ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Sistemas de Información Gerencial

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN CENTRALIZADA DE SEGURIDAD DE INFORMACIÓN Y EVENTOS A TRAVÉS DEL SOFTWARE OPEN SOURCE OSSIM."

TRABAJO DE TITULACIÓN

Previo a la obtención del Título de:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

AUTOR

CHRISTIAN JOSÉ CASTILLO VALAREZO

GUAYAQUIL – ECUADOR

AÑO: 2018

AGRADECIMIENTO

Agradezco a Dios y a la virgen del cisne, por todas las bendiciones concedidas, y por permitir terminar este proyecto de grado.

A mis padres, Flor y José, por su amor, sacrificio, enseñanzas y su apoyo incondicional. Son unos excelentes padres, mi gratitud hacia ustedes.

A mi hermano, por brindarme su apoyo a pesar de lo bueno; lo malo; siempre ayudándome a conseguir mis metas.

A mis amigos, son mis consejeros, y me han permitido crecer como ser humano y a nivel profesional.

Gracias a todos.

DEDICATORIA

“Si tienes un sueño y crees en él, corres el riesgo de que se convierta en realidad.”

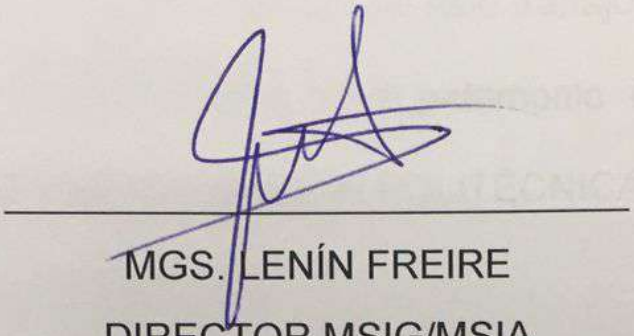
Walt Disney

A nuestro Padre celestial,

A mi familia;

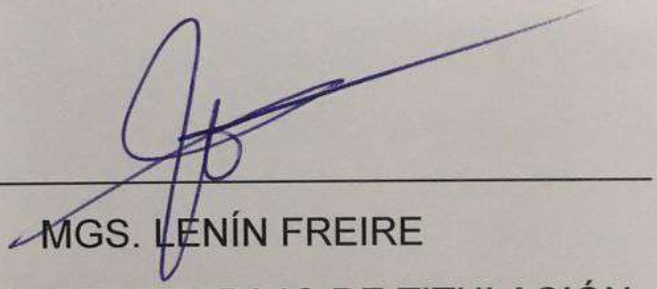
La razón que me levanta todos los días.

TRIBUNAL DE SUSTENTACIÓN



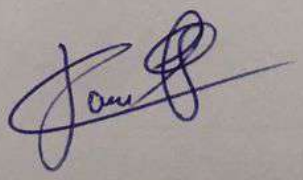
MGS. LENÍN FREIRE

DIRECTOR MSIG/MSIA



MGS. LENÍN FREIRE

DIRECTOR DEL TRABAJO DE TITULACIÓN



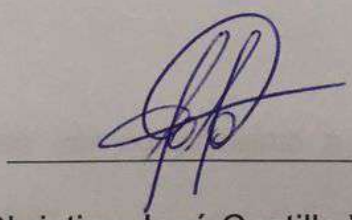
MGS. JUAN CARLOS GARCÍA

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este trabajo de titulación, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL)



Christian José Castillo Valarezo

RESUMEN

En la actualidad la institución pública del Ecuador se dedica a facilitar el control y gestión aduanera, la cual necesita cubrir las necesidades de la Dirección Nacional de Auditoría Interna, seguridad informática y base de datos para la aplicación de Pistas de Auditoría, las mismas que fueron indicadas en la emisión del Acuerdo Ministerial Nro. 166 emitido en el 2013 por la Secretaría Nacional de la Administración Pública, ahora Ministerio de Telecomunicaciones y Sociedad de la Información para la Gestión de Seguridad de la Información, en cuyos artículos indica que: “Los programas de software o archivos de datos de auditoría se deben separar de los sistemas de información y de desarrollo de la entidad”.

En este sentido, para dar cumplimiento a estos controles, se tiene los siguientes resultados que:

a) Se encontró que no existe base de datos de pista de auditoría, donde se almacene de forma centralizada y automática los eventos de seguridad. Se resolvió mediante la base de datos interna de la aplicación donde se almacena los eventos de seguridad, la cual se encuentra de manera aislada de las otras base de datos que está supervisando.

b) Las actividades de monitoreo de base de datos de eventos de seguridad no se evidencia, por lo no se puede mitigar o tomar acciones. La herramienta OSSIM cuenta con gráficas de eventos de seguridad, permite tomar acción de manera pro activa.

c) La institución no emite reportes de pista de auditoría. La personalización de reportes es una necesidad que se resolvió mediante la utilización del aplicativo OSSIM, este modulo permite emitir información de manera detallada.

d) El análisis de vulnerabilidades es una necesidad que tiene el área de seguridad informática, esto hace que no pueda emitir recomendaciones. El modulo de análisis de vulnerabilidades permitió resolver está necesidad, el área de seguridad de la información tomo acción sobre vulnerabilidades encontradas.

De acuerdo a lo mencionado, se recomienda la herramienta correlacionador de eventos de seguridad, es la que permite encontrar manipulaciones en los sistemas y posibles ataques. El software que se ajusta a la institución mediante el Acuerdo Ministerial Nro. 166 y artículo 145 del Código Orgánico De La Economía Social De Los Conocimientos, se determinó utilizar OSSIM (Open Source Security Information Management), herramienta de gestión de eventos y seguridad de la información, plataforma avanzada dedicadas al monitoreo en línea de eventos y actividades sospechosas, que permite alertar antes posibles ataques a la seguridad de la institución.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BD	Data base, base de datos
FW	Firewall, Cortafuegos
IPS	Intrusion Prevention System, sistema de prevención de intrusos.
IDS	Intrusion Detection System, sistema de detección de intrusos.
ISO	Organización Internacional de Normalización
OSSIM	(Open Source Security Information Management), sistema de administración de eventos y de información de seguridad de código abierto.
SIEM	Security Information and Event Management, Sistema de Gestión de eventos e Información de Seguridad.
SI	sistema de seguridad
SSH	Secure Shell, Intérprete de Órdenes Seguras.
TPS	transacciones por segundo.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Las principales problemáticas de seguridad que sufre la institución es la fuga de información, gestión del acceso no autorizado a las bases de datos, el robo de información, la suplantación de identidad, entre otros. Los cuales afectan a los criterios principales de la seguridad de la información como la confidencialidad, integridad, disponibilidad y trazabilidad (Ma, Johnston, & Pearson, 2008). Debido a estas problemáticas de seguridad se tiene la necesidad de implementar controles en las áreas que administran la información como son Base de datos, Auditoría y seguridad informática, sin embargo, el control actualmente establecido no permite garantizar los cuatro criterios de seguridad. Además, en el año 2016 la institución fue notificada, mediante Acuerdo Ministerial Nro. 166 emitido en el 2013 por la Secretaría Nacional de la Administración Pública, en cuyo artículo indica que: “Los programas de software o archivos de datos de auditoría se deben separar de los sistemas de información y de desarrollo de la entidad”.

Este proyecto busca implementar un sistema de gestión de seguridad de la información mediante la herramienta correlacionador de eventos, cuya expectativa es de proporcionar un sistema que permita visibilizar los eventos de la base de datos en tiempo real, de forma que garantice el procesamiento de la información, ayudando la detección de intrusos y anormalidades en el sistema. Asimismo, proveer de reportes para garantizar a los administradores de una vista de los eventos relativos a la seguridad información.

En el primer capítulo se abordará los problemas que está actualmente sufriendo la institución, por los que se ha planteado soluciones y cumplir objetivos a corto plazo.

En el segundo capítulo Marco Teórico, el estudio teórico y conceptos de los temas más relevantes que hagan referencia a los términos a tratar dentro del proyecto, que permiten el respaldo de la propuesta. Los principales

componentes, así como los mecanismos de captura, análisis, correlación de la información y reportaría que presenta la herramienta.

En el tercer capítulo, levantamiento de información, corresponde a la información que se obtuvo en la institución, el análisis de las áreas que fueron objeto de estudio del proyecto y de los inconvenientes que presenta. Análisis de las causas de los problemas.

En el cuarto capítulo: Análisis de la Propuesta tecnológica. El contenido está formado por el Análisis de la Factibilidad, entre los que interviene la factibilidad técnica, operacional, económica y legal.

En el quinto capítulo: analiza las diferentes etapas de las metodologías aplicadas para el proyecto, todo esto ligado con los entregables y criterios de

validación para la propuesta, basándose para establecer las conclusiones y recomendaciones.

Por último, se incluye en el sexto capítulo la descripción de los resultados por obtener con la aplicación de nuestra propuesta, detallando por cada opción sus beneficios y métodos de trabajo dando las mejores recomendaciones para poder obtener los mejores resultados.

CAPÍTULO 1

GENERALIDADES

1.1 PLANTEAMIENTO DEL PROBLEMA

La información es considerada un activo crítico de información el cual juega un papel estratégico para todas las organizaciones, tomando en cuenta que la información debe ser almacenada en repositorios que garanticen la confidencialidad, integridad, disponibilidad y trazabilidad de la información almacenada en ellas.

En la República del Ecuador rigen las Normas de esquema gubernamental de la seguridad de la información (EGSI), las cuales constituyen guías generales emitidas por la Contraloría General del Estado, orientadas a promover una adecuada administración de los recursos públicos y a determinar el correcto funcionamiento administrativo de las entidades y organismos del sector público ecuatoriano, en las cuales rigen controles específicos para tratamiento de la

información sensible y el control de acceso a la misma, las cuales indispensablemente deben ser cumplidas.

Actualmente, el sistema de la institución mantiene ambientes tecnológicos diferentes tanto producción, desarrollo y pruebas, con sus bases de datos respectivamente. Adicionalmente, se debe considerar que algunas bases de datos comparten información hacia otras instituciones públicas existiendo el riesgo que haya fuga de información. Las áreas que actualmente presentan problemas de seguridad son tres, cada una con diferentes problemáticas como las describimos a continuación:

Base de Datos.

- Las bases de datos actualmente no permiten identificar el usuario, lo que podría causar que no se pueda determinar con precisión quien accede a la base de datos, con el objetivo de garantizar el no repudio.
- La información de los logs se guarda en la misma base de datos, causando un alto consumo de almacenamiento.
- Los logs de la base de datos no son analizados, por lo cual no se podría detectar un incidente de seguridad en tiempo real.

