FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE TECNOLOGÍAS DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD PARA UN PROVEEDOR DE SERVICIOS DE INTERNET

AUTORES

Oscar Santiago Figueroa Alemán

Valeria Estefanía Masache Narváez

AÑO

2018

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE TECNOLOGÍAS DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD PARA UN PROVEEDOR DE SERVICIOS DE INTERNET

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingenieros en redes y telecomunicaciones

Profesor Guía

Mg. William Eduardo Villegas Chiliquinga

Autores

Oscar Santiago Figueroa Alemán

Valeria Estefanía Masache Narváez

Año

2018

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo, Análisis de tecnologías de un centro de operaciones de ciberseguridad para un proveedor de servicios de internet, a través de reuniones periódicas con los estudiantes, Oscar Santiago Figueroa Alemán y Valeria Estefanía Masache Narváez, en el semestre 2018-2, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

William Eduardo Villegas Chiliquinga

Magister en Redes de Comunicaciones

CI: 1715338263

DECLARACIÓN DEL PROFESOR CORRECTOR

Declaro haber revisado este trabajo, Análisis de tecnologías de un centro de operaciones de ciberseguridad para un proveedor de servicios de internet, de Oscar Santiago Figueroa Alemán y Valeria Estefanía Masache Narváez, en el semestre 2018-2, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

Carlos Marcelo Molina Colcha

Magister en Gestión de las Comunicaciones y Tecnologías de la Información

C.I. 1709624215

DECLARACIÓN DE AUTORÍA DE LOS ESTUDIANTES

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

Oscar Santiago Figueroa Alemán	Valeria Estefanía Masache Narváez
CI: 1715900302	CI: 1725438210

AGRADECIMIENTOS

En primer lugar, agradezco a Dios quien me ha acompañado en cada instante de mi vida, a mis padres Gonzalo y Piedad quienes me apoyaron en todo momento para continuar con mi carrera.

Agradezco a mi familia y amigos quienes siempre creyeron en mí a pesar de todos los obstáculos y a mi novio Santiago quien fue mi pilar y mi fuerza cuando los momentos se pusieron difíciles, gracias por tu paciencia y tu amor.

Valeria

AGRADECIMIENTOS

A mis compañeros y maestros que cada día me enseñaron algo nuevo, a toda mi familia por sus sabios consejos y el apoyo incondicional que me han brindado en el transcurso de toda mi carrera.

A mi madre Blanca que ella siempre creyó en mí para hacer este sueño realidad y a todas las personas que estuvieron siempre apoyándome y terminar mis estudios.

Oscar

DEDICATORIA

Esta tesis se la dedico a mi hermano Oscar de quien espero ver también un hombre profesional y luchador y especialmente esta tesis me la dedico a mí ya que pude demostrarme que con esfuerzo puedo lograr todo lo que me proponga.

Valeria

DEDICATORIA

Dedico este proyecto con profundo amor y gratitud a Dios que me dio la vida y que nunca me ha desamparado, a mi principal fuente de inspiración mi esposa y mi hijo Verónica y Joel, a mi madre Blanca Alemán, que han depositado en mí la confianza y el impulso para conseguir mis sueños y a toda mi familia que de una u otra manera siempre me estuvieron apoyando.

A mis supervisores en donde trabajo ya que ellos me ayudaron para poder seguir estudiando.

Oscar

RESUMEN

El presente proyecto tiene como objetivo ser una guía para los proveedores de servicios de internet acerca de las tecnologías que se utilizarán en el diseño y la implementación de un CSOC (Centro de operaciones de ciberseguridad), adicional se realizará una simulación del mismo dentro del data center experimental de la Universidad De Las Américas utilizando máquinas virtuales con sistemas de software libre.

Para la realización de este trabajo, el mismo se ha seccionado en cuatro partes, de manera introductoria se describen los conceptos principales de la ciberseguridad, así como sus elementos y estándares necesarios para la implementación del CSOC.

El capítulo dos presenta una propuesta de diseño del SOC donde se indica todo lo necesario para la implementación del centro; la arquitectura sugerida y las marcas de equipos que en la actualidad son líderes según el cuadrante mágico de Gartner, adicionalmente se indican los recursos humanos necesarios y todos los procesos que se deben seguir según el estándar ISO 27001.

El tercer capítulo aplica los conceptos de vulnerabilidades y ethical hacking donde se evidencia un caso práctico realizado en el data center experimental de la UDLA.

El cuarto capítulo muestra las pruebas realizadas dentro del data center y como se dio su funcionamiento; adicional ciertas observaciones acerca de los sistemas utilizados.

Para finalizar se presentan las conclusiones y recomendaciones que se obtuvieron de este trabajo.

ABSTRACT

The following project aims to be a guide for internet service providers about the technologies that will be used in the design and implementation of a CSOC (cybersecurity operations center), an additional simulation will be performed within the experimental data center of De Las Américas University using virtual machines with free software systems.

In order to carry out this work, it is divided into four sections, in an introductory way, the main concepts of cybersecurity are described, as well as their elements and necessary standards for the CSOC implementation.

Chapter two presents a SOC design proposal where everything necessary for the implementation of the center is indicated; the suggested architecture and the equipment brands that are currently leaders according to Gartner's magic quadrant, the necessary human resources and all the processes that must be followed according to the ISO 27001 standard are indicated.

The third chapter applies the concepts of vulnerabilities and ethical hacking where a practical case made in the experimental data center of the UDLA is evidenced.

The fourth chapter evidences the tests carried out within the data center and how it was run; additional certain observations about the systems used.

Finally, the conclusions and recommendations that were drawn from this work are presented.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Antecedentes

Hace aproximadamente 40 años la tecnología trajo consigo un concepto de seguridad informática, 15 años después se transformó en seguridad de la información; en la actualidad se comenzó a hablar de la ciberseguridad debido a que el objetivo no solo es proteger la información sino la infraestructura tecnológica. (Gómez, 2013)

El proceso de la digitalización de la economía y el avance de nuevas tendencias tecnológicas han hecho que la variedad de ciber amenazas sean cada vez más grandes, esto con el paso del tiempo influyó en la manera en que las organizaciones operan en donde sus actividades se fueron desarrollando cada vez más en el ciberespacio; las amenazas que comúnmente eran conocidas como virus, gusanos y troyanos evolucionaron y ahora se conocen como ataques de denegación de servicio, malware hasta el uso de técnicas como el phishing. (Instituto de auditores internos de España, 2016, pág. 7)

Por lo anotado anteriormente; las empresas hoy en día se ven frente a un nuevo reto que es imprescindible que se gestione, ya que, según el último informe global del foro económico mundial, los riesgos en la ciberseguridad van en aumento. “Los ataques en contra de empresas casi se han duplicado en cinco años (…). El impacto financiero de toda violación contra la ciberseguridad va en aumento y dan cuenta de algunos de los costos más elevados en 2017 referentes con relación a ataques con ransomware” (Foro Económico Mundial, 2018)

Para poder ofrecer un grado mínimo de disponibilidad y alarmas tempranas dentro de una empresa, se debe contar con una infraestructura de supervisión y monitorización, el Ciber Security Operation Center (CSOC) ofrece servicios 24x7 que trabaja para resolver situaciones que pueden presentar las empresas, las estadísticas de este servicio muestran que se cierran un 83 % de los casos

en menos de 24 horas y 22 % de estos en menos de 12 horas. (Hoyos, 2015, pág. 9).

> Contar con un SOC se ha convertido en un imperativo para la gestión de seguridad de la información e infraestructura, dado que reúne al personal y herramientas que realmente se necesitan para soportar la seguridad que la actividad del negocio requiere. (Deloitte Ecuador, 2017, pág. 19)

Alcance

El presente proyecto pretende:

Realizar un análisis de las tecnologías que serán utilizadas para un centro de operaciones de ciberseguridad, el cual supervise y proteja los activos críticos de un proveedor de servicios de internet tomando como referencia el estándar ISO27001.

Realizar una propuesta de diseño del SOC, donde incluya la factibilidad técnica y tecnológica además de su estimación económica, esto mediante un análisis de mercado acerca de las nuevas tendencias de ciberseguridad y tecnologías.

Efectuar una simulación de ciber ataques utilizando el Data Center experimental de la Universidad de las Américas, por medio de la implementación de un servicio de base de datos y un servicio web.

Justificación

Hay que tomar en consideración que para el Ecuador es un tema innovador, ya que para este año un cierto porcentaje de empresas necesitarán los servicios de un SOC. Esto debido a que el año pasado varias empresas a nivel nacional reportaron tener diversas brechas de seguridad.

Por tal razón, el presente proyecto tiene como finalidad el realizar un análisis de factibilidad técnica y tecnológica para la implementación de un centro de operaciones de ciberseguridad en un ISP.

Además, servirá como referente para los proveedores de servicios quienes deseen desarrollar los procesos de implementación de un SOC.

Finalmente, es conveniente para la universidad el desarrollo de este proyecto ya que la protección de los datos más que una tendencia es una necesidad en las grandes empresas, por lo que servirá a la institución como un punto de referencia en futuras investigaciones de los estudiantes.

Objetivo General

Analizar las tecnologías de un centro de operaciones de ciberseguridad que servirá como guía de implementación para los proveedores de servicios de internet.

Objetivos específicos

1. Analizar componentes de hardware, software y recursos humanos que serán considerados para el diseño del SOC.

2. Diseñar la arquitectura del centro de operaciones de ciberseguridad donde se incluya la factibilidad técnica y tecnológica además de su estimación económica.

3. Evaluar el sistema propuesto a través de simulaciones de hacking ético en el datacenter experimental de la UDLA utilizando herramientas virtuales de monitoreo y control de vulnerabilidades.

Metodología

En el proyecto se aplicarán los siguientes métodos:

El método inductivo con el cual se planteará la propuesta de diseño del SOC, el mismo que se basará en la información investigada sobre los requisitos básicos y datos recolectados sobre incidencias de seguridad.

El método experimental basará sus datos en un software de simulación de monitoreo, donde se dispondrá de los equipos de la universidad para simular ataques y de esa manera comprobar que resultados fueron obtenidos.

1. CAPÍTULO I: MARCO TEÓRICO

1.1. Introducción

La seguridad de la información ha ido cambiando y evolucionando a pasos agigantados, los hackers hoy en día son cada vez más implacables, haciendo que la seguridad de la información sea progresivamente más compleja. De acuerdo con *Under cyber attack*: la Encuesta Global de Seguridad de la Información de EY, el 59 % de los encuestados ha visto un incremento en las amenazas externas en los últimos 12 meses". (EY Entono de negocios, 2013, pág. 3).

El informe que emitió la empresa EY sobre el crimen cibernético en 2013 dice que en el mundo actual la seguridad de la información no es opcional es una necesidad que cubre todos los aspectos de la metadata.

Por lo tanto, las organizaciones más grandes buscan mejorar su estado actual emprendiendo acciones más audaces en lugar de esperar a que las amenazas vengan a ellos. Estas empresas buscan realizar un monitoreo constante para encontrar una pronta solución a la amenaza la cual es probable que no siempre se pueda controlar.

1.2. Centro de Operaciones de Seguridad

Un Centro de Operaciones de Seguridad (SOC) es un espacio que como afirma EY Entorno de negocios (2013, pág. 3) "es un centro que funcionando de forma correcta puede ser el corazón de una detección efectiva a cualquier amenaza

de seguridad, puede responder más rápido para cualquier vulnerabilidad de hacking”.

El SOC ayuda a empresas con alto grado de riesgo de sufrir cyber ataques y donde el costo puede ser demasiado alto como para asumir el riesgo. Esto permite mitigar cualquier amenaza en el menor tiempo en base a las capacidades operativas y tecnológicas que haya contratado el cliente. (EY Entono de negocios, 2013, pág. 5).

Las consolas de monitoreo dan información de vulnerabilidades, amenazas de interés para los operadores y monitoreo de todos los ataques que ocurren en el mundo. Además, un mapa general de la actividad sospechosa en las principales redes de datos del planeta. (EY Entono de negocios, 2013, págs. 6-7)

Uno de los mayores retos del SOC es la inversión que se tiene ya que los equipos son muy costosos, pero el enfoque y talento de los operadores harán que el centro sea exitoso y tenga rentabilidad.

Las tecnologías del SOC tendrán que tener código abierto y si se instalan programas licenciados aumentará el gasto para la empresa, además se requiere especialistas más experimentados los cuales podrán configurarlos sin ningún problema.

Adicionalmente, las empresas necesitan desarrollar un marco de gobierno en donde los temas de seguridad y evaluación de las vulnerabilidades tengan políticas y estándares para establecer una cultura organizacional. De otra manera el SOC no tiene autoridad para tomar acción en repuesta de hallazgos, y se llegaría a tener desorganización y estado de confusión y debilidad. (EY Entono de negocios, 2013, págs. 10-13).

1.2.1. Operaciones de seguridad vs Operaciones de red

Los SOC y Centros de Operaciones de Red (NOC), son en varios aspectos similares, los dos funcionan de manera que se debe monitorizar la red y los equipos. Estos comparten algunas herramientas, pero cada uno tiene técnicas individuales, la diferencia es que mientras que el NOC está principalmente preocupado con servir al negocio, el SOC está enfocado a protegerlo. (EY Entono de negocios, 2013).

Las diferencias y similitudes del SOC y NOC son muy beneficiosas para la empresa entre estas se tienen las siguientes:

- Mejores comunicaciones y conocimiento compartido para mejorar la concientización situacional y las capacidades de respuesta.
- Tiempos de respuesta a incidentes reducidos al habilitar la función de seguridad de la información y de Tecnología de la Información (TI) para trabajar juntas hacia metas comunes.
- Planeación mejorada de contramedidas a través de la responsabilidad conjunta para la identificación y resolución de causas raíz.
- Reporteo de administración de incidentes racionalizado con un contexto técnico valioso.

1.3. Dispositivos de seguridad

1.3.1. AntiDDos

El objetivo final de un ataque DDOS es consumir los recursos de la red o de la máquina causando indisponibilidad de servicios. Esta agresión no es considerada como hacking ya que no es hecho para robar información o irrumpir en un sistema de forma forzada, sino que interrumpe los servicios ofrecidos. (cogeco, 2017).

Arbor network realizó una arquitectura en varios niveles y lo que obtuvo es una mitigación hibrida de DDos, el enfoque que tuvo es la compresión de los ataques de DDos para poder ser mitigados en el sitio, sea físico o en la nube.

La tecnología de Arbor Network es multiprotocolo esto significa que detectará y mitigará los ataques. (Portal Arbor Networks, s.f).

Un botnet o “ejercito de zombis” es un grupo de dispositivos infectados con un bot que se hace de forma remota y es la fuente de un ataque DDoS es casi imposible encontrar un patrón para los dispositivos atacantes.

Estos ataques DDoS se pueden entender observando la Figura 1:

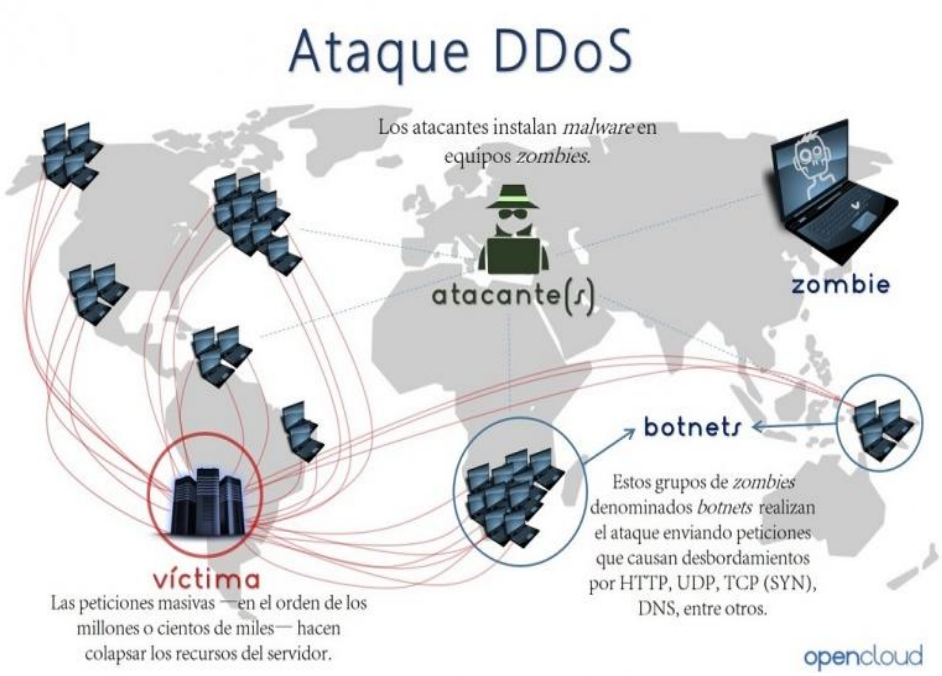


Figura 1. Secuencia de un ataque DDoS.
Tomado de OpenCloud, 2016.

La solución Akamai Kona Site ofrece una defensa multicapa que protege eficazmente sitios web y aplicaciones web frente a la creciente amenaza de los ataques DDoS.

Entre sus principales características se tiene:

- **Controles de capa de red:** al definir y hacer cumplir listas blancas y listas negras de IP, puede permitir o restringir solicitudes de regiones geográficas específicas y ciertas direcciones IP.

- **Monitor de seguridad:** obtener visibilidad en tiempo real de los eventos de seguridad.
- ***Site Shield:*** oculte su origen de la Internet pública para protegerse contra ataques directos a origen.

La solución Incapsula de la empresa Imperva no necesita modificar los registros de DNS para redirigir el tráfico a través de la red, asegura más bien este servicio y lo inspecciona por capas progresivas. Incapsula identifica y filtra el tráfico de ataques dejando pasar solo el tráfico legítimo y enmascara la IP de servidor impidiendo los mismos. (Portal Imperva Incapsula, 2017).

Según el portal web BlueHosting (2016).El impacto de un ataque de DDoS es muy alto ya que se ve afectado primeramente por la reputación de la empresa ya que pierde la disponibilidad y se ve afectada en el nivel de servicio que ofrece y por ende la ésta pierde economía, servicio y calidad, por esto es importante estar protegidos de este tipo de agresiones.

1.3.2. Firewall

Un firewall es un sistema de defensa que consiste en instalar una barrera en un dispositivo o red, el mismo es el encargado de denegar o autorizar las diferentes clases de tráfico.

El firewall analiza todas las solicitudes de acceso y el servicio para asegurarse de que la dirección de internet y dominio sean seguros y conocidos. Examinan cada paquete de datos entrantes buscando códigos incluidos en una *blacklist* (lista de acceso denegado), también analiza los paquetes en función de su similitud con otros, que han sido permitidos. (Kaspersky, 2018).

1.3.2.1. Intrusión, prevención y detección (IDP)

IDP es un servicio que controla las aplicaciones tales como troyanos y aplicaciones de puerta trasera que se pueden infiltrar en la red. IDP utiliza

tecnología de inspección profunda que proporciona la flexibilidad necesaria para poder bloquear programas específicos no permitidos.

Según el portal (Cisco, s.f) existen dos tipos de firewall:

- **Entrante**

Como su nombre lo indica, controla las conexiones que entran al sistema y de esta manera puede comprobar que direcciones IP quieren establecer conexión con los servicios.

Es muy utilizado en sistemas cliente-servidor, los routers que establecen conexión con ADSL tienen un firewall entrante activado por defecto.

- **Saliente**

Controla a los clientes para monitorizar a que direcciones IP desean conectarse y aunque es un firewall más seguro es menos utilizado que el entrante.

1.3.3. Firewall de aplicación web (WAF)

En la actualidad las aplicaciones web que se desarrollan no cuentan con un sistema de seguridad. Esta falta de recursos conlleva a tener una página web que simplemente es insegura y afecta directamente al cliente que abre el portal web como a la empresa.

Un WAF es una aplicación física o virtual con módulos o componentes diseñadas para que las aplicaciones web no sufran falencias de seguridad. (Cloud Security Services, 2013).

Existen varias soluciones que son tendencia en el mercado, por ejemplo, el F5 Advanced WAF que puede defender de los siguientes ataques:

- Ataques automatizados y bots que pueden sobrecargar los recursos de la aplicación.

- Ataques que roban las credenciales de la aplicación o se aprovechan de las cuentas comprometidas.
- Ataques de capa de aplicación que evaden las soluciones de seguridad basadas en la reputación y la reputación.
- Nuevas superficies de ataque y amenazas debido a la rápida adopción de API.
- Bots dirigidos a clientes móviles y basados en navegador.

La solución de Imperva se llama SecureSphere Web Application Firewall, su funcionamiento, como se muestra en la figura 2, es analizar a los usuarios de las aplicaciones y aprende dinámicamente del comportamiento de ellas. Este análisis se realiza en tiempo real para así dar una protección a ataques de lógica de negocios o spam de comentarios.

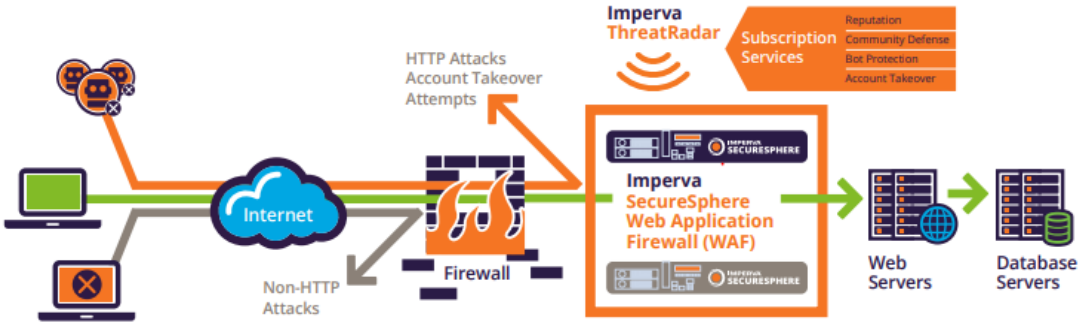


Figura 2. Funcionamiento de SecureSphere Web Application Firewall*.*
Tomado de Imperva, 2017.

El firewall trabaja justamente en la capa de red y el WAF lo hace en la capa de aplicación por lo que si se implementa un WAF en una empresa es necesario instalarlo detrás del firewall convencional. Por lo tanto, el WAF será un sistema complementario para la seguridad en la empresa. (Ramos, 2015). El modo de implementación se puede observar en la figura 3.

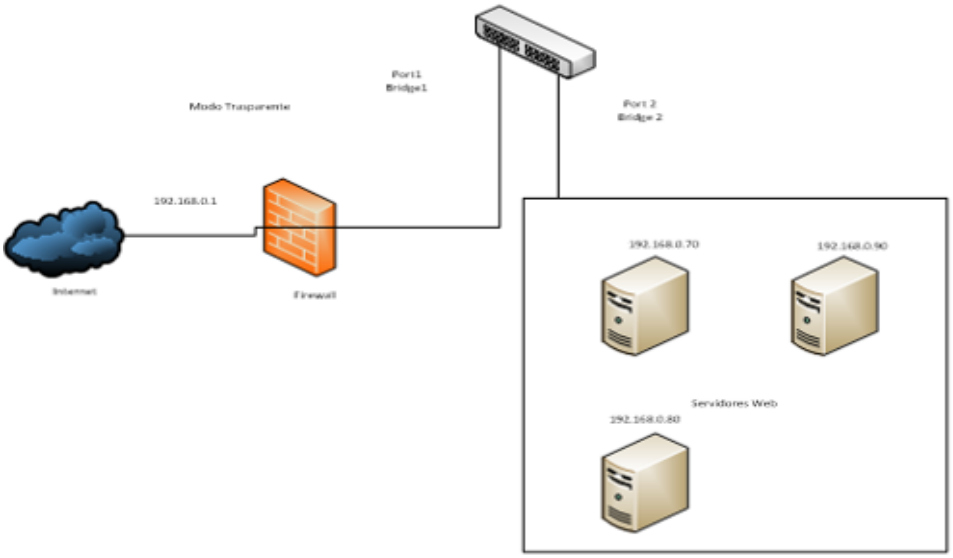


Figura 3. Modo de implementación del WAF

Adaptado de Ramos, 2015, p.277.

En la figura 3 se observa que los dos segmentos de red se interconectan, el primero del firewall a red WAN y el otro a la LAN desde el WAF al servidor web. (Ramos, 2015).

Cuando un usuario se conecta con una página web e intenta llenar un formulario de registro; éste será procesado por el WAF el cual realizará una comparación con una base de datos que tiene las firmas de vulnerabilidades. Si la comparación sale positiva el WAF realizará la remediación que tenga definida para bloquear el ataque. (Ramos, 2015).

En el libro *Hacking y seguridad de páginas web* (Ramos, 2015) indica que existen modelos de seguridad del WAF y tipos de ataques que son capaces de bloquear.

- **Negativo:** en este modelo el WAF deja pasar todas las peticiones web y niega solo las que el sistema detecte como un ataque, funciona con una base de firmas de vulnerabilidades que es actualizado a diario.

- **Positivo:** en este modelo el WAF, deniega todo el tráfico hacia el servidor web y deja realizar las transacciones de la aplicación web, se basa en reglas de heurística, esto quiere decir que no depende de las firmas más bien se deja que el WAF aprenda las peticiones maliciosas y no maliciosas para que detecte el falso positivo.

Si se comparan dichos modelos se dice que el negativo tiene la desventaja de tener que comparar con la base de firmas. Si un atacante ingresa con una vulnerabilidad no conocida, el ataque se realizará con éxito. Mientras tanto que el positivo en el momento de aprendizaje puede que asimile un proceso que no fue un embate y lo rechace indicando que fue un falso positivo.

1.3.4. Sistemas de información y gestión de eventos (SIEM)

Un SIEM tiene la función de analizar eventos de sistemas informáticos en tiempo real permitiendo realizar un análisis forense de los incidentes ocurridos. (certsi, 2017)

Sus funciones principales son:

- **Gestión de información de seguridad**

Con esta función se puede recolectar reportes y análisis de incidentes de seguridad donde su fuente principal pueden ser aplicaciones, sistemas operativos, herramientas de seguridad o dispositivos de red.

- **Gestión de eventos de seguridad**

Actúa como un repositorio central para los procesos generados por las herramientas de seguridad para poder seleccionar mediante reglas lógicas dichos eventos que son de interés.

SIEM en una combinación de dos términos; SEM (Gestión de eventos de seguridad) y SIM (Gestión de seguridad de la información). La diferencia entre estos términos es que SEM se ocupa del monitoreo en tiempo real, y muestra

las respectivas notificaciones de seguridad; SIM ofrece un almacenamiento a largo plazo, así como también un análisis y comunicación de datos. (Pico, 2016, pág. 18).

Un ejemplo de implementación de un SIEM en Ecuador se lo realizó en el año 2016 en Pelileo, se utilizó un sistema de software libre para la seguridad operacional en las pymes donde existían sistemas de información que no contaban con aplicaciones o dispositivos de seguridad confiables.

En este proyecto se realizó una propuesta de diseño basado en las estructuras de red de las pymes, se agregó un sensor SIEM además de un router y un switch dentro de la red actual como se aprecia en la Figura 4.

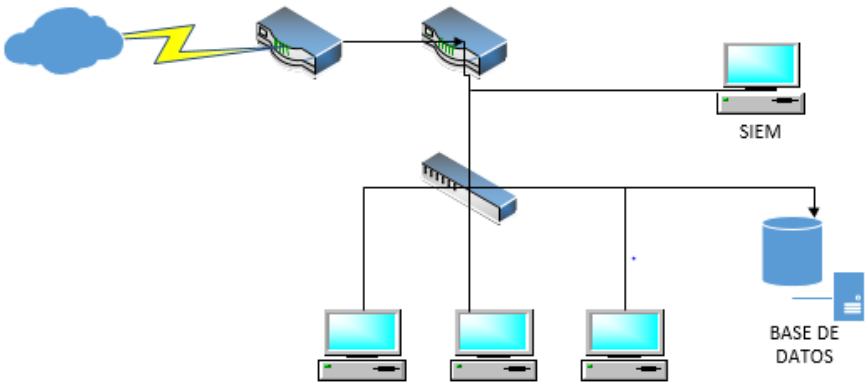


Figura 4. Propuesta de diseño para la implementación de un SIEM en Pelileo. Tomado de Pico, 2016.

Por lo tanto, el SIEM ayuda a la recopilación, análisis y presentación de la información que fue recogida por los dispositivos de seguridad y la almacena en bases de datos. Esta herramienta es muy útil para el análisis de vulnerabilidades y monitoreo de los equipos de red.

1.3.5. Sistema de prevención de intrusos

Para poder hablar de un Sistema de Prevención de Intrusos (IPS) también se tiene que saber que es el Sistema de Detección de Intrusos (IDS).

IDS es el sistema de detección de intrusos que permite identificar el mal uso de la red mediante un monitoreo del tráfico y recursos, la detección y alertas que son enviadas de la red. (networkworld, s.f).

IPS es la evolución del IDS ya que estos pueden monitorear y detectar cualquier anomalía en la red con la diferencia que puede prevenir el ataque de intrusos. Los IPS permiten tener análisis más completos del uso de la red teniendo en cuenta un enfoque preventivo en caso de que esta tenga paquetes maliciosos. (Díaz & Salcedo, 2014, pág. 28).

Además, tanto el IPS como el firewall se complementan ya que el firewall puede dejar pasar el paquete que va en el encabezado como normal mientras el IPS verifica que este contenga datos maliciosos.

1.3.5.1. Modelos de detención

Detención basada en firmas: los IPS contienen una base de firmas que se encargan de detectar si algo está mal en el paquete, estos tienen la capacidad de reconocer determinadas cadenas, dentro de las cuales las firmas son actualizadas de manera constante por los proveedores para bloquear cualquier ataque, si no existe en la base de las firmas no podrá contenerlo. (networkworld, s.f).

1.3.5.2. Modo de funcionamiento

Generalmente los IPS se instalan en modo online, esto conlleva a que el dispositivo no tenga asociada una dirección IP por lo que resulta invisible a los ataques. Sin embargo, un IPS también puede ser desplegado como un router de capa tres y la ventaja de esto es que se puede tener un mayor control en la forma de encaminar el tráfico. (networkworld, s.f).

Los IPS se clasifican en cuatro diferentes tipos:

- **Basados en Red LAN (NIPS):** monitorizan la red LAN en busca de tráfico de red sospechoso.
- **Basados en Red Wireless (WIPS):** control de la red inalámbrica para buscar tráfico sospechoso al analizar la actividad por protocolo de comunicación inalámbrico.
- **Análisis de comportamiento de red (NBA):** Examina el tráfico de red para identificar amenazas que generan tráfico inusual.
- **Basados en Host (HIPS):** Se efectúa mediante la instalación de paquetes de software que monitoriza un host único en busca de actividad sospechosa.

IBM cuenta con una herramienta de administración conocida como IBM QRadar Security Intelligence Plataform la cual se compone de QRadar SIEM en su núcleo. La solución brinda funciones complementarias como administración de registros, monitoreo de red o vulnerabilidades, además también ofrece su servicio a través de la nube.

Splunk es otra solución que tiene dos versiones, Enterprise Security la cual brinda capacidades específicas de monitoreo de seguridad y la versión User Behavior Analytics agrega operadores analíticos avanzados que complementan a Enterprise Security.

Finalmente, McAfee Enterprise Security Manager incluye una interfaz de usuario basado en la web, una base de datos de incidentes, capacidad para generar informes. Como información adicional, tiene dos componentes; el primero recopila eventos y su normalización (*Event Receiver*) y otro recopila, administra y almacena todos los mismos en bruto. (Enterprise Log Manager). (Gartner, 2017).

1.4. Marco de referencia relacionada con la seguridad

1.4.1. Information Technology Infraestructure (ITIL)

ITIL son las siglas de una metodología desarrollada a finales de los años 80s por iniciativa del gobierno de los Estados Unidos.

Esta metodología ayuda a la gestión de servicios de Tecnologías de Información en todo el mundo. La misma es una recopilación de las mejores prácticas tanto del sector público como del sector privado. Las cuales se dan en base a toda la experiencia adquirida con el tiempo en determinada actividad. (Márquez, 2014).

Este método también propone utilizar documentación para cada actividad realizada, ahí se escribe la fecha en la que se hace el cambio, una breve descripción de los canjes que se hicieron, quien fue la persona que lo creó. Esto ayuda a establecer cierto control en el sistema de las modificaciones y así siempre va a haber un responsable que conoce los procedimientos y cambios efectuados. (Ingenia, 2018).

1.4.2. Control Objectives for Information Systems (COBIT)

El COBIT es un marco aceptado internacionalmente para auditar la gestión y control de los sistemas de información. Este permite controlar la tecnología y los riesgos haciendo posible declarar una política la cual convenga a los involucrados en el proceso.

Las metas de COBIT constituyen el enfocarse en las necesidades del negocio mejorando la comunicación entre los implicados, son ayuda para mejorar los asuntos de seguridad y control en el área de operación.

Se aplica a los sistemas de información de toda la empresa. Están basadas en los recursos TI que necesitan ser administrados por un conjunto de procesos naturalmente agrupados. (Portal Nextech, s.f).

1.4.2.1. Beneficios COBIT

- Mejor alineación basada en una focalización sobre el negocio.

- Visión comprensible de TI para su administración.
- Clara definición de propiedad y responsabilidades.
- Aceptabilidad general con terceros y entes reguladores.
- Entendimiento compartido entre todos los interesados basados en un lenguaje común.
- Cumplimiento global de los requerimientos de TI planteados en el Marco de Control Interno de Negocio COSO.

1.4.3. Normas ISO 27001

Esta norma fue elaborada por el subcomité SC que define los sistemas de gestión de seguridad de la información (SGSI). Su implementación reduce los riesgos relacionados con la confidencialidad, disponibilidad e integridad de la información en una empresa u organización.

ISO 27001 se encuentra dividida en 11 secciones además de un anexo; no es obligatorio implementar las secciones 0 al 3 ya que estas son introductorias. (Pico, 2016).

A continuación, se muestra un resumen de cada una de las secciones que conforman la norma ISO 27001 tomando como referencia el libro de la norma técnica ISO 27001:2011, además de la versión actualizada de la norma ISO 27001 del año 2013.

Las secciones que serán utilizadas para el desarrollo del proyecto serán las siguientes:

1.4.3.1. Sección 1

Esta norma se aplica a cualquier tipo de organización ya que los requisitos que se establecen son genéricos y cuando una empresa declara que cumple con la norma ISO 27001, no podrá excluir ninguno de los requisitos que se describen en las secciones siguientes a partir de la sección cuatro.

1.4.3.2. Sección 4

Se describen los requisitos generales para un SGSI dentro de las actividades empresariales, algunos de los pasos para la creación del SGSI son:

- La definición del alcance y los límites del SGSI basándose en las características del modelo de negocio que tiene la empresa.
- Definición de una política SGSI acorde con el modelo de negocio en donde se incluya un marco para la fijación de objetivos y directrices con relación a la seguridad de la información.
- Luego de la definición de la política de SGSI se dará un enfoque en la evaluación de riesgos de la organización especificando una metodología de evaluación adecuada. Aquí se identificarán los riesgos en los activos, las vulnerabilidades y el impacto que los mismos pueden causar a la empresa.
- Después de evaluar los riesgos sobre los activos se dará una valoración respectiva para luego enfocarse en el tratamiento de estos.
- Se especifica que los documentos exigidos por el SGSI deben estar protegidos y tener un formato establecido que deberá ser aprobado antes de su distribución e ir actualizando de ser necesario.

1.4.3.3. Sección 5

Aquí se establecen las responsabilidades de la dirección, cómo se realizará la gestión de recursos. También se especifica que todo el personal que tenga compromisos relacionados con el SGSI debe capacitar y contratar personal competente para satisfacer las necesidades requeridas.

1.4.3.4. Sección 6

Esta es la fase de planificación en donde se determinan los requerimientos para la evaluación de riesgos y el tratamiento de estos.

1.4.3.5. Sección 7

Se fijan los requisitos de disponibilidad de recursos, competencias, control de documentos y registros, la Dirección revisa continuamente el SGSI para asegurar que se mantiene conveniencia y eficacia además de buscar oportunidades de mejora y necesidad de cambios.

1.4.3.6. Sección 8

Aquí se define la implementación de la evaluación y el tratamiento de riesgos, además de los controles y los procesos requeridos para el cumplimiento de la seguridad de la información.

1.4.3.7. Sección 9

Se muestran los requerimientos necesarios para la realización del control, medición, análisis y evaluación por parte de la dirección.

1.4.3.8. Sección 10

La organización debe mejorar de manera continua, es por eso por lo que se debe aplicar una acción correctiva identificando las no conformidades y sus causas. Además, se debe evaluar la necesidad de adoptar acciones para que las no conformidades no se vuelvan a producir.

1.4.3.9. Anexo

Finalmente, el anexo contiene un catálogo de medidas de seguridad distribuidos en secciones. Los detalles de este se encuentran el Anexo 1 de este documento.

1.4.3.10. Proceso para aplicar ITIL /Cobit

Para poder aplicar COBIT, se plantea 37 procesos distribuidos en 5 dominios; el primero evalúa supervisa y orienta los servicios de TI, mientras que los

demás se encargan de todo el ciclo de vida; este se encarga de llevar los estándares de la gestión. Cuando se trata de la parte de seguridad de la información también va de la mano con ITIL que son 26 procesos que comparten todo el ciclo de vida de la misión, en los cuales se puede ir monitoreando el comportamiento para mejorar cada día, en los procesos se mejora el diseño la transición y la operación del servicio.

1.4.4. Vulnerabilidad

Para realizar un análisis de vulnerabilidades también es necesario tener en claro su concepto. Una vulnerabilidad es un defecto a nivel de hardware o software que, si es descubierto por usuarios malintencionados, estos intentan explotarla para realizar los ataques. (CeroUno Software Corportaivo, s.f).

Existen varias clasificaciones que describen y ordenan las diferentes vulnerabilidades que se han descubierto; una de las más importantes es la base de datos Bugtraq, la cual se actualiza muy frecuentemente y es vital para encontrar mucha información acerca de los errores detectados de un software. (García, 2013, pág. 97).

Los pasos que deben realizarse para un correcto análisis de vulnerabilidades son los siguientes:

- Escaneo de seguridad tanto de vulnerabilidades internas como externas.
- Revisión de políticas de seguridad.
- Revisión de procesos, pólizas de soporte y configuraciones que comprometan la seguridad informática.
- Planeación ante eventos de incidentes de seguridad y revisión de políticas de respaldos como planes de recuperación ante desastres.
- Generación de documentos de recomendación de eventos de seguridad.

1.4.4.1. Tipos de vulnerabilidades

Las vulnerabilidades de un sistema son una puerta para los posibles ataques que se puedan filtrar, y son de tres tipos los cuales pueden afectar a nuestros programas:

Vulnerabilidades conocidas sobre aplicaciones instaladas: son las que ya tienen conocimiento las empresas que desarrollan el programa al que afecta y de las que ya se sabe la solución y se la tiene en forma de parche. (Cisco, s.f).

Vulnerabilidades conocidas sobre aplicaciones no instaladas: son las que no se sabe cómo actúan y no se tiene solución.

Vulnerabilidades aun no conocidas: estas son las que aún no han sido detectadas por las empresas y si otra persona detestara esta falla podría utilizarla contra todos los equipos que tiene instalado el programa. (infosegur, 2013).

1.4.4.2. Amenaza

La amenaza se puede definir como toda acción capaz de encontrar o atentar contra la seguridad informática, surgen de las vulnerabilidades de un sistema que pueda ser aprovechada. (Lujan, 2014).

Su clasificación por el tipo de personas que comenten el fraude pueden ser los siguientes:

- **Hackers:** expertos informáticos con habilidades para descubrir las vulnerabilidades, pero sin sacar provecho económico.
- **Crackers:** conocen cómo romper la seguridad de un sistema y aprovechan este fallo con fines económicos.
- **Phreakers:** personas que encontraron una vulnerabilidad en las redes telefónicas para conseguir llamadas gratuitas.
- **Sniffer:** expertos en redes que obtienen la información de terceros extrayéndola del tráfico de datos.

- **Lammers:** aquellos que se consideran a sí mismos hackers sin tener conocimientos de informática.
- **Newbie:** hacker novato.
- **Ciberterrorista:** son espías en la red que trabajan para alguna empresa sacando información.
- **Programadores de virus:** crean programas maliciosos que afectan un sistema o aplicaciones.
- **Carders:** infringen los sistemas de tarjetas como los cajeros automáticos.

1.4.5. Introducción al Ethical Hacking

El crecimiento de los sistemas informáticos ha traído muchas ventajas como la banca en línea, correo electrónico, tiendas en línea; pero con este desarrollo también han surgido nuevas formas de delincuencia informática.

Las empresas han innovado sus tecnologías, pero temen que sus sistemas puedan ser vulnerables a los ataques, para estos problemas hoy en día existe el hacking ético.

Hacking es la violación de un sistema para piratear robar o irrumpir en un sistema de forma ilegal para fines de lucro económico. Si a hacking se le agrega la palabra ético se pensaría que es una contradicción, pero el hacking ético es la penetración controlada a un sistema con previa autorización. Con esto se identifican las falencias de los sistemas y se realiza un informe con las penetraciones logradas. La información confidencial conseguida consecuentemente se presentará recomendaciones y soluciones previsoras de intrusiones no autorizadas. (Hacking, 2013).

Proceso que se realiza en ethical hacking:

- La organización desea saber si sus sistemas son seguros.
- Contrata servicio profesional de ethical hacking.
- Planifica como se realizará y el alcance.

- Luego el profesional lleva a cabo un análisis del sistema simulando ataques reales sin comprometer los datos del sistema.
- Analiza los resultados.
- Realiza un reporte para que la empresa lo evalué.
- Soluciona la vulnerabilidad y mitiga para dejar el sistema más seguro.

1.4.5.1. Tipos de Ethical Hacking

Los hackers éticos utilizan varios métodos para simular un ataque los cuales son:

- Red remota es en la que se intenta simular un ataque a través de internet, lo que se hace es simular una vulnerabilidad fuera de la red LAN.
- Red dial-up remota se realiza ejecutando un ataque contra el pool de módems también llamado *war dialing* es el proceso para marcar hasta encontrar un sistema abierto.
- Red local se realiza usando un acceso no autorizado a la red local.
- Equipo robado se encarga de ingresar a un equipo físico el cual se roba nombres usuario contraseñas configuraciones de seguridad como si se tratara de robar un equipo portátil.
- Ingeniería social se intenta comprobar la integridad de las personas usando la comunicación con las redes sociales o medios de comunicación con el fin de sacar información de nombres contraseñas etc.
- Entrada física lo que se trata es comprometer el acceso físico a los equipos con el fin de plantar virus, troyanos, gusanos por hardware.

1.4.5.2. Tipos de pruebas de ethical hacking

Las pruebas que se realizan simulan un atacante con diferentes niveles de conocimiento estos tipos son los siguientes.

- *Black Box* (caja negra) implica realizar pruebas de seguridad sin que se sepa cómo está la infraestructura de la red, la prueba es simular un ataque desde fuera de la empresa.
- *White Box* (caja blanca) se trata de realizar una prueba de seguridad con el conocimiento de la infraestructura de la red es decir como si se tratara de un administrador de red.
- *Grey Box* (caja gris) esta prueba se realiza examinando el grado de acceso que tienen los empleados con información privilegiada dentro de la red. (hacker, 2013).

1.4.6. Malware

Malware es un término que engloba a todo tipo de código malicioso cuyo objetivo es dañar el funcionamiento de algún sistema entre los malware existen los virus, troyanos, gusanos, etc. (Kaspersky, 2018).

1.4.6.1. Tipos de malware

- **Spyware:** está diseñado para rastrear y espiar al usuario final, este tipo de malware realiza actividad de recopilación de pulsación de teclas y captura de datos además que con frecuencia se agrupa con el software como un troyano.
- **Adware:** este software se caracteriza por brindar anuncios automáticamente, se instala con programas legítimos, pero hay veces que se instala con un spyware.
- **Bot:** viene de la palabra rebot este está diseñado para hacer acciones automáticamente, la mayoría de bots son inofensivos, pero si se realiza un botnets puede infectarse con bots programados para atacar silenciosamente.
- **Ransomware:** está diseñado para tener cautivo los datos hasta que se realice un pago, esto se encuentra encriptado con un usuario y contraseña desconocido, se esparce por algún archivo descargado en la computadora.

- **Rookit:** este malware modifica el sistema operativo hasta crear una puerta trasera, la cual queda abierta para que el atacante pueda ingresar y extraer la información remotamente; modifica las herramientas forenses por lo que es muy difícil detectarlos si su computador es infectado lo que se debe hacer es cargar nuevamente el sistema operativo.
- **Virus:** es un código que ejecuta a otros archivos legítimos, la mayoría del virus necesita ser activado por los usuarios y pueden producirse en fechas específicas, lo virus pueden ser de dos 2 tipos los que son inofensivos y los que pueden borrar información.
- **Troyano:** estos ejecutan operaciones maliciosas en una operación deseada, este código malicioso cambia los privilegios de los archivos y se diferencia de un virus porque se adjunta con un archivo.
- **Gusano:** este tipo de malware se replica mediante la explotación de las vulnerabilidades en las redes, ralentizándolas; estos gusanos puede ejecutarse por sí mismos esto quiere decir que no necesitan la interacción del usuario.
- **Hombre en el medio:** este tipo de malware permite tener el control de un dispositivo sin conocimiento del usuario, el atacante puede capturar información antes de que transmita a su destino.

1.4.7. Elementos de seguridad

La seguridad informática consiste en asegurar el primer recurso que son los datos o la información de una empresa, mantener los recursos con procedimientos basados en políticas y normas.

La seguridad se basa en los elementos que son los siguientes:

- **Confidencialidad** ocultar la información para terceros es decir que los datos sensibles solo puedan ser manipuladas por personas autorizadas como en la declaración de impuestos, descifrar claves etc.

- **Autenticidad** es la veracidad de que un documento es elaborado por quien dice ser la garantía del origen de la información

El AAA integra Autenticación, Autorización y Auditoria.

- **Autorización** es el proceso donde los datos son permitidos para ser usados o no.
- **Auditoria** es registrar los datos en la red, se almacena en una base de datos todo lo que acontece en la red.
- **Integridad** es la fiabilidad de que los datos no fueron alterados sin autorización y verificar que no se ha producido ninguna manipulación en el documento original.
- **Disponibilidad** Se garantiza que los servicios estén disponibles las 24 horas los 7 días de la semana los 365 días del año, además que los usuarios autorizados tengan todo lo que necesiten cuando se lo requiera.

1.4.8. Ataques

1.4.8.1. Vector ataque

Partiendo de que un vector ataque es el medio que utiliza un hacker para tomar el control de un activo dentro de una empresa, es importante evaluar los riesgos en una red, buscar las posibles vulnerabilidades en los activos y luego de esta previa evaluación aplicar un tratamiento adecuado. Esto lo indica norma ISO 27001 sección 4. (López, 2017).

Entre los datos que se pueden extraer de un activo pueden ser el nombre de dominio, la dirección IP, y servicios como TCP o UDP; por ejemplo, si se necesita saber la potestad en la que se encuentra una empresa, primero se debe buscar la página oficial en internet y así se puede ver el dominio de la organización. Además, en la web existen grupos de noticias y foros donde se hablan sobre configuraciones de dispositivos e instalaciones de software y muchas veces las personas ingresan información sensible de su empresa y con

los archivos que envían es fácil obtener la dirección IP. (García, 2013, págs. 56-57).

Con la dirección IP también es posible realizar un ataque a través de un barrido de ping, se puede enviar un ping a la dirección del dominio e inmediatamente se mostrará la IP, o también se puede hacer ping a la dirección de broadcast y el comando se lanzará hacia todos los dispositivos de la red. (García, 2013, págs. 65-66).

Una vez que se obtienen los datos de un activo, un hacker podrá obtener herramientas con la que pueda realizar un ataque. Por ejemplo, existen herramientas de sniffing como el whireshark para interceptar los paquetes que *v*iajan *a* través de la red para luego ser analizados.

> El secreto del sniffing radica en la posibilidad de configurar un dispositivo de red para que acepte cualquier paquete entrante. Esta modalidad se llama promiscuos mode (modo promiscuo). Al configurar el dispositivo en promiscuos mode, todos los paquetes que lleguen al equipo serán aceptados. (Katz, 2015, págs. 246-247)

2. CAPÍTULO II: DISEÑO

2.1. Introducción al diseño

Para diseñar el SOC se propone basarse en una metodología ya definida, en este caso se utilizará la metodología propuesta por Cisco conocida como *Top Down,* la primera fase será realizar un análisis del negocio en donde el SOC será implementado, la siguiente será definir los requerimientos necesarios para resolver la problemática y finalmente mostrar una propuesta realizando un diseño lógico y físico del servicio planteado.

El negocio al que se encuentra enfocado este proyecto es para los proveedores de servicios de internet (ISP), los cuales son entidades que proveen la infraestructura necesaria para facilitar la transmisión de información de un punto a otro.

Hoy en día disponer de personal especializado no es suficiente para mantener la seguridad de una red, se necesita de herramientas, procesos y conocimientos necesarios para poder actuar ante un incidente de seguridad por lo que implementar un SOC es necesario para cualquier tipo de compañía. (GMS, 2018).

Para el modelo lógico se va a especificar el direccionamiento IP, los protocolos utilizados y se definirá como va a estar distribuida la red.

Para la parte física los servicios que se va a brindar es el monitoreo de seguridad de la red (SIEM), WAF, ANTIDDos, firewall e IPS/IDS; los cuales van a estar distribuidos para dar protección tanto a equipos dentro de la empresa como fuera de ella.

2.2. Requerimientos

La norma ISO 27001 en la creación y gestión de un SGSI plantea que se debe realizar un análisis de los riesgos de la empresa y los niveles de estos.

En base a esto, un ISP definirá los requisitos de diseño del SOC; los cuales pueden variar para cada empresa, pero en general la tabla 1 muestra los requisitos más comunes que varias organizaciones han publicado.

Tabla 1.

Requerimientos para el diseño de un SOC.

Nombre	**Detalle**
Automatización de tecnología	La tecnología debe permitir reducir al máximo la carga de trabajo de los analistas, en donde los mismos puedan realizar procesos, como control de incidentes, monitorización de servicio críticos, gestión de vulnerabilidades, etc.
Anticipación a eventos de seguridad.	Para ello se requerirá realizar el análisis de vulnerabilidades para conocer los riesgos que presenta la red, adicional se pueden

	realizar pruebas de ethical hacking para conocer el grado de riesgo que se puede correr en caso de algún tipo de ataque.
Personal especializado	Se debe contar con un equipo especializado que cuente con la formación y la experiencia necesaria para atender cualquier tipo de incidente de seguridad que se presente.
Control de operaciones según convenga	La organización puede definir su control de operación según crea conveniente, puede ser desde: 8 horas por 5 días (8x5) o 24 horas por 7 días (24x7).

En base a los requerimientos descritos anteriormente, se puede dividir el SOC en tres elementos fundamentales planteados también por la metodología ITIL que son personas, procesos y plataformas como se muestra en figura 5.

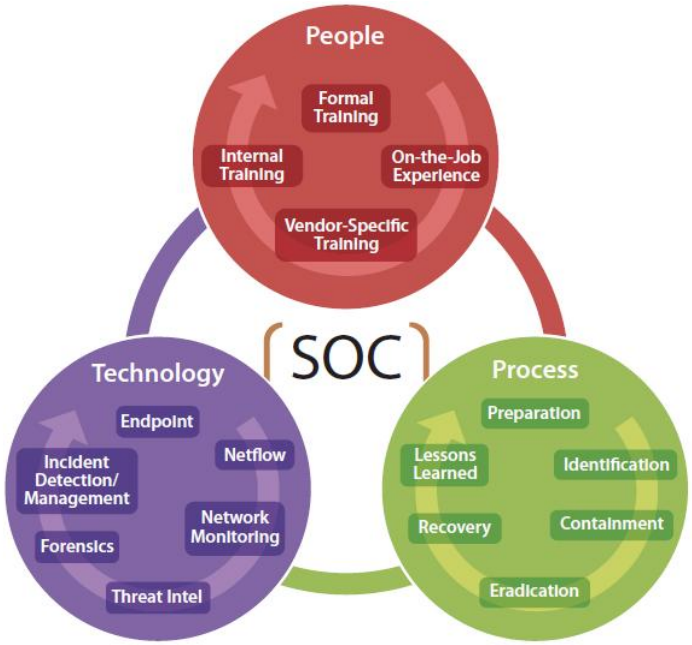


Figura 5. Modelo ITIL para diseño de un Soc.

Tomado de UTI Servicios, 2018

2.3. Plataformas

2.3.1. Modelos de equipos y herramientas

Los modelos analizados para el diseño son tomados en base al cuadrante mágico de Gartner. Este cuadrante se basa en diferentes criterios como son capacidades para ejecutar un servicio, su usabilidad y rapidez; además analiza su perspectiva de desarrollo en el tiempo y la cantidad de clientes que utilizan un producto. (UDESIGN, 2015)

Los costos que se detallan aquí son precios aproximados tomados de diferentes proveedores que ofrecen estos equipos y soluciones. Existen varias marcas y diferentes características para cada necesidad y es lo que un proveedor de servicios de internet debe tomar en cuenta al momento de escoger un producto o servicio.

2.3.1.1. Anti-ataque de denegación de servicios (Anti-DDos)

Una de las soluciones que tiene mayor ranking es Arbor Network seguido de Imperva y F5.

En la tabla 2, se muestran los diferentes modelos de AntiDDos y sus principales especificaciones técnicas.

Tabla 2.

Descripción de equipos anti-DDoS

Modelo	**Grafico**	**Descripción**	**Precio**
F5 VIPRION C2400 Chassis		2 AC power supplies 120/230 V (1400W) auto ranging con cuatro slots para las cuchillas.	$ 14 000

Arbor network Cisco ASR 9000 vDDoS		Hasta 40 Gbps por VSM múltiple VSM soporta tráfico de 10, 20 o 40 Gbps	$ 25 000
Imperva AV2500		500 MB Throughput anti DDos y WAF consola centos 6.3	$ 3 596

2.3.1.2. Firewall

Las marcas líderes en firewalls consideradas como NGFW o firewall de nueva generación son Palo Alto, Checkpoint y Fortinet; la última considerada según Gartner como la única solución que ofrece escalamiento, automatización y buen desempeño para la protección de los equipos empresariales. (Gartner, 2017).

A continuación, se muestra la tabla 3 con las características de los equipos y su estimación económica.

Tabla 3

Descripción de los equipos Firewall

Modelo	Gráfico	Descripción	Precio
PAN-PA-4050 Palo Alto Firewall Enterprise		Capacidad de cortafuegos de 10Gbps, capacidad de prevención de amenazas de 5Gbps, 300 certificados SSL entrantes, 60000 nuevas sesiones por segundo.	$ 45 000
Checkpoint 12400 appliance		25 Gbps de capacidad de cortafuegos, 12 Gbps de rendimiento de IPS, alta densidad de puertos (hasta 26 puertos), 500 GB de disco duro	$ 27 584,89
FortiGate 7060E		Rendimiento de cortafuegos de 510 Mbps, Rendimiento de IPS de 360 Gbps, nuevas sesiones por segundo de 1,8 millones, latencia de firewall de 7 microsegundos	$ 263490,73

2.3.1.3. Firewall de aplicación web (WAF)

Gartner indica que el WAF debe tener las siguientes características para poder ser el mejor en el mercado.

- Maximizar la tasa de detección y captura de amenazas conocidas y desconocidas.
- Reducir al mínimo los falsos positivos y adaptación a las aplicaciones web en continua evolución.
- Facilidad de uso y el impacto mínimo en el rendimiento.
- Automatizar el flujo de trabajo de respuesta a incidentes para ayudar a los analistas de seguridad de aplicaciones web.
- Proteger clientes, usuarios internos, aplicaciones web y API.

Con esas características se determinó que los líderes en soluciones WAF son F5, Imperva y Akamai.

La tabla 4 muestra a continuación las últimas tendencias de equipos WAF con sus principales características.

Tabla 4

Descripción de equipos WAF

Marca	**Modelo**	**Detalle**	**Precio**
F5 Chassis Local Traffic Manager + WAF C2400		21.2"D x 6.9"H x 17.6"W dimensiones y peso 42.5 libras	$ 1000
WAF Imperva Cloud Securityphere		Throughput de 100mbps	Costo por mes $ 450

2.3.1.4. Gestión de eventos e información de seguridad (SIEM)

A continuación, la tabla 5 muestra las principales características de las soluciones SIEM las cuáles pueden escogerse dependiendo la necesidad de la organización. Tomando en cuenta que un SIEM puede ser adquirido como hardware o software también se hace una referencia al precio aproximado del mismo.

Tabla 5

Descripción de herramientas SIEM

Modelo	**Descripción**	**Precio**
IBM QRadar SIEM	Base de datos centralizada, acceso basado en roles, cinco paneles predeterminados, captura de datos de flujo de red de capa cuatro en tiempo real, cargas útiles de aplicación de capa 7.	$ 14 847,80
Splunk Enterprise Security	Volumen de indexación de 500MB, control de acceso basado en roles, monitoreo en tiempo real, seguimiento asociado con amenazas avanzadas.	Licencia anual $ 1 800 por GB, licencia perpetua $ 4 500 por GB.
McAfee Enterprise Security Manager	Diseñada para grandes empresas, recolecta hasta 300000 eventos por segundo, almacenamiento de hasta 14Tb.	Software $ 39 995 Hardware $ 47 994

2.3.1.5. Sistema de previsión de intrusos (IPS)

Los equipos más cotizados o los primeros en la lista del cuadrante mágico de Gartner son Cisco y McAfee los cuales llevan un informe anual de las vulnerabilidades que puede haber en el mundo y cargan una base de datos de estas para poder detectar ataques de este tipo.

Tabla 6

Descripción de equipos IPS

Marca	**Modelo**	**Detalle**	**Precio**
Serie Firepower 8100		Inspección de amenazas de 10 a 20 Gbps Incluye AVC, con AMP	$ 34.804,46
McAfee Network Security Platform M-8000		Método de autentificación LDAP, RADIUS, TACACS soporta ipv6 IDS, IPS 2 Gbps Throughput 60 Gbps.	$195.495.75

2.3.1.6. Software Libre

Hoy en día la virtualización es una de las opciones más comunes ya que las mismas ahorran espacio, costos y facilitan la administración de estas; para este proyecto se buscó utilizar distribuciones de Linux que sean compatibles entre sí y que tengan las herramientas necesarias para su respetiva implementación.

A continuación, en la tabla 7 se muestran las características del software que será utilizado para cada herramienta del SOC.

Tabla 7

Características del software utilizado.

Nombre	**Distribución de Linux**	**Características**
IDS Snort	Ubuntu	Configuración simple, detección automática de servicios, obtiene paquetes través de la librería libcap. (certsi, 2017).
Alien Vault OSSIM	Debian	Descubrimiento de los activos conectados a la red, evaluación de vulnerabilidades, correlación de eventos y control de comportamiento; esto ayuda al usuario a conocer sobre eventos maliciosos en tiempo real. (AlienVault, 2018).
Endian Firewall	Debian	Establecimiento de reglas de firewall NAT Soporte para DNS dinámicos Soporte para DMZ Interfaz de administración web mediante protocolo HTTPS. Alta disponibilidad.

2.4. Asignación de personal

Para poder asignar el personal para el SOC, se debe tener en cuenta primero que va a ver tres niveles de asignación, dependiendo de los conocimientos y las tareas asignadas, como se muestra en la siguiente tabla 8.

Tabla 8

Detalle de los perfiles del personal requerido para el SOC

PERFILES	**OBLIGACIONES**
Analista de alertas nivel 1	Monitoreo constante de las alertas, monitorea la salud de los sensores de seguridad y los dispositivos finales; recolecta datos necesarios para iniciar el nivel 2.
Encargado de responder incidentes nivel 2	Realiza un análisis profundo de los incidentes al correlacionar datos de varias fuentes; determina si un sistema de datos crítico ha sido impactado; aconseja varias soluciones; brinda soporte para nuevos métodos analíticos para detectar amenazas.
Experto en amenazas y riesgos nivel 3	Posee conocimiento profundo acerca de la red, dispositivos finales, inteligencia de las amenazas, ingeniería inversa forense y malware, así como el funcionamiento de aplicaciones específicas, infraestructura de IT subyacente, actúa como un incidente sin esperar para escalar incidentes; estrechamente implicados en el desarrollo, ajustar e implementar análisis de detección de amenazas
Administrador del SOC	Maneja recursos para incluir personal, presupuesto, programación de turnos y estrategia tecnológica para cumplir con el

	SLA; funciona como un punto organizacional para incidentes críticos de negocio; proporciona una dirección general para el SOC y aporta información a la estrategia general de seguridad.

Adaptado de (APPROACH, 2018); (SIMPLYHIRED, 2017)

2.4.1. Conocimiento y experiencia requeridos

2.4.1.1. Analista de SOC

El rol que desempeña un analista del SOC es muy importante y depende de los conocimientos y habilidades que tenga para obtener un cargo más elevado en esta área. Las habilidades son trasferibles con las experiencias pero tiene que tener habilidades propias como son: ser analítico por naturaleza, tener deseo de trabajo duro, adaptarse y estar dispuesto a aprender nuevas tecnologías.

El perfil descrito a continuación tiene como referencia los requerimientos de varias empresas de telecomunicaciones a nivel internacional las cuáles tienen implementado un SOC en su infraestructura.

Los conocimientos que debe tener son:

- Realizar análisis de primer nivel y tener la comprensión para interpretar la información de los sistemas del SOC, análisis de incidentes y procedimientos de escalamientos.
- Tener educación de tercer nivel en informática o redes, carreras afines, capacitación en la parte de análisis de seguridad de TI, amenazas y vulnerabilidades.
- Conocimiento en múltiples plataformas de sistemas operativos como Windows, Linux, etc.
- Tener habilidades de herramientas como IDS/IPS, SIEM, AntiDDos y Firewall.

- Conocimiento de TCP/IP y saber resolver problemas de tipologías de red captura de datos y paquetes de red.

La experiencia que debe tener un analista del SOC será la siguiente:

- Mínimo tres años de experiencia en seguridad informática.
- Tener las certificaciones o dominio de las prácticas de seguridad ISO 27001/27002, NIST, etc.
- Herramientas de gestión de riesgos como EAR/PILAR, CRAMM o EBIOS.
- Prácticas de configuración de servidores y de red.
- Profesional Gerente de Seguridad de la Información Certificado (CISM).
- Auditor Certificado del Sistema de Información (CISA).
- Certificado en arquitectura de seguridad (CISSP-ISSAP).

2.4.1.2. Administrador del SOC

Además de tener la experiencia de un analista de SOC deber poseer una personalidad de liderazgo, saber resolver problemas de tipologías de red, vulnerabilidades y riesgos. Además tener conocimiento pleno de dispositivos de seguridad y configuración de estos y saber múltiples lenguajes de programación como Python, Perl, java etc.

2.5. Procesos

Se requiere incorporar procesos claramente definidos con el fin de armonizar las herramientas, las habilidades y la metodología de las operaciones de seguridad para proporcionar una defensa detallada y proteger los activos de información críticos.

Cabe recalcar que todos los procesos realizados deben cubrir las mejores prácticas operacionales como son ITIL y COBIT mencionadas en el capítulo anterior.

2.5.1. Requerimientos de formalización de procesos

Se sugiere seguir los siguientes procesos detallados en la tabla 9.

Tabla 9

Requerimientos para formalización de procesos

COD	PROCESO	REQUERIMIENTO
01	Monitorización de seguridad y gestión de alertas de seguridad.	Procedimientos para la detección de eventos de seguridad, bajo esquemas de correlación de eventos (SIEM) y equipamiento de seguridad básico (Consola IPS, Firewall).
02	Gestión de incidentes.	Procedimiento que detalle las fases de notificación y la recepción de un incidente, clasificación, respuesta, análisis y resolución.
03	Gestión de amenazas y vulnerabilidades	Procedimientos para la Detección, Análisis, Tiempos de respuesta y Coordinación de Vulnerabilidades.
04	Monitoreo de red e infraestructura- NOC	Monitoreo de red e infraestructura, escalamiento y definición de tiempos de respuesta.
05	Evaluación / Gestión de calidad.	No se formalizará procesos, se formulará reportes bajo demanda.

Para solventar los requerimientos de cada proceso se realizará un inventario de procesos detallado a continuación en la tabla 10.

Tabla 10

Inventario de procesos

N°	Nombre del proceso	Servicio
01	Monitoreo de seguridad y gestión de alertas de seguridad.	- Registro de alertas y avisos de seguridad. - Reporte de desempeño de SIEM.
02	Gestión de incidentes	- Guías de decisión para gestionar varios tipos de incidentes. - Registro de incidente (Diario, semanal y mensual) - Informes de incidentes.
03	Gestión de amenazas y vulnerabilidades.	- Informe de análisis de riesgos. - Resultado de os protocolos de prueba. - Informe de pruebas y vulnerabilidades. - Planes de remediación.
04	Monitoreo de red e infraestructura- NOC	- Reporte de desempeño de equipos. - Reporte de revisión de logs de equipos. - Informe de monitoreo de red.
05	Evaluación /Gestión de calidad	- Formato de informe de pruebas. - Evaluación o certificación de la arquitectura.

2.5.2. Facilities

Para que los procesos puedan ser llevados a cabo de manera eficiente, es necesario tener comunicaciones unificadas entre los analistas del SOC, para ello es recomendable utilizar *facilities* como los sugeridos a continuación:

Utilizar una red telefónica privada por ejemplo 1800 SOCSOC (1800-762762); al marcar este número se escuchará una respuesta de voz interactiva (IVR) la cual puede dar las siguientes opciones:

Opción 1: Especialistas Nivel 1

Opción 2: Especialistas Nivel 2

Opción 3: Especialistas Nivel 3

La llamada automáticamente se direccionará a la línea telefónica según la elección requerida.

Una red telefónica se puede crear a través de una central telefónica o a través de la implementación de un IP Multimedia SubSystem (IMS) según convenga.

El proceso se muestra en la figura 6.

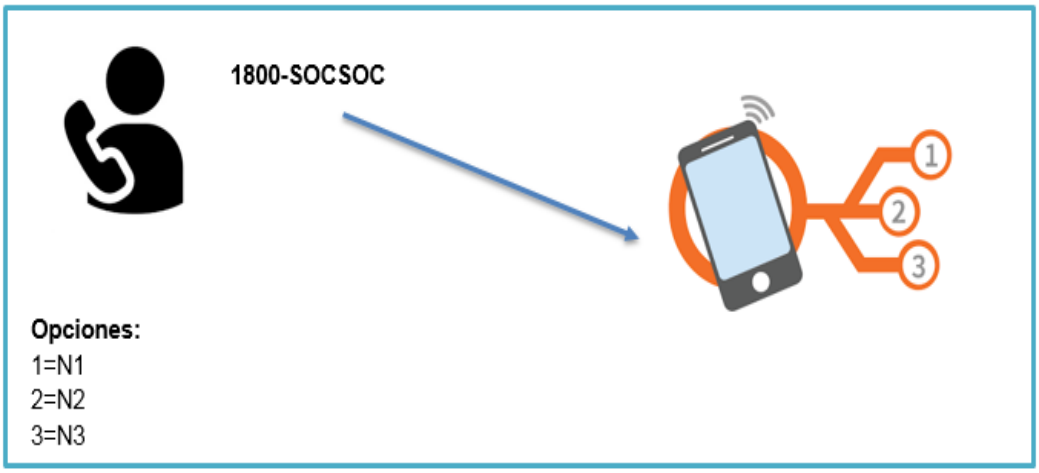


Figura 6. Facility para una red telefónica privada.

Otra manera de mantener las comunicaciones centralizadas es implementar un sistema de generación de tickets al momento que se lance una alerta de seguridad, así se podrá llevar un seguimiento de las incidencias de seguridad y de ser necesario escalarlas a los diferentes analistas de cada nivel. Esto se muestra en la figura 7.

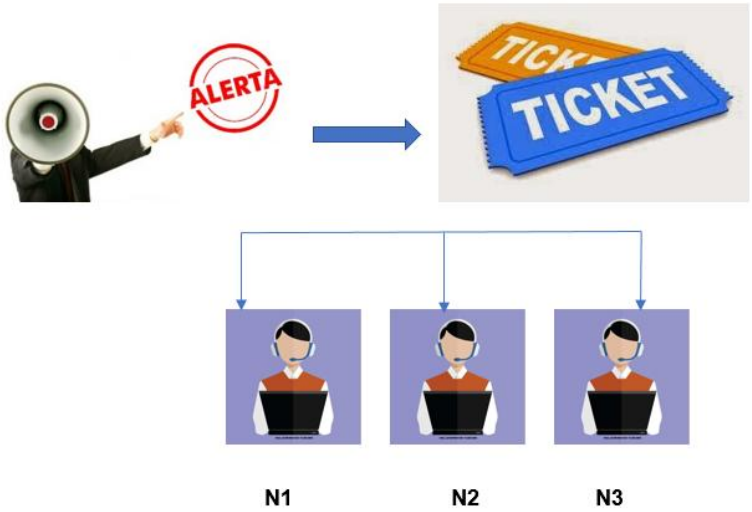


Figura 7. Procesos de generación de tickets.

2.6. Arquitectura

2.6.1. Modelo lógico

En la siguiente figura se muestra el modelo de funcionamiento que más se acopla a las necesidades de una empresa.

Como se puede observar en la figura 8, lo que se busca es centralizar todos los eventos dentro de un solo software que en este caso es el SIEM. Aquí llegarán todos los logs y las alertas provenientes tanto de los servicios como de los equipos de seguridad.

El SOC a la vez trabaja juntamente con el centro de operaciones de red NOC, el cual se encuentra monitorizando la conexión a la red y el estado de los servicios que se encuentran ahí.

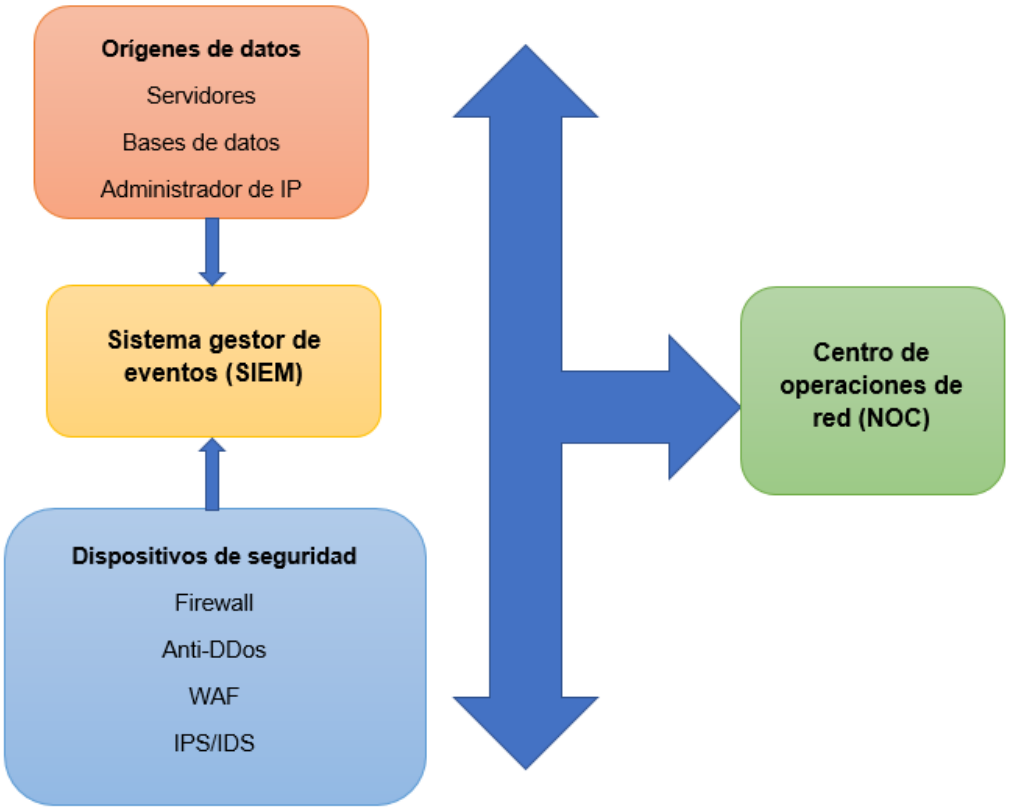


Figura 8. Diagrama lógico del SOC.

2.6.2. IP Planing

Una organización debe tomar en cuenta la planeación de las direcciones IP; no existe un estándar definido para esto ya que la red será planificada dependiendo del tamaño del centro y la cantidad de equipos con el que contará.

En este caso, se asignaron las siguientes direcciones IP detalladas en la tabla 11 para cada dispositivo que será utilizado.

Tabla 11

Tabla de asignación de direcciones IP.

Nombre	**Direcciones IP**
SIEM AlienVault	10.170.1.63; 10.170.1.66
Endian Firewall	10.170.1.61; 10.170.1.62
Snort IDS	10.170.1.64
WEB, DNS, Phpmyadmin	10.170.1.65

En la implementación del Firewall y el SIEM se han empleado dos tarjetas de red para su funcionamiento por lo tanto los mismos cuentan con dos direcciones IP.

2.7. Modelo físico

2.7.1. Equipos y herramientas sugeridas

Para definir los equipos necesarios para un centro de operaciones de ciberseguridad, primero hay que definir qué es lo que se quiere proteger y cómo se quiere proteger. (INEN, 2011).

Los equipos y herramientas descritos en la tabla 12, son una base sugerida para proveedores de servicios de internet que no solo quieran proteger sus activos, sino que también pretendan emprender proyectos de ciberseguridad

para otras organizaciones. Sin embargo, las empresas deben acoplarse a sus necesidades y tomar en cuenta su presupuesto disponible, por lo que es recomendable utilizar técnicas de ingeniería económica como son el VAN y el TIR para conocer qué tan factible puede ser un proyecto de implementación de un SOC tomando como referencia los costos descritos anteriormente.

Tabla 12

Descripción de equipos sugeridos

Descripción	**Cantidad**	**Fabricante**	**Modelo**
Anti DDoS	2	F5	VIPRION LTM C2400
Consola Administración FW	2	IBM	
Firewall	2	Checkpoint	12400
IPS	2	McAfee	M8000
WAF	2	F5	VIPRION LTM C2400
Enterprise Security Manager	1	McAfee	ETM-5600
Enterprise Log Manager	1	McAfee	ELM-5600
Event Receiver	1	McAfee	ERC-4600

Adicional, los equipos descritos en la tabla 12 fueron referencia de un proveedor de servicios de internet conocido en el país, el cual se encuentra emprendiendo proyectos de implementación de un centro de operaciones de seguridad para sí mismo y para sus clientes.

En la figura 9 se visualiza la arquitectura de un SOC. Es recomendable utilizar equipos de backup los cuales se conectan a través de una red MPLS y para equilibrar el trabajo se enlaza a un balanceador de carga. En la sección de monitoreo se muestran las diferentes consolas de administración donde los analistas llevan seguimiento de la red.

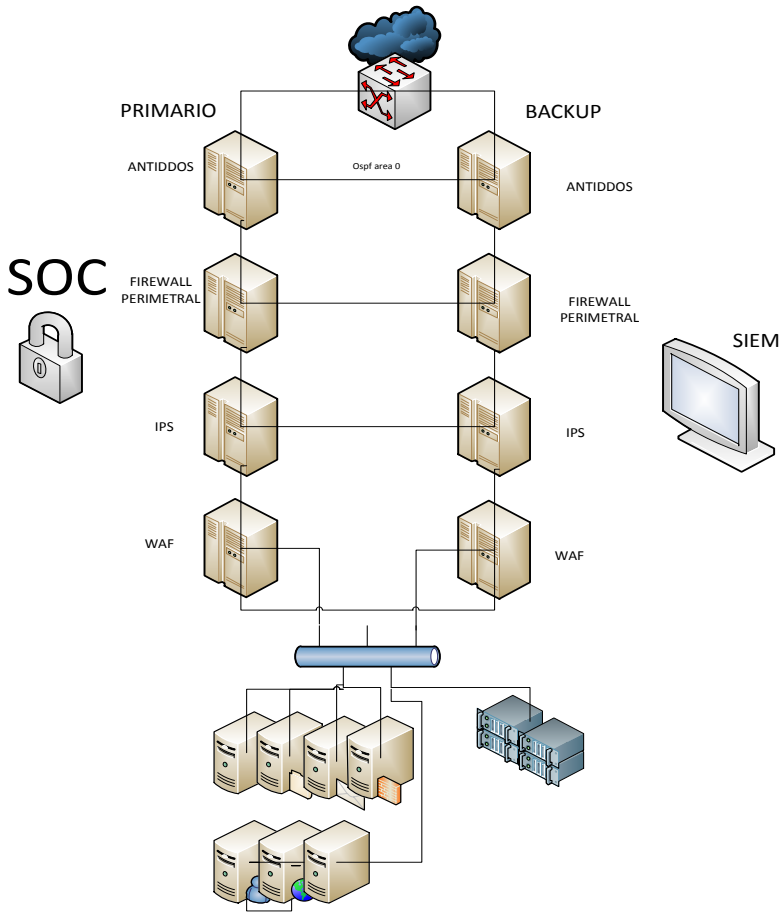


Figura 9. Diagrama físico del SOC.

3. CAPÍTULO III: ANÁLISIS DE VULNERABILIDADES Y ETHICAL HACKING

3.1. Análisis de vulnerabilidades

Se la conoce como una herramienta especial o un servicio que ayuda para la búsqueda y eliminación de las vulnerabilidades de seguridad de un sistema; además detecta áreas de mejora y propone una correcta arquitectura para proteger la infraestructura de una organización. (CeroUno Software Corportaivo, s.f).

Utilizando la herramienta SIEM Alien Vault se realizó un análisis de vulnerabilidades existentes en la red y se lograron encontrar las descritas en la tabla 13.

Tabla 13

Análisis de vulnerabilidades

Host	**Nivel de riesgo**	**Descripción**	**Solución**
10.170.1.61	Medio	El servidor remoto ssh está configurado para permitir algoritmos de cifrado débiles.	Deshabilitar algoritmos de cifrado débiles.
10.170.1.64	Medio	Se condujo un traceroute desde el servidor de escaneo hasta el sistema de destino. Este traceroute se proporciona principalmente con fines informativos únicamente. En la gran mayoría de los casos, no representa una vulnerabilidad. Sin embargo, si el traceroute que se muestra contiene direcciones privadas que no deberían haber sido públicamente visibles, entonces tiene un problema que debe corregir.	Bloquear paquetes no deseados.

10.170.1.65	Medio	El servidor web remoto contiene una imagen gráfica que es propensa a la divulgación de información.	Elimine el archivo 'favicon.ico' (ícono que aparece a la izquierda del nombre la página web) o cree uno personalizado para su sitio.

La ventaja de esta herramienta es que además de escanear los hosts de la red, también genera un reporte de las vulnerabilidades existentes y las posibles soluciones. En base a esto se podrán crear las políticas de seguridad correspondientes para cada vulnerabilidad. Las posibles causas de estas pueden ser las siguientes:

- La falta de implementación de políticas dentro del firewall como puede ser bloquear accesos al puerto 22.
- La escritura de claves demasiado fáciles para el ingreso a consolas de administración por lo que se recomienda establecer una política de claves seguras.

3.2. Ethical Hacking

3.2.1. Implementación de ethical hacking

La implementación de ethical hacking se realiza al atacar a los servicios ya implementados para encontrar las falencias de seguridad. Uno de los ataques que se realizó en este caso fue un embate de diccionario o de fuerza bruta utilizando un software Kali Linux; el mismo es un programa que ingresa a una

dirección IP específica y envía de manera aleatoria los posibles usuarios y claves de autenticación.

El ataque se muestra en la figura 10 a continuación.

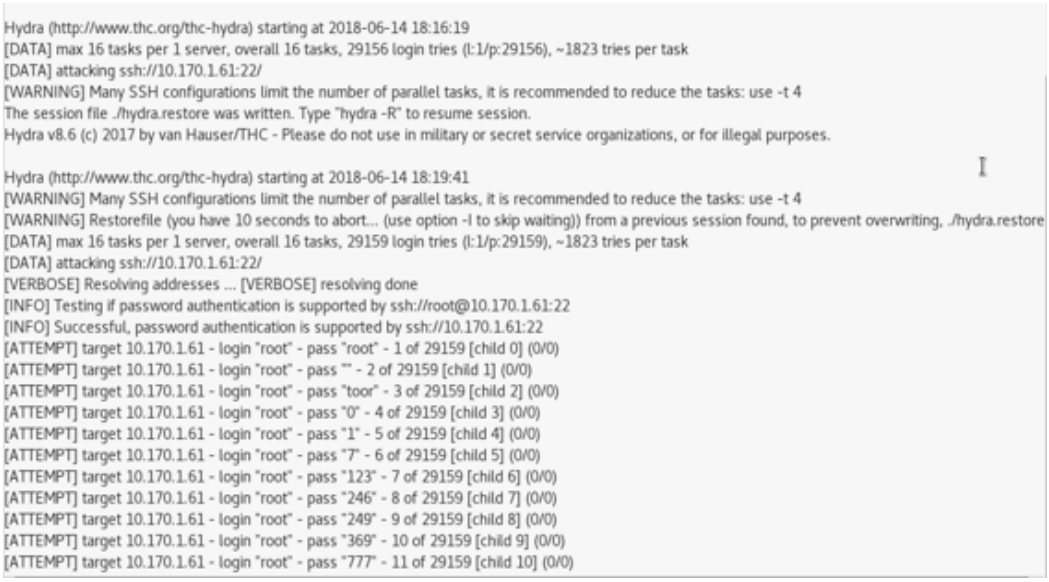
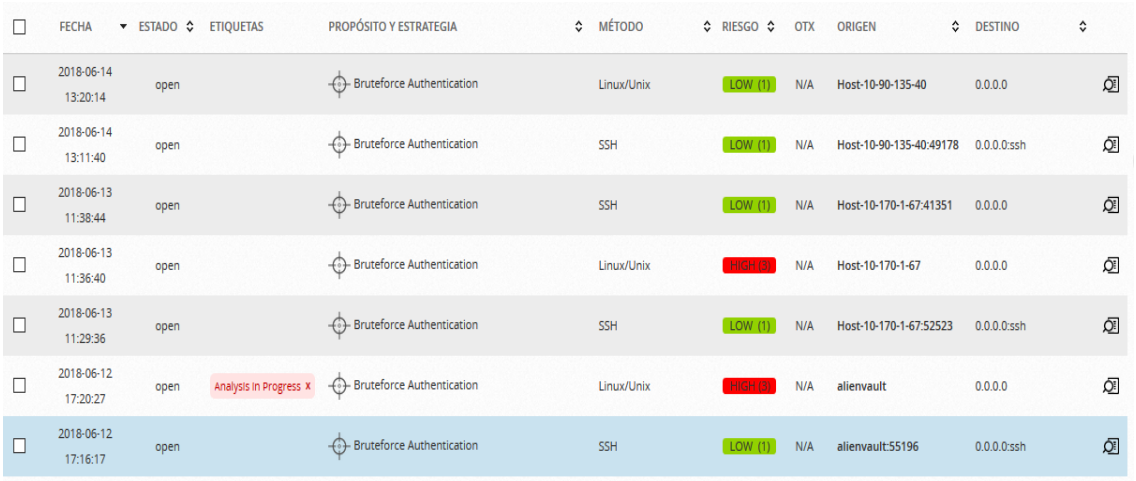


Figura 10. Ataque de diccionario

Este ataque se realizó en la dirección IP del firewall por el cual se intentó ingresar a través del puerto ssh. Esto provocó que la conexión remota que se tenía abierta se bloquee automáticamente debido a la cantidad de pedidos de login y generando varias alertas de un ataque de fuerza bruta en el SIEM. La figura 11 muestra las alarmas en la consola de administración.

Figura 11. Detección de ataque por el SIEM

La consola además cuenta con un monitoreo en tiempo real de todas las actividades que ocurren dentro de la red. Al momento de realizar el ataque de fuerza bruta se empezaron a generar varios logs de ingreso no autorizado, lo cual se puede observar en la figura 12.



FECHA	ESTADO	ETIQUETAS	PROPÓSITO Y ESTRATEGIA	MÉTODO	RIESGO	OTX	ORIGEN	DESTINO
2018-06-14 13:20:14	open		Bruteforce Authentication	Linux/Unix	LOW (1)	N/A	Host-10-90-135-40	0.0.0.0
2018-06-14 13:11:40	open		Bruteforce Authentication	SSH	LOW (1)	N/A	Host-10-90-135-40:49178	0.0.0.0:ssh
2018-06-13 11:38:44	open		Bruteforce Authentication	SSH	LOW (1)	N/A	Host-10-170-1-67:41351	0.0.0.0
2018-06-13 11:36:40	open		Bruteforce Authentication	Linux/Unix	HIGH (3)	N/A	Host-10-170-1-67	0.0.0.0
2018-06-13 11:29:36	open		Bruteforce Authentication	SSH	LOW (1)	N/A	Host-10-170-1-67:52523	0.0.0.0:ssh
2018-06-12 17:20:27	open	Analysis In Progress	Bruteforce Authentication	Linux/Unix	HIGH (3)	N/A	alienvault	0.0.0.0
2018-06-12 17:16:17	open		Bruteforce Authentication	SSH	LOW (1)	N/A	alienvault:55196	0.0.0.0:ssh

Figura 12. Logs por ataque de fuerza bruta

Los eventos ocurridos se guardan en la memoria de Alien Vault y van generando reportes de los mismos de manera automática. Esto ayuda a conocer diariamente el estado de la red. La figura 13 muestra un reporte estadístico del ataque realizado. Aquí se observa que describe la alarma como un embate de fuerza bruta e identifica los dos medios por los que se hizo el mismo, un software Linux a través del puerto ssh y el número de ocurrencias del ataque.

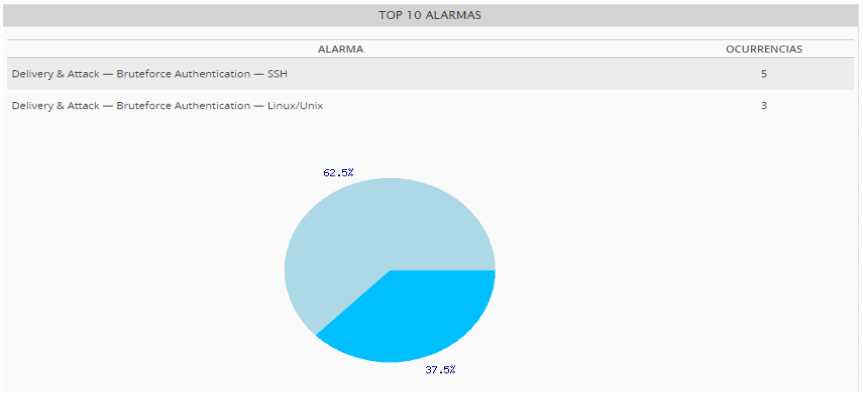


Figura 13. Reporte de alarmas

3.3. Documentos entregables

Después de realizar un análisis de vulnerabilidades y ethical hacking es necesario hacer los respectivos informes para de esta manera tomar las decisiones correspondientes acerca de la seguridad de la red dentro de una empresa. Los documentos sugeridos que se deben entregar son los siguientes:

3.3.1. Solicitudes de servicio

a. Formato de Solicitud de desempeño de equipos (SIEM, IPS, FIREWALL, SERVIDORES).
b. Formato de reporte de desempeño de equipos.
c. Formato de solicitud de revisión de LOGS de equipos.
d. Formato de reporte de revisión de LOGS de equipos.

3.3.2. Análisis de riesgos

a. Informe de Análisis de Riesgos.
b. Resultado de los protocolos de prueba.
c. Informe de Pruebas de Vulnerabilidades.
d. Planes de Remediación.

4. CAPÍTULO IV: PRUEBAS Y RESULTADOS

4.1. Generalidades

Para el cumplimiento de los objetivos planteados, es necesario realizar pruebas de simulación de un SOC dentro del data center experimental de la Universidad De Las Américas. Aquí se procede a subir máquinas virtuales de un firewall, IDS, SIEM y un servidor web; las mismas se virtualizan en VMware y se suben con un formato OVF. Las configuraciones realizadas en las máquinas virtuales se muestran en la tabla 14.

Tabla 14

Especificaciones de máquinas virtuales

Nombre	Tipo	RAM	Disco y número de procesadores	Sistema Operativo
Snort	IDS	2 GB	20 GB y un procesador	Linux Ubuntu
Endian	Firewall	2GB	20 GB y un procesador	Linux Debian
Alien Vault	SIEM	13 GB	50 GB y cuatro procesadores	Linux Debian
Apache, PHPmyadmin	Web Server, Base de datos	2 GB	20 GB y un procesador	Linux Ubuntu

Una vez configuradas las máquinas virtuales, se crean 3 archivos los cuales se suben en la plataforma del hipervisor, los servicios deben estar funcionales como muestra la figura 14.

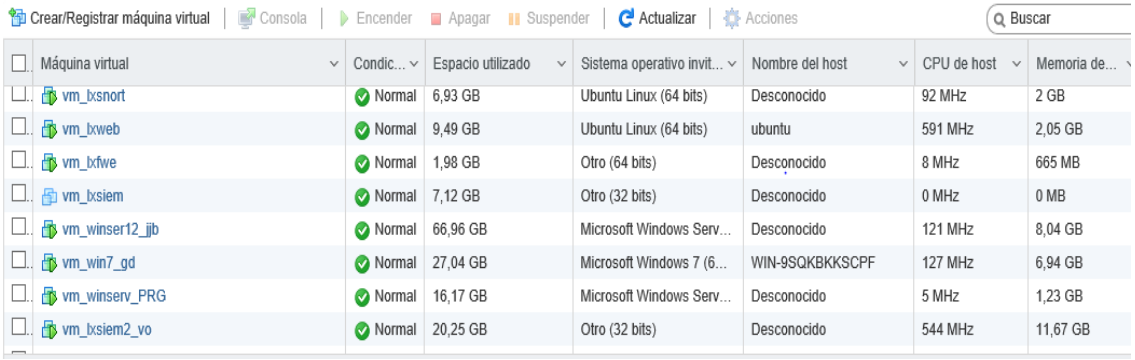


Figura 14. Servicios funcionando en el hipervisor.

4.1.1. Arquitectura de la implementación

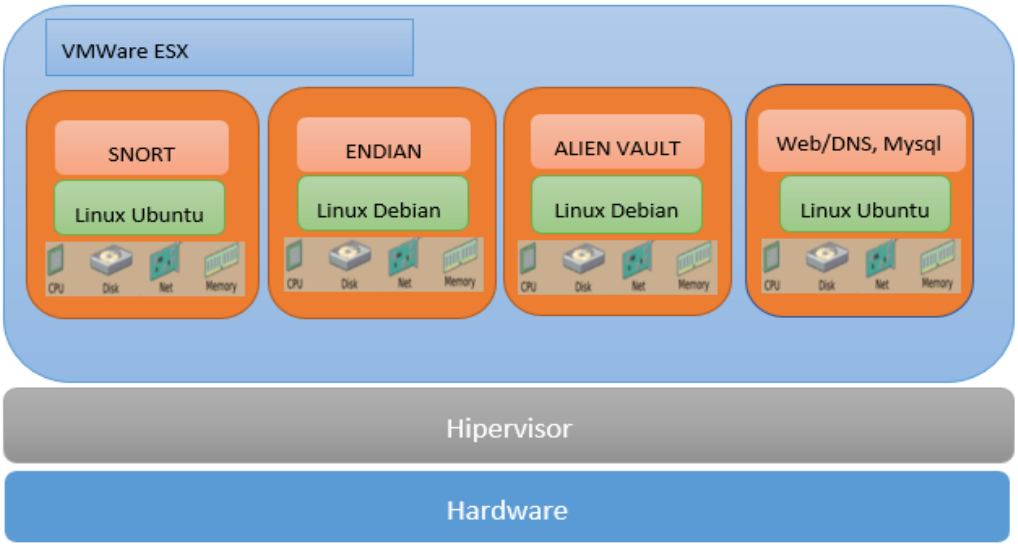


Figura 15. Arquitectura de implementación.

En la figura 15 se muestra la arquitectura utilizada para realizar las pruebas de simulación, en las que se utilizan máquinas virtuales montadas sobre un hipervisor, cada una de estas tendrá instalado el servicio ssh que permitirá facilitar la administración de estas.

4.1.2. Pruebas con Endian firewall

Endian firewall puede tener hasta 4 tarjetas de red para dividir el tráfico, esto quiere decir que se distribuirán cada una de estas para cada red como puede ser la LAN, WAN, los DMZ, y la última se puede utilizar para otro propósito como otra LAN. En el proyecto solo se utilizó 2 tarjetas las cuales fueron una para la WAN y la otra para la LAN. La figura 16 muestra la arquitectura de Endian Firewall.

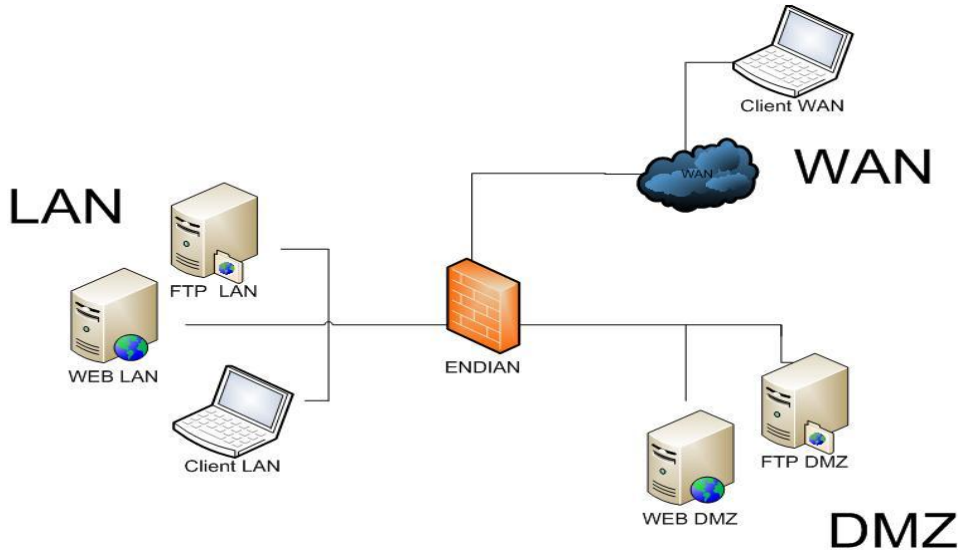


Figura 16. Arquitectura de Endian firewall

Endian Firewall cuenta con una consola de administración web, aquí se muestra el estado del tráfico en la red. En la figura 17 se ve claramente como está definida la red por colores así se define la red LAN en verde la WAN en azul y los DMZ en naranja es así como se diferencia cada una y se puede validar el tráfico por estos colores también se puede ver las políticas y las reglas de permisos para habilitar el tráfico.

Figura 17. Configuraciones de la red en el firewall

En la figura 18 se indica cómo crear las reglas dentro del firewall una vez definidas las redes, se crea en el lado izquierdo la red de origen (se puede definir también solo una IP o un host o toda la red) y por el lado derecho la IP de destino, en la parte de abajo se puede escoger el puerto a denegar o permitir es así como una vez aceptados los cambios se agregará la regla al sistema y hará lo que se le indique.

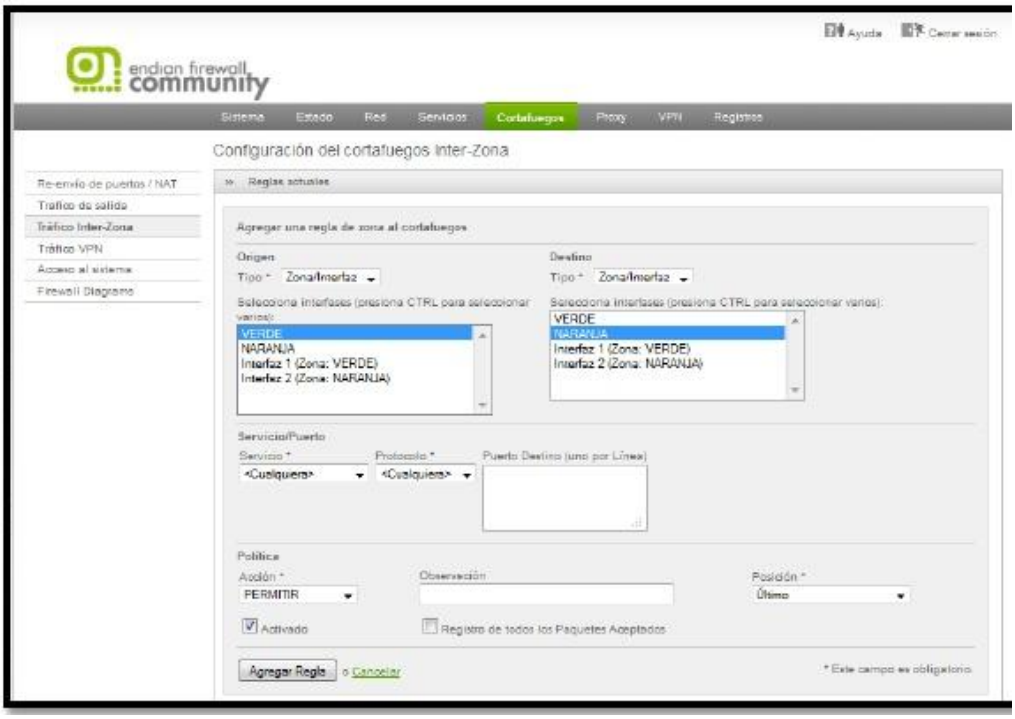


Figura 18. Creación de reglas

4.1.3. Pruebas con IDS Snort

Un ataque de denegación de servicio es algo que se puede identificar por medio de IDS Snort. Uno de los ataques más conocidos es el ping de la muerte el cual realiza un acuse de envío y recibo que puede causar el colapso de un servicio o de la red.

Se evidenció el funcionamiento de snort por medio de un ping de la muerte hacia una IP activa y el resultado fue una alerta como la que se muestra en la figura 19. Aquí se puede observar una alerta ICMP donde la IP 10.90.16.147 pertenece a la máquina que realizó el ataque y 10.170.1.64 es la IP de destino.

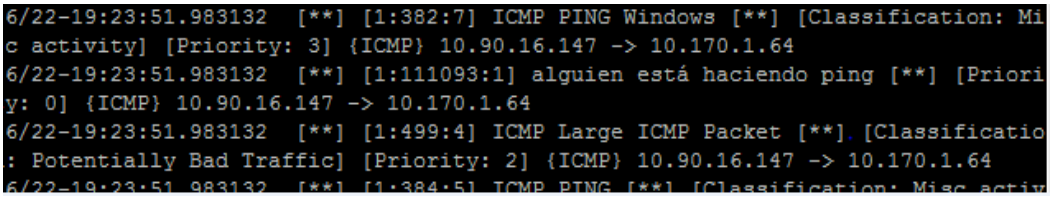


Figura 19. Alarma generada por ping de la muerte

El IDS también viene por default configurado para lanzar una alerta en caso de que alguien se encuentre escaneado las direcciones IP de una red. Se realizó una prueba utilizando un programa llamado Advanced IP Scanner.

El resultado de esta prueba se puede ver en la figura 20.

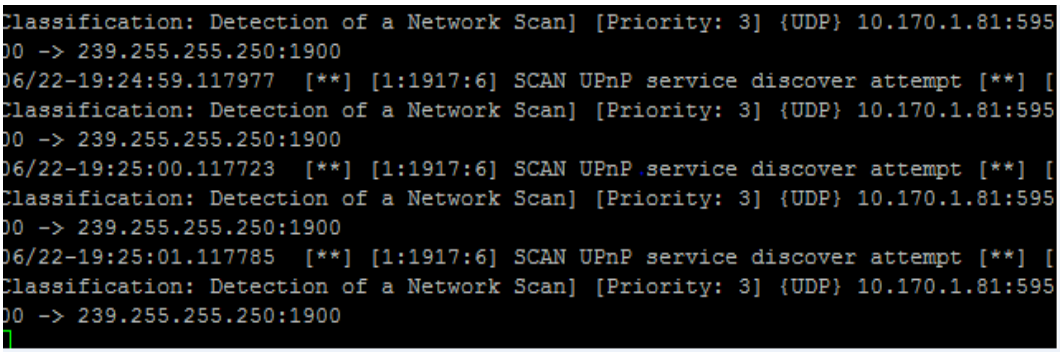


Figura 20. Alerta generada por el analizador de IP.

La alerta que se generó fue de tipo Scan UPnP, lo cual significa que alguien está tratando de descubrir las IP activas en determinada red local por medio de un analizador *Universal Plug and Play* (UPnP).

Como punto adicional, mientras se configuraba el SIEM, este realizó un escaneo de las redes existentes y se pudo observar que el IDS lanzó una alerta diferente. Esta se puede ver en la figura 21.

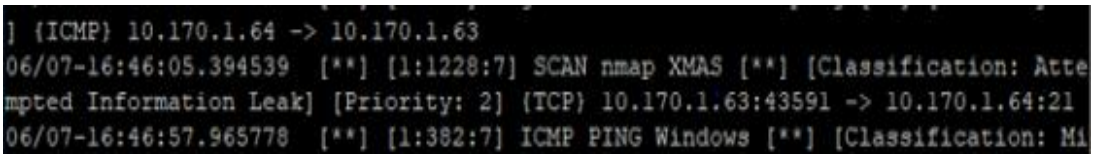


Figura 21. Alerta generada por el SIEM.

Si se compara con la alerta de la figura 20, se observa que no es la misma, sino que es un avizor de tipo Scan nmap XMAS. Este tipo de escaneos diferencia entre los puertos abiertos o cerrados de una red. En los puertos

abiertos se extrae la información del sistema conectado a ese puerto y es lo que colecta el SIEM.

En este caso este tipo de alarma no es de alto riesgo ya que se trata del sistema de monitoreo utilizado en la simulación. Sin embargo, en la realidad si se debe tener mucha precaución con este tipo de alarmas.

4.1.4. Pruebas con SIEM Alien Vault

Después de la instalación se observa que no se tiene una consola con código sino un menú en el cual se puede se pude seleccionar y cambiar la configuración cada vez que se desee. La figura 22 indica la consola.

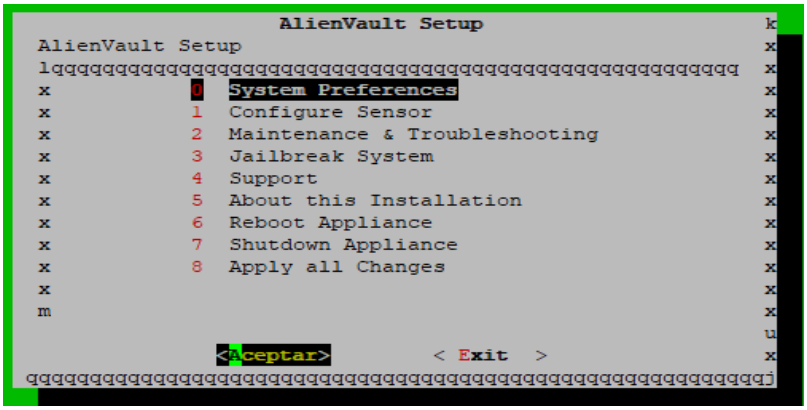


Figura 22. Consola de ALIEN VAULT OSSIM

Alien Vault OSSIM se administra a través de una consola web a la cual una vez ingresada se debe realizar las configuraciones iniciales. Como se mencionó anteriormente, el SIEM necesita dos tarjetas de red donde una es para administración y otra servirá para la recolección de logs.

En la figura 23 se puede ver cómo se configuran las 2 tarjetas de red.

Figura 23. Administración de tarjetas de red del SIEM

A continuación, se debe apuntar los servidores a la tarjeta que recibe los logs con la dirección IP. Una vez realizado esto se debe configurar los dispositivos que se va a detectar, en este caso se puede evidenciar en la figura 24 los dispositivos configurados.

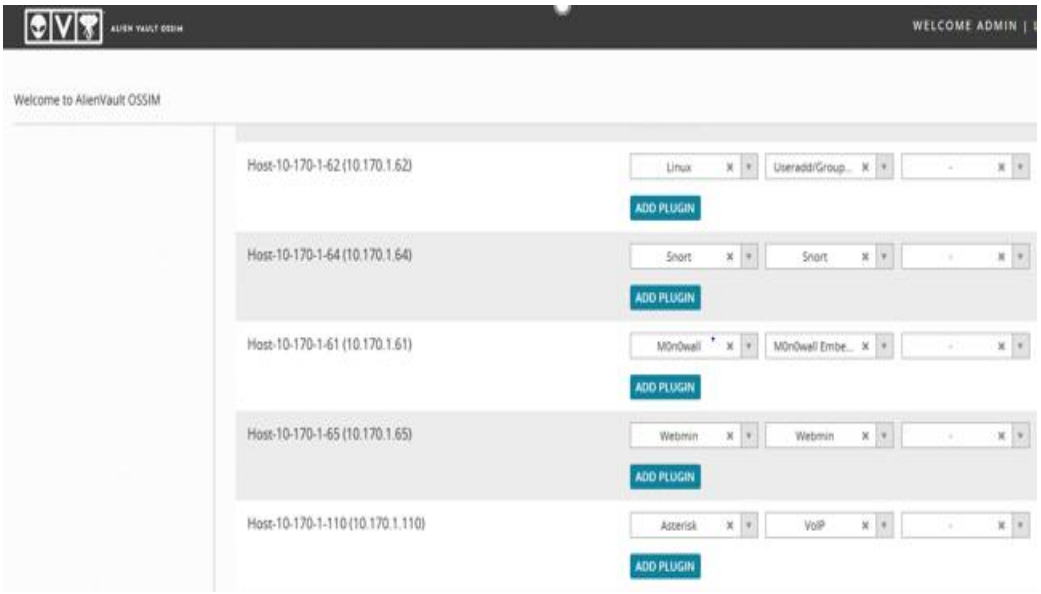


Figura 24 .Configuración de dispositivos

Terminada la configuración se necesita habilitar los plugins de cada servicio que se va a implementar, esto se realiza mediante consola y se empieza a administrar cada log que ingrese por la tarjeta de recolección en la figura 25 se puede ver la activación de los plugins.

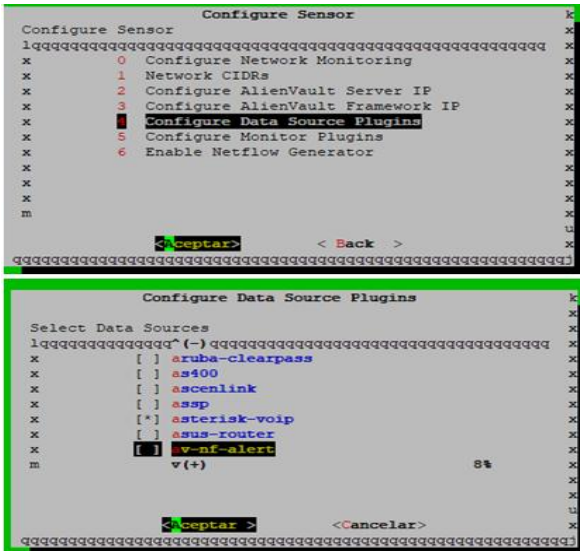


Figura 25. Plugins activos

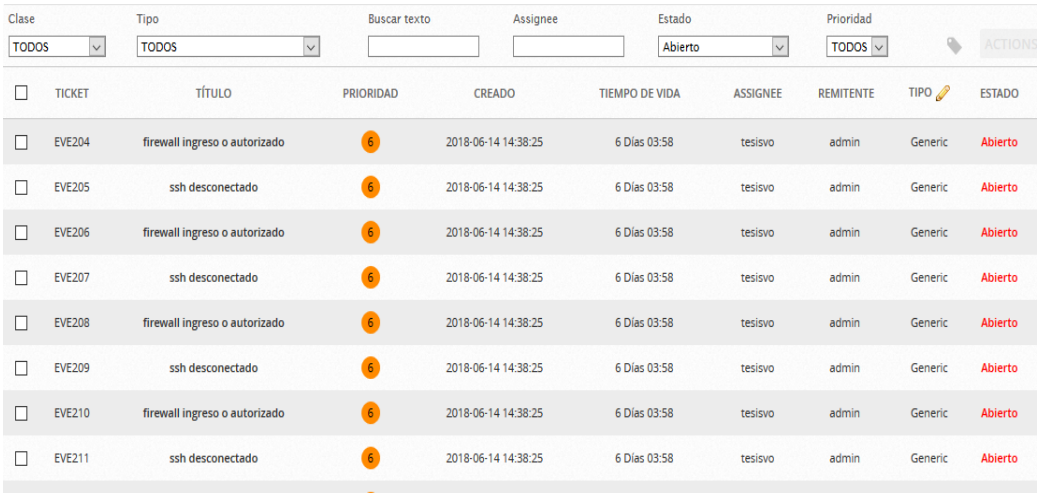
Una vez terminada la configuración, se realiza la detección de los eventos en la aplicación web de la herramienta en la cual se pueden validar los syslogs, los eventos fallidos y posibles ataques.

En el capítulo anterior se realizó un ataque que intentó realizar un login al firewall por medio de ssh, como la consola muestra eventos en tiempo real estos se lograron registrar como muestra la figura 26.

Figura 26. Eventos generados por Alien Vault SIEM.

Para facilitar la administración de los eventos de seguridad es necesario crear tickets que ayuden a clasificar los ataques. El SIEM tiene habilitada esta solución por lo que se hizo una prueba programando que un ticket se abra automáticamente si alguien intenta autenticarse en la consola de firewall. Al

momento de realizar el ataque mencionado en el capítulo anterior, se generó lo siguiente en la interfaz de alarmas de la figura 27.



Clase: TODOS | Tipo: TODOS | Buscar texto | Assignee | Estado: Abierto | Prioridad: TODOS | ACTIONS

TICKET	TÍTULO	PRIORIDAD	CREADO	TIEMPO DE VIDA	ASSIGNEE	REMITENTE	TIPO	ESTADO
EVE204	firewall ingreso o autorizado	6	2018-06-14 14:38:25	6 Días 03:58	tesisvo	admin	Generic	Abierto
EVE205	ssh desconectado	6	2018-06-14 14:38:25	6 Días 03:58	tesisvo	admin	Generic	Abierto
EVE206	firewall ingreso o autorizado	6	2018-06-14 14:38:25	6 Días 03:58	tesisvo	admin	Generic	Abierto
EVE207	ssh desconectado	6	2018-06-14 14:38:25	6 Días 03:58	tesisvo	admin	Generic	Abierto
EVE208	firewall ingreso o autorizado	6	2018-06-14 14:38:25	6 Días 03:58	tesisvo	admin	Generic	Abierto
EVE209	ssh desconectado	6	2018-06-14 14:38:25	6 Días 03:58	tesisvo	admin	Generic	Abierto
EVE210	firewall ingreso o autorizado	6	2018-06-14 14:38:25	6 Días 03:58	tesisvo	admin	Generic	Abierto
EVE211	ssh desconectado	6	2018-06-14 14:38:25	6 Días 03:58	tesisvo	admin	Generic	Abierto

Figura 27. Tickets generados en el SIEM.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Los factores económicos son muy importantes para la implementación de un SOC, por lo que virtualizar los servicios brinda menor costo y ocupa menores recursos de los sistemas. También es posible instalar servicios de código abierto para evitar costos de licenciamiento; esto depende del tamaño de la empresa y las características del software. Al momento de analizar los equipos físicos se pudo observar que los mismos son de mayor costo y que el firmware necesita actualizaciones para su correcto funcionamiento, si los ISP's son empresas grandes y líderes en el país pueden optar por adquirir equipos físicos con software licenciado.

La solución permite la administración de los activos de una empresa de manera centralizada. La misma ayudará a los analistas de un SOC a conocer las alertas de seguridad generadas y poder actuar de una manera más óptima y eficiente frente a las brechas de seguridad de una organización.

Hoy en día los ataques informáticos son mucho más complejos, por esto necesitan la ayuda de sistemas que los puedan controlar, no obstante, también necesitan personas que sean expertos en análisis de herramientas de seguridad de redes para así llevar un mejor control de la red.

Los softwares escogidos son consolas de administración fáciles de utilizar en la realización de las pruebas de simulación y como tienen interfaz gráfica también son cómodas para realizar la programación de las mismas.

Las empresas que decidan tener este tipo de sistema van a lograr tener mayor control de sus redes y bajara su impacto en cuanto a las vulnerabilidades que los asechen.

5.2. Recomendaciones

Se recomienda tomar en cuenta las siguientes sugerencias para un correcto funcionamiento del centro de operaciones de ciberseguridad, basado en los problemas que se presentaron a lo largo de la realización de este proyecto.

Se debe considerar los requisitos previos de cada uno de los componentes del SOC ya que muchos de ellos necesitan mayor procesamiento y memoria RAM.

Los ambientes virtuales se han convertido en una tendencia ya que la misma ahorra costos de implementación y de espacio para dispositivos, por lo que si es factible se debe implementar un SOC de manera virtual aprovechando los beneficios del mismo. Por otro lado, si es necesaria la implementación de equipos debido al tamaño de la red, tomar en cuenta que los mismos necesitan actualizaciones cada cierto tiempo y además se requiere planificar mantenimiento de dispositivos para asegurar el alto rendimiento y disponibilidad del SOC.

REFERENCIAS

AlienVault. (2018). *Allien Vault Ossim.* Recuperado el 23 de marzo de 2018 de https://www.alienvault.com/products/ossim

APPROACH. (2018). *Centro de operaciones de seguridad.* Recuperado el 26 de marzo de 2018 de https://www.approach.be/en/soc-analyst.html

Bonini, E. (2014). *Creación de un centro de operaciones de seguridad.* Recuperado el 18 de marzo de 2018 de https://es.slideshare.net/DiegoBonini1/creacion-de-un-centro-de-operaciones-de-seguridad

CCNA. (2013). *Introduccion a la cyberseguridad*. Recuperado el 12 de mayo de 2018 de https://static-course-assets.s3.amazonaws.com/CyberSec2/es/index.html#2.1.3.1

CCNA. (2015). *Introduccion a la cyberseguridad.* Recuperado el 12 de mayo de 2018 de https://static-course-assets.s3.amazonaws.com/CyberSec2/es/index.html#2.1.1.1

CCNA. (2015). *Introducion a la cyberseguridad*. Recuperado el 13 de mayo de 2018 de https://static-course-assets.s3.amazonaws.com/CyberSec2/es/index.html#2.1.3.1

CeroUno Software Corportaivo. (s.f). *¿Qué es un análisis de vulnerabilidades informáticas?* Recuperado el 16 de mayo de 2018 de http://blog.cerounosoftware.com.mx/que-es-un-analisis-de-vulnerabilidades-inform%C3%A1ticas

certsi. (2017). *Diseño y configuración de IPS, IDS y SIEM en sistemas de control industrial.* Recuperado el 15 de abril de 2018 de https://www.certsi.es/sites/default/files/contenidos/guias/doc/certsi_diseno_configuracion_ips_ids_siem_en_sci.pdf

Cisco. (s.f). *¿Qué es un firewall?* Recuperado el 16 de abril de 2018 de https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Cloud Security Services. (2013). *WAF: Web Application Firewall.* Recuperado el 29 de marzo de 2018 de https://hacking-etico.com/2013/01/28/waf-web-aplication-firewall/

Cogeco. (2017). *El coste de los ataques de DDos*. Recuperado el 25 de abril de 2018 de https://www.cogecopeer1.com/wp-content/uploads/2017/03/calculando-los-costos-de-ataques-ddos-servicios-ddos-documentotecnico-pdf.pdf

CUVIV. (2016). *newsletter*. *Fundamentos de la gestión de TI.* Recuperado el 17 de abril de 2018 de http://www.cuviv.com/newsletter/newsletters_cuviv_files/newsletter_agosto_cuviv.pdf

Deloitte Ecuador. (2017). S*eguridad de la informacción en Ecuador.* Recuperado el 20 de marzo 2018 de https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/deloitte-analytics/Estudios/SeguridadInformacion2017.pdf

Díaz, J., & Salcedo, J. (2014). *Sistema de Prevención de Intrusos para mejorar la seguridad de los servidores de*. Recuperado el 23 de abril de 2018 de http://www.inf.unitru.edu.pe/revistas/2014/6.pdf

EMC2. (2013). *Resumen tecnico RSA*. Recuperado el 18 de mayo de 2018 de https://peru.emc.com/collateral/technical-documentation/h11533-intelligence-driven-security-ops-center.pdf

Enagas. (2013). *Politicas de ciberseguridad.* Recuperado el 23 de mayo de 2018 de http://www.enagas.es/stfls/ENAGAS/Documentos/Pol%C3%ADtica%20de%20ciberseguridad.pdf

EY Entono de negocios. (2013). *Centro de Operaciones de seguridad contra el crimen*. Recuperado el 25 de marzo de 2018 de http://www.ey.com/Publication/vwLUAssets/EY-Centros-de-Operaciones-Seguridad-crimen-cibernetico/$FILE/EY-Centros-de-Operaciones-de-Seguridad.pdf

F5 Silverline. (s.f). *Web Application Firewall.* Recuperado el 29 de mayo de 2018 de https://www.f5.com/pdf/products/f5-silverline-web-application-firewall-datasheet.pdf

Foro Económico Mundial. (2018). *Informe global de riesgos.* Recuperado el 26 de marzo de 2018 de http://reports.weforum.org/global-risks-2018/files/2018/01/Global-Risk-Report-2018-Executive-Summary-Spanish.pdf&embedded=true

García. (2013). *Hacking y seguridad en Internet.* Bogotá: Ediciones de la U.

Gartner. (2017). *Magic Quadrant for Security Information and Event Management*. Recuperado el 30 de marzo de 2018 de https://www.gartner.com/doc/reprints?id=1-4JMUB31&ct=171031&st=sb

GMS. (2018). *Gms Seguridad SOC*. Recuperado el 20 de marzo de 2018 de https://gmsseguridad.com/SOC.html

Gómez, Á. (2013). *Enciclopedia de la seguridad informática.* México: AlfaOmega.

Hacker, C. E. (2013). *Certified Ethical Hacker Review Guide*. Recuperado el 26 de marzo de 2018 de http://www.it-docs.net/ddata/863.pdf

Hacking. (2013). *Introducción al hacking ético y sistemas de redes*. Recuperado el 16 de mayo de 2018 de http://ucys.ugr.es/download/taller1/Taller1_Intro_hacking.pdf

Hoyos, V. (2015). *¿Qué tal esta Colombia en cuestión de ciberseguridad?* Recuperado el 23 de marzo de 2018 de https://repository.unimilitar.edu.co/bitstream/10654/7794/1/Qu%C3%A9

%20tal%20esta%20Colombia%20en%20cuesti%C3%B3n%20de%20ciberseguridad.pdf

Imperva. (2017). *SecureSphere Web Application Firewall.* Recuperado el 28 de abril de 2018 de https://www.imperva.com/docs/DS_SecureSphere_Web_Application_Firewall.pdf

INEN. (2011). *Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27001:2011.* Quito: Primera edición.

Infosegur. (2013). *Conceptos basicos de la seguridad informatica.* Recuperado el 18 de mayo de 2018 de https://infosegur.wordpress.com/tag/vulnerabilidades/

Ingenia. (2018). *Centro de operaciones de seguridad (eSOC)*. Recuperado el 31 de marzo de 2018 de https://www.ingenia.es/es/servicio/centro-de-operaciones-de-seguridad-esoc

Instituto de auditores internos de España. (2016). *Buenas prácticas en gestión de riesgos*. Recuperado el 21 de marzo de 2018 de https://auditoresinternos.es/uploads/media_items/guia-supervision-ciberseguridad-fabrica-pensamiento-iai.original.pdf

Kaspersky. (2018). *¿Qué es un firewall?* Recuperado el 17 de abril de 2018 de https://latam.kaspersky.com/resource-center/definitions/firewall

Katz, M. (2015). *Redes y seguridad.* Buenos Aires: AlfaOmega.

López, E. (2017). *Pruebas de penetración en aplicaciones web usando hacking ético.* Recuperado el 19 de abril de 2018 de http://redicces.org.sv/jspui/bitstream/10972/3018/1/Articulo2.pdf

Lujan, U. (2014). *Amenazas de seguridad de la información.* Recuperado el 18 de abril de 2018 de http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Márquez, J. (2014). *Modelos ITIL y Cobit.* Recuperado el 30 de marzo de 2018 de https://es.slideshare.net/skyburn/cobit-itil-38308372

Martínez, S. (s.f). *ITIL.* Recuperado el 30 de marzo de 2018 de http://materias.fi.uba.ar/7546/material/ITIL%20v2.0.pdf

Mentor, a. (2013). *Vulnerabilidades de un sistema informatico*. Recuperado el 14 de abril de 2018 de http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/vulnerabilidades_de_un_sistema_informtico.html

Networkworld. (s.f). *Prevención de intrusiones.* Recuperado el 16 de abril de 2018 de http://www.networkworld.es/seguridad/prevencion-de-intrusiones

Odom, W. (2010). *CCNA ICDN2 Guía general para el examen de certificación.* Madrid: Pearson Education.

Oracle. (2010). *¿Cómo diseñar un sistema de direcciones IPv4?* Recuperado el 16 de mayo de 2018 de https://docs.oracle.com/cd/E19957-01/820-2981/ipplan-5/index.html

Pico, F. (2016). *SIEM bajo software libre para la seguridad operacional en las pymes de la ciudad de Pelileo*. Recuperado el 2 de abril de 2018 de http://dspace.uniandes.edu.ec/bitstream/123456789/4691/1/PIUAMIE003-2016.pdf

Portal Akamai. (2018). *Avisos sobre amenazas más recientes.* Recuperado el 18 de marzo de 2018 de https://www.akamai.com/es/es/about/our-thinking/state-of-the-internet-report/

Portal Arbor Networks. (s.f). *Arbor DDoS Protection.* Recuperado el 31 de marzo 2018 de https://www.arbornetworks.com/ddos-protection-products

Portal BlueHosting. (2016). *Introducción a ataque DDOS y método Anti-DDos*. Recuperado el 31 de marzo de 2018 de https://docs.bluehosting.cl/tutoriales/conocimientos-generales/introduccion-a-los-ataques-ddos-y-metodos-anti-ddos.html

Portal FraudWatch International. (2018). *Taking down phishing in banking.* Recuperado el 5 de mayo de 2018 de https://fraudwatchinternational.com/phishing/taking-down-phishing-in-banking/

Portal Imperva Incapsula. (2017). *Paraliza ataques Anti-DDoS.* Recuperado el 5 de abril de 2018 de https://pages.incapsula.com/ddos-protection-spanish/?utm_source=google-ppc-sa&utm_medium=cpc&utm_term=%7Bkeyword%7D&utm_campaign=7A-DDoS-Protection-Search-Spanish-Worldwide&placement=7A-DDoS-Protection-Search-Spanish-Worldwide&gclid=Cj0KCQjw5LbWBRDCARIsAL

Portal Nextech. (s.f). *¿Qué es COBIT y para qué sirve?* Recuperado el 7 de abril de 2018 de https://nextech.pe/que-es-cobit-y-para-que-sirve/

Portal Protegerse. (2016). *¿Que sabemos del ataque ddos que dejó algunos servicios de internet al borde del colapso?* Recuperado el 10 de abril de 2018 de https://blogs.protegerse.com/2016/10/24/que-sabemos-del-ataque-ddos-que-dejo-algunos-servicios-de-internet-al-borde-del-colapso/

Ramos, A. (2015). *Hacking y seguridad de páginas web.* Bogotá: Ediciones de la U.

Secureit. (2015). *Los Beneficios del hacking ético para las empresas.* Recuperado el 19 de mayo de 2018 de https://www.secureit.es/los-beneficios-del-hacking-etico-para-las-empresas/

SIMPLYHIRED. (2017). *Business Intelligence Analyst jobs near Burnley.* Recuperado el 18 de mayo de 2018 de https://www.simplyhired.co.uk/search?q=business+intelligence+analyst&l=burnley&job=ZkrPQGrvvhyPYWzHUJ7sh7X6gtbTXXKd_UVYN7PEEKNQzIYBJff0Gg

Telefónica. (s.f). *Acens Technologies. ¿Qué es el phishing y como protegerse?* Recuperado el 14 de abril de 2018 de https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf

UDESIGN. (2015). *Criterios de evaluación cuadrante mágico de Gartner*. Recuperado el 9 de abril de 2018 de https://incared.net/criterios-de-evaluacion-cuadrante-magico-de-gartner/

UNAM. (2017). *Firewall de bases de datos*. Recuperado el 20 de mayo de 2018 de https://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos

ANEXOS

ANEXO 1

Objetivos de control y controles

Tabla A.1

A.5. Política de seguridad		
A.5.1 Política de seguridad de la información **Objetivo: La dirección proporcionará indicaciones y dará apoyo a la seguridad de la información de acuerdo con los requisitos del negocio y con la legislación y las normativas aplicables.**		
A.5.1.1	Documento de política de seguridad de la información.	Control La dirección debe aprobar un documento de política de seguridad de la información, publicarlo y distribuirlo a todos los empleados y terceros afectados.
A.5.1.2	Revisión de la política de seguridad de la información.	Control La política de seguridad de la información debe revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
A.6. Aspectos organizativos de la seguridad de la información		
A.6.1. Organización interna **Objetivo: Gestionar la seguridad de la información dentro de la organización.**		
A.6.1.1	Compromiso de la Dirección con la seguridad de la información.	Control La Dirección debe prestar un apoyo activo a la seguridad dentro de la organización a través de directrices claras, un compromiso demostrado, asignaciones explícitas y el

		reconocimiento de las responsabilidades de seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información.	Control Las actividades relativas a la seguridad de la información deben ser coordinadas entre los representantes de las diferentes partes de la organización con sus correspondientes roles y funciones de trabajo.
A.6.1.3	Asignación de responsabilidades relativas a la seguridad de la información.	Control Deben definirse claramente todas las responsabilidades relativas a la seguridad de la información.
A.6.1.4	Proceso de autorización de recursos para el tratamiento de la información.	Control Para cada nuevo recurso de tratamiento de la información, debe definirse a implantarse un proceso de autorización por parte de la Dirección.
A.6.1.5	Acuerdos de confidencialidad.	Control Debe determinarse y revisarse periódicamente la necesidad de establecer acuerdos de confidencialidad o no revelación, que reflejen las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con las autoridades.	Control Deben mantenerse los contactos adecuados con las autoridades competentes.
A.6.1.7	Contacto con grupos de especial interés.	Control Deben mantenerse los contactos adecuados con grupos de interés

		especial, u otros foros, y asociaciones profesionales especializadas en seguridad.
A.6.1.8	Revisión independiente de la seguridad de la información.	Control El enfoque de la organización para la gestión de la seguridad de la información y su implantación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información), debe someterse a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.
A.6.2. A Terceros **Objetivo: Mantener la seguridad de la información de la organización y de los dispositivos de tratamiento de la información que son accesados, procesados, comunicados o gestionados por terceros.**		
A.6.2.1	Identificación de los riesgos derivados del acceso de terceros.	Control Deben identificarse los riesgos para la información y para los dispositivos de tratamiento de la información de la organización derivados de los procesos de negocio que requieran de terceros, e implantar los controles apropiados antes de otorgar el acceso.
A.6.2.2	Tratamiento de la seguridad en la relación con los clientes.	Control Deben tratarse todos los requisitos de seguridad identificados antes de otorgar acceso a los clientes, a los activos o a la información de la organización.
A.6.2.3	Tratamiento de la	Control

	seguridad en contratos con terceros.	Los acuerdos con terceros que conlleven acceso, procesamiento, comunicación o gestión, bien de información de la organización, o de los recursos de tratamiento de la información, o bien la incorporación de productos o servicios a los recursos de tratamiento de la información, debe cubrir todos los requisitos de seguridad pertinentes.
A.7 Gestión de activos		
A.7.1 Responsabilidad sobre los activos **Objetivo: Conseguir y mantener una protección adecuada de los activos de la organización.**		
A.7.1.1	Inventario de activos	Control Todos los activos deben estar claramente identificados y debe elaborarse y mantenerse un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y activos asociados con los recursos para el tratamiento de la información deben tener un propietario que forme parte de la organización y haya sido designado como propietario.
A.7.1.3	Uso aceptable de los activos	Control Se debe identificar, documentar e implantar las reglas para el uso aceptable de la información y los activos asociados con los recursos para el tratamiento de la información.

A.7.2 Clasificación de la información **Objetivo: Asegurar que la información recibe un nivel adecuado de protección.**		
A.7.2.1	Directrices de clasificación.	Control La información debe ser clasificada según su valor, los requisitos legales, la sensibilidad y la criticidad para la organización.
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implantar un conjunto adecuado de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

Tomado de: INEN, 2011

ANEXO 2

Problemas presentados en las pruebas realizadas dentro del data center.

En primer lugar, uno de los mayores problemas que se presentaron fue la instalación y configuración de Alien Vault OSSIM el cual necesita utilizar demasiados recursos de la máquina, por lo cual al querer instalar y configurar el SIEM, la máquina se colgaba o daba pantallazo azul ya que ocupaba toda la memoria RAM; después de realizar varias pruebas se determinó que se necesitaba una máquina de 16GB de RAM ya que el SIEM ocupó aproximadamente 10 GB de RAM.

Otro problema se presentó después de configurar el SIEM ya que se debía habilitar el SSH para una administración remota y al querer modificar la IP para tener acceso al internet; la plataforma SIEM se desconfiguró.

Adicional, después de obtener las máquinas virtuales ya completamente configuradas existieron problemas al subir las máquinas al ambiente del datacenter, por lo que se tuvo que crear las máquinas en virtual box y luego exportar a OVF de VMWare, así se logró solucionar el problema, además, se tuvo que deshabilitar la tarjeta de red WAN del firewall y configurarle ya dentro del ambiente del datacenter.

Otro de los problemas que tiene esta red es que la hora de los eventos no se encuentra bien configurada ya que no se encuentra instalado un servidor NTP esto quiere decir que cada servicio va a disponer de la hora que tiene configurada en su sistema.

Cuando se tuvo problemas para subir el firewall por el problema de las tarjetas de red se quiso realizar un cambia Monowall, pero este tuvo mayores inconvenientes, ya que este era uno muy básico y ni siquiera se pudo configurar las interfaces en el datacenter, luego se decidió continuar con Endian firewall ya que este era muy completo pero una vez definidas bien las interfaces y configurarlas bien se tuvo acceso y se pudo realizar las pruebas con este firewall.

Un problema que se tuvo con el SIEM es que cuando se habilito la segunda tarjeta de red para recolectar los logs el SIEM empezó a colgarse por lo cual hubo muchos inconvenientes. Esto sucedió porque la máquina virtual no soportaba la instalación de las 2 interfaces, una vez migrado a ovf lo que se hizo es aumentar la 2 tarjeta de red una vez instalada en el datacenter así se estabilizo y dejo de dar el problema

Finalmente, al tener las máquinas virtuales subidas dentro del ambiente del datacenter, se necesitó muchas configuraciones adicionales ya que en un principio no se tenía las IP’s bien definidas y una vez subidas al datacenter tocó cambiarlas.