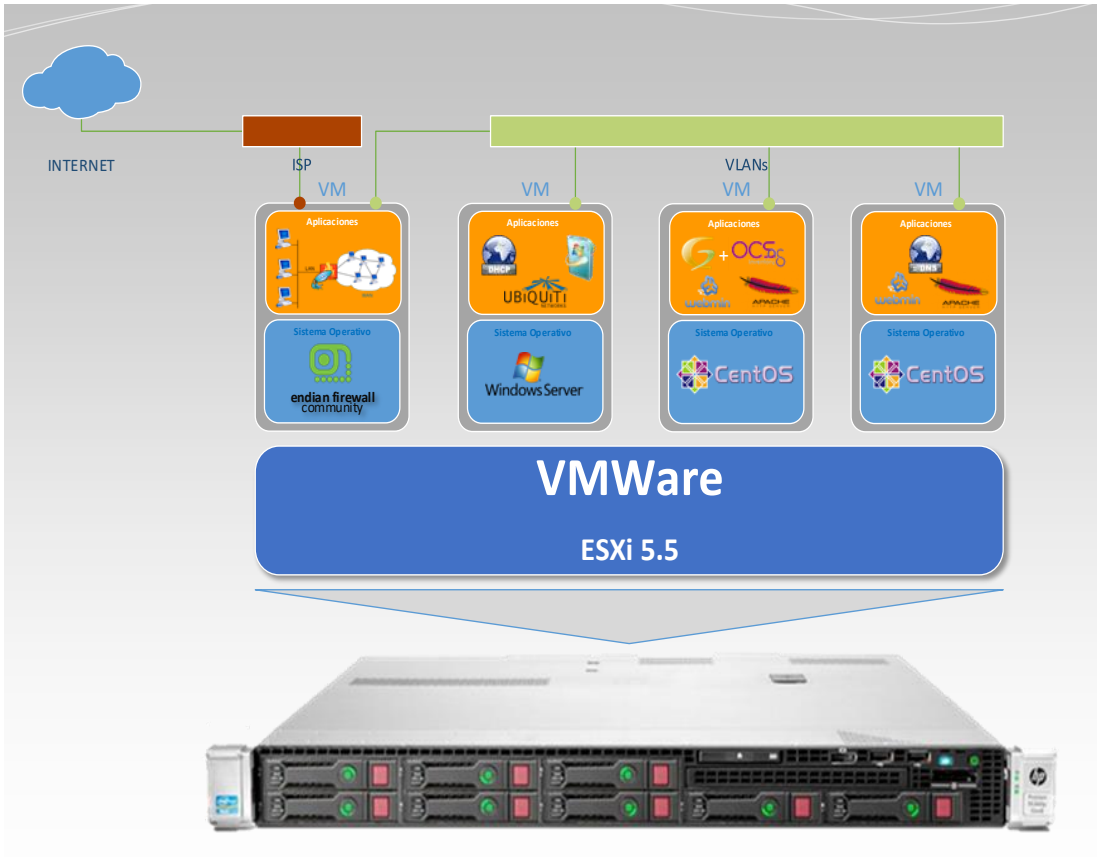


Figura 1. ESXi, virtualización dentro de la red - UESMA
Fuente: (Anchundia, 2000)

Por ello, esta arquitectura de software se integra completamente al esquema de red utilizado, basado en segmentación por VLAN, porque permite implementar cualquier servicio y ponerlo a disposición de un segmento de red.

Este sistema operativo esta implementado sobre dos servidores con las características descritas en el **¡Error! No se encuentra el origen de la referencia.**.

Las capacidades del servidor le han permitido a la UESMA la implementación de máquinas virtuales para los servicios detallados en la Tabla 1.

Tabla 1. Servicio de la red - UESMA

Servicio	Descripción
Gateway de Internet	Permite el acceso a internet de los equipos de la LAN (Reyes, 2012).
Servidor DHCP	Servidor de red que facilita y asigna automáticamente direcciones IP, puertas de enlace predeterminadas y otros parámetros de red a los dispositivos del cliente (Infoblox, 2018).
Servidor para centralizar las descargas de actualizaciones	Admite que cada sistema pueda recibir y realizar todas las actualizaciones necesarias de manera automática (Barrios, 2018).
Servicio para seguimiento de Access Points	Permite la gestión de los puntos de acceso inalámbricos, y admite a los usuarios invitados conectarse a el SSID y monitorear remotamente el uso de la red (Magoni, 2016).
WebServer	Este software se encarga de enviar el contenido de un sitio web al usuario, en este acaso del sitio web de la institución (Borges, 2019).

Sistema (control equipos e incidencias)	Administra el control sobre los equipos e incidencias que se pueden generar por diferentes eventos, se lo visualiza desde una consola centralizada (GLPI Network, 2017).
Sistema para automatización de inventario	Automatiza el proceso de inventario sobe cada equipo de cómputo perteneciente a la institución, se integra al sistema para control de los equipos e incidencias (OCS inventory, 2001).
Servicio de Vigilancia	Permite monitorizar las cámaras instaladas en la institución (Anchundia, 2000).

Nota: Se detalla generalidades sobre cada uno de los servicios que posee la UESMA.

1.1. VMware

El software virtualiza componentes de hardware como la tarjeta de video, los adaptadores de red y el disco duro (Computer Hope, 2017). La institución posee este software con el fin de crear servidores virtuales, ahorrando tiempo y dinero. A través de las capacidades del servidor y de la plataforma de VMware la UESMA cuenta con los servicios descritos en la Tabla 1.

1.2. Proxy HTTP

Dentro de la institución es el servidor intermediario que separa los usuarios finales de las páginas por las que navegan. Los servidores proxy proporcionan diferentes niveles de funcionalidad, seguridad y privacidad dependiendo del caso de uso, necesidades o política de la empresa (Petters, 2019).

1.3. Equipo de Control Perimetral Firewall

El firewall bloquea el acceso no autorizado del tráfico entrante y saliente de la red de la UESMA (Cisco, 2020). En la Figura 2, se observa cómo esta implementado el firewall sobre la red de la UESMA (Anchundia, 2000).

Firewall - UESMA

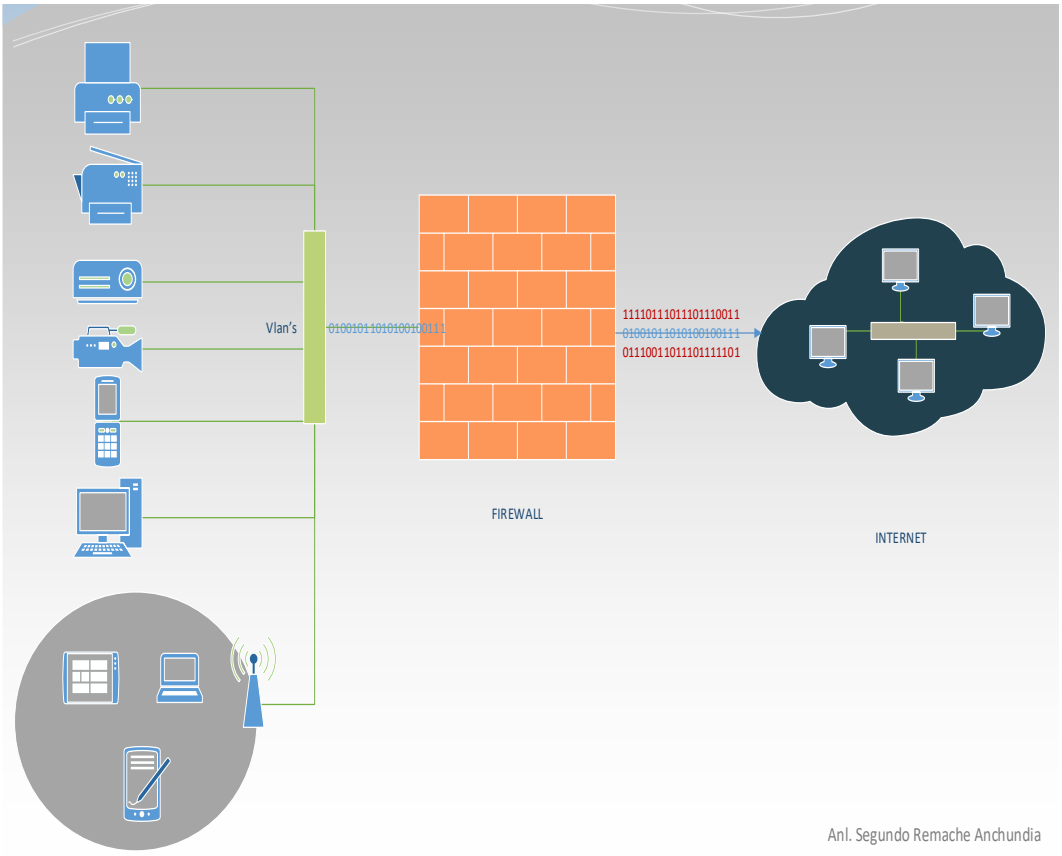


Figura 2. Diagrama Firewall – Red UESMA
Fuente: (Anchundia, 2000)

1.4. Servicios WSUS

WSUS (*Windows Server Update Services*, en español «servicios de actualización de windows server») permite implementar las recientes actualizaciones de productos de Microsoft sobre las computadoras de la red (Barrios, 2018).

1.5. Servicio DHCP

DHCP (*Dynamic Host Configuration Protocol*, en español «protocolo de configuración dinámica de host») en la UESMA permite la gestión de forma rápida de la distribución del direccionamiento IP en la red (Speedcheck, 2017). La Figura 3, muestra como esta implementado el protocolo DHCP, sobre la red de la UESMA.

Servidor DHCP

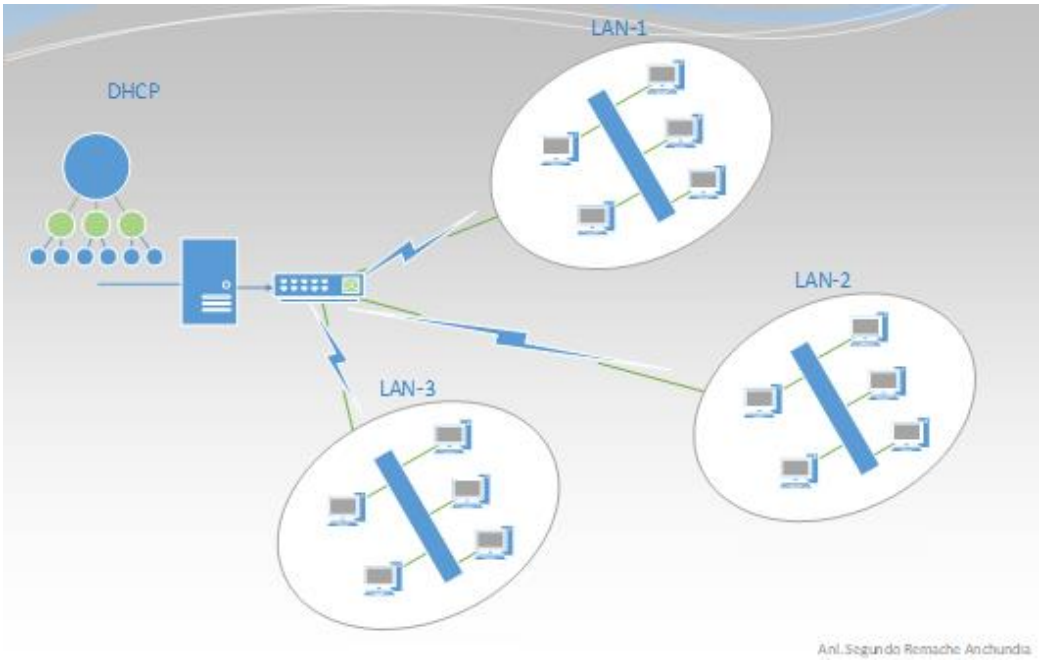


Figura 3. Protocolo HDCP – Cliente/Servidor
Fuente: (Anchundia, 2000)

1.6. Servicio de Controlador de Access Point

El controlador para la gestión de red inalámbrica es una solución de software que permite administrar múltiples redes inalámbricas usando un navegador web (Ubiquiti Networks, 2016). En la UESMA permite ejercer control sobre los Access Point instalados además, de configuraciones masivas, respaldos y despliegues de la configuración en todos los equipos.

Los requisitos de topología de red son los siguientes:

- Una red habilitada para DHCP (para que el punto de acceso alámbrico obtenga una dirección IP, así como para los puntos de acceso inalámbricos después de la implementación).
- Una computadora de la estación de administración que ejecute el software del controlador, ubicado en el sitio y conectado a la misma red de capa 2, o fuera del sitio en una nube o NOC (Ubiquiti Networks, 2016).

1.7. Servicio para control de los equipos e incidencias

En la UESMA ayuda a planificar y administrar los cambios del departamento de TICS, resuelve problemas de manera eficiente (Open Source Guide, 2017). También, permite el registro de asistencia a usuarios, enlazado al equipo en donde se está llevando a cabo dicho proceso. Facilita el historial de cada una de las incidencias en los equipos informáticos registrados en el departamento de TICS (Anchundia, 2000).

1.8. Servicio de inventario y reportería

Solución Open Source que está enfocado en la automatización del inventario del área informática de la institución. Ofrece integración total con el Sistema para control de los equipos e incidencias, lo que permite la fusión de las dos soluciones teniendo como resultados: inventarios automatizados de los equipos y el control de las asistencias técnicas realizadas (OCS inventory, 2001).

El Servicio de inventario y reportería dispone de un plugin que se instala en el equipo a ser inventariado cuya función es enviar los datos del equipo hacia el servidor, lo que permite registrar cualquier cambio que sufra el cliente.

1.9. LAN

La implementación realizada en la institución está basada en una topología estrella mediante concepto de núcleo colapsado según Cisco, significa que la LAN (Red de área local) cuenta con dos capas que se encargan de la comunicación de todos los dispositivos conectados.

Las capas en mención son Core o Núcleo y Acceso que permiten administrar la LAN de una manera eficiente, teniendo entre otras cosas: segmentación de redes creando LAN virtuales, ruteo entre las LAN virtuales, control de acceso, entre otros (Anchundia, 2000). La **¡Error! No se encuentra el origen de la referencia.**, muestra la distribución física de los equipos dentro de la infraestructura de la UESMA.

Topología física de la red

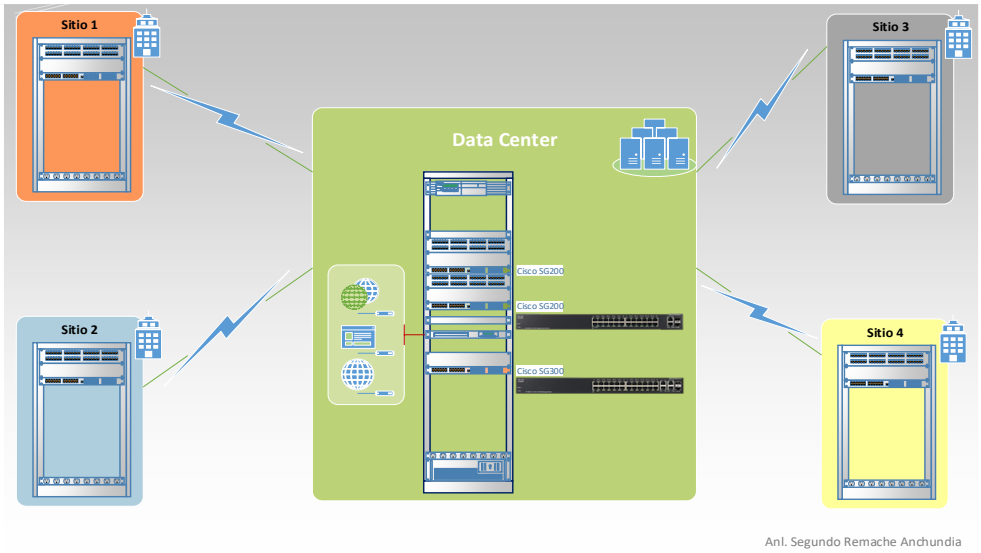


Figura 4. Diagrama LAN – Física
Fuente: (Anchundia, 2000)

En la Figura 5, muestra la topología lógica de la infraestructura de red de la UESMA, por cuestiones de seguridad se omiten las IP verdaderas.

Topología lógica de la red

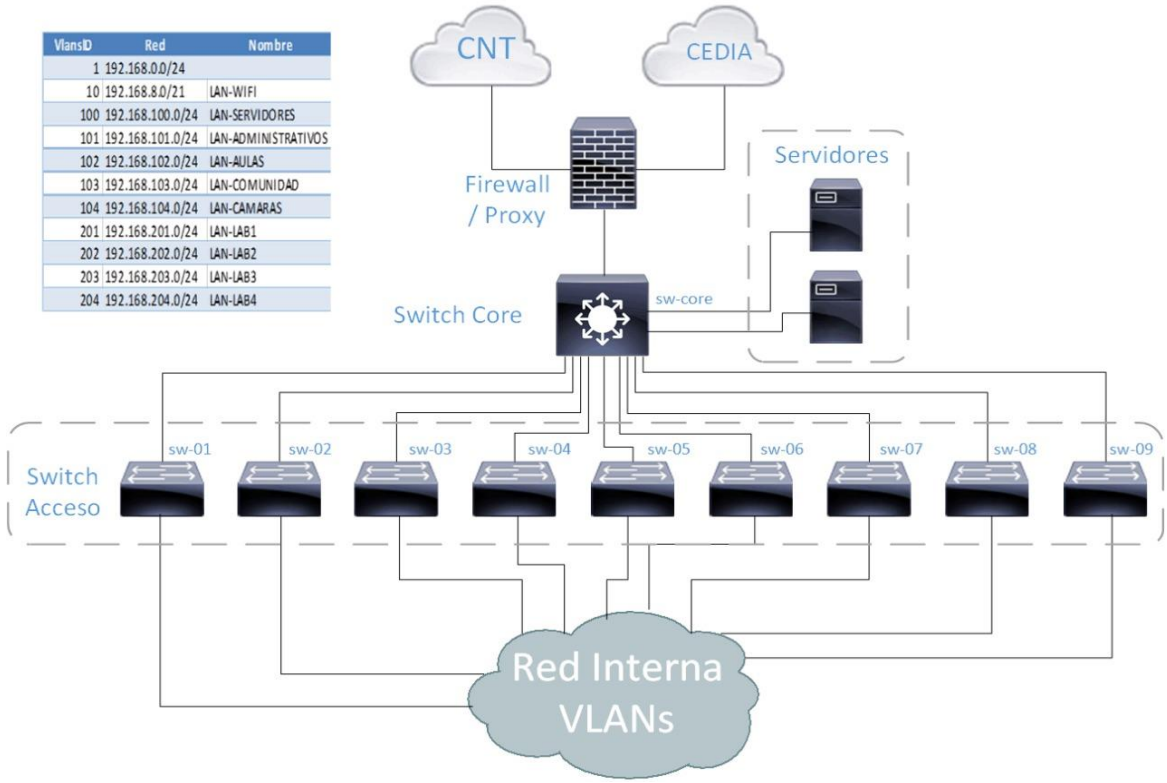


Figura 5. Diagrama LAN – Lógica
Fuente: (Anchundia, 2000)
Elaborado por: Mariuxi Márquez y Bryan Ramos

1.9.1. Switch Core

La UESMA para su implementación utilizó un switch Cisco SG300-28, el cual está instalado en el Data Center, configurado para que funcione en capa, es decir; para que trabaje en la capa IP según el modelo OSI y permite realizar todo el ruteo de paquetes inter-VLAN (Joan, 2013-2014).

En topología estrella, se concentran todas las conexiones y enlaces de fibra hacia los diferentes racks instalados en la institución. Así mismo, parte de su implementación es albergar la configuración de las VLAN y sus direcciones IP el cual lo convierte en el Default Gateway de cada VLAN en la red.

Finalmente, el switch core, almacena todas las políticas de acceso inter-VLAN, ya que por naturaleza este switch rutea los paquetes entre las diferentes VLAN creadas en su configuración.

1.9.2. Switch Acesso

Los switches de acceso, Cisco Serie SG-200, son equipos que forman los extremos de la topología estrella, instalados en los racks ubicados estratégicamente dentro de la institución.

A estos equipos llega un enlace de fibra óptica desde el Data Center, y son los responsables de dar la conectividad a los equipos cliente dentro de la LAN Corporativa (Anchundia, 2000).

1.10. Evaluación del Estado Actual de la red de la UESMA

La evaluación del estado actual permite tener un punto de partida, del estado en el que se encuentra la institución y ver alternativas al momento del diseño del SOC, Tabla 2.

Tabla 2. Evaluación del Estado Actual – UESMA

UESMA	
Áreas	**Estado Actual**
Perfil de Usuarios	No manejan perfiles de identificación y autenticación centralizado, pero cada PC tiene usuario administrador gestionado por TICS y uno local destinado para el usuario.
Políticas de Seguridad	Disponen de las siguientes políticas: ▪ Bloqueos de puertos. ▪ Bloqueos de acceso al panel de control. ▪ Bloqueos a redes sociales. Al no manejar perfiles de usuario no aplican políticas a cada perfil.
Estructura Tecnológica	No disponen de un esquema físico o lógico de la infraestructura tecnológica.
Infraestructura	En general los equipos que poseen tienen más de 10 años, pero se les realizan mantenimientos periódicos. Cuentan con: ▪ Diez (10) switch. ▪ Dos (2) servidores. ▪ Laptops (no se especifica cantidad). Para información más detallada ver **¡Error! No se encuentra el origen de la referencia.**.
Gestión de Alertas	No registran software que manejen la gestión de alertas mediante SNMP.

Control Perimetral	Mediante el firewall examina el tráfico entrante y saliente de la red, se inspecciona el contenido de cada mensaje para tomar la decisión de bloquear todo aquello que no cumplan los criterios de seguridad (Anchundia, 2000).
Recopilación y almacenamiento de logs y alertas	No se evidencia la existencia de un proceso o una herramienta para recopilar y almacenar logs y alertas.
Respuesta a los incidentes	Mediante la integración del servicio de control de equipos e incidencias y el servicio de inventario y reportería se automatizan las tareas descritas anteriormente.

Nota: La tabla se basa en la información proporcionada por el personal de TICS de la UESMA.

CAPÍTULO 2 - BASE TEÓRICA Y METODOLÓGICA

2. MARCO TEÓRICO

A continuación, se describen los conceptos fundamentales para la realización del presente proyecto:

2.1. CIA

Las comunicaciones seguras se componen de tres elementos:

2.1.1. Confidencialidad

Es el principio de seguridad que inspecciona el acceso a la información. Está diseñado para certificar que los usuarios equivocados no puedan obtener acceso a información confidencial, lo que garantiza el uso de la información solo para aquellos usuarios autorizados (Bashay, 2018).

Dentro de un grupo de usuarios autorizados, puede haber limitaciones adicionales y más estrictas sobre exactamente a qué información se les permite acceder (Walkowski, 2019).

Algunos de los medios más comunes utilizados para administrar la confidencialidad incluyen listas de control de acceso, encriptación de volumen y archivos, permisos de archivos, entre otros (CIA Triad, 2019).

2.1.2. Integridad

Se refiere a proteger la información de ser cambiada o alterada por terceros no autorizados (Chia, 2012). La información solo tiene valor si esta es integra, por ello aquella información que ha sido manipulada podría resultar riesgosa (Samaniego, 2013).

El control de los datos debe generar medidas de seguridad y permisos a los archivos de la organización, los datos deben mantener su estructura sin ser cambiados al momento de enviarlos o procesarlos (Bashay, 2018).

2.1.3. Disponibilidad

La información, el sistema y los datos solo deben de estar disponibles para los usuarios autorizados. Las medidas de disponibilidad preservan el acceso oportuno e ininterrumpido al sistema (Certmike, 2017-2019).

Un plan de recuperación de desastres rápido y adaptativo es crucial para los peores escenarios, ayuda a prevenir las pérdidas de información (Bashay, 2018). Además, las salvaguardas contra las interrupciones en las conexiones y la pérdida de datos deben considerar eventos impredecibles, como: un incendio un desastre natural, etc.

Para evitar la pérdida de datos, la copia de seguridad debe situar una ubicación geográficamente separada a la organización. Así mismo, para evitar el tiempo de inactividad debido a ataques maliciosos, como ataques de denegación de servicio de DOS e intrusiones en la red, se deben utilizar software adicional y equipos de seguridad (Bashay, 2018).

2.2. SANS

SysAdmin Audit, Networking and Security Institute - Instituto de Auditoria, Redes y Seguridad SysAdmin SANS (SANS Institute, 2014). “Es la fuente de capacitación más confiable de seguridad de la información en el mundo” (SANS™ Institute, 2000 - 2019).

Fundado el año de 1989 con políticas organizacionales, visión de investigación y educación. La confiabilidad de SANS es mundial, el material que publican ayuda a formar una gran cantidad de profesionales en diferentes áreas de seguridad, desde personas que manejan auditorias informáticas, prevención de ciberataques, administradores de seguridad de redes y un sinnúmero más de roles en el ámbito informático y el resguardo de la información (SANS™ Institute, 2000 - 2019).

2.2.1. Las personas en el SOC, que define la SANS

La SANS en uno de sus apartados del 2014 "*Security Operations Center* (SOC) in a Utility Organization" define los roles que debe poseer una organización para operar un SOC (SANS Institute, 2014).

Según el instituto SANS, se dividen en cuatro los roles de las personas de los SOC (SANS™ Institute, 2000 - 2019):

- **Analista de alertas de categoría 1:**

  El personal dentro de la UESMA se encargará de monitorear alertas entrantes, verificar que los incidentes hayan ocurrido y reenviar los informes a la categoría 2 si es necesario (CISCO, 2019).

- **Personal de respuesta ante los incidentes de categoría 2:**

  Responsables de investigar los incidentes en detalle y sugerir soluciones o medidas que deben adoptarse (CISCO, 2019).

- **Experto en la materia (SME)/buscador de categoría 3:**

  Las personas que trabajen en el SOC de la UESMA, deben ser profesionales expertos en redes, terminales, inteligencia de amenazas e ingeniería inversa de *malware*. Son especialistas en seguir los procesos del *malware* para determinar su impacto y cómo eliminarlo.

  Además, están profundamente involucrados en búsquedas y la implementación de herramientas de detección de amenazas dentro de la red en la UESMA (CISCO, 2019).

- **Administrador del SOC:**

  Deberá administrar todos los recursos del SOC de la UESMA y sirve como punto de contacto para el cliente o la organización en su totalidad (CISCO, 2019).

La Figura 6, representa cómo interactúan entre sí los roles del SOC.

Las personas en el SOC

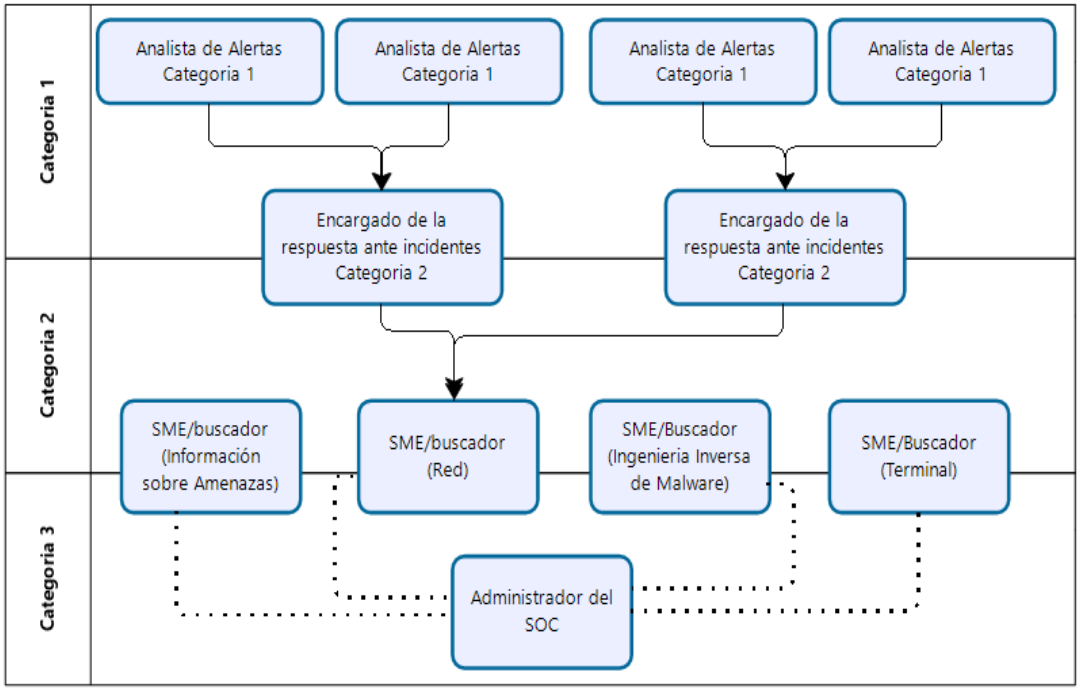


Figura 6. Categorias - SANS Institute
Fuente: (CISCO, 2019)
Elaborado por: Mariuxi Márquez y Bryan Ramos

A continuación, en la Tabla 3, se define los deberes y los conocimientos requeridos de las personas en el SOC:

Tabla 3. Deberes y Entrenamientos requeridos – SOC

SANS INSTITUTE		
Nivel	**Deberes**	**Conocimientos**
Nivel 1	-Monitoreo continuo de las alertas.	-Capacidad para la creación y parametrización sobre alertas de seguridad y detección de intrusos. -Administración de eventos de seguridad mediante herramientas SIEM. -Entrenamientos que investigan nuevas vulnerabilidades y herramientas informáticas.

Nivel 2	-Ejecutar análisis especializados para correlacionar diferentes fuentes de seguridad. -Brinda recomendaciones de remediación frente a incidentes de seguridad.	-Análisis de *malware* mediante herramientas por ejemplo Cuckoo Sandbox. -Evaluación e inteligencia sobre amenazas. Análisis forense de redes.
Nivel 3	-Expertos en redes	-Entrenamiento avanzado en detección de anomalías. -Capacitación específica en almacenamiento de data y análisis e inteligencia sobre amenazas. -Manejo avanzado de incidentes. -Habilidades para el desarrollo del *pentesting*.
Gerente SOC	-Gestionar al personal y hardware del SOC. -Emite reportes ejecutivos del SOC a las autoridades institucionales. -Aplica el SLA (Acuerdo de Nivel de Servicio).	-Capacitación en administración de proyectos. -Entrenamiento en administración de respuesta a incidentes. Habilidades para la administración de personal. Inclusión de certificaciones como CISM, CISSP, CISA y CGEIT. -Experiencia para guiar a los demás integrantes del equipo. -Experiencia mínima: 5 años como analista SOC/líder del equipo.

Nota: La tabla presenta información en detalle de los roles del SOC.

2.3. SOC

Un *Security Operation Center* (SOC) es el responsable del monitoreo, la detección y aislamiento de incidentes, y la administración de los productos de seguridad, dispositivos de red, dispositivos de usuarios finales y sistemas de las instituciones (McAfee & Intel Security, 2016).

Debido al funcionamiento permanente, en el SOC se concentra todo el personal y los sistemas que están dedicados a las tareas de seguridad (McAfee & Intel Security, 2016).

Estas son algunas herramientas que suelen encontrarse en un SOC:

2.3.1. Software de captura de paquetes de red

Este software es útil para la captura de paquetes de red, se trata de una herramienta primordial para un analista del SOC, ya que permite observar y entender cada detalle sobre la red (CISCO, 2019).

2.3.2. Herramientas de análisis de *malware*

En el caso de detección de un nuevo *malware*, estas herramientas permiten a los analistas ejecutar y observar con seguridad el funcionamiento de malware sin poner en riesgo sistemas subyacentes (CISCO, 2019).

2.3.3. Sistemas de detección de intrusiones - IDS

Herramientas usadas para el monitoreo e inspección de tráfico en tiempo real. Si cualquier aspecto del tráfico que fluye actualmente coincide con cualquiera de las reglas establecidas, se ejecuta una acción previamente definida (CISCO, 2019).

2.3.4. Firewalls

Herramientas con las cuales se pueden especificar reglas, la cuales indican si se permite el ingreso o la salida de paquetes de la red.

2.3.5. Administración de información y eventos de seguridad - SIEM

Herramientas que proporcionan análisis en tiempo real de alertas y entradas del registro que hayan generado dispositivos de red, como IDS y firewalls (CISCO, 2019).

2.3.6. Sistemas de tickets

Herramienta que se encarga de la asignación, edición y registro de incidencias en los equipos de la infraestructura.

2.4. Elementos de un SOC

La protección contra las amenazas actuales demanda un enfoque formalizado, estructurado y disciplinado a cargo de profesionales de centros de operaciones de seguridad (CISCO, 2019).

Los SOC ofrecen una gran cantidad de servicios, que incluyen desde el seguimiento y la gestión hasta soluciones contra amenazas y seguridad alojadas que se pueden personalizar para satisfacer las necesidades del cliente, en este caso la necesidad de la UESMA.

Los elementos principales de un SOC:

- Las personas.
- Los procesos.
- La tecnología.

2.5. Las tecnologías en el SOC

En la Figura 7, muestra que el SOC necesita un “Sistema de administración de Información y Eventos de Seguridad - SIEM” (Pratt, 2017). Este sistema combina datos de varias tecnologías.

Las tecnologías en el SOC

Figura 7. Sistema de Monitoreo del SOC
Fuente: (CISCO, 2019)

Los sistemas SIEM se usan para recopilar y filtrar datos; detectar, clasificar, analizar e investigar amenazas; y administrar recursos a fin de implementar medidas preventivas y afrontar futuras amenazas (CISCO, 2019).

2.6. Diseño del SOC

La flexibilidad que proporciona Linux es una característica grandiosa para el SOC. Todo el sistema operativo se puede adaptar para convertirlo en la plataforma perfecta de análisis de seguridad (CISCO, 2019).

Por ejemplo, se pueden agregar al sistema operativo solamente los paquetes necesarios, es decir que es posible instalar y configurar herramientas de software específicas para trabajar en conjunto, lo que permite personalizar las herramientas para que se adapten al flujo del trabajo del SOC (CISCO, 2019).

2.6.1. PfSense

Software de distribución gratuita que puede actuar como IDS/IPS con paquetes adicionales como Snort (Netgate Docs, 2018).

PfSense, características:

- Cortafuegos y enrutador.
- VPN.
- IPS/IDS.
- Autenticación de usuario.
- Proxy y filtrado de contenido (Innovablack, 2019).

PfSense es muy flexible y se puede adaptar fácilmente a numerosas aplicaciones que van desde un enrutador doméstico incluso un firewall para una red corporativa grande. Además, PfSense es fácil de instalar y mantener, brinda una interfaz de usuario basada en la web muy accesible (Kear, 2018).

2.6.2. Dispositivos de Detección y Prevención de Intrusos

En la Figura 8, se establece un diagrama comparativo entre ventas y desventajas de un IDS-IPS.

Diagrama IDS – IPS

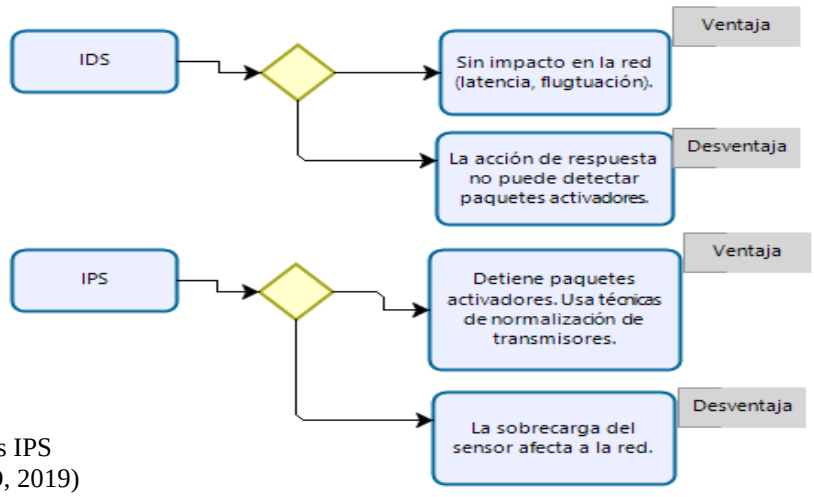


Figura 8. IDS vs IPS
Fuente: (CISCO, 2019)
Elaborado por: Mariuxi Márquez y Bryan Ramos

2.6.2.1. SNORT

"Sistema de Detección de Intrusos (IDS) basado en red (IDSN) open source" (Delgado, 2017). Es implementado en modo sin conexión, no tiene problemas con el flujo del tráfico de la red, así mismo no genera latencia que son problemas comunes al momento de medir el flujo del tráfico (CISCO, 2019).

"Snort funciona como sniffer" (Delgado, 2017) es decir, se conseguirá observar al instante lo que ocurre sobre la red, los logs, patrones de trasferencias, configuraciones, y demás (Beal, 2016).

2.6.3. Sandbox

En ciberseguridad, un sandbox es un medio aislado en una red que imita entornos operativos del usuario final. Los sandbox se usan para ejecutar de forma segura códigos dudosos sin correr riesgos de perjudicar los dispositivos host o la red (Sandbox Security, 2018).

El Sandboxing es una técnica que permite analizar y ejecutar en un entorno seguro los archivos sospechosos (CISCO, 2019). Además, es un estrategia de gestión de software que aísla las aplicaciones de los recursos críticos del sistema y otros programas. Proporciona una capa adicional de seguridad, evita que el *malware* o las aplicaciones dañinas afecten negativamente al sistema (Techterms, 2016).

2.6.3.1. Cuckoo Sandbox

Es un sandbox de sistema gratuito para el análisis de malware, se puede ejecutar localmente y usarlo para analizar muestras de malware (CISCO, 2019).

El archivo que analiza indica la procedencia de este solo en minutos, además del score en un rango máximo de 10 que posee el archivo, así mismo revela mediante varias capturas de pantalla el procedimiento que se ejecutó al instante que el malware hizo contacto con la máquina o al

sistema infectado. Mas aún, el informe que genera Cuckoo es en detalle minucioso e indica la situación actual del archivo (Avila, 2020)

No es simplemente analizar el archivo malicioso, el deber del personal del SOC mediante esta herramienta es percibir el contexto, la motivación del atacante y el objetivo de la infección informática (OSI, 2016).

2.6.4. Moloch

"Herramienta de análisis de paquetes de red" (Velasco, 2014) de código abierto. Se integró al Cuckoo para ser el visualizador de los datos que se almacenan en Elasticsearch.

Moloch posee una interfaz accesible, entre ella varias características:

- Página de sesiones.

  Lista de sesiones indexadas para el período de tiempo seleccionado y la expresión de búsqueda. Incluye un gráfico de línea de tiempo y un mapa de los resultados de la sesión (Moloch , 2019).

- Página de vista y de Gráfico de SPI

  SPI (Información del perfil de sesión) le permite ver valores únicos con recuentos de sesiones para cada uno de los campos capturados (Moloch , 2019).

- Página de conexiones.

  Muestra un gráfico de red de sus resultados de búsqueda (Moloch , 2019).

2.6.5. Servidor de antivirus

McAfee ePolicy Orchestrator trabaja con administración centralizada sobre la seguridad en la red lo que facilita y optimiza la administración de los riesgos y el cumplimiento de normativas (Brighttalk, 2018).

Además, reduce brechas de seguridad y garantiza que las herramientas implementadas sobre la infraestructura funcionen en conjunto con controles orquestados (Mcafee, 2019).

2.6.6. SIEM

Security Information and Event Management - Gestión de Eventos e Información de Seguridad, tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad, a través del procesamiento de datos y priorización de amenazas (HelpSystems, 2020).

SIEM incluye las siguientes funciones esenciales:

- **Análisis de informática forense.**

  Permiten realizar búsquedas en registros de eventos a partir de fuentes en toda la organización. Proporcionan información más completa para el análisis de informática forense.

- **Correlación**.

  Analizan logs y eventos de diferentes sistemas o aplicaciones, lo que acelera la detección de las amenazas de seguridad y la capacidad de reacción ante ellas.

- **Agregación**.

  Reducen el volumen de datos de eventos mediante la consolidación de registros duplicados.

- **Informes**.

  Permiten ver los datos sobre eventos correlacionados y acumulados mediante monitoreo en tiempo real y resúmenes a largo plazo.

Con esta información, los analistas de seguridad de la red pueden evaluar rápidamente y con precisión el grado de cualquier evento de seguridad (CISCO, 2019).

SIEM, es utilizado en muchas organizaciones para proporcionar informes en tiempo real y estudios a largo plazo de sucesos de seguridad (CISCO, 2019), como se ve en la Figura 9.

SIEM y la recopilación de archivos de registro

Figura 9. Componentes SIEM
Fuente: (CISCO, 2019)

2.6.6.1. ELK

Una solución de SIEM popular y de código abierto es ELK, que integra las aplicaciones "Elasticsearch, Logstash y Kibana" (Elastic, 2019).

- **Elasticsearch.**

  Motor de búsqueda de texto completo orientado a documentos (CISCO, 2019).

- **Logstash**.

  Sistema de procesamiento de flujo que conecta entradas a salidas con filtros opcionales en el medio (CISCO, 2019).

  Permite seleccionar datos de distintas fuentes, procesarlos, normalizarlos y distribuirlos (García, 2019). Además, recoge mensajes registrados y los retransmite a ElasticSearch (Pérez, 2018).

- **Kibana**.

  Análisis con base en el navegador y tablero de búsqueda para Elasticsearch (CISCO, 2019).

2.6.7. GLPI

Sistema donde se registran incidentes y requerimientos que conforman todo el servicio de TI, para gestionarlos de modo rápido y ordenado (Ochoa, 2018).

2.6.8. Zabbix

Software de monitoreo de código abierto que recopila información de la estructura, servicios, aplicaciones, y recursos de la red (Zabbix, 2001-2020).

Características:

- Colección métrica inteligente y altamente automatizada.
- Detección avanzada de problemas.
- Alerta inteligente y remediación.

Así mismo Zabbix se puede implementar en base a dos tipos de monitoreo (Linuxize, 2018):

- Monitoreo basado en agentes.
- Monitoreo sin agentes.

2.6.9. Grafana

Pluging instalado en Zabbix que permite visualización de métricas, es un software de código abierto (Zobnin, 2020).

Grafana es una buena alternativa a los paneles de Zabbix ya que facilita la creación de gráficos y paneles basados en datos de varios sistemas de monitoreo (Kalsin, 2016). Se pueden combinar diferentes tipos de gráficos (pasteles, líneas, barras, etc.) los cuales van a ser mostrados en el dashboard en tiempo real.

2.7. Principios de la seguridad de una red

2.7.1. Vulnerabilidad

Una debilidad en un sistema o en su diseño que un atacante podría aprovechar (CISCO, 2019).

2.7.2. Amenaza

Un peligro potencial para un activo, como los datos o la propia red (CISCO, 2019).

2.7.3. Ataque

Mecanismo que se emplea con el fin de aprovechar una vulnerabilidad para poner en riesgo un activo (Fernández, 2017). Estos ataques pueden ser locales o remotos.

El ataque remoto, tiene lugar en la red sin acceso previo al sistema de destino. El atacante no necesita una cuenta en el sistema final para aprovechar la vulnerabilidad. Por otro lado, un ataque local el agente de amenaza tiene algún tipo de acceso de usuario o administrador al sistema final. Un ataque local no significa, necesariamente, que el atacante tenga acceso físico al sistema final (CISCO, 2019).

2.7.4. Riesgo

Probabilidad de que una amenaza específica aproveche una vulnerabilidad particular de un activo y provoque una consecuencia indeseable (Yunda, 2016).

2.8. Diseño de tres capas

El diseño en capas facilita la implementación de funciones sobre la red de la UESMA. En la Figura 10, se observa el modelo jerárquico de tres capas.

Modelo tres capas, diseño jerárquico

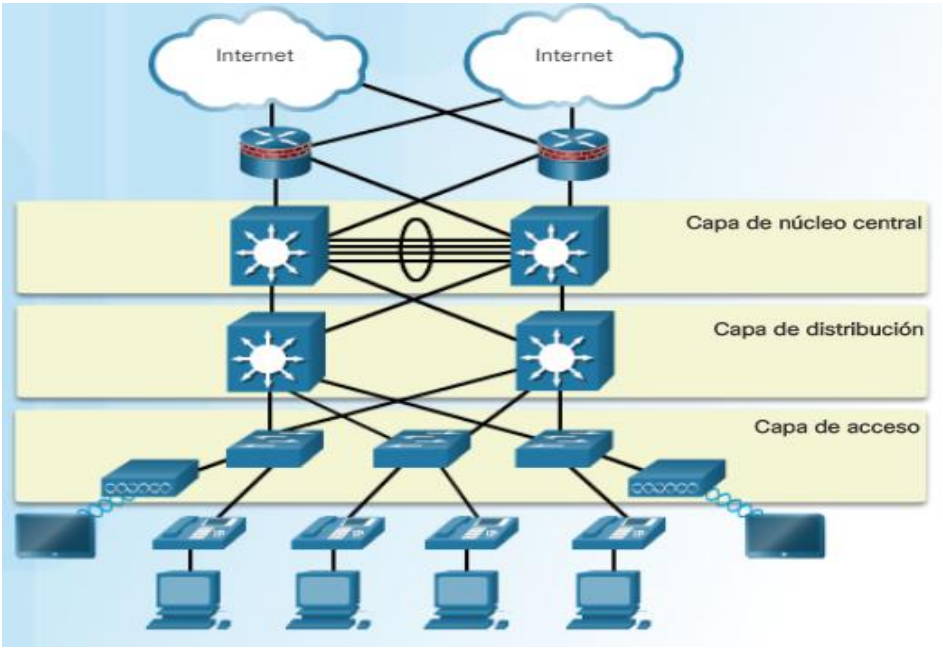


Figura 10. Modelo del Diseño Jerárquico
Fuente: (CISCO, 2019)

En la Figura 11, un diseño jerárquico de dos niveles, las capas de núcleo y de distribución se combinan en una, lo que reduce el costo y la complejidad (CISCO, 2019).

Núcleo contraído

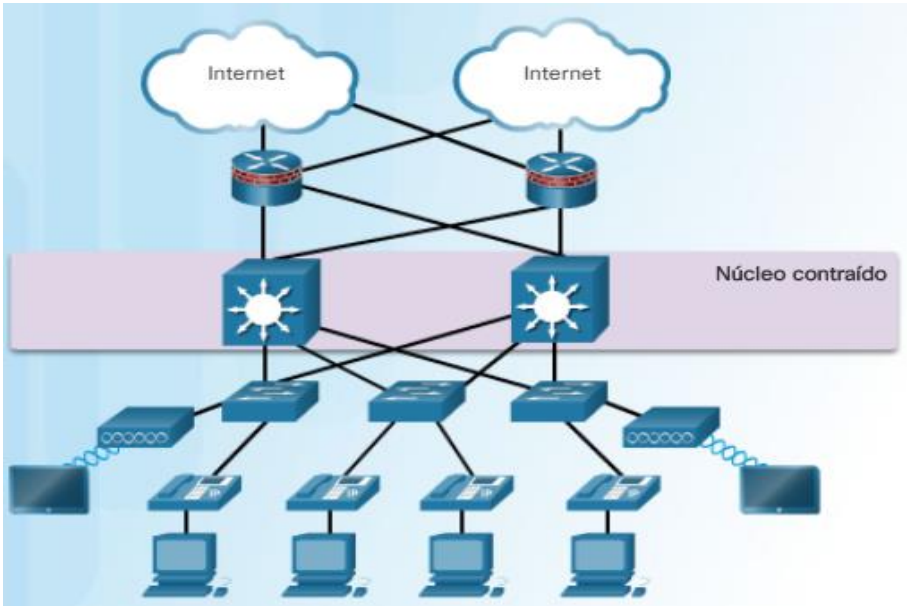


Figura 11. Modelo del Diseño Núcleo Contraído
Fuente: (CISCO, 2019)

2.9.Virtualización

El software de virtualización es VMware, posee una capa de hardware físico, hipervisor ESXI, capa de máquina virtual y capa del sistema operativo invitado (Paessler, 2020). Se obtienen estas capas, mediante VMware vSphere el cual permite al departamento de sistemas gestionar de manera adecuada los recursos del trabajo sobre las aplicaciones informáticas que maneja la organización (Stroud, 2018).

2.10. Sistema Operativo

Los sistemas operativos que se listan a continuación fueron utilizados para la realización del proyecto, ver Figura 12.

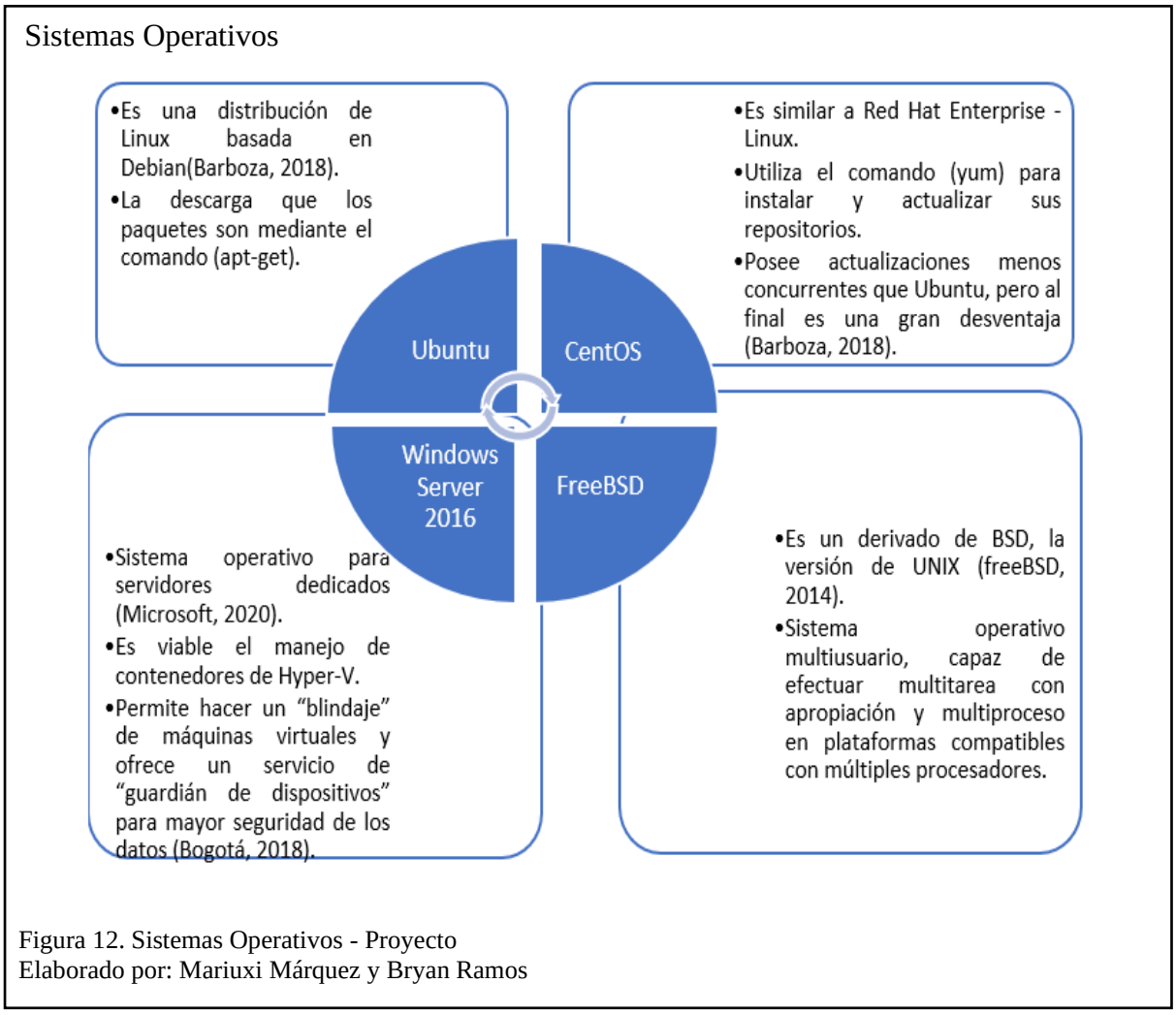


Figura 12. Sistemas Operativos - Proyecto
Elaborado por: Mariuxi Márquez y Bryan Ramos

2.11. Metodología

Este ejercicio de sistematización se desarrolló de acuerdo con la metodología propuesta por Patricio Emanuelli A., Fabián Milla A., Ruth Sepúlveda M. y Juan Andrés Torrealba M. en el documento “Hoja de ruta para la implementación de proyectos piloto”, a través de la cual se define un punto de partida, se hace una delimitación de la experiencia a sistematizar, se describe la experiencia, realizan un análisis, se presentan los resultados y recomendaciones (Emanuelli A, Milla A, Sepúlveda M, & Torrealba M).

Se lista el proceso de las etapa:

- En la Etapa de Análisis Preliminar se realizará el levantamiento de la información mediante la elaboración de estudios (entrevistas y toma de datos), para determinar el estado actual de la red de la UESMA.
- En la Etapa de Implementación se trabaja en un ambiente de simulación que permita hacer un bosquejo de la red actual, es decir cómo se van a manejar los incidentes y las vulnerabilidades que se tengan.
- En la Etapa de Operación se ponen en práctica las diferentes pruebas sobre la recopilación de los datos del rendimiento.
- En la etapa de evaluación de resultados se deben generar y documentar recomendaciones basadas en el análisis de la SANS con los datos recolectados por el SOC, indicando las acciones de mejora y ayuda al desempeño de las actividades de la UESMA.

CAPÍTULO 3 - ANÁLISIS Y DISEÑO

En la actualidad las amenazas sobre ciberseguridad traen desafíos como la rápida detección de las mismas, es por esto que las personas que trabajan para los SOC deben vigilar constantemente los sistemas de seguridad, ya que su objetivo es detectar y combatir el ciberdelito (CISCO, 2019).

En este capítulo, se realizó el análisis de la información recopilada y el diseño del prototipo de la solución, para esto se tomó en cuenta las funciones sustantivas que den apoyo a la UESMA.

3.1. Funciones sustantivas que apoyen a la UESMA

Según la entrevista realizada a los técnicos de TICS, la UESMA maneja datos e información importante, las funciones sustantivas como: el sistema de contabilidad, la facturación electrónica y el sistema de calificación permite tener una base para evaluar los problemas de seguridad que se puedan presentar como el robo de información.

El SOC prototipo responde al análisis del estado actual de la red de la UESMA mostrado en la Tabla 2, del **CAPÍTULO 1 - ESTUDIO DEL PROBLEMA** y se resume en la Tabla 4.

Tabla 4. Respuesta de la Evaluación del Estado Actual - UESMA

UESMA	
Áreas	**Respuesta al Estado Actual**
Perfil de Usuarios	A través del almacenamiento y procesamiento de logs, se podría determinar cuando un usuario realice alguna acción sobre el equipo, por ejemplo, ejecutar una tarea anómala con el perfil de administrador en un horario inusual.
Políticas de Seguridad	A través del firewall se permite el acceso a internet de una forma más segura, bloquea y examina el tráfico considerado como malicioso.

	Al establecer un DNS seguro como por ejemplo el de OpenDNS permite restringir el acceso a ciertas páginas que los estudiantes no deben acceder. Contar con un antivirus centralizado permite mantener la seguridad en los endpoint constantemente actualizada y así proteger de la descarga de contenido malicioso.
Estructura Tecnológica	El diagrama físico-lógico de la red permite visualizar los elementos que componen la infraestructura tecnológica de la red y como se trasmite el flujo de información. Al contar con el diagrama se pueden detectar y resolver los problemas de una manera eficaz y eficiente.
Infraestructura	Mediante la virtualización se obtienen beneficios como los mencionados anteriormente en el tema de **Virtualización**, cabe destacar entre estos beneficios la reducción de costos y la aceleración en el despliegue de los aplicativos. En el presente trabajo, al contar con recursos suficientes para la virtualización, se utilizó un solo servidor en el cual se desplegaron las máquinas virtuales que componen el SOC. Mediante las herramientas embebidas en el hipervisor se puede también virtualizar las redes y las conexiones internas en la interacción entre estas máquinas virtuales.
Gestión de Alertas	Mediante la gestión de alertas se puede observar los problemas que presenta la infraestructura de red, con esto es posible tomar acciones con las cuales se corrijan los problemas y así proceder a resolver incidentes.

	El SIEM cuenta con herramientas para el monitoreo de la infraestructura y la recolección de alertas, también cuenta con una interfaz web en donde se puede filtrar y visualizar de manera gráfica las alertas generadas en los equipos que componen la infraestructura.
Control Perimetral	A través del Firewall y SNORT tanto los paquetes entrantes como los salientes se pueden inspeccionar en búsqueda de anomalías en su interior, al ser SNORT un conjunto de reglas que a través de la comunidad son periódicamente actualizas, la institución se asegura de estar al día en cuanto a los diferentes tipos de ataques, esto siempre y cuando se apliquen las reglas de SNORT pertinentes que no interfieran en el funcionamiento normal de la infraestructura, junto con el Firewall en donde se pueden establecer reglas personalizadas para el acceso y el bloqueo del tráfico alrededor de la red; estas herramientas componen una sólida protección del perímetro de red. ▪ **Recopilación y almacenamiento de logs y alertas.** Mediante el SIEM que está compuesto de las herramientas de Elasticsearch, Logstash y Kibana, haciendo uso de las dos primeras se procesan y almacenan todos los logs que son generados por los diferentes componentes de la infraestructura de red. ▪ **Respuesta a los incidentes** Es necesario contar con una herramienta que ayude a llevar el control de los incidentes que se presentan en la red, por ello el

	uso de una herramienta como GLPI facilita la gestión y asignación de tareas para la resolución de los incidentes que se puedan presentar.

Nota: La tabla responde al análisis de estado actual de la UESMA.

3.2. Diseño SOC siguiendo los roles definidos por el instituto SANS

El diseño del SOC debe poseer una distribución organizacional que facilite tareas, funciones y deberes al momento de hallar indecencias sobre el monitoreo de la red de la UESMA. Mediante normativa internacional la SANS divide en cuatro los roles de las personas de los SOC (SANS™ Institute, 2000 - 2019).

En contraste con lo anterior se detalla el proceso que cumplen cada uno de los roles del SOC:

- **El analista de alertas de categoría 1**

El personal de esta categoría trabaja bajo un monitoreo continuo y análisis de alertas de seguridad informáticas, lo que facilita detección de intrusos a los sistemas de la UESMA.

Sobre la infraestructura propuesta se tiene al SIEM, que administra eventos de seguridad, analiza logs y eventos de los diferentes sistemas, lo que acelera la rápida detección de amenazas. Para el SIEM se seleccionaron las herramientas que componen ELK (Elasticsearch, Logstash y Kibana). Elasticsearch almacena todos los logs, Logstash como tarea principal recibe y procesa los logs que junto a Kibana, la interfaz web, ayuda a buscar y visualizar los logs, como se muestra en la Figura 13.

Analista categoría 1

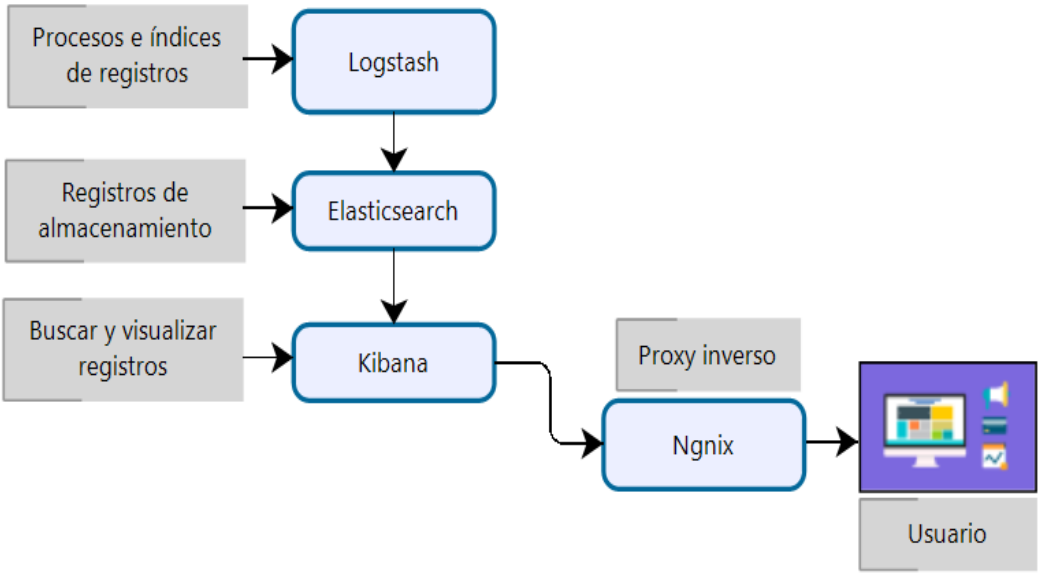


Figura 13. Funcionamiento ELK
Elaborado por: Mariuxi Márquez y Bryan Ramos

- **Personal de respuesta ante los incidentes de categoría 2**

Procede a investigar de manera minuciosa y en detalle el incidente, presentando posibles soluciones que no tergiversen la información. Brinda recomendaciones frente al incidente de seguridad.

Mediante Cuckoo Sandbox se procederá a la captura de la información relevante al ejecutar un archivo sospechoso que sea detectado en la red ya sea a través del firewall, IDS o el antivirus, la información que se obtiene es la captura del tráfico, la captura de los logs al ejecutar el archivo sospechoso y el procedimiento que se lleva a cabo emulando la interacción que tendría el usuario al ejecutarlo. Esto último se evidencia a través de las capturas de pantalla realizadas por el Cuckoo.

Además, ejecuta y analiza el malware detectado en la red, descifra el contenido y procedencia del archivo, por ejemplo, se observa la dirección IP de destino, el host, la máquina donde fue el

ataque y mediante que técnica de encriptación fue realizado el ataque entre otros datos importantes.

- **Experto en la materia (SME - Gestión de Eventos de Seguridad) /buscador de categoría 3**

El personal de este nivel investiga información sobre las amenazas detectadas en los dos niveles anteriores, aplica técnicas de ingeniera inversa de malware, son especialistas en seguir procesos que realizó el malware para determinar el impacto que causo sobre la red y como proceder a eliminarlos.

Mediante Cuckoo se pueden visualizar las firmas que fueron comprometidas en la ejecución del malware, con esto se puede categorizar el malware y mediante MD5, SHA-1, SHA256 o SHA512.

Estas listas generan un identificador único el cual se puede cotejar con las bases de datos de virus y amenazas, como por ejemplo “VirusTotal”.

Con Moloch se puede analizar a fondo el paquete de tráfico capturado por el sandbox, y así determinar cuál fue la interacción de la amenaza con la red.

- **Administrador del SOC**

Tiene comunicación directa con la UESMA, indicando los procedimientos, hallazgos y soluciones de las incidencias presentadas en la red. Mediante GLPI se posee un control centralizado de las tareas que se llevan a cabo sobre los incidentes, además se pueden generar reportes de tareas y procedimientos que se han llevado a cabo, indicando el estado de ejecución en el que se encuentran los tickets.

3.2.1. Modelo de Proceso – SANS

Para entender los pasos del funcionamiento del SOC se creó un "modelo de procesos", es decir un diagrama de procesos para la gestión ante un incidente. La SANS en su apartado "Incident Response Playbook Creation" (Taylor, 2018) propone niveles que se deberían aplicar al detectar un malware.

Estos procedimientos ayudan al SOC a descartar falsos positivos, dividir al equipo del SOC por roles de manera correcta y generar nuevas métricas en procedimientos de incidentes. En la Figura 14, se observa el modelo de proceso de respuestas ante incidentes de seguridad, aplicables a la estructura del SOC.

Modelo de proceso

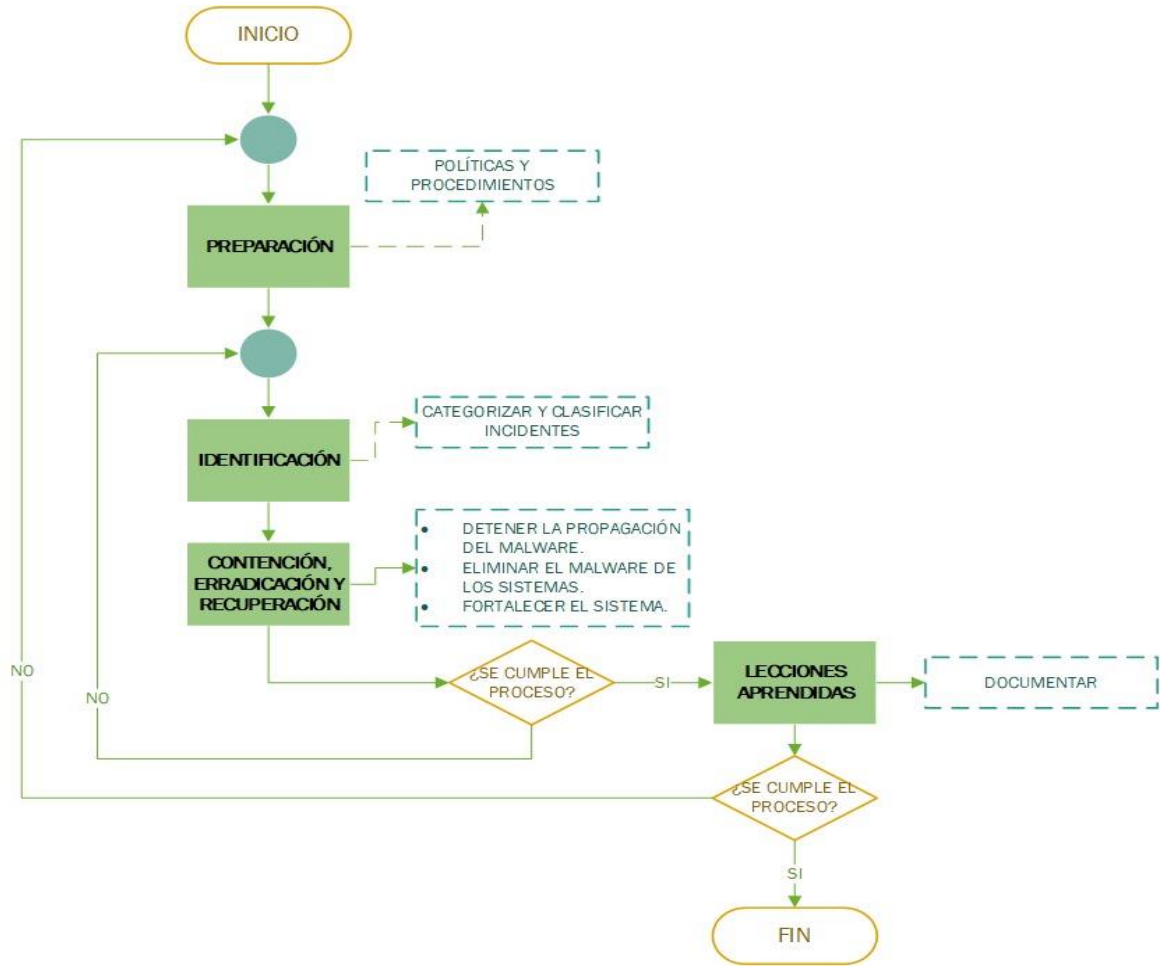


Figura 14. Diagrama de Procesos del manejo de incidentes - SANS
Elaborado por: Mariuxi Márquez y Bryan Ramos

3.2.2. Capturas de aplicaciones del SOC prototipo

En el **¡Error! No se encuentra el origen de la referencia.**, se muestran las principales capturas de las aplicaciones del prototipo del SOC

3.2.3. Topología Lógica - Diseño del SOC

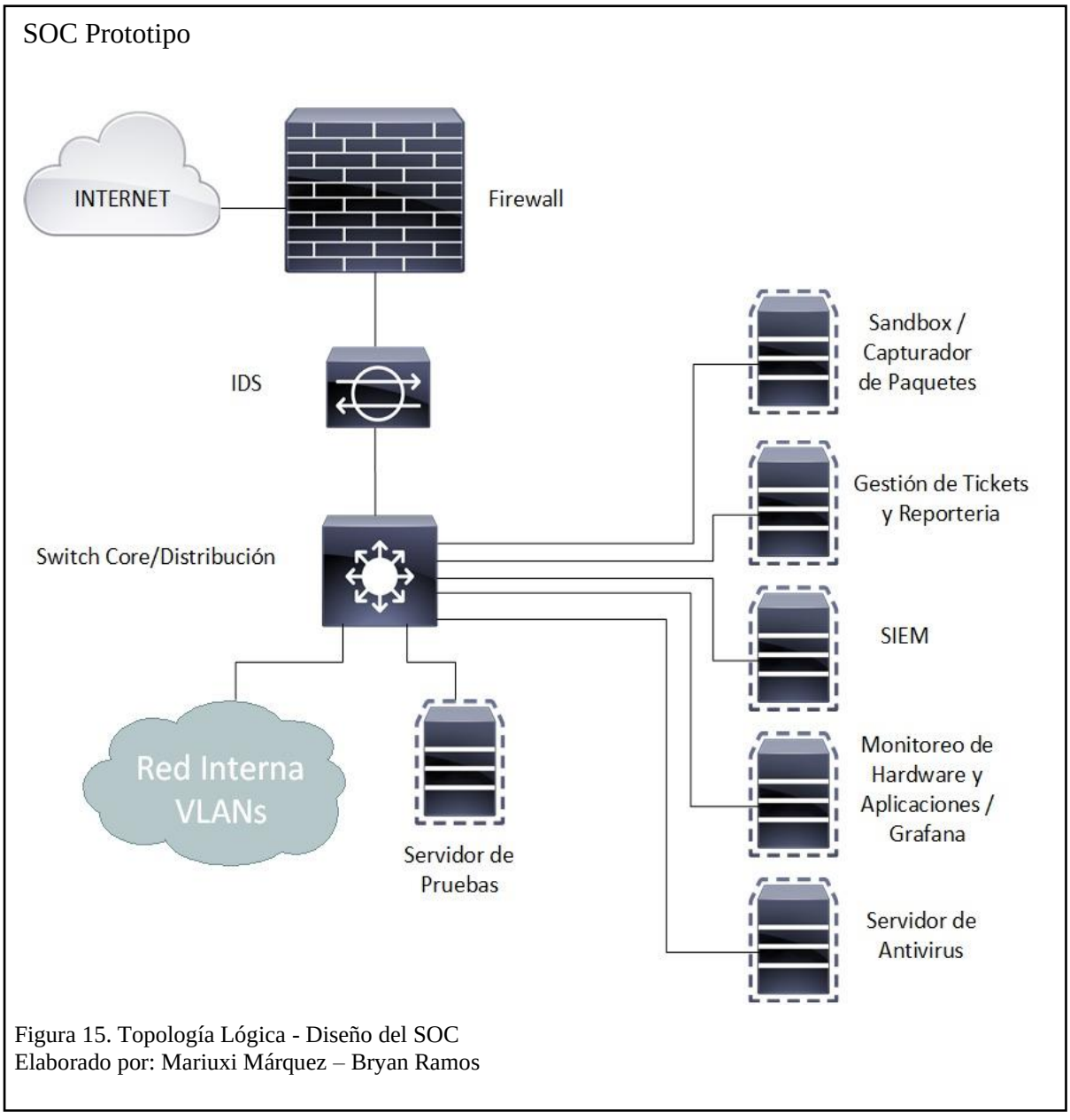


Figura 15. Topología Lógica - Diseño del SOC
Elaborado por: Mariuxi Márquez – Bryan Ramos

3.3.Implementación del prototipo del SOC

La implementación del SOC se lo realizó en una red prototipo, en este caso bajo un entorno de simulación. Se instaló PfSense, Cuckoo Sandbox, Zabbix, SIEM, McAfee ePolicy Orchestrator y finalmente el sistema de tickets y reportería.

Los sistemas operativos usados para instalar estos servicios fueron UBUNTU, CentOS y Windows Server.

- **Requerimientos máquina virtual**

Los recursos que fueron utilizados para el diseño prototipo del SOC se detallan a continuación

1. **Host**

Montado sobre VMware, Esxi versión 6.5.0 la Tabla 5, presenta los recursos del host en el cual se instalaron las máquinas requeridas para el diseño del SOC.

Tabla 5. Hardware del servidor anfitrión

Tipo	Información
Fabricante	Cisco Systems Inc
Modelo	UCSG-C220-M4S
CPU	20 CPUs x Intel(R) Xeon(R) CPU E5-2640 v4 @2.40GHz
Memoria	127.74 GB

Nota: Recursos utilizados para el hardware virtualizado.

2. **PfSense**

Tabla 6. PfSense VMware

VMware	
Información General	
Nombre Host	PfSense Firewall
Configuración Hardware	
CPU	1 vCPUs
Memoria	4 GB
Disco Duro 1	100 GB

Adaptador de Red 1	WAN (Conectado)
Adaptador de Red 2	LAN (Conectado)

Nota: Información de la máquina PfSense Virtualizada.

3. Sandbox

Tabla 7. Sandbox VMware

VMware	
Información General	
Nombre Host	Sandbox
Configuración Hardware	
CPU	4 vCPUs
Memoria	8 GB
Disco Duro 1	100 GB
Adaptador de Red 1	LAN (Conectado)

Nota: Información de la máquina Sandbox Virtualizada.

4. SIEM

Tabla 8. SIEM VMware

VMware	
Información General	
Nombre Host	ELK UESMA
Configuración Hardware	
CPU	2 vCPUs
Memoria	8 GB
Disco Duro 1	100 GB
Adaptador de Red 1	LAN (Conectado)

Nota: Información de la máquina SIEM Virtualizada.

5. GLPI

Tabla 9. GLPI VMware

VMware

Información General	
Nombre Host	Sistema tickes
Configuración Hardware	
CPU	2 vCPUs
Memoria	2 GB
Disco Duro 1	80 GB
Adaptador de Red 1	LAN (Conectado)

Nota: Información de la máquina GLPI Virtualizada.

6. Zabbix

Tabla 10. Zabbix VMware

VMware	
Información General	
Nombre Host	Zabbix UESMA
Configuración Hardware	
CPU	1 vCPUs
Memoria	4 GB
Disco Duro 1	50 GB
Adaptador de Red 1	LAN (Conectado)

Nota: Información de la máquina Zabbix Virtualizada.

7. Servidor de antivirus

Tabla 11. Antivirus McAfee ePolicy Orchestrator

VMware	
Información General	
Nombre Host	McAfee Antivirus
Configuración Hardware	
CPU	2 vCPUs
Memoria	12 GB
Disco Duro 1	200 GB
Adaptador de Red 1	LAN (Conectado)

Nota: Información de la máquina McAfee Virtualizada.

CAPÍTULO 4 - EVALUACIÓN DE RESULTADOS

En este capítulo, se realizó un análisis de los resultados sobre el diseño del SOC prototipo de forma técnica, económica y legal, donde se explica la fiabilidad de la propuesta.

4.1. Análisis Técnico

En la Tabla 3, se describieron las funciones que debe cumplir un SOC, analizando el entrenamiento del SOC por cada categoría y su rendimiento.

4.1.1. Entrenamiento del SOC por cada categoría

En la Tabla 12, se detalla cómo se realizan las funciones del SOC basado en los roles de la SANS.

Tabla 12. Entrenamiento categoría 1 - SANS

Tipo: Analista de alertas de categoría 1			
Entrenamiento planteado:	**Evaluación**		
	SI	NO	Observación
Sistema de clasificación, que permita revisar las colas y comportamientos anómalos, de las alertas de seguridad de la red.	x		
Investigar cada una de las alertas.	x		
Revisar y excluir los “falsos positivos”.	x		
Monitoreo permanente del funcionamiento del hardware de la red informática institucional.	x		

Nota: Análisis sobre procedimiento de la categoría 1 - SOC.

Tabla 13. Entrenamiento categoría 2 - SANS

Tipo: Personal de respuesta ante los incidentes de categoría 2			
Entrenamiento planteado:	**Evaluación**		
	SI	NO	Observación
Propone una metodología o procedimientos para el análisis del incidente.	x		El nivel de expertise es mayor que la categoría 1. La categoría 1 informa del incidente.
De la información detallada se determina si el incidente afecta a las funciones sustantivas de la UESMA.	x		
Estudia el impacto que ha causado sobre el hardware de la red informática institucional.	x		
Análisis de malware mediante herramientas de Cuckoo Sandbox.	x		
Recomienda una posible solución.	x		

Nota: Análisis sobre procedimiento de la categoría 2 – SOC.

Tabla 14. Entrenamiento categoría 2 - SANS

Tipo: Experto en la materia (SME)/buscador de categoría 3			
Entrenamiento planteado:	**Evaluación**		
	SI	NO	Observación
Sólido conocimiento en redes.	x		Tiene un nivel de expertise en las herramientas de Sandbox y Wireshark.
Obtiene datos de la actividad maliciosa.	x		

Emite informes sobre el análisis del incidente.	x		

Nota: Análisis sobre procedimiento de la categoría 3 – SOC.

Tabla 15. Entrenamiento Administrador del SOC

Tipo: Administrador del SOC			
Entrenamiento planteado:	**Evaluación**		
	SI	NO	Observación
Gestionar al personal y hardware del SOC.	x		Responsable máximo del SOC
Emite reportes ejecutivos del SOC a las autoridades institucionales.	x		
Aplica el SLA (Acuerdo de Nivel de Servicio).	x		El SLA es determinado por las autoridades institucionales.

Nota: Análisis sobre entrenamiento del administrador del SOC.

4.1.2. Rendimiento del SOC

Las gráficas que se muestran a continuación representan el rendimiento de la infraestructura donde se consideraron como parámetros el CPU, RAM y almacenamiento de los servidores, así como el tráfico de red tanto interno como externo del prototipo diseñado.

Para las muestras de las gráficas se tomaron como referencia la cantidad de máquinas que serán supervisadas por el prototipo. Incrementando dos máquinas (un servidor y un cliente) en cada nueva muestra, hasta realizar un total de seis muestras en la Figura 16, se observa el dashboard de una de las muestras realizadas, las demás capturas que muestran los resultados obtenidos se las puede encontrar en el **¡Error! No se encuentra el origen de la referencia.**, que por motivos de confidencialidad se especifican en esta parte del documento.

Muestra de pruebas de rendimiento

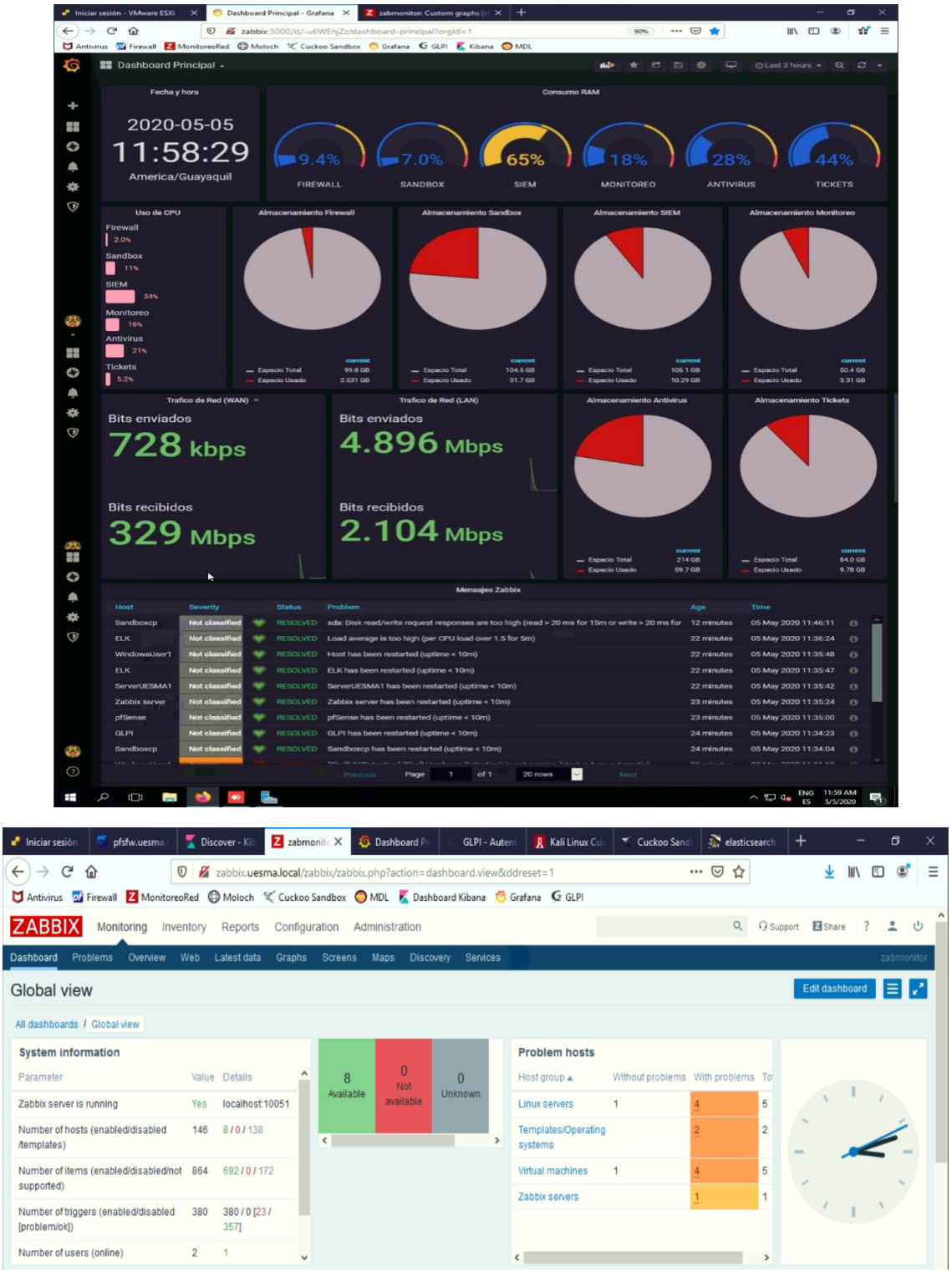


Figura 16. Muestra rendimiento en Grafana y Zabbix
Elaborado por: Mariuxi Márquez y Bryan Ramos

En la Figura 17, se observa que en el Sandbox la RAM de la tercera a la quinta muestra presenta una fluctuación en sus parámetros, sin embargo, en la sexta muestra regresa a la medida normal.

En el CPU las primeras cinco muestras mantienen datos constantes excepto la sexta, en la cual se observa un incremento mínimo del (0,3%) de consumo del CPU. Finalmente, en el almacenamiento se observa que los datos durante la captura de las seis muestras tienen el mismo valor.

Cabe recalcar que este es un servicio pasivo en la infraestructura del prototipo, es decir que solo actuará cuando los analistas de categoría 2 y 3 lo requieran.

Pruebas de rendimiento

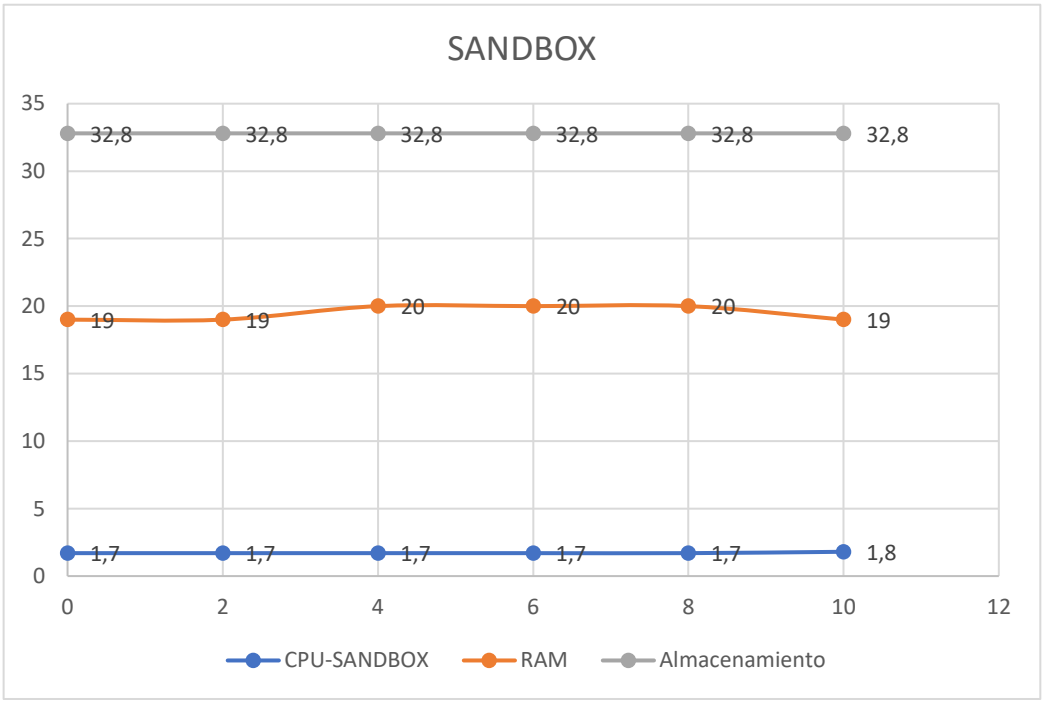


Figura 17. Rendimiento Sandbox
Elaborado por: Mariuxi Márquez y Bryan Ramos

En la Figura 18, se observa que en el Firewall, la RAM en la segunda y tercera muestra presenta un incremento del (0,8%) a las demás muestras. En el CPU si bien se observa que en la segunda muestra existe un incremento del (1%) desde la tercera muestra este valor decrece hasta llegar a su valor habitual (0,8%) en la sexta muestra.

En el almacenamiento se puede observar que desde la tercera muestra su valor incrementa en 0,1% hasta la sexta muestra.

Pruebas de rendimiento

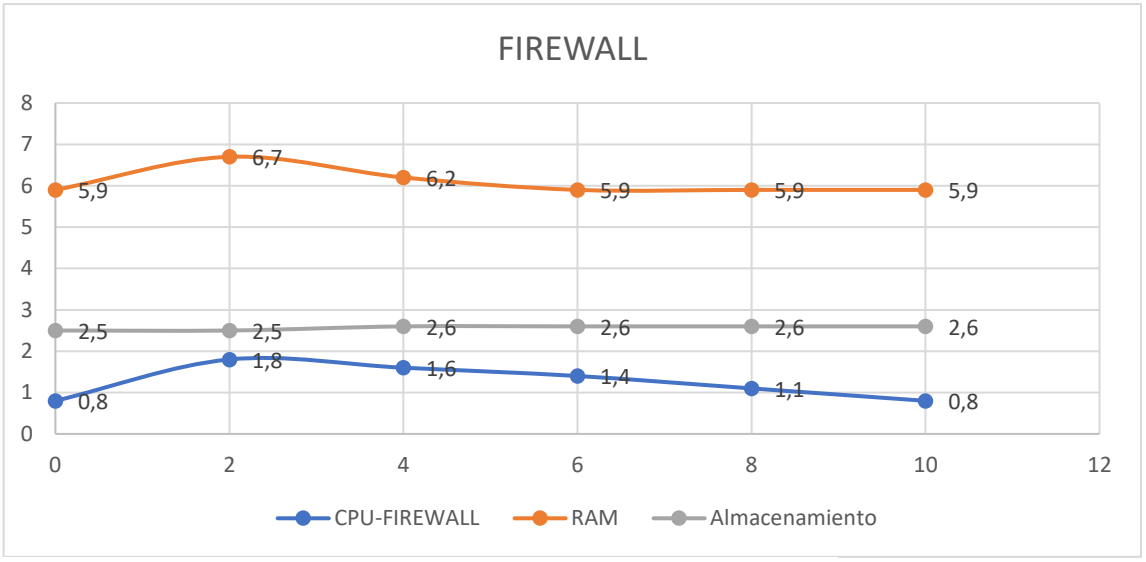


Figura 18. Rendimiento Firewall
Elaborado por: Mariuxi Márquez y Bryan Ramos

En la Figura 19, se observa que en la máquina de monitoreo de la infraestructura, la RAM tiene un incremento (1%) a partir de la cuarta muestra que se mantiene durante las dos muestras posteriores. En el CPU se observa que el valor de consumo incrementa en cada muestra tomada. Finalmente, en el almacenamiento se observa que los datos son constantes durante la captura de las muestras.

Pruebas de rendimiento

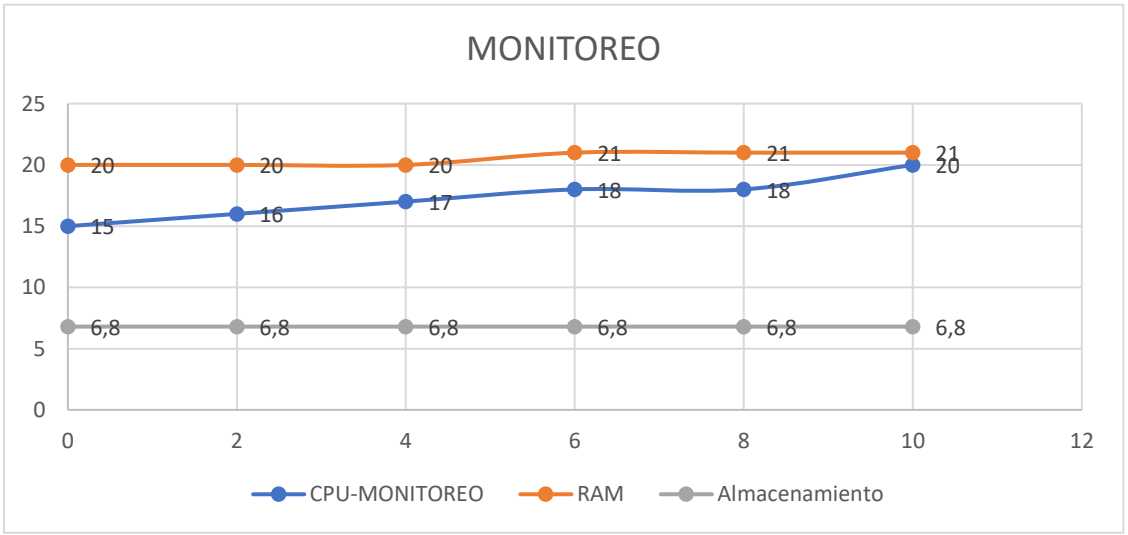


Figura 19. Rendimiento Monitoreo
Elaborado por: Mariuxi Márquez y Bryan Ramos

En la Figura 20, se observa que en la máquina del SIEM, la RAM y el Almacenamiento permanecen constantes en el transcurso de la captura de las muestras. Por otro lado, el rendimiento del CPU muestra una gráfica casi similar a una onda sinusoidal.

Pruebas de rendimiento

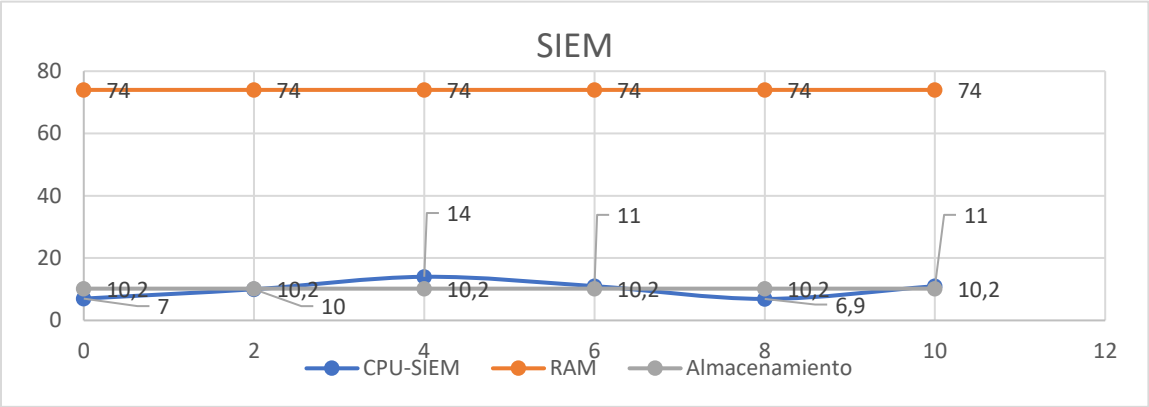


Figura 20. Rendimiento SIEM
Elaborado por: Mariuxi Márquez y Bryan Ramos

En la Figura 21, se observa que en la máquina del antivirus, la RAM presenta un incremento lineal del 1% de la primera a la tercera muestra, y desde la cuarta muestra a la sexta decrece linealmente en 1%. En el CPU se puede observar que su valor de consumo incrementa en cada muestra. Por otro lado, el almacenamiento permanece constante en cada una de las muestras tomadas. En consideración este servidor también proporciona los servicios de: DNS, Active Directory y DHCP.

Pruebas de rendimiento

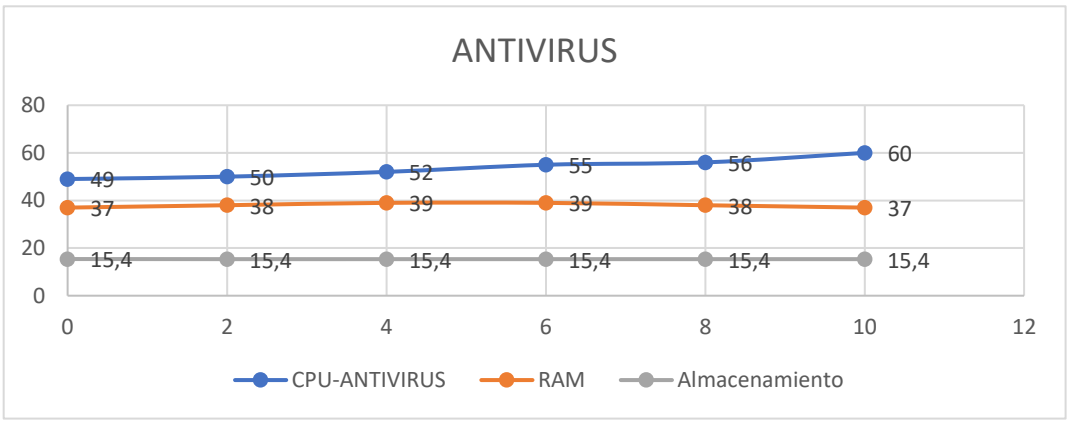


Figura 21. Rendimiento Antivirus
Elaborado por: Mariuxi Márquez y Bryan Ramos

En la Figura 22, se observa que en la máquina del GLPI, la RAM y el almacenamiento no presentan cambios durante la captura de las muestras. En el CPU se observa que, en la última muestra existe un incremento del 0,1% con respecto a los valores previos.

Hay que considerar que este servicio es independiente de los otros servicios, ya que es utilizado para crear tickes, lo cual no representa un consumo significativo de recursos.

Pruebas de rendimiento

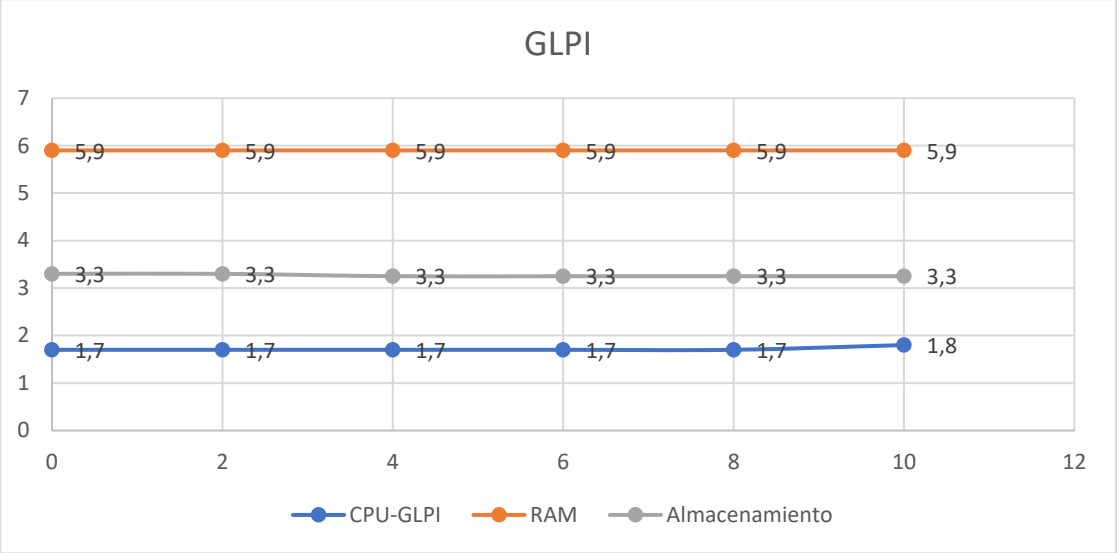


Figura 22. Rendimiento GLPI
Elaborado por: Mariuxi Márquez y Bryan Ramos

En la Figura 23, se puede observar el rendimiento general del prototipo con los datos mencionados en el análisis de rendimiento previo.

En la segunda parte del **¡Error! No se encuentra el origen de la referencia.**, se desglosa el análisis de variación porcentual de las pruebas de rendimiento.

Prebas de rendimiento

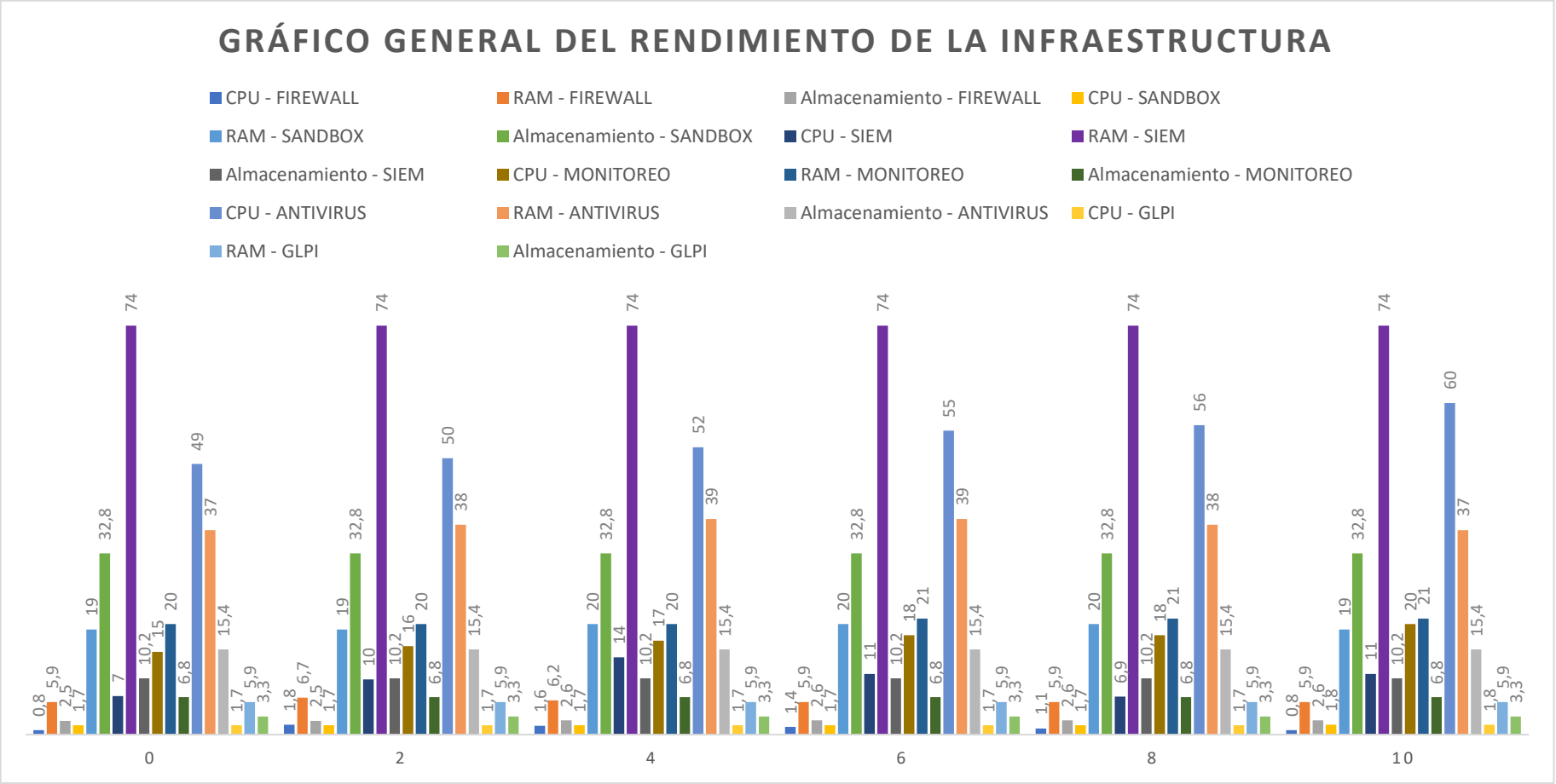


Figura 23. Gráfico General - Pruebas de Rendimiento
Elaborado por: Mariuxi Márquez y Bryan Ramos

En la Figura 24, **¡Error! No se encuentra el origen de la referencia.**se observa como la cantidad de bits enviados por la interfaz LAN es mayor a la cantidad de bits recibidos en cada muestra tomada, ya que el Firewall es quien responde a las consultas realizadas desde la red LAN.

Rendimiento la red

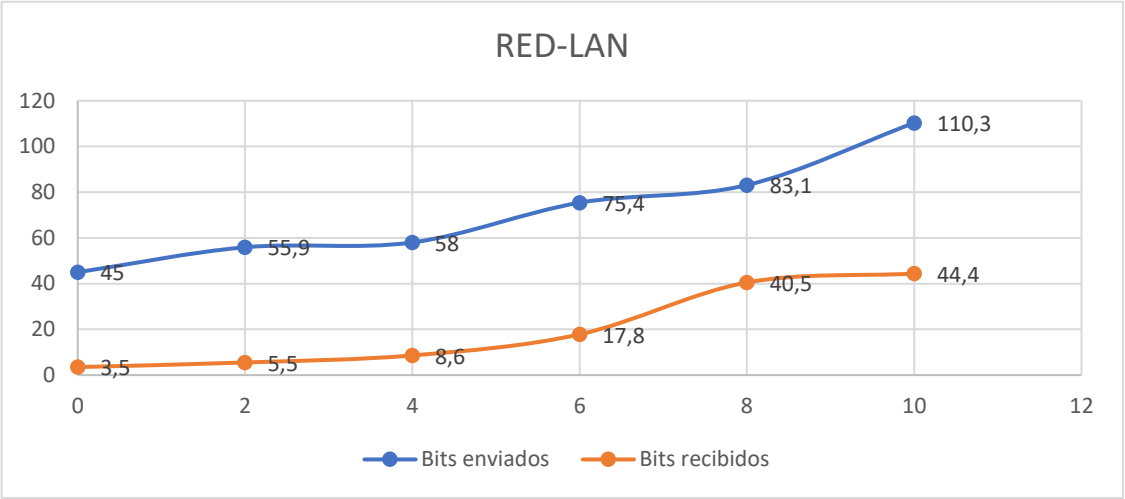


Figura 24. RED - LAN
Elaborado por: Mariuxi Márquez y Bryan Ramos

En la Figura 25, se observa que la cantidad de bits recibidos por la interfaz WAN es mayor a la cantidad de bits enviados en cada muestra tomada, debido a que esta interfaz enruta el tráfico hacia el internet.

Rendimiento la red

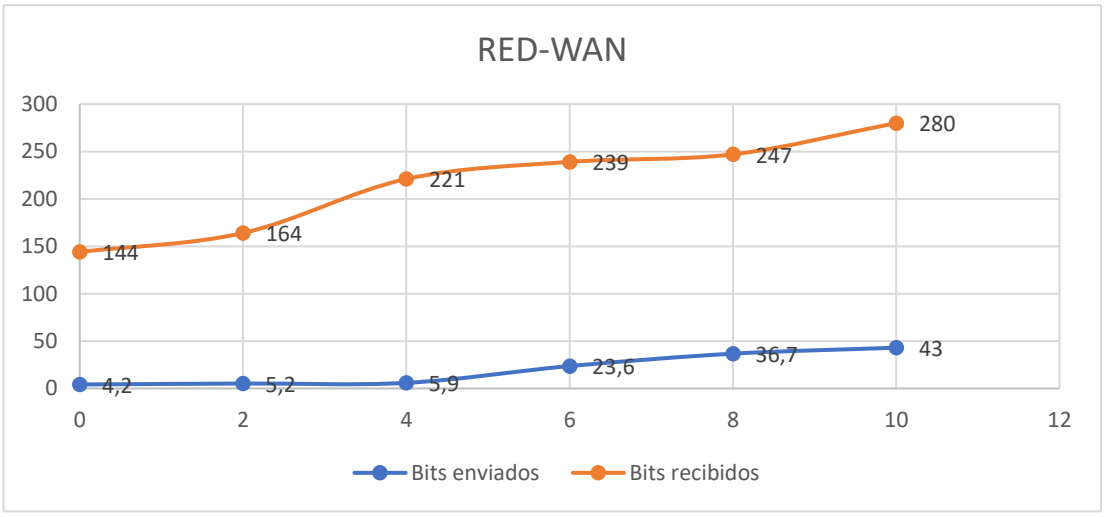


Figura 25. RED - WAN
Elaborado por: Mariuxi Márquez y Bryan Ramos

4.1.3. Prueba de penetración de red

La prueba fue realizada en la red del SOC prototipo. Para eso se ha tomado como referencia el checklist del blog de Gbhackers, que se usa para realizar pruebas de penetración de red (Gurubaran, 2020). En el **¡Error! No se encuentra el origen de la referencia.**, se evidencian los resultados obtenidos.

Los resultados mostraron que, al intentar penetrar la red desde un punto externo está se encuentra protegida por el firewall, el cual al intentar escanear vulnerabilidades no mostró resultados que puedan comprometer a la infraestructura. Por otro lado, desde el punto de vista de un ataque interno, en el análisis se pueden encontrar ciertas vulnerabilidades las cuales Nessus asigna un valor de riesgo, pero es importante analizar el impacto que presentan las vulnerabilidades encontradas para la institución.

La Figura 26, define los procesos para la gestión de vulnerabilidades.

Procesos para la gestión de vulnerabilidades

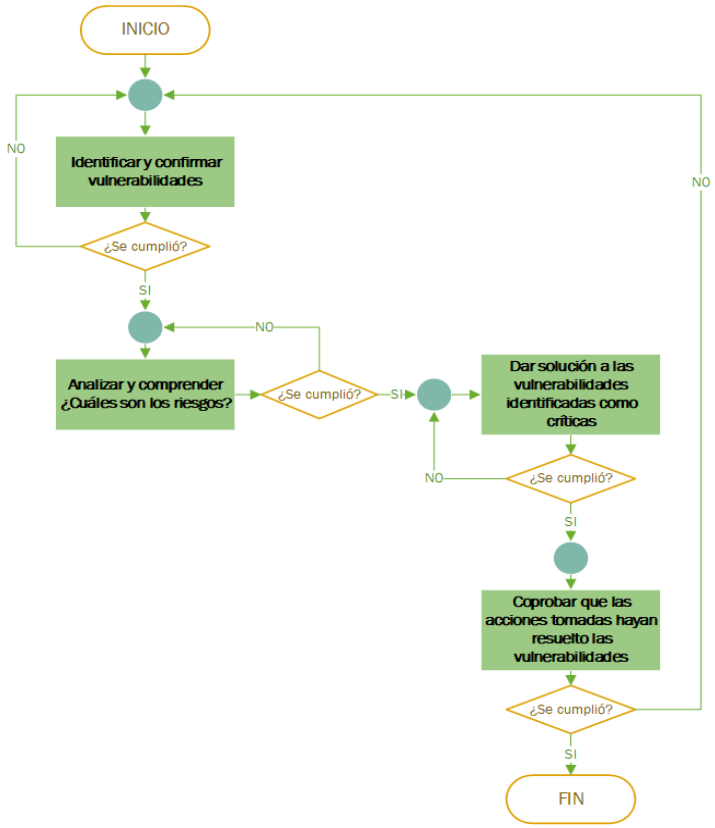


Figura 26. Gestión de Vulnerabilidades
Elaborado por: Mariuxi Márquez y Bryan Ramos

4.2. Análisis Económico

En las siguientes tablas se presentarán los costos que conlleva la implementación, el mantenimiento y la operación del SOC propuesto, considerando que en términos tecnológicos la vigencia del equipamiento de la infraestructura es de tres a cinco años (DELL, 2015).

En la Tabla 16. Costo Capital – SO, se presenta un desglose del costo de la implementación (costos fijos) con un total de **$ 55.700,00** en la Tabla 17, los costos recurrentes anuales (costos variables) con un total de **$ 14.000,00** y por último en la Tabla 18, se observan los costos anuales de nómina (costos variables) con un total de **$ 63.047,28** anual para la operación del SOC (Wilson, 2018)**.**

El costo del primero año tiene un valor de **$ 132.747,28** y a partir del segundo año **$ 77.047,28**. Cabe recalcar, que la suma sin contemplar los valores de los salarios de los empleados está en **$ 69.700,00** para el primer año, y a partir del segundo año un total de **$ 14.000,00**.

Tabla 16. Costo Capital – SOC

COSTO DE LA IMPLEMENTACIÓN			
Tipo	**Unidad**	**Costo Unitario**	**Costo Total**
Costo de implementación y personalización de SIEM.	16 horas	$ 2.400	$ 2.400
Costo de implementación y personalización de servidor de antivirus.	20 horas	$ 3.000	$ 3.000
Costo de implementación y personalización de GLPI.	12 horas	$ 1.800	$ 1.800
Costo de implementación y personalización de Cuckoo Sandbox	8 horas	$1.200	$1.200
Costo de implementación y personalización de Zabbix.	24 horas	$ 3.600	$ 3.600
Costo de implementación y personalización de PfSense	6 horas	$ 900	$ 900

Servidor Hardware con las siguientes especificaciones: -RAM: 32 GB -Almacenamiento: 1.2 TB -Procesadores: 1 con 16 núcleos. -Hypervisor (VMware, Nutanix, Hyper-V)	1	$ 35.000	$ 35.000
Estación de monitoreo consta de: -Dos (2) monitores 55”. -Controlador videowall (2x2). -Dos (2) desktop**.	1	$7.000	$7.000
Una (1) unidad de Rack**	1	$ 800	$ 800
		Total	**$ 55.700**

Nota: Se coloca valores aproximados del costo capital para implementar un SOC.
**Puede ser que se ahorre estos costos porque la UESMA podría contar con esta infraestructura.

Tabla 17. Costos Recurrentes Anuales - SOC

COSTOS RECURRENTES ANUALES	
Tipo	**Costo Total**
Capacitación del personal, actualización de habilidades.	$ 8.000
Fuentes de inteligencia de amenazas (por ejemplo, SNORT, Talos, etc)	$ 3.000
Mantenimiento anual de la solución.	$3.000
Total	**$ 14.000**

Nota: Tabla sobre el costo recurrente anual total.

Tabla 18. Costos Anuales de Nómina del SOC

COSTOS ANUALES DE LA NÓMINA DEL SOC			
Tipo	**Meses**	**Costo Mensual**	**Costo Total**
No. 1 – Analistas	12	$ 937,24	$ 11.246,88
No. 2 – Analistas	12	$ 1.150,11	$ 13.801,32
No. 3 – Analistas	12	$ 1.361,36	$ 16.336,32

Administrador del SOC	12	$ 1.805,23	$ 21.662,76
		Total	**$ 63.047,28**

Nota: Tabla sobre el costo anual de nómina del SOC.
**Los valores presentados se basan en la estimación de SALARIOS MÍNIMOS SECTORIALES 2020 del Ecuador.

Por otro lado, no se realizó un análisis económico basado en TIR, VAN ya que estos parámetros tratan la estimación de los flujos de caja que tenga la institución y la valoración del negocio respectivamente, hay que considerar que el SOC prototipo evitará que la UESMA tenga pérdidas ocasionadas por sanciones o multas.

Por ejemplo, tomando como referencia un escenario en el cual la UESMA sea víctima del robo de registros de una base de datos, la unidad educativa podría ser objeto de una demanda por parte de las personas que hayan sido afectadas como lo indica el artículo 180 del COIP, que conlleva una sanción de cuatro a diez SBU como lo indica el artículo 70. Considerando la sanción más alta de diez SBU y que la cantidad de personas afectadas que demanden a la unidad educativa pertenezcan a un paralelo de aproximadamente cuarenta estudiantes, las pérdidas que representarían rondarían los $ 160.000,00.

Al obtener estos valores se puede apreciar que con la inversión inicial en el prototipo del SOC de $ 132.747,28 la UESMA se podría proteger de estas pérdidas, con lo cual los costos estarían justificados.

Para conocer valores exactos del beneficio económico de contar con herramientas de seguridad, debería realizarse un estudio de análisis de riesgo y un plan de contingencia, lo cual no es parte del objetivo del presente trabajo.

4.3. Análisis Legal

Mediante contacto telefónico con la UESMA se solicitó información acerca del marco legal que maneja la institución para contar con una referencia de las normativas respecto a la

infraestructura de red. Los técnicos de TICS de la UESMA mencionan que el ministerio no exige el cumplimiento de una normativa legal específica en materia de ciberseguridad.

Por ello la investigación se realizó en base a leyes que Ecuador ha publicado referente a los delitos informáticos.

En el Ecuador el Código Orgánico Integral Penal (COIP, 2014) y la Ley Orgánica de Protección de Datos (LOPD, 2019) establecen sanciones para delitos basados en ciberseguridad por ellos en el **¡Error! No se encuentra el origen de la referencia.**, se listan las leyes con las cuales la UESMA se puede respaldar en caso de ser víctima de un delito informático, que podría ser sustentado con el centro de operaciones de seguridad - SOC.

CONCLUSIONES

- La recopilación de datos arrojó que la institución no podía entregar los registros sobre las operaciones del firewall, antivirus o algún otro dispositivo de seguridad, identificando que se necesita la adición de nuevas medidas y políticas de seguridad.
- El análisis de los datos recopilados mostró que su operación de seguridad e infraestructura tecnológica era vulnerable. La institución debe implementar políticas y procesos que resguarden la integridad, confidencialidad y disponibilidad de sus datos e información.
- El objetivo es mejorar el departamento de TICS, afinando los procesos mediante el diseño del SOC prototipo. Por tanto los roles definidos por la SANS fueron adaptados en el diseño para organizar las actividades del personal de TICS en la operación del SOC. Este diseño contempló monitorear las funciones sustantivas de la institución, que cuenta con herramientas de software para mostrar gráficamente aspectos como alertas de seguridad, rendimiento de los dispositivos de la red, análisis y clasificación de amenazas.
- Para comprobar la eficiencia del SOC prototipo se realizaron pruebas en un entorno de simulación VMware, con los resultados obtenidos se confirmó que el SOC aumentaría la seguridad de la infraestructura de la red.
- La prueba de penetración de red realizada al SOC prototipo, mostró que al ejecutar el análisis de vulnerabilidades con Nessus desde un punto externo de la red no encontró vulnerabilidades, por otro lado, al llevar a cabo el mismo análisis desde un punto interno de la red se detectaron vulnerabilidades, a las cuales Nessus analizó, clasificó y asignó valores de criticidad. Al aprovechar una de estas vulnerabilidades se comprobó la eficiencia de las herramientas del SOC, ya que detectaron anomalías y emitieron alertas,

que junto al firewall filtró el tráfico impidiendo que se pueda comprometer la infraestructura de la red.

- La institución educativa no posee un rubro específicamente destinados para la adquisición o implementación de algún sistema de seguridad, por ello se enfocó el diseño con herramientas open source para disminuir los costos del SOC, que se justificarían por los valores que no se pagarían debido a multas causadas por violaciones de seguridad.
- La institución necesita de políticas de seguridad formalmente generadas que junto con la base legal sugerida, tomada del COIP y LOPD, se puede apoyar la UESMA en caso de ser víctima de un ciberdelincuente.

RECOMENDACIONES

- Para mejorar las capacidades de detección del SOC es recomendable contar con suscripciones a servicios de fuentes de inteligencia de amenazas.
- Se recomienda que se cree un cronograma para el escaneo de vulnerabilidades en la infraestructura ya que con el cambio constante de los sistemas se pueden presentar una mayor cantidad de estas.
- Se sugiere a partir de las diferentes estadísticas de rendimiento realizar pruebas y estudios para redimensionar el SOC.
- Se aconseja analizar la viabilidad de implementar el SOC dentro de la institución o solo rentar los servicios que ofrecen terceros cubriendo los procesos que propone un diseño del SOC.
- Es recomendable que la institución cuente con un plan de gestión de riesgo, contingencia y normativa de seguridad.
- Se aconseja llevar a cabo investigaciones más profundas de las capacidades de las aplicaciones, para aprovechar todas las características con las que cuentan.
- Se recomienda contar con guías importantes para tomar medidas adecuadas en el diseño de soluciones de seguridad, como las de las SANS que es una organización dedicada a la seguridad de red.
- Se sugiere tomar en cuenta para una posible implementación la complejidad del acoplamiento de las herramientas open source para que trabajen en conjunto con las demás herramientas.
- Es recomendable que la institución genere y comunique las políticas de seguridad que se deben aplicar a todos los sistemas de información.

LISTA DE REFERENCIAS

Netgate Docs. (2018). *IDS / IPS Configuración previa de la configuración automática de WPAD para el paquete Squid.* Obtenido de https://docs.netgate.com/pfsense/en/latest/ids-ips/index.html

Acosta, D. (16 de septiembre de 2014). *Sistemas de detección/prevención de intrusiones (IDS/IPS).* Obtenido de Controles Técnicos de PCI DSS parte V: https://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-v-sistemas-de-deteccionprevencion-de-intrusiones-idsips/

Anchundia, S. R. (2000). *Manual técnico de redes.* Esmeraldas,Ecuador.

Ariganello, E. (20154). *Guía de estudio para la certificación CCNA Security.* Obtenido de Redes CISCO: https://books.google.com.ec/books?id=kI2fDwAAQBAJ&pg=PA194&lpg=PA194&dq=%EF%82%A7+Firewall+basado+en+host+(servidor+y+personal):+una+computadora+o+servidor+que+ejecuta+software+de+firewall.&source=bl&ots=Jp7R39MyAr&sig=ACfU3U3XUT4FlJDA7QT2HvShzzntqUa5uA&h

Avila, F. (24 de enero de 2020). *Análisis de malware automatizado.* Obtenido de http://www.disoftin.com/2020/01/analisis-de-malware-automatizado.html

Banka, L. (2017). *IT Risks Report.*

Barboza, G. (11 de mayo de 2018). *CentOS vs Ubuntu: ¿Cuál elegir para tu servidor web?* Obtenido de https://www.hostinger.es/tutoriales/centos-vs-ubuntu-elegir-servidor-web/

Barrios, L. (15 de noviembre de 2018). *¿Qué es Windows Server Update Services (wsus) y Cómo lo uso?* Obtenido de https://luisiblogdeinformatica.com/que-es-windows-server-update-services-wsus-y-como-usar/

Bashay, F. (2 de febrero de 2018). *WHAT IS THE CIA TRIANGLE AND WHY IS IT IMPORTANT FOR CYBERSECURITY MANAGEMENT?* Obtenido de https://www.difenda.com/blog/what-is-the-cia-triangle-and-why-is-it-important-for-cybersecurity-management

Beal, V. (2016). *Snort.* Obtenido de https://www.webopedia.com/TERM/S/Snort.html

Bogotá, A. (04 de septiembre de 2018). *Servidores Dedicados Windows Server 2016 – Características y Versiones.* Obtenido de https://www.internetya.co/servidores-windows-server-2016-caracteristicas-y-versiones/

Bonilla Blanco, B. M., & Rojas, A. (s.f.). *DISEÑO Y PLANIFICACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD INFORMÁTICA APLICADO COMO SERVICIO POR LA ORGANIZACIÓN A3SEC BAJO MARCOS DE TRABAJO PROPUESTOS POR SANS, ISACA Y NIST.* Obtenido de FACULTAD DE INGENIERIA: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/5814/00005153.pdf?sequence=1

Borges, S. (4 de enero de 2019). *Servidor Web.* Obtenido de https://blog.infranetworking.com/servidor-web/#Que_es_un_servidor_web

Brighttalk. (2018). *McAfee ePolicy Orchestrator (ePO).* Obtenido de https://www.brighttalk.com/webcast/9671/119275/conectar-administrar-automatizar-mcafee-epolicy-orchestrator-epo

Capgemini. (2017). *Centro de operaciones de seguridad.* Obtenido de Casi todas las organizaciones experimentarán una violación de seguridad de datos este año. Lo que marca la diferencia es

cómo respondes.: https://www.capgemini.com/service/cybersecurity-services/security-operations-center/

CEDIA. (2018). *CSIRT.* Obtenido de Equipo de respuesta a incidentes de seguridad.: https://www.cedia.edu.ec/es/servicios/tecnologia/infraestructura/csirt

Certmike. (2017-2019). *Confidentiality, Integrity And Availability – The CIA Triad.* Obtenido de https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/

Chia, T. (20 de agosto de 2012). *Confidentiality, Integrity, Availability: The three components of the CIA Triad.* Obtenido de https://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

CIA Triad. (2019). *What is the CIA Triad?* Obtenido de The CIA triad defined, explained, and explored: https://www.forcepoint.com/cyber-edu/cia-triad

CIC. (12 de abril de 2016). *W6 – Inteligencia operacional – ELK.* Obtenido de https://www.cic.es/w6-inteligencia-operacional-elk/

CISCO. (2019). *CCNA Cybersecurity Operations.* Obtenido de CyberOps: https://static-course-assets.s3.amazonaws.com/CyberOps11/es/index.html#0.0.1.1

Cisco. (2020). *What Is a Firewall?* Obtenido de https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Ciso. (15 de agosto de 2018). *Ciso.* Obtenido de ¡NOC, SOC, CSIRT,CERT no es lo mismo!: https://www.blogdelciso.com/2018/08/15/noc-soc-csirtcert-no-es-lo-mismo/

COIP. (2014). *Código Orgánico Integral Penal.* Obtenido de Ministerio de Justicia, Derechos Humanos y Cultos Subsecretaría de Desarrollo Normativo: https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_con_judi_c%C3%B3d_org_int_pen.pdf

Computer Hope. (17 de octubre de 2017). *VMware.* Obtenido de https://www.computerhope.com/jargon/v/vmware.htm

ComputerPro. (20 de octubre de 2017). *Security Operations Center, ¿cuándo es una buena opción?* Obtenido de https://www.muycomputerpro.com/2017/10/20/security-operations-center-opcion

Consejo de Educacion Superior. (2016). *ESTATUTO ORGÁNICO POR PROCESOS DEL CONSEJO DE EDUCACIÓN SUPERIOR.* Obtenido de RPC-SO-21-No.3 35-2016 : http://www.ces.gob.ec/doc/historico_LOTAIP/Estatuto/ESTATUTO%20ORG%C3%81NICO%20POR%20PROCESOS%20DEL%20CONSEJO%20DE%20EDUCACI%C3%93N%20SUPERIOR.pdf

Coopers, P. W. (2015). *The Global State of Information Security® SurveY.*

Crespo, A. (17 de enero de 2017). *DMZ: qué es, para qué sirve y cómo utilizarlo.* Obtenido de https://www.redeszone.net/2017/01/17/dmz-routers-descubre-mejor-forma-utilizacion/

Cuckoo Sandbox. (2014-2019). *What is Cuckoo?* Obtenido de https://cuckoosandbox.org/

CuckooInstalling. (2010-2018). *Installing Cuckoo.* Obtenido de Edit on GitHub: https://cuckoo.readthedocs.io/en/latest/installation/host/installation/

CuckooRequirements. (2010-2018). *Requirements - Cuckoo.* Obtenido de Edit on GitHub: https://cuckoo.readthedocs.io/en/latest/installation/host/requirements/

Delgado, D. O. (21 de marzo de 2017). *Qué es Snort: Primeros pasos.* Obtenido de https://openwebinars.net/blog/que-es-snort/

DELL. (03 de marzo de 2015). *Vida útil hardware.* Obtenido de https://www.dell.com/community/Pc-de-Escritorio-General/Vida-util/td-p/5295179

Deloitte Ecuador. (2017). *Seguridad de la Información.* Obtenido de https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/deloitte-analytics/Estudios/SeguridadInformacion2017.pdf

Denning, D. E. (2012). *Stuxnet: What Has Changed?* Obtenido de USA:Department of Defense Analysis, Naval Postgraduate School: https://www.mdpi.com/1999-5903/4/3/672

El Telégrafo. (24 de abril de 2019). *12 ataques por segundo se registran en Ecuador.* Obtenido de https://www.eltelegrafo.com.ec/noticias/judicial/12/delitosinformaticos-coip-policia-fiscalia

Elastic. (2019). *¿Qué es el ELK Stack?* Obtenido de https://www.elastic.co/es/what-is/elk-stack

Elastic. (2019). *El corazón del Elastic Stack.* Obtenido de https://www.elastic.co/es/elasticsearch

Emanuelli A, P., Milla A, F., Sepúlveda M, R., & Torrealba M, J. A. (s.f.). *Documentos.* Obtenido de Hoja de ruta para la implementación de proyectos: http://www.reddccadgiz.org/documentos/doc_843564181.pdf

ESET. (2015). *CSIRT .* Obtenido de https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Fernández, B. (23 de agosto de 2017). *Pasos a seguir ante un ataque informático.* Obtenido de https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

Férnandez, R. P. (04 de julio de 2019). *Configuración de ACLs con Packet Tracer.* Obtenido de https://www.raulprietofernandez.net/blog/packet-tracer/configuracion-de-acls-con-packet-tracer

Flores, A. G. (2017). *Historia - ANTECEDENTE CONTEXTUAL.* Obtenido de Unidad Educativa Fiscomisional "María Auxiliadora" Esmeraldas: http://mauxiliadora92.blogspot.com/p/historia.html

Florez, F. H. (2018). *Curso Profesional de Endian Firewall Community (Español).* Obtenido de https://www.udemy.com/course/curso-de-endian-firewall/

frebsd. (2019). *FreeBSD.* Obtenido de https://www.freebsd.org/es/

freeBSD. (03 de marzo de 2014). *FreeBSD.* Obtenido de https://www.freebsd.org/es/

García, V. (23 de abril de 2019). *Monitorización de aplicaciones usando ELK Stack.* Obtenido de https://www.enimbos.com/blog/monitorizacion-de-aplicaciones-usando-elk-stack/

Garzón, A. (2017). *Security Operations Center.* Obtenido de https://www.muycomputerpro.com/2017/10/20/security-operations-center-opcion

GLPI. (2015). *Gestión de TI.* Obtenido de https://glpi-project.org/

GLPI Network. (2017). *¿QUÉ ES LA RED GLPI?* Obtenido de https://www.teclib-edition.com/en/teclib-products/glpi-network-itsm/

Gómez, V. (27 de noviembre de 2019). *¿Qué es SpiceWorks?* Obtenido de https://instintobinario.com/spiceworks/

Gray, C. (diciembre de 2014). *8 Ways to Defend Higher Education against Cyberattacks.*

Gray, C. (8 de diciembre de 2014). *Ocho maneras de defender la educación superior contra los ciberataques.* Obtenido de https://er.educause.edu/articles/2014/12/8-ways-to-defend-higher-education-against-cyberattacks

Gurubaran. (24 de febrero de 2020). *Most Important Network Penetration Testing Checklist.* Obtenido de https://gbhackers.com/network-penetration-testing-checklist-examples/

HelpSystems. (27 de mayo de 2020). *¿Qué es un SIEM?* Obtenido de https://www.helpsystems.com/es/blog/que-es-un-siem

HostingPedia. (02 de junio de 2017). *CentOS Linux.* Obtenido de https://hostingpedia.net/centos-linux.html

INCIBE. (20 de marzo de 2017). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* Obtenido de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Infoblox. (2018). *What is a DHCP Server?* Obtenido de https://www.infoblox.com/glossary/dhcp-server/

Innovablack. (2019). *FIREWALL PFSENSE.* Obtenido de https://www.innovablack.com/firewall/

Ionos. (39 de noviembre de 2019). *El DHCP y la configuración de redes.* Obtenido de https://www.ionos.es/digitalguide/servidores/configuracion/que-es-el-dhcp-y-como-funciona/

Joan, A. O. (2013-2014). *Diseño de una Red Coorporativa.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28625/6/aobisTFC0114memoria.pdf

Kalsin, V. (13 de noviembre de 2016). *Cómo instalar y configurar Grafana para trazar hermosos gráficos de Zabbix en CentOS 7.* Obtenido de https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-grafana-to-plot-beautiful-graphs-from-zabbix-on-centos-7

Kear, S. (16 de enero de 2018). *¿Qué es pfSense?* Obtenido de https://turbofuture.com/computers/Introduction-to-pfSense-An-Open-Source-Firewall-and-Router-Platform

Kumar, R. (10 de septiembre de 2019). *How to Install Zabbix Agent on CentOS/RHEL 7/6.* Obtenido de https://tecadmin.net/install-zabbix-agent-on-centos-rhel/

Linux Zone. (2016). *Ubuntu.* Obtenido de Descripción de Ubuntu, descarga, características de Ubuntu: https://linuxzone.es/distribuciones-principales/ubuntu/

Linuxize. (28 de enero de 2018). *How to Install and Configure Zabbix on CentOS 7.* Obtenido de https://linuxize.com/post/how-to-install-and-configure-zabbix-on-centos-7/

Linuxize. (28 de junio de 2018). *How to Install and Configure Zabbix on CentOS 7.* Obtenido de https://linuxize.com/post/how-to-install-and-configure-zabbix-on-centos-7/

LOPD. (19 de septiembre de 2019). *Proyecto de la Ley Orgánica de Ptotección de Datos Personales.* Obtenido de https://www.nmslaw.com.ec/wp-content/uploads/2019/09/Proyecto-de-Ley-Org%C3%A1nica-de-Protecci%C3%B3n-de-Datos-Personales.pdf

Losada, S. (30 de julio de 2018). *¿QUÉ ES ELK? ElasticSearch, Logstash y Kibana.* Obtenido de https://openwebinars.net/blog/que-es-elk-elasticsearch-logstash-y-kibana/

Lubna, A., Baber, A., & Umar, K. (2015). *Security Operations Center – A Need for an Academic Environment.* doi:10.1109/WSCNIS.2015.7368297

Magoni, V. (27 de enero de 2016). *Gestión de puntos de acceso UniFi: Controller UniFi o Tanaza?* Obtenido de https://www.tanaza.com/es/blog/gestion-de-puntos-de-acceso-unifi-controller-unifi-o-tanaza/

Mcafee. (2019). *McAfee ePolicy Orchestrator.* Obtenido de https://www.mcafee.com/enterprise/en-us/products/epolicy-orchestrator.html

Medina, R. G. (29 de enero de 2018). *¿Qué es Benchmarking y para qué sirve?* Obtenido de https://www.cubica.co/marketing-digital/que-es-benchmarking-y-para-que-sirve/

Mendoza, M. Á. (28 de mayo de 2015). *¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?* Obtenido de https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

Microsoft. (21 de mayo de 2017). *Windows Server Update Services (WSUS).* Obtenido de https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

Microsoft. (2020). *Windows Server.* Obtenido de https://www.microsoft.com/es-xl/licensing/product-licensing/windows-server-2016

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (15 de abril de 2019). *Más de 40 millones de ataques al Ecuador neutralizados desde el retiro del asilo a Julian Assange.* Obtenido de https://www.telecomunicaciones.gob.ec/mas-de-40-millones-de-ataques-al-ecuador-neutralizados-desde-el-retiro-del-asilo-a-julian-assange/

Moloch . (2019). *Moloch - Full Packet Capture.* Obtenido de https://molo.ch/

Montero, R. S. (2016). *Plan de negocios para la creación de una empresa que oferte servicios de monitoreo de incidentes informáticos llamado SOC (Security Operation Center) para instituciones financieras en la ciudad de quito.* Obtenido de http://dspace.udla.edu.ec/bitstream/33000/5809/1/UDLA-EC-TIC-2016-78.pdf

Muniz, J. M. (2015). *Security Operations Center.* Obtenido de Building, Operating, and Maintaining Your SOC. Cisco Press.: https://ieeexplore.ieee.org/abstract/document/7368297

Mutai, J. (16 de octubre de 2019). *How To Install GLPI on Ubuntu 18.04 LTS.* Obtenido de https://computingforgeeks.com/how-to-install-glpi-on-ubuntu-18-04-lts/?fbclid=IwAR30Mjad1CLbRuvyZmNmplVcjeid2QsILUPr1tSQfPFfqzpaAVmd2UXD1ac

N. H. Ab Rahman, K. K. (2015). *A survey of information security incident handling in the cloud.* Obtenido de Comput. Secur., vol. 49: https://ieeexplore.ieee.org/abstract/document/8440963/references#references

Networkworld. (18 de octubre de 2017). *¿Qué es un firewall?* Obtenido de https://www.networkworld.es/seguridad/que-es-un-firewall

Nube Digital. (2016). *Qué es VMware?* Obtenido de https://nubedigital.co/clientes/knowledgebase/58/Que-es-VMware.html

Ochoa, K. (2018). *MANUAL DE USUARIO SISTEMA GLPI.* Obtenido de Dirección de Tecnologías y Comunicación: https://www.finanzas.gob.ec/wp-content/uploads/downloads/2014/02/Manual-Usuario-final-v2-GLPI.pdf

OCS inventory. (2001). *About OCS inventory.* Obtenido de https://ocsinventory-ng.org/?lang=en

Open Source Guide. (04 de diciembre de 2017). Obtenido de http://www.open-source-guide.com/en/Solutions/Infrastructure/It-asset-and-inventory-management/Glpi

OSI. (11 de octubre de 2016). *Malware. Cuál es su objetivo y cómo nos infecta.* Obtenido de https://www.osi.es/es/actualidad/blog/2016/10/11/malware-cual-es-su-objetivo-y-como-nos-infecta

Ostec. (2018). *Jun Pentest: ¿qué es y cuáles son los principales tipos?* Obtenido de https://ostec.blog/es/seguridad-perimetral/pentest-concepto-tipos

P. Jacobs, A. A. (2013). *Classification of security operation centers.* Obtenido de nf Secur. South Africa-Proc. ISSA 2013 Conf. 2013.: https://ieeexplore.ieee.org/abstract/document/6641054

Paessler. (2020). *How to monitor your VMware vSphere environment.* Obtenido de https://www.paessler.com/support/how-to/vmware?utm_source=google&utm_medium=cpc&utm_campaign=ROW_EN_DSA_website_Categories&utm_adgroup=virtual%20machine&utm_adnum=dsa_en_03&utm_campaignid=608925097&utm_adgroupid=28376614365&utm_targetid=dsa-153941441778&u

Pérez, J. (7 de agosto de 2018). *ELK Stack: ¿Qué es y cómo implementarlo fácilmente mediante DOCKER?* Obtenido de https://www.avantica.net/es/blog/elk-stack-implementacion-facil-con-docker

Petters, J. (19 de enero de 2019). *What is a Proxy Server and How Does it Work?* Obtenido de https://www.varonis.com/blog/what-is-a-proxy-server/

pfSense. (2017). *pfSense®: caracteristicas y notas de las ultimas versiónes.* Obtenido de http://www.firewallhardware.es/pfsense.html

Pratt, M. (28 de noviembre de 2017). *What is SIEM software? How it works and how to choose the right tool.* Obtenido de https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html

QUASAR. (25 de septiembre de 2014). *¿QUÉ ES ENDIAN?* Obtenido de https://quasarbi.com/endian.html

Ramiro, R. (20 de enero de 2018). *25 Tipos de ataques informáticos y cómo prevenirlos.* Obtenido de https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Reyes, C. (30 de mayo de 2012). *ENDIAN FIREWALL CONFIGURACION Y ADMINISTRACION*. Obtenido de http://donjuanblogo.blogspot.com/2012/05/endian-firewall-configuracion-y.html

Rodríguez, A. (18 de enero de 2016). *Trustdimension.* Obtenido de La importancia de la Seguridad Informática: https://www.trustdimension.com/la-importancia-de-la-seguridad-informatica/

Samaniego, C. (13 de noviembre de 2013). *El valor de la gestión de datos.* Obtenido de Qué se entiende por integridad de los datos: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/348870/qu-se-entiende-por-integridad-de-los-datos

Sandbox Security. (2018). *Sandbox Security Defined.* Obtenido de https://www.forcepoint.com/cyber-edu/sandbox-security

SANS Institute. (17 de septiembre de 2014). *SANS Institute, Information Security Reading Room.* Obtenido de https://www.sans.org/reading-room/whitepapers/ICS/security-operations-centre-soc-utility-organization-35502

SANS™ Institute. (2000 - 2019). *SANS Institute: About*. Obtenido de SANS: https://www.sans.org/about/

SOFECOM. (14 de mayo de 2018). *SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran.* Obtenido de https://sofecom.com/que-es-un-siem/

Speedcheck. (2017). *DHCP.* Obtenido de https://www.speedcheck.org/es/wiki/dhcp/

Stroud, F. (2018). *VMware vSphere.* Obtenido de https://www.webopedia.com/TERM/V/vmware-vsphere.html

Symantec Corporation. (1995-2019). *Norton*. Obtenido de Symantec: https://us.norton.com/online-threats/glossary/i/ips-intrusion-prevention-system.html

Symantec Corporation. (1995-2019). *Norton*. Obtenido de Symantec: https://us.norton.com/online-threats/glossary/i/ids-intrusion-detection-system.html

Taylor, C. (2018). *INCIDENT RESPONSE PLAYBOOK CREATION.* Obtenido de https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1559689083.pdf

Technology Institute SANS . (febrero de 27 de 2020). *SANS 2017 Security Operations Center Survey.* Obtenido de Incident Handling: https://www.sans.org/reading-room/whitepapers/incident/paper/37785

Techterms. (08 de julio de 2016). *Sandboxing Definition.* Obtenido de https://techterms.com/definition/sandboxing

Teclib. (2019). *¿QUÉ ES GLPI NETWORK?* Obtenido de https://www.teclib-edition.com/es/productos-teclib/glpi-network-itsm/

Telefónica. (20 de septiembre de 2018). *Ecuador: Telefónica presentó su Centro de Operaciones de Seguridad (SOC).* Obtenido de https://www.computerworld.com.ec/actualidad/tendencias/1415-telefonica-presento-su-centro-de-operaciones-de-seguridad-soc.html

Ubiquiti Networks. (2016). *UniFi Controller User Guide.* Obtenido de https://dl.ubnt.com/guides/UniFi/UniFi_Controller_V3_UG.pdf

UESMAE. (08 de marzo de 2019). *UESMAE*. Obtenido de Quiénes Somos: http://www.uesmae.edu.ec/sdb1/index.php

Velasco, R. (08 de noviembre de 2014). *Analiza el tráfico de una red desde la web con Moloch.* Obtenido de https://www.redeszone.net/2014/11/08/analiza-el-trafico-de-una-red-desde-la-web-con-moloch/

Walkowski, D. (09 de julio de 2019). *What Is The CIA Triad?* Obtenido de Understanding the significance of the three foundational information security principles.: https://www.f5.com/labs/articles/education/what-is-the-cia-triad

Wilson, M. (27 de diciembre de 2018). *The True Cost of a Security Operations Center (SOC).* Obtenido de https://www.btbsecurity.com/mindshare/blog/component/k2/item/82-the-true-cost-of-a-security-operations-center-soc

Wireshark. (2019). *About Wireshark.* Obtenido de https://www.wireshark.org/

Yunda, L. F. (08 de febrero de 2016). *RIESGOS INFORMATICOS.* Obtenido de https://es.calameo.com/books/002949916549b9d86a30e

Zabbix. (2001-2020). *Programa de Entrenamiento Profesional Zabbix.* Obtenido de https://www.zabbix.com/

Zobnin, A. (20 de abril de 2020). *Plugin Zabbix para Grafana.* Obtenido de https://grafana.com/grafana/plugins/alexanderzobnin-zabbix-app

ANEXOS

- Entrevista departamento de TICS – **¡Error! No se encuentra el origen de la referencia.**
- Dashboard de las aplicaciones del SOC – **¡Error! No se encuentra el origen de la referencia.**
- Rendimiento del SOC – **¡Error! No se encuentra el origen de la referencia.**
- Prueba de Pentesting – **¡Error! No se encuentra el origen de la referencia.**
- Marco Legal – **¡Error! No se encuentra el origen de la referencia.**

Para revisar los anexos de este trabajo, por favor diríjase al CD.