Seguridad Informática.

- La institución no cuenta con una base de conocimientos interna de los ataques y vulnerabilidades de la base de datos. Está situación aumenta el riesgo de nuevas formas de ataque.
- El usuario conectado por medio aplicativos no está siendo registrando las direcciones IP de los usuarios, permitiendo no tener un registro de direcciones IP autorizadas y no autorizadas.
- Los ingresos fallidos al sistema no se registran. En consecuencia, es posible podrían sufrir ataques de denegación de servicio.

Auditoría de Sistemas

- Reportes de usuarios que consulta información delicada, podría presentarse una posible fuga de información.
- Reportes de ingresos al sistema en horarios no laborables, permitiendo a usuarios en horario no laboral realicen acciones no permitidas.

1.2 JUSTIFICACIÓN

De acuerdo a la problemática se implementa una herramienta, que ayude a monitorizar, controlar y gestionar la correlación de los eventos que se presenten dentro de la institución, para que sea de ayuda en la toma de decisiones de la SI.

Es por esto que surge la necesidad de analizar e implementar una herramienta Open Source que nos garantice la detección y corrección oportuna de amenazas que sufre constantemente la institución.

Debido a los altos costos de licenciamiento en software de seguridades se opta por escoger está herramienta de código abierto ya que el costo es bajo para su implementación el mismo que ayudara a monitorizar la red de cualquier institución. Por las características antes mencionadas y al tratarse de un proyecto de implementación de software basado en código abierto, la institución se acoge a lo establecido en el artículo 145 del Código Orgánico De La Economía Social De Los Conocimientos, Creatividad e Innovación donde dice lo siguiente [1]:

“Las Instituciones del sector público deberán realizar una evaluación de factibilidad de migrar sus tecnologías digitales a tecnologías digitales libres con los criterios establecidos en el reglamento correspondiente. Se evaluará la criticidad del software, debiendo considerar los siguientes criterios:

1. Sostenibilidad de la solución;
2. Costo de oportunidad;
3. Estándares de seguridad;
4. Capacidad técnica que brinde el soporte necesario para el uso del software**.”**

La facilidad de gestión de la herramienta es otro detalle muy importante, ya que involucra que la información generada y almacenada cumpla con las propiedades de la información como son: Confidencialidad, Integridad, trazabilidad y Disponibilidad. Se detallan en la tabla #1 algunas características que se deberían considerar al momento de elegir una Herramienta de Pistas de Auditoría.

Tabla 1. Características funcionales de la Herramienta

No.	**Características funcionales**	**Confidencialidad**	**Disponibilidad**	**Integridad**	**Trazabilidad**
1	Proteger los datos auditados frente a cualquier modificación, de manera que los informes e investigaciones realizados con los datos auditados tengan un alto nivel de integridad.	x	x	x	x
2	Brindar la capacidad de consolidar y organizar los datos auditados de manera que sean administrados, accedidos y analizados por las personas autorizadas.	x	x	x	x
3	Monitorear en tiempo real toda actividad de las bases de datos a fin de detectar fugas de información y transacciones no autorizadas.	x	x	x	x
4	Recopilar y consolidar los datos auditados de manera eficiente, brindando información respecto de quién hizo qué a cuales datos y cuándo lo hizo.	x	x	x	x

5	Administrar, analizar-, almacenar y archivar grandes volúmenes de datos auditados para que se encuentren disponibles para las personas autorizadas.	x	x	x	x
6	Impedir acciones no autorizadas en tiempo real a usuarios con privilegios; como por ejemplo: cambiar valores en datos sensibles en una base de datos, crear nuevas cuentas de usuario y/o modificar privilegios.	**x**	x	x	x
7	Recopilar datos auditados de múltiples fuentes para analizar la información.	x	x	x	x
8	Generar informes de evaluación de auditorías en los sistemas de procesamiento de información.	x	x	x	x
9	Generar alertas en caso de que se produzca alguna actividad sospechosa o algún intento por obtener acceso no autorizado a los datos auditados.	x	x	x	x
10	Generar notificaciones de eventos específicos, actuando como un sistema preventivo frente a las amenazas internas y ayudando a detectar actividades que podrían potencialmente impedir el cumplimiento de pistas de auditoría.	x	x	x	x
11	Detectar amenazas, esto ayuda al moni toreo continuo de los datos auditados. Estas alertas pueden estar relacionados con cualquier evento que pueda auditarse, como los cambios en las tablas de la bases de datos, el otorgamiento de roles y la creación de usuarios.	x	x	x	x

12	Proteger datos auditados al utilizar controles sofisticados, que permita que los usuarios administradores de base de datos no puedan ver ni modificar los datos auditados.	x	x	x	x
13	Definir las políticas de auditoría desde una consola central que pueda ser utilizada por auditores internos y el personal de seguridad de Infraestructura Tecnológica.	x	x	x	x
14	Proporcionar, en tiempo real, el control, la auditoría y la generación de informes, de manera automatizada, para los distintos entornos de bases de datos.	x	x	x	x
15	Proporcionar la trazabilidad detallada de los datos auditados que indican el quién, que, cuándo, dónde y cómo, de todas las transacciones.	x	x	x	x

Fuente: Normas Técnicas Ecuatorianas NTE INEN1SO/IBC 27000

1.3 IMPORTANCIA

Este proyecto es un beneficio directo a los administradores de la información. Permite mejorar el control de los eventos y les permitirá el monitoreo ágil y eficaz, además optimizará significativamente los tiempos mediante la utilización de la herramienta en tiempo real. Al tener controles aislados de seguridad aumente los tiempos detectar la falla o problema de seguridad.

El uso de esta herramienta garantiza la disponibilidad, integridad, confidencialidad y trazabilidad de la información de detectando oportunamente todas las amenazas, vulnerabilidades y ataques de los que son víctima cada uno de los elementos de la red.

1.4 CAUSAS Y CONSECUENCIAS DEL PROBLEMA

Las posibles causas y consecuencias del presente trabajo de titulación planteado se detallan en el siguiente cuadro.

Tabla 2. Causas y Consecuencias del problema

CAUSAS	CONSECUENCIAS
• El sistema de comercio electrónico ofrece múltiples servicios.	• Se pierde la administración de la información.
• Claves de usuarios administrador compartidas por múltiples usuarios.	• Uso inadecuado de claves
• Múltiples usuarios pueden consultar con información privilegiada.	• Fuga información
• Acceso a base de datos no restringida	• No se alerta sobre acceso no autorizado

Fuente: Servicio Nacional de aduanas

1.5 OBJETIVO GENERAL

Implementar un sistema de gestión centralizada de seguridad de información y eventos a través del software libre OSSIM.

1.6 OBJETIVOS ESPECÍFICOS.

- Seleccionar un modelo de mejores prácticas para la gestión centralizada de eventos de seguridad.
- Poner en práctica la guía metodológica de la gestión centralizada de registros con base en recomendaciones de la ISO 27002.

- Evaluar los pasos propuestos en la guía metodológica propuesta mediante la definición e implementación de una prueba de concepto.
- Analizar los resultados recolectados por la herramienta OSSIM.

1.7 ALCANCE DEL PROBLEMA

Considerando los eventos de los futuros usuarios de la infraestructura tenemos como resultado el análisis funcional de diferentes opciones que facilitan y a su vez agilizan el proceso de control de eventos.

La presente investigación consiste en monitorear y verificar la correlación de eventos en tiempo real con el uso de la herramienta OSSIM ALIENVAULT y comprobar la funcionalidad integral de la información dentro de una organización y ayudará a los administradores de red en la toma de decisiones para salvaguardar la seguridad de la red de la empresa. Con este proyecto se podrá realizar una demostración de cómo lograr la integración de la información y reducción de riesgos de seguridad de la red.

CAPÍTULO 2

MARCO TEÓRICO

2.1 TECNOLOGÍAS DE SOFTWARE

Cada vez resulta más difícil hacer frente a los ataques que ocurren en las redes informáticas o el robo de información, los sistemas SIEM (Sistema Gestión de Eventos e Información de Seguridad) están ayudando a los administradores de la información a automatizar este trabajo para posibilitar una gestión de la seguridad de la red más eficiente.

La demanda en sistemas SIEM está creciendo en las organizaciones eso se lo puede reflejar en el informe de Forecast, “Information Security, Worldwide, 2015-2021, 3Q17 Update”, las ventas de SIEM en el año 2016 fueron 2.167 billones de dólares tiene una tasa de crecimiento anual del 8% de 2016 a 2021 [2].

Hoy en día la gestión y el tratamiento de la amenaza es uno de los aspectos más importantes en las organizaciones modernas, dedicando los recursos necesarios para poder responder a los nuevos incidentes de seguridad. Los SIEM actúan como repositorio de eventos de seguridad, usado para monitorizar, identificar y documentar los incidentes de seguridad.

La teoría en la cual se basa este proyecto de investigación es en los conceptos claves para realizar la centralización de eventos como parte de una evidencia digital. Esto cubre los temas relacionados mecanismo de registros de log, correlacionado de registros, métodos de transportación de los logs y evidencia digital.

También se cubren temas relacionado con temas de seguridad informática como los tipos de ataques informáticos y los métodos de protección, con el fin de conocer las herramientas que usualmente son utilizadas para la protección de la información y generan registros de eventos de seguridad

2.2 PRINCIPIOS DE LA SEGURIDAD

El presente documento se genera debido a una revisión general de la recomendación No. 15 del Comité de Gestión de Seguridad de la Información sustentado en el Acuerdo Ministerial No.166 que Dispone a las entidades de la

Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN1SO/IBC 27000 para Gestión de Seguridad de la Información [3].

Con el objeto que se apliquen los términos de manera correcta, a continuación, se presentan algunas definiciones inherentes a informe:

Integridad: Es la garantía que la información no ha sido modificada, manipulada ni alterada por parte de terceros.

Confidencialidad: Es la garantía que el acceso a la información sea sólo para aquellas personas autorizadas.

Disponibilidad: Es la garantía que las personas autorizadas tengan acceso a la información toda vez que lo requieran.

Trazabilidad; Procedimiento preestablecido que permite conocer el histórico, ubicación o la trayectoria de un producto a través de herramientas determinadas.

2.3 MECANISMO DE REGISTRO DE LOG DE SEGURIDAD

El mecanismo que utilizaremos para guardar log es el syslog. A continuación, describiremos información de la herramienta.

2.3.1 SysLog

La herramienta correlacionadora de eventos de seguridad utiliza SYSLOG como su sistema de generación de logs, la herramienta

capta los mensajes que emiten los sistemas, aplicaciones y dispositivos de red [4].

Él envió de mensajes Syslog es frecuentemente utilizados en sistemas basados en UNIX para registrar eventos de aplicaciones, sistema operativo o red.

Es común que equipos de redes utilicen estás herramientas para generar y enviar mensajes Syslog a equipos configurados con un demonio que los reciba [5]. El termino syslog es utilizado para describir como una librería que envía mensajes.

2.3.2 MENSAJES SYSLOG

Un mensaje syslog cuenta con tres campos descritos a continuación:

- PRI**:** Es el campo de prioridad, está compuesto de 2, 4 o 4 caracteres y debe estar rodeado de corchetes. La prioridad representa a la vez la facilidad y severidad las cuales se codificadas numéricamente con valores decimales.

El sistema operativo es el que asigna los valores de prioridad. Si a algún proceso no tiene asignado ningún número de prioridad, puede usar cualquiera prioridad de uso local o nivel de usuario, las prioridades han sido asignadas en la tabla 3, así como como sus códigos numéricos.

Tabla 3. Prioridades y su código numérico

Código Numérico	Facilidad
0	Mensajes de kernel
1	Mensajes de nivel de usuario
2	Sistema de correo
3	Demonios del sistema
4	Mensaje de seguridad/autorización
5	Mensaje generado internamente por syslogd
6	Subsistema de impresora en línea
7	Subsistema de noticias de red
8	Subsistema UUCP
9	Demonio de reloj(nota 2)
10	Mensaje de seguridad/autorización(nota 1)
11	Demonio FTP
12	Subsistema NTP
13	Auditoría de eventos (nota 1)
14	Alerta de eventos (nota 2)
15	Demonio de reloj (nota 2)
16	Uso local 0
17	Uso local 1
18	Uso local 2
19	Uso local 3
20	Uso local 4
21	Uso local 5
22	Uso local 6
23	Uso local 7

Fuente: IETLF RFC 3164

Cada Prioridad de mensaje tiene un indicador de Severidad decimal. Estás severidades son descritas en la tabla 4:

Tabla 4. Severidades y su código numérico respectivo

Código Numérico	Severidad
0	Mensajes de kernel
1	Mensajes de nivel de usuario
2	Sistema de correo
3	Demonios del sistema
4	Mensaje de seguridad/autorización
5	Mensaje generado internamente por syslogd
6	Subsistema de impresora en línea
7	Subsistema de noticias de red

Fuente: IETLF RFC 3164

El valor de la Prioridad se calcula multiplicando el valor de prioridades por 8 y sumándole el valor de la severidad.

- HEADER**:** La cabecera contiene, fecha y hora del mensaje, nombre máquina, proceso (nombre e identificador) que lo ha generado.

La fecha y hora del mensaje. Corresponde a la fecha y hora local del dispositivo que trasmite. Estás se encuentran en formato “Mmm dd hh:mm:ss” donde:

- Mmm corresponde a la abreviatura en ingles del mes. Las tres primeras letras del mes. Este valor puede ser: Jan, Feb, Mar, Apr.
- Dd corresponde a la abreviatura en ingles del día. Si los días es menor a 10 se debe representar con un espacio y el número de dia. Ejempo. “Aug 7”.
- Hh:mm: ss. Corresponde a la hora local. Las horas (hh) están representadas en un formato de 24 horas. Los valores permitidos entre 00 y 23, incluye. Los minutos (mm) y segundos.

El valor correspondiente al nombre de maquina corresponde al nombre del servidor, la dirección ip4 o ip6 especificado en STD 13 [6]. El nombre no va incluidos espacios. Si se utiliza la dirección ipv6, se debe usar con el formato RFC 2373.

- MSG**:** El mensaje o MSG tiene 2 campos. Etiqueta y Contenido. El primero representa el nombre del programa o el proceso que origino el evento. El contenido es el texto del mensaje.

2.4 SOFTWARE CORRELACIÓN DE REGISTRO DE EVENTOS.

La correlación de registro tiene como objetivo el de encontrar un incidente los cuales son una serie de eventos que sucede tanto en el servidor como en la red [7]. En otras palabras, el correlacionado de eventos trata de asociar los eventos con información útil.

2.4.1 OSSIM

OSSIM se presenta como solución de código abierto para la gestión de seguridad de la información; le proporciona funciones como recopilación, análisis y correlación de eventos. Desarrollado para los ingenieros de seguridad debido a la falta de productos de código abierto, OSSIM fue creado específicamente para abordar la realidad que muchos profesionales de seguridad que enfrentan vulnerabilidades en su infraestructura: Un SIEM, ya sea de código abierto o comercial, es virtualmente inútil sin los controles de seguridad básicos necesarios para la seguridad visibilidad.

La capacidad de la consola OSSIM para obtener información detallada y selecta, de los eventos de los dispositivos y herramientas de la red, le permite ser una herramienta muy útil. A los administradores de seguridad, les da una opción de seguridad que le

permite detectar amenazas y disponer un nivel más de seguridad para la protección de la información y equipos de red [8]. La herramienta aborda esta realidad al proporcionar una plataforma unificada con muchas de las capacidades de seguridad esenciales que necesita, como:

- Descubrimiento de activos
- Evaluación de vulnerabilidad
- Detección de intrusos
- Control del comportamiento
- Correlación de eventos SIEM
- Alertas automáticas y presentación de informes técnicos.

2.4.2 ELEMENTOS PARA LA CORRELACIÓN.

En la arquitectura de correlación podemos decir que consta de 2 elementos claramente diferenciados para ofrecer información:

- Los monitores. Que son indicadores de lo que pase en nuestra red y servidores.
- Los detectores. Que nos ofrecen alertas por cualquier tipo de evento.

Las salidas que obtenemos de nuestros detectores se pueden convertir en reportes y correos.

2.5 TECNOLOGÍA DEL MODELO DE CORRELACIONADOR DE EVENTOS

Un sistema correlacionador de eventos SIEM por sus siglas en ingles es una combinación compleja de tecnología diseñadas para proporcionar una visión más clara de la arquitectura TI, beneficiando a los encargados de la seguridad informática dela empresa. La herramienta SIEM combina dos tecnologías SEM Y SIM [9].

- **SEM** (Administrador de Eventos de Seguridad), Procesa y proporciona un monitoreo en tiempo de real de los eventos producidos en la red. Su función principal consiste en recolectar la información de los sensores instalados en los dispositivos (FW, IDS, BD, etc), los correlaciona y genera alertas.
- **SIM** (Administrador de información de Seguridad). La herramienta de gestión de seguridad de la información es el encargado de recolectar, correlacionar y analizar la información histórica, está herramienta está optimizada para trabajar con grandes volúmenes de información y almacenarla con una gran compresión.

Estos dos sistemas permiten aplicar sistemas de control y administración, que buscan aminorar las amenazas de seguridad, asegurando la

disponibilidad de tus sistemas de la organización. En los capítulos siguientes se realizará el análisis de la herramienta.

2.6 SIEM (SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EVENTOS)

En la actualidad los ataques son más sofisticados e inmunes a cualquier detención de algún dispositivo de convencional. Los ataques cada vez se hacen difíciles detectar y pueden pasar desapercibido para los administradores de seguridad informática, por lo que es necesario soluciones completas que permitan un fácil control de eventos, que nos lleven la posibilidad de detectar un intruso, como lo es el SIEM.

SIEM es un sistema híbrido del SIM Y SEM, se encarga de analizar, monitorear en tiempo real, recolectar y correlacionar los eventos de seguridad generados por los dispositivos. La solución permite detectar y alertar posibles amenazas que son imperceptibles para otros equipos de seguridad como es el IDS.

El termino SIEM fue dado por Amrit T. Williams y Mark Nicolett, donde detalla las capacidades de los productos de recopilación, análisis y presentación de la información de eventos de seguridad, gestión de equipos tecnológicos vulnerables y políticas de cumplimiento [8]. Unos de los objetivos es controlar los privilegios de los usuarios y alteraciones de configuración de sistemas.

2.7 CAPACIDADES DEL SIEM

La solución SIEM se basan en analizar y correlacionar en tiempo real eventos de seguridad sospechosos que amenazan los sistemas institucionales; permitiendo cumplir con las políticas se seguridad [10]. En la figura 2.1. Se puede observar las capacidades de la solución.

Figura 2.1 Capacidades de la arquitectura SIEM

Fuente: Alienvault 2016

Los sistemas SIEM cumplen capacidades como dos tecnologías **SEM y SIM,** como los vemos a continuación**:**

- **Recolección y retención de los logs**: Mantiene una base de datos de todos los datos históricos, generados por la correlación de eventos pasados (FW, IDS, Servidores, Aplicaciones, etc). Está base de datos realiza análisis de los

datos, normalizado en los distintos sensores que tiene todos los dispositivos, estos datos son enviados al SIEM. El cual son organizados y les aplica políticas de retención para satisfacer los requerimientos de la organización. Estos datos son utilizados por los administradores de seguridad.

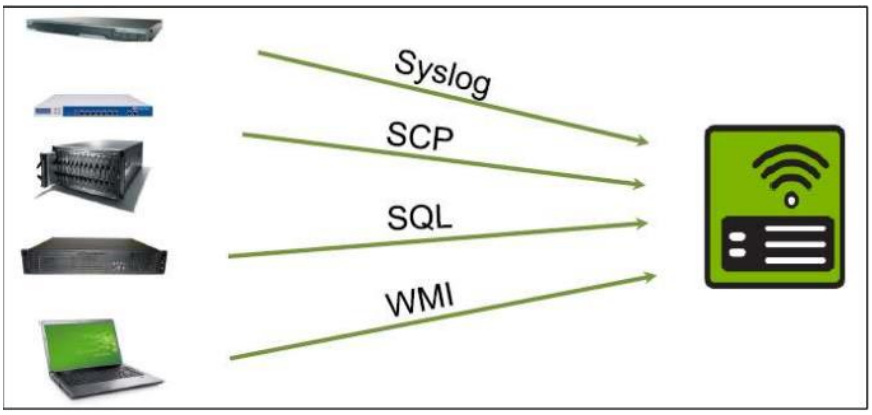


Figura 2.2 Capacidad de recolección y retención de logs.

Fuente: Alienvault 2016

- **Monitorización**: Es la capacidad del SIEM para monitorear los eventos en tiempo en real. Es capaz de analizar todos los eventos de seguridad y notificar solo los eventos con alto grado de correlación.

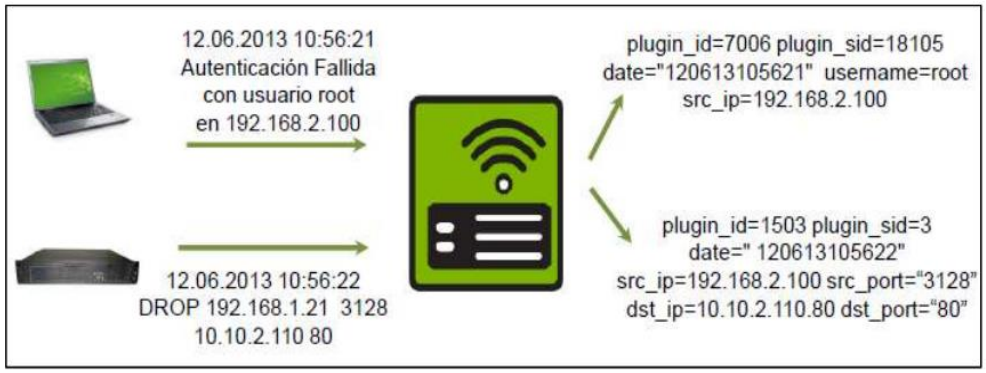


Figura 2.3 Capacidad de monitorización.

Fuente: Alienvault 2016

- **Informe:** La herramienta tiene capacidad de realizar informe de seguridad técnicos e informe ejecutivos amigables para el usuario final.
- **Cumplimiento de las políticas de seguridad.** Los eventos de seguridad son recolectados en logs, los cuales son filtrados bajo reglas de auditoría informática y validado por cumplimiento impuesto organizaciones de políticas de seguridad asociados a regulaciones vigentes.
- **Análisis Forense.** La capacidad de análisis forense nos ayuda a la reconstrucción posterior de los eventos y análisis de la evidencia posterior al ataque informático. Anticipa ataque más especializados.
- **Alertas en Tiempo real.** El SIEM analiza los diferentes eventos, la frecuencia de eventos, los horarios de los mismos. Para establecer la

veracidad de los eventos la herramienta debe eliminar los falsos positivos después debe unirlos y debe reportarse como un solo incidente.

- **Correlación de eventos.** La capacidad de correlación de eventos, es capaz de identificar un incidente de seguridad tras recolectar y correlacionar con eventos de seguridad para estar seguro, con la capacidad de notificar y reaccionar frente al incidente.

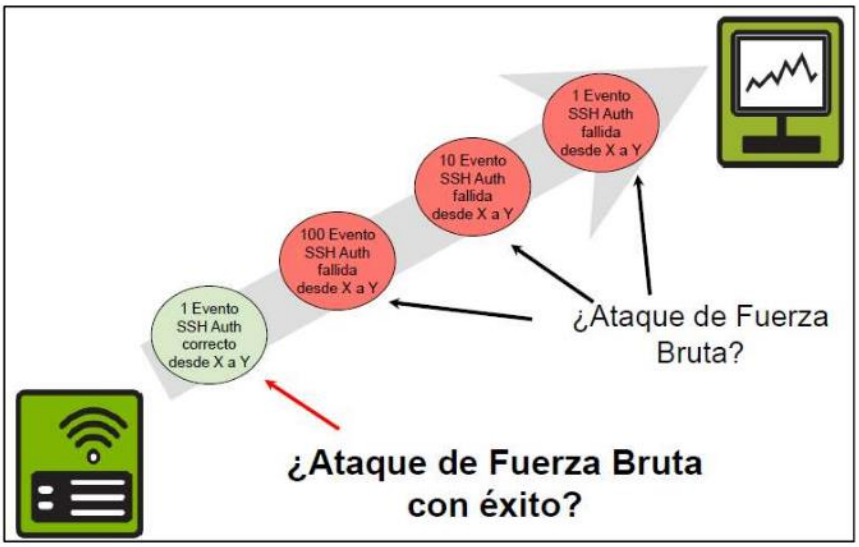


Figura 2.4 Capacidad de correlacionado

Fuente: Alienvault 2016

- **Dashboard.** – La capacidad de mostrar de manera gráfica por medio tableros ejecutivos pueden personalizarse para dar una visión general sobre la seguridad y el cumplimento de normas.

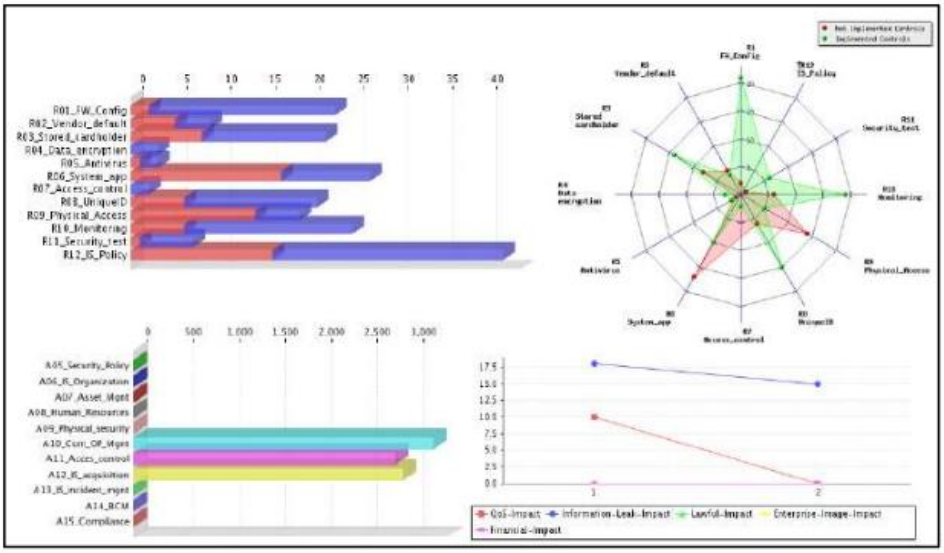


Figura 2.5 Capacidad de dashboard

Fuente: Alienvault 2016

CAPÍTULO 3

DEFINICIÓN DE LA SITUACIÓN ACTUAL DEL PROCESO

3.1 LEVANTAMIENTO DE INFORMACIÓN

La dirección de Tecnología de información tiene bajo su responsabilidad la administración del Sistemas Informáticos facilitan el comercio electrónico, los cuales prestan diferentes servicios considerados prioritarios para cumplir con los objetivos de la institución hacia los ciudadanos.

Cada uno de los sistemas mantienen tres diferentes ambientes: desarrollo, pruebas y producción, contando con diferentes bases de datos para cada uno de los ambientes y sistemas. Adicionalmente se debe considerar que algunas bases de datos son compartidas por los sistemas que consumen información en diferentes instancias.

La información que se recopila mediante el uso de pistas de auditoría, sirve de insumo para llevar a cabo un proceso de auditoría, debido a que permite

recopilar la evidencia suficiente y apropiada que respalden los hallazgos que se presente en dicho proceso.

En particular, se realizó el levantamiento de información en los motores de bases de datos del sistema institucional, de manera que se pueda obtener el número de transacciones por segundo, en relación a la utilización del procesador del servidor.

En el siguiente cuadro se resumen de la información recolectada en la infraestructura tecnológica de la institución el cual sirvió para dimensionar el hardware y software de la herramienta pista de auditoría existentes en el mercado.

Tabla 5 Dimensionamiento de la solución

Resumen de Dimensionamiento		
Crecimiento Estimado TPS(transacciones por segundo)**	Procesadores Totales Base de Datos	27
	TPS TOTAL Actual	27000(Cores * 1000)
15%	TPS Año dos	31050 (15% Anual)
	TPS Año tres	35707 (15% Anual)

** Una transacción es una unidad lógica de trabajo que comprende una o más sentencias SQL a cargo de un único usuario. De acuerdo con el estándar SQL ANSI / ISO, una transacción comienza con una primera

instrucción SQL ejecutable del usuario. Una transacción termina cuando se realiza un COMMIT o ROLLBACK por parte del usuario de forma explícita.

Actualmente las bases de datos cuentan con protección a nivel de usuario y contraseña para ingreso al servidor, y usuarios propios de las base de datos con permisos de lectura o escritura, sin embargo el control actualmente establecido no permite garantizar los tres principios de seguridad (confidencialidad, integridad y disponibilidad). Las bases de datos no poseen un control de auditoría completo en el cual se pueda registrar e identificar las actividades o accesos hacia dichas bases.

Tabla 6. Principios de la Seguridad Informática

Principios	Descripción
Confidencialidad	Propiedad que permite que la información no sea divulgada, para que se garantice que sea accesible únicamente por personal autorizado (ISO/IEC, 27001:2005). Los sistemas de seguridad informática deben proteger de fugas de información, para ellos se debe mantener implementar la asignación de roles para garantizar que la información sea accesible solo para aquellos usuarios autorizados.
Integridad	Propiedad de mantener inalterada la información ante intentos malicioso (ISO/IEC, 27001:2005). Los sistemas de seguridad informática deben mantener la veracidad de los datos tal cual fueron generados; sin alteraciones por parte de tercero. Se debe verificar la autenticidad de la fuente.

Disponibilidad	Propiedad de acceso y utilización de la información por parte de los individuos o entidades autorizadas (ISO/IEC, 27001:2005). Es decir que los sistemas informáticos deben estar en permanente funcionamiento, brindando acceso a los usuarios que requieran información. Además, deben recuperarse antes posibles fallos.
Trazabilidad	Propiedad que permite conocer las transacciones históricas, así como la ubicación y la trayectoria a lo largo de la cadena del sistema informático (ISO/IEC, 27001:2005). Es decir, el sistema de seguridad informática debe mantener el registro histórico del flujo de la transacción de tal manera que pueda relacionar en un momento la información.

Fuente: ISO/IEC, 27001:2005

A continuación, se detallará el proceso de auditoría en cada una de las áreas:

BASE DE DATOS

En el área de Base de datos, como parte de sus funciones, ejecuta cambios en tablas de sistemas y pases a producción de objetos, para lo cual ha venido desarrollando una serie de controles y labores de monitoreo manuales con la finalidad de mitigar los riesgos asociados a la seguridad en las bases de datos.

Las actividades de control de auditoría de base de datos son:

- Activación de pista de auditoría, se activa la función flashback propio de la base de datos en la cual consiste activar

el registro de auditoría que contiene ciertos como fecha y hora registro, tipo de DML y el usuario. Para el posterior análisis por parte de los funcionarios de auditoría interna.

- Control de base de datos, por medio de trigger que son programas que trabajan en conjunto con las tablas y guardan el usuario que realizo el cambio con su ip.

AUDITORÍA INTERNA

Debido a la importancia de la auditoría el servicio informático se mantiene un módulo de auditoría el cual consta con la configuración 21 tablas altamente transaccionales que guardan los cambios que diariamente realizan en el sistema. En las tablas configuradas se realizan la creación de una tabla log la cual registra las inserciones, actualización y eliminación de registros, la información es guarda en la misma base de datos. Luego de que se haya registrado se procesa estas pueden ser consultadas por los funcionarios de auditoría.

SEGURIDAD INFORMÁTICA

El área de seguridad informática, es la encargada de otorgar los permisos en el sistema, establece controles según su perfil y el monitoreo de acceso no autorizado. Mediante aplicativos que

mantiene dispersos en la red interna de la instrucción. De lo que se hace una actividad engorrosa monitorear el acceso.

En el año 2016 la institución fue notificada por contraloría por mantener sistemas dispersos en el control de la auditoría, mediante Acuerdo Ministerial Nro. 166 emitido en el 2013 por la Secretaría Nacional de la Administración Pública, en el artículo que indica: “Los programas de software o archivos de datos de auditoría se deben separar de los sistemas de información y de desarrollo de la entidad”. Por lo que no se cuenta con una solución informática especializada que permita, no solamente, el control y monitoreo automatizado y en tiempo real, sino también que brinde alertas tempranas para evitar ataques a las Bases de Datos.

3.2 DEFINICIÓN DE LOS REQUERIMIENTOS

Adquirir una solución de software open source, con un propósito específico para la función de Monitoreo, Auditoría y Seguridad de Base de datos acorde a las necesidades de la institución. La herramienta debe tener las siguientes capacidades:

- Visibilidad en tiempo real de toda la actividad en la base de datos, incluyendo aquella sobre objetos específicos definidos como sensibles.

- Capacidad de detectar en tiempo real o por demanda, las vulnerabilidades asociadas a la plataforma de base de datos que son objeto del monitoreo, incluyendo plataforma de gestión, configuración y comunicaciones.
- Capacidad para realizar el seguimiento y mitigación parcial o definitiva de vulnerabilidades.
- Capacidad para implementar políticas de seguridad en tiempo real o por demanda, con el fin de controlar el acceso a la información.
- Capacidad para el descubrimiento automático de bases de datos en los servidores protegidos por la solución, además permite la clasificación de la sensibilidad de los datos encontrados.
- Capacidad de visibilizar en tiempo real y de forma gráfica, los resultados y/o gestión.
- Capacidad de actualización de la base de conocimiento y los mecanismos de seguridad. Además, permite la actualización del firmware y/o versiones de la solución tecnológica suministrada, durante 3 años.
- Capacidad para no impactar el desempeño de las bases de datos al monitorear y/o controlar.
- Capacidad para poder monitorear diferentes tipos y versiones de bases de datos de forma simultánea.

- Deberá soportar al menos 5000 transacciones por segundo.
- Deberá generar alertas sobre problemas en el funcionamiento del componente de hardware.

3.3 NECESIDAD INSTITUCIONAL

Actualmente la institución tiene bajo su responsabilidad la administración de varios sistemas que prestan diferentes servicios considerados prioritarios para la prestación de servicios a los ciudadanos. Cada uno de los sistemas administrados consta con una arquitectura es imprescindible aplicar controles de protección de la información sensible en base de datos.

En base a la realidad actual de la institución se requiere implantar controles que permitan:

- Controlar los cambios que se estén realizando hacia la base de datos de producción.
- Poder identificar acciones realizadas en la base de datos, incluyendo las acciones llevadas a cabo por los administradores.
- Establecer procedimientos específicos para la manipulación de la información de la base de datos.
- Registrar y controlar el acceso como las acciones sobre la base de datos.

- Control de acceso por permiso definidos,
- Generación de alertas tempranas en caso de una violación directa a la base de datos.

Siendo la información uno de los principales recursos de la Institución, se hace necesario contar con una herramienta tecnológica, que permita proteger a la misma. Adicionalmente a los controles requeridos es importante mencionar que al contar con una herramienta se puede mitigar ciertas necesidades como: identificación de vulnerabilidades, monitoreo en línea, ejecución de medidas correctivas de forma automática y parametrizable, y manejo de históricos con el fin de mitigar posibles riesgos de mal uso de información y/o fraude; apoyando de esta manera al cumplimiento de los objetivos estratégicos.

CAPÍTULO 4

ANÁLISIS Y DISEÑO DE LA OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN.

4.1 ANÁLISIS DEL SIEM.

El mercado se encuentra un sin número de opciones de seguridad de la información que permite llevar a cabo la correlación de eventos de seguridad, es importante indicar que hay herramientas de distribución gratuita y que puede integrarse a cualquier red. Para implementar este tipo herramientas se debe realizar un análisis de los objetivos de la institución para buscar una solución adecuada.

SIEM (Seguridad de la Información y Correlación de Eventos) proviene de una combinación de SEM y SIM. SEM (Gestión de Eventos de Seguridad) proporciona monitoreo en tiempo real, recopilación de eventos y correlación en tiempo real, y una consola grafica para gestión de eventos; y SIM

(Gestión de Seguridad de la Información) análisis de evento histórico de seguridad y la presentación de informes de eventos de seguridad.

En resumen, la plataforma SIEM están formadas por una colección compleja de tecnologías diseñadas para el monitoreo completo, mediante recopilación y correlación de evento en tiempo real algunos de ellos son: acceso a servidores, logs de dispositivos de red (Router, firewall, IPS), logs de aplicación. En base a los resultados predecir el comportamiento del sistema ante posibles ataques o vulnerabilidades de la seguridad, permitiendo alerta de manera inmediata y tomar acción.

4.2 PRODUCTOS SIEM

Para solventar las diferentes necesidades de seguridad de las instituciones, existe una variedad de producto que varía en forma proporcional a su costos y escalabilidad, teniendo elementos básicos como son el monitoreo, recopilación y administración de eventos de seguridad. A continuación, mostraremos una tabla # 6 que actualmente existe en el mercado del SIEM.

Tabla 6 . Tabla de productos de SIEM

PRODUCTOS SIEM	
LogLogic	LogRhythm
IBM QRADAR	AlienVault (USM) / (OSS
HP ArcSight	SolarWinds LEM
Trustwave SIEM Security	RSA Security Analytics

4.3 EVALUACCIÓN DEL SIEM.

Para evaluar las mejores soluciones SIEM que existentes en el mercado, lo podemos analizar con el reporte del cuadrante mágico de Gartner [11]. El gráfico realiza un análisis de los productos tecnológico líderes en un tiempo determinado. Tal como se observa en la figura 4.1. Correspondiente a productos SIEM.

Figura 4.1 "Cuadrante Mágico" de Gartner para SIEM 2017.

Para comprender el cuadrante se debe tomar el eje de la X que muestra la visión que tiene el producto en a sus mejoras innovadoras que está realizado, el eje de las Y es la capacidad que ellos tiene en cuanto a la venta y las distribuciones del producto. Con esta información lo evalúan y los que tenga nivel más alto se los coloca en el cuadro de líderes esto no implica que uno sea mejor que el otro.

Cabe recalcar que AlientVault corresponde a una versión pagada y OSSIM a la versión gratuita; es una versión limitada por sus capacidades ya que en esta versión no cuenta con soporte en línea y tampoco mecanismo de prevenir un ataque. Pero sin embargo es muy conveniente para las instituciones que quieran un sistema que gestione la información de seguridad informática.

En base al Cuadrante Mágico de Gartner 2017, presentado en la Figura 4.1, se seleccionó 4 productos IBM del cuadrante de líderes, DELL RSA del cuadrante de aspirantes y OSSIM del cuadrante jugadores que es la única solución gratuita de todas las soluciones, además un producto Gratuito Hyperic HQ para que sirva de comparación con la herramienta que va hacer implementada. A continuación, se detalla los aspectos relevantes.

Tabla 7 Tabla comparativa de SIEM

Característica	IBM	DELL RSA	OSSIM	Hyperic HQ
Costo de Licencia	$200.000	$124.000	Gratuito	Gratuito
Exploración de redes	√	√	√	X
Detección de intrusos	√	√	√	√
Detección de vulnerabilidades	√	√	√	√
Monitorización de equipos Host	√	√	√	√
Plugins gratuitos	X	X	√	X
Notificaciones automáticas	√	√	√	√
Network IDS	√	√	√	X
Interface de usuario Web	√	√	√	X
Cantidad de usuarios	Múltiples	Múltiples	Uno	Uno
Registros a largo plazo	√	√	√	√
Soporte	Profesional	Profesional	Comunitario	Comunitario

4.4 ANÁLISIS DE LA INFRAESTRUCTURA TECNOLÓGICA.

La institución se dedica al comercio electrónico de todas las empresas del país su principal software es el FACILPASS permite facilitar los servicios aduaneros de manera ágil y transparente, orientados hacia la facilitación y control de la gestión aduanera en el comercio exterior, sobre la base de procesos integrados y automatizados. Por su alta infraestructura, por el tipo de información delicada que maneja la institución se hace imprescindible contar un sistema de manejo de log para evitar posible pérdida de datos.

4.4.1 Infraestructura de la red.

La institución cuenta actualmente con su matriz en la ciudad de Guayaquil donde se realiza las principales gestiones de la operación. Además, cuenta con 4 distritos distribuida en partes del territorio ecuatoriano.

Aproximadamente cuenta con 1000 empleados, los cuales se encuentra distribuido entre la matriz y en las otras sucursales. El crecimiento de la actividad portuaria ha conllevado a implementar nuevas medidas de seguridad información que se maneja a través de la red.

A continuación, se muestra en la figura 4.2 el gráfico de la red.

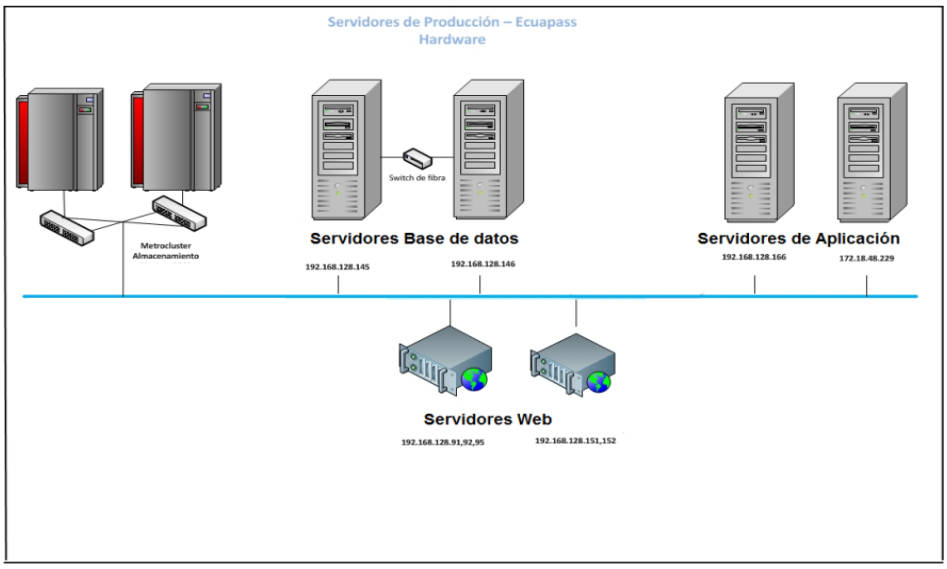


Figura 4.2 Red de la infraestructura tecnología existente.

La matriz está formada por una red donde se encuentra la parte operativa y administrativa de la institución, es por ellos que se encuentra la mayoría de equipos de usuarios y equipos de comunicación. La red de la matriz se encuentra en la ciudad de Guayaquil.

4.4.2 DEPARTAMENTOS ADMINISTRATIVOS

La estructura organizacional se encuentra compuesta de la siguiente forma:

- Dirección General
- Financiero
- Jurídico

- Intervención
- Unidad de Vigilancia Aduanera
- Recursos Humanos
- Seguridades y Auditoría
- Sistemas
- Control
- Seguridad Ocupacional
- Soporte Técnico

Todos los departamentos administrativos se encuentran físicamente en la ubicada matriz. En las sucursales se encuentra un director distrital, unidad Vigilancia aduanera y soporte técnico.

4.4.3 SERVIDORES

El centro de cómputo cuenta con 5 servidores que manejan el funcionamiento operativo de la institución. Estos servidores se encuentran en el centro de cómputo de Guayaquil, el mismo que cuenta con seguridades físicas; restricción de ingreso, climatización, vigilancia mediante cámaras ip, dispositivos de detección de humo.

Tabla 8 Servidores existentes

MARCA	MODELO	FUNCIÓN
IBM	POWER 7	Servidor de Base de Datos
IBM	POWER 7	Servidor de Archivos
IBM	POWER 7	Servidor de Web
IBM	POWER 7	Servidores de aplicación
IBM	POWER 7	Domain Controler, DNS y DHCP
IBM	POWER 7	Servidor de Virtualización

4.4.4 SEGURIDADES

Para controlar la seguridad de la red se cuenta con un cortafuego, el cual sus funciones son de filtrar paquetes que salen al ingresar a la red spam, gestiona al acceso a la vpn, control de ips.

Tabla 9 Equipos de seguridad existentes

MARCA	MODELO	FUNCIÓN
CHECKPOINT	R70	IPS, Filtrado de paquetes

4.5 ANÁLISIS DEL PROCESO DE AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN ACTUAL

Actualmente el proceso de auditoría se realiza por un sistema interno de pistas de auditoría están habilitadas desde el sistema informático FACILPAS. Desde ese tiempo se ha configurado 21 tablas donde se encuentra información sensible, en las mismas que se registran eventos tales como: inserción, actualización y eliminación de registros. Los registros que se

guardan son: el usuario y la fecha de modificación, está información puede ser accedida desde las opciones de pistas de auditoría.

Lo que permite que las tablas registren esos datos, es una configuración llamada Flashback Data Archive es una herramienta propia de la base de datos Oracle, la misma que se encuentra activada y guarda un histórico de todos los cambios que se haga sobre los registros de la tabla. Está opción es usada por la base de datos para fines de recuperación, pero también se la ha estado utilizando con la finalidad de evidenciar los cambios hechos por un usuario.

Figura 4.3 Sistema actual de pista de auditoría.

Es importante tener en cuenta que la utilización de la auditoría propia del motor de base de datos, provoca un gran crecimiento de la misma en espacio y afecta el rendimiento y desempeño de dichas bases de datos, debido a la alta transacciónalidad que manejan la base datos para prestar

servicio a los diferentes sistemas que cumplen con el objetivo de servicio a la ciudadanía, es por esto que al tener una herramienta dedicada no se afecte el rendimiento, desempeño y disponibilidad de las Bases de Datos Institucionales, ni aumentar el procesamiento de las mismas.

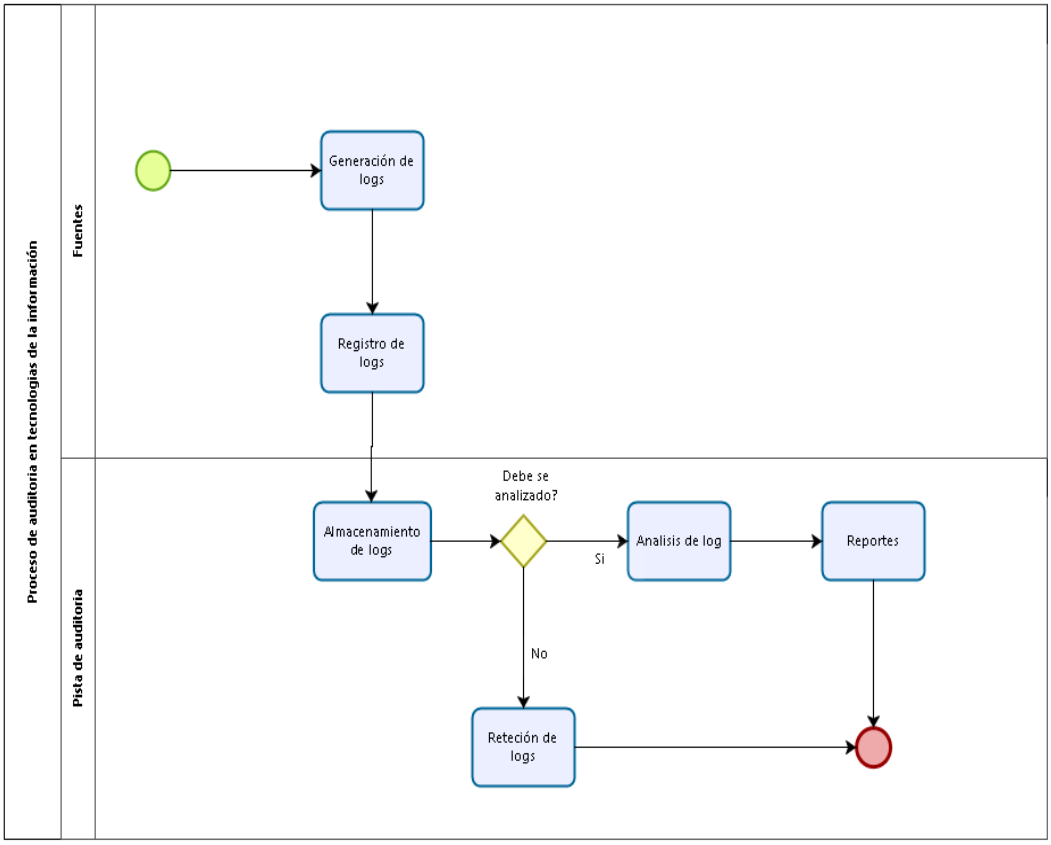


Figura 4.4 Proceso actual de pista de auditoría.

4.5.1 Descripción del proceso actual

El proceso actual consiste en el almacenamiento de los logs de 19 tablas configuradas en la aplicación, el cual se describirá en los siguientes pasos:

1. El proceso comienza con obtención de los logs de los cambios realizados como de las modificaciones o la inserción de las tablas.
2. Registro de los logs en tablas temporales, las cuales retiene la información por un máximo de 3 días antes de ser borradas.
3. Luego la información mediante un proceso batch para hacer almacenadas en tablas históricas.
4. El usuario que utiliza la aplicación es el que decide qué información de la tabla pasa hacer analizada.
5. La información es analizada tanto la hora que se realizó la inserción, modificación del registro, dirección ip y el usuario.
6. La información analizada pasa a un reporte que el usuario se descarga.
7. Luego la información es retenida según la configuración que es por disposición de contraloría de 7 años.

4.6 MEJORAS DEL PROCESO DE AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN.

La institución ve la necesidad de mejorar el proceso de seguridad de la información que permita cumplir con lo señalado en las Normas del acuerdo 166, así como las normas internacionales de Seguridad de la Información.

En base a la realidad actual de la institución se requiere implementar controles:

- Controlar los cambios que sean necesarios sean hechos directos en las bases de datos de producción.
- Poder identificar acciones realizadas en las bases de datos, incluyendo las acciones llevadas a cabo por los Administradores.
- Establecer procedimientos específicos para la manipulación de la información de las bases de datos.
- Llevar una auditoría completa de las acciones ejecutadas sobre las bases de datos.
- Registrar y controlar tanto el acceso como las acciones que se ejecuten sobre una base de datos.
- Control de acceso por permisos definidos.
- Generar alertas tempranas en caso de una violación directa a las bases de datos.

Dando cumplimiento a los controles planteados, se ve la necesidad de respaldar los logs de los dispositivos que interviene en el nuevo proceso de correlación de eventos de seguridad. Para ellos se describe los pasos

1. El proceso comienza con la obtención de los logs por parte de un agente.
2. Él envió de los al componente principal mediante protocolos SSH.
3. Después es el almacenamiento y retención según la configuración del componente principal.
4. Análisis del log mediante la configuración del equipo.
5. Se normaliza, Correlaciona y Reporta los logs generados por los agentes.
6. Relazado el reporte se puede alertar a los administradores de seguridad.
7. Alerta el administrador está en la capacidad de atender y remediar el incidente.
8. Seguridad de log, se protegen lo logs mediante cifrado.
9. La etapa de eliminación es según la configuración y normas de seguridad de la institución.

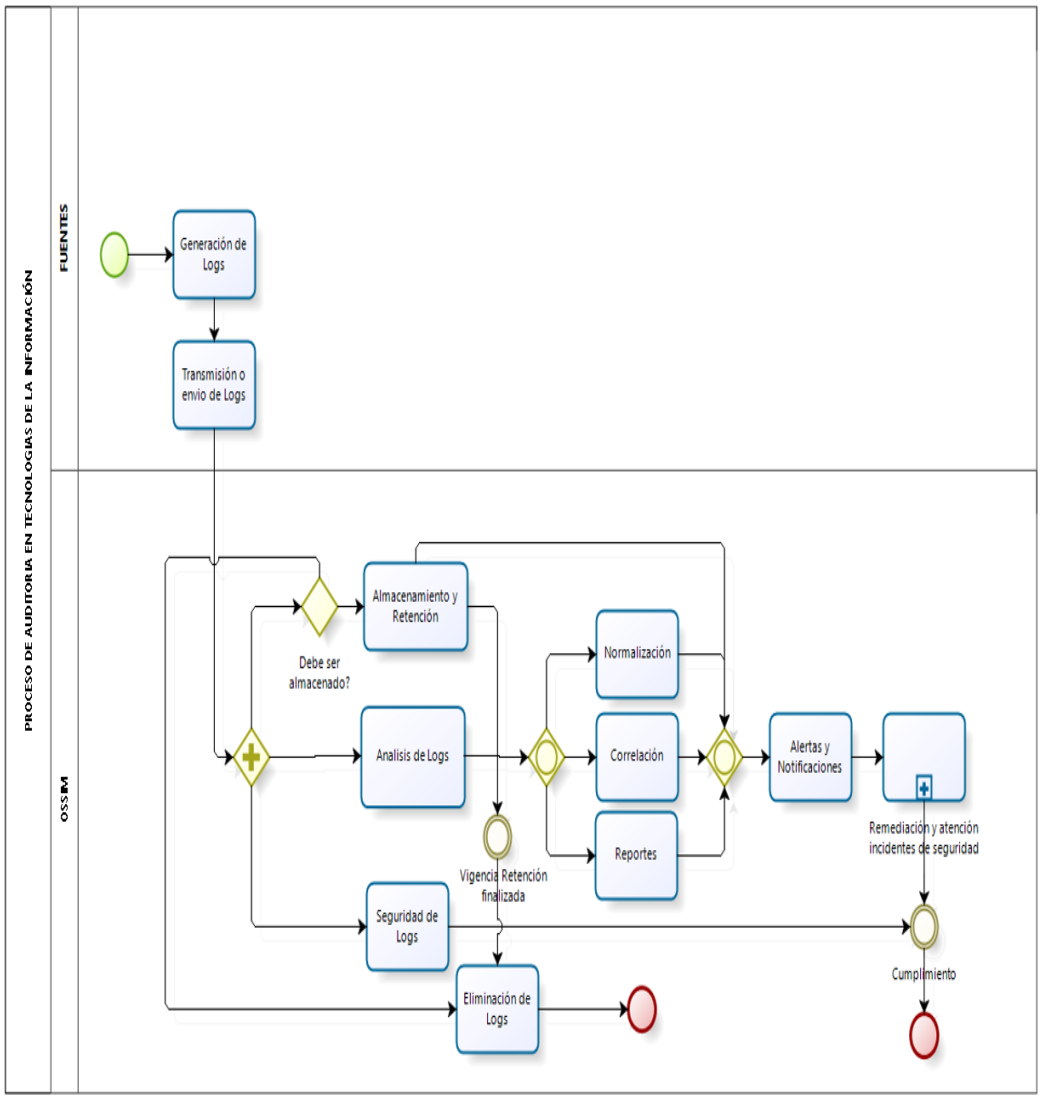


Figura 4.5 Mejora del Proceso actual con la herramienta OSSIM.

4.7 ARQUITECTURA PROPUESTÁ PARA HERRAMIENTA OSSIM

La arquitectura mostrada en la figura 4.10, indica el esquema de conexión del servidor OSSIM con equipos tecnológicos que son comúnmente utilizados en una infraestructura de red tradicional. El servidor OSSIM, es un elemento virtual

a través de software, por sus prestaciones se ha otorgados la mejor prestación a nivel de hardware, para un correcto despliegue y administración.

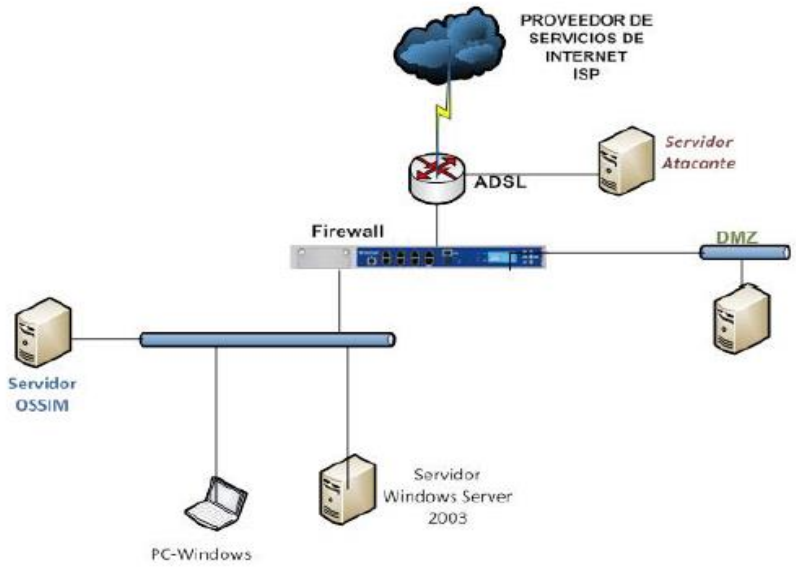


Figura 4.6 Red de la infraestructura tecnología propuesta.

4.7.1 SELECCIÓN DE FUENTE DE EVENTOS

Los equipos tecnológicos son variados (Windows y Linux) que fueron seleccionados como fuente de eventos, que es comúnmente empleada en las instituciones pequeñas. En las tablas 10 y 11 se detalla el tipo de fuente, servicio que presta y el aplicativo a ser integrado en la solución propuesta para el escenario de pruebas.

Tabla 10 Equipos de prueba de concepto

Nombre del servidor o equipo	Hostname	Sistema Operativo
Sistema de gestión de eventos de seguridad informática	OSSIM	UNIX
Sistema de seguridad perimetral	Firewall	Unix
Servidor de aplicación web	Apache- Server	Unix
Servidor de Base de datos	Base de datos	Unix

Descripción Nombres Identificadores de Fuente de Eventos.

Tabla 11 Descripción de los equipos de prueba de concepto

Nombre del servidor o equipo	Fuente	Descripción
Sistema de gestión de eventos de seguridad informática	Logs de Seguridad	Servidor de sistema de gestión de eventos de seguridad informática
Sistema de seguridad perimetral	Logs de Firewall de Seguridad	Servidor que aplica reglas de seguridad a la intranet
Servidor de aplicación web	Log de seguridad de acceso web	Servidor donde registran las operaciones del negocio
Servidor de Base de datos	Log de seguridad de acceso de base de datos	Servidor de base de datos donde registran las transacciones del negocio

CAPÍTULO 5

IMPLEMENTACIÓN DE LA HERRAMIENTA OSSIM OPEN SOURCE

5.1 APLICACIÓN DE LA GUIA METODOLÓGICA

Para la creación se la guía metodológica se tomó como base teórica el Acuerdo Ministerial numeral 166 [12] publicado por la secretaria Nacional de Administración pública que en su numeral 6.26 solicita:

a) Identificar el nombre del usuario
b) Registra fecha, hora y detalle de los eventos, registro de inicio y de cierra.
c) Registro de cambios de configuración.
d) Registro de intentos ingreso aceptados y rechazados.
e) Registro del uso de privilegio.
f) Registro el uso del sistema.

g) Registro de acceso al sistema

h) Registra los protocolos y direcciones de red.

i) Definir alarmas originada por el sistema.

De acuerdo estás bases teóricas se proponen gestionar y administrar adecuadamente los logs de los equipos y dispositivos de red mediante el uso de la herramienta coleccionadora de eventos OSSIM que cumple con esta metodología.

Adicionalmente dando cumplimiento con la norma emitida por la Organización Internacional de Normalización (ISO), la cual describe cómo gestionar la seguridad de la información, se ha analizado las buenas prácticas que constan en la norma ISO 27002 en la cual se describe los objetivos de control y controles que se integran dentro de todos los requisitos de la norma ISO 27001 en relación con el tratamiento de los riesgos.

En la sección Protección de los datos de prueba del sistema, es importante poder aplicar los siguientes controles:

- Identificar por cada sistema, los datos que pueden ser copiados de un ambiente de producción a un ambiente de pruebas.

- Solicitar autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba y poder ejercer el control de la ejecución de este tipo de acciones incluyendo a los administradores de bases de datos.
- Identificar los datos críticos que deberán ser modificados o eliminados del ambiente de pruebas y poder tener un módulo de auditoría que permita comprobar la correcta ejecución de dichas acciones autorizadas.
- Eliminar inmediatamente, una vez completadas las pruebas, la información de producción utilizada.
- Registrar la copia y la utilización de la información para futuras auditorías.
- Controlar que la modificación, actualización o eliminación de los datos operativos (de producción) serán realizados a través de los sistemas que procesan esos datos, y de acuerdo al esquema de control de accesos implementado en los mismos.
- Se considerarán como excepciones, los casos en que se requiera realizar modificaciones directamente sobre la base de datos, para lo cual el personal asignado definirá los procedimientos para la gestión de dichas excepciones.

Las normas que dictan las buenas prácticas recomiendan:

- La información nunca sea eliminada, es decir, puede ser modificada o actualizada.

- Crear cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones, las cuales deben ser protegidas, mediante contraseñas, monitorizadas y sujetas a los mismos controles de seguridad que establezcan los procedimientos de la institución.
- Es indispensable que se registren todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por la persona que sea asignada para el monitoreo responsable de las mismas.

La institución ve la necesidad de adquirir una herramienta tecnológica de seguridad de Base de Datos que permita cumplir con lo señalado en las Normas de Control Interno, así como las normas internacionales de Seguridad de la Información.

5.2 DIAGRAMA DE FLUJO DE LOS CONTROLES TECNOLÓGICOS DE LA HERRAMIENTA OSSIM

La estructura de guía metodológica se basa en el siguiente diagrama de flujo de datos, en el cual se exponen cada uno de los pasos que hacen parte de la guía metodológica.

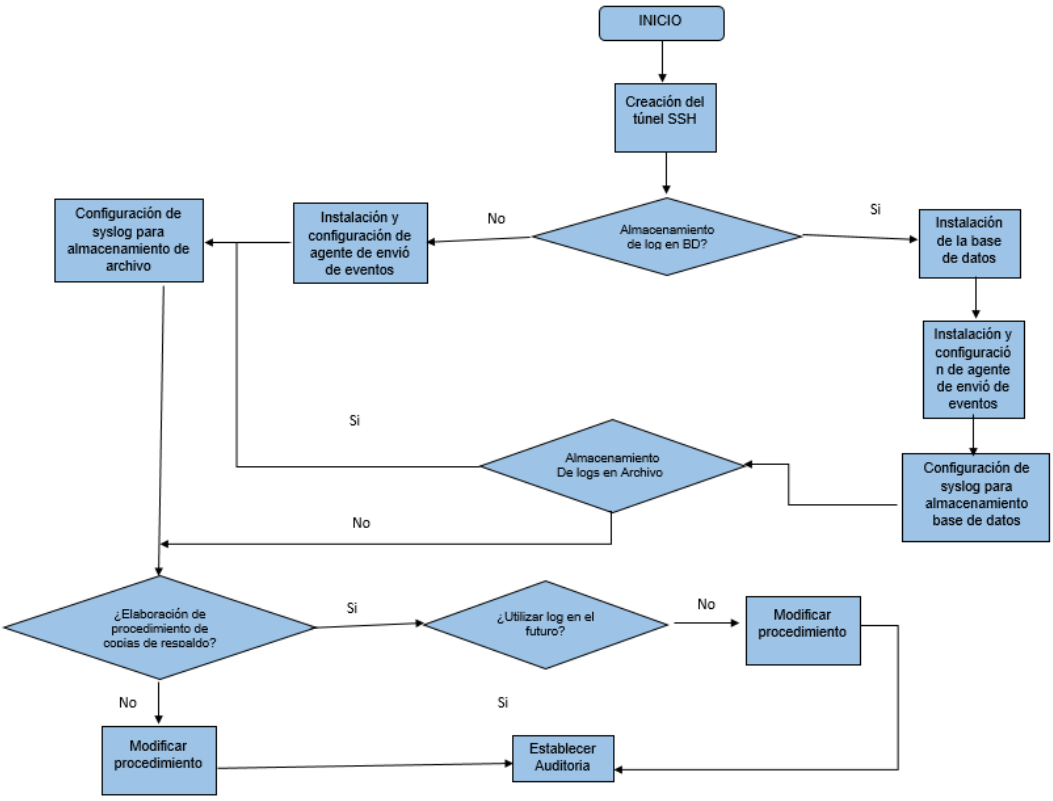


Figura 5.1 Diagrama de flujo de la metodología

5.2.1 Creación de Túnel SSH

Para la creación del Túnel SSH se debe realizar bajo un mecanismo de autenticación, el mecanismo más recomendado es por llaves públicas o privadas. Con el fin del establecimiento de túnel que pueda hacerse con un servicio del sistema operativo, y adicional la creación de un túnel y un proceso de autenticación que sea transparente para el usuario final.

En los sistemas operativos Windows, el establecimiento de túnel, es necesaria contar con privilegios de administrador. El objetivo es la creación de la cuenta para establecer el servicio, ya que deben estar ligados a la cuenta del usuario.

5.2.2 Instalación de la base de datos.

El almacenamiento de logs, tiene dos opciones: almacenamiento de base de datos o almacenamiento de logs en archivos. Las dos opciones son: almacenamiento de logs en la base de datos o promedio de archivos planos.

Para el almacenamiento en Base de datos, se deber realizar la instalación de Mysql en el servidor de logs. Luego, se debe realizar la creación de la base de datos de logs y finalmente se debe configurar, el cual se encargará de realizar la comunicación entre syslog y mysql.

5.2.3 Instalación del agente de envió de eventos

Para la recepción de registro de eventos de seguridad antes de la instalación del syslog, es necesario instalar el agente, después se debe configurar para que sincronice con el servidor.

Luego se debe realizar la instalación del syslog como un servicio del servidor, con el fin de inicializar el sistema operativo. Al configurar de esta manera hace que el sys-log levante automáticamente.

Adicionalmente, por medio de un archivo de configuración el syslog decide se va realizar el almacenamiento de logs por medio de archivos planos o por medio de la base de datos.

Esto se realizar con el fin que los eventos de seguridad queden registrados y puedan ser consultado en el presente o en el futuro según sea necesario. La copia de seguridad, se van realizar dependiendo la configuración, siempre se debe indicar la periodicidad que se va realizar y la identificación de los archivos.

5.2.4 Establecer Auditoría.

Después que se haya seguidos los pasos, se debe garantizar que los eventos los eventos fueron generados o modificados por un sistema que se base en la guía metodológica, se sugiere que se realice auditorías periódicas, en la cuales evalué su funcionamiento.

5.3 IMPLEMENTACIÓN Y CONFIGURACIÓN SERVIDOR OSSIM

La implementación del prototipo del sistema de gestión de eventos de seguridad, contará con un entorno virtual, con ayuda del software VMWARE; previo a la creación de la máquina virtual para el servidor OSSIM, se detalla brevemente, los requerimientos de hardware del servidor OSSIM.

5.3.1 Dimensionamiento de Hardware

Los requerimientos que se requiere de hardware dependen de mucho de los eventos de seguridad que tenga que analizar, como también la cantidad de registro que se almacene en la base de datos y en los repositorios de los clientes (agentes) que se requiere en la red, de acuerdo al dimensionamiento EPS de la Tabla 1, se estableció los requerimientos mínimos como muestra la tabla.

Tabla 12 Requerimientos mínimos de Hardware

Parámetro	Valor
Procesador	1 núcleo
Memoria	3 GB
Disco Duro	20 GB
Tarjeta de Red	10/100 Mbps
Interfaces	Óptica, USB

5.3.2 Requisitos Previos a la Instalación de OSSIM

Además de los requerimientos técnicos de hardware descriptos en la tabla 12, es importante indicar a los administradores del sistema OSSIM los conocimientos básicos necesarios, para interpretar, analizar y administrar adecuadamente el OSSIM, los conocimientos mínimos son los descriptos a continuación:

- Tener un conocimiento medio de Seguridad Informática.
- Tener conocimientos básicos de Redes
- Demostrar conocimiento medio en Sistemas Windows y Linux.
- Conocer e interpretar a nivel avanzado los registros o logs de seguridad.
- Tener un conocimiento medio en seguridad de la información y normas ISO/IEC 27002.

5.3.3 Requerimiento funcionales

Los registros de eventos deben quedar guardados en un repositorio central.

El elemento principal es el transporte del logs al repositorio central ubicado en el servidor OSSIM. De este modo el registro queda ubicado en punto central donde puede ser analizado.

Es necesario que el registro del evento de seguridad quede un formato para su correlación. Este formato debe contener la identificación del sistema que género el evento en tiempo y el detalle.

La estructura del ventó enviado al servidor OSIIM, está compuesto por tres campos: PRI (prioridad del evento, HEADER (se encuentra el tiempo y el origen del evento) y MSG (contiene el nombre de programa y el detalla del evento.

El tiempo del servidor OSSIM y el agente debe estar sincronizado

Al sincronizar el tiempo en los dos dispositivos se garantiza que el tiempo presentado en el registro del evento sea el correcto. Adicional, el protocolo syslog, se configura para que el formato se muestre en fecha y hora.

5.3.4 Requerimiento No funcionales

La comunicación entre el agente y el servidor debe ser confiable: se debe garantizar la integridad de datos y los datos debe ser cifrados.

El protocolo SSH es el medio de comunicación entre el agente y el servidor. El protocolo es orientado a la conexión. Es un protocolo que suministra privacidad de datos utilizado algoritmo de cifrado Las llaves publicas garantiza que los datos llegan al servidor OSSIM.

Se debe asegurar que los logs no sufran ningún cambio para su correlación.

EL protocolo SSH garantiza la integridad de los datos mediante el uso de algoritmo HASH garantizando la integridad de los datos.

Los registros de eventos de seguridad no deben ser eliminados en tiempo presente y futuro.

Para permitir que los eventos de seguridad permanezcan en el tiempo se debe procedimientos internos documentados en los cuales se describa el proceso de respaldo. Las normas de la contraloría general del estado en el ACUERDO No. 013, en su artículo 10 nos indica “La documentación sujeta a control y seguimiento institucional, debe ser

conservada durante 7 años contados a partir de la fecha de emisión de la misma, sea en un formato físico o medio digital.” [13]

5.4 INSTALACIÓN DEL SERVIDOR OSSIM

5.4.1 Instalación de Máquina Virtual y Sistema Operativo del Servidor OSSIM

A continuación, se detalla la instalación de la máquina virtual de 64 bits del servidor OSSI. De acuerdo la instalación se debe habilitar la tecnología VT para poder instalar el sistema OSSIM de 64 bits sin ningún problema.

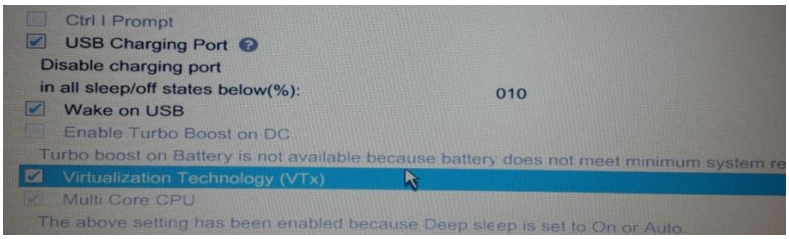


Figura 5.2 Habilitación en el BIOS de la tecnología VT.

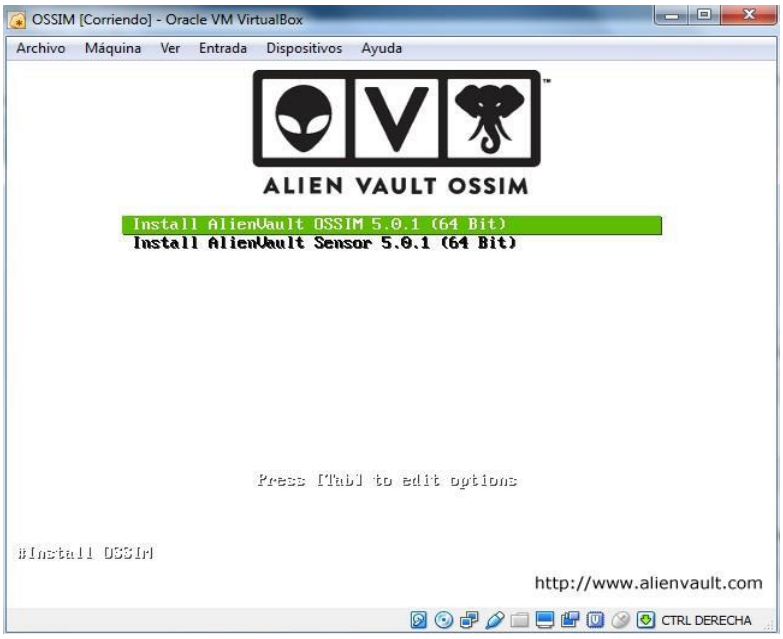


Figura 5.3 Pantalla de Inicio de la instalación

Figura 5.4 Pantalla de selección de idioma

Figura 5.5 Pantalla de selección país

Figura 5.6 Configuración IP

Figura 5.7 Configuración de mascara de red.

Figura 5.8 Configuración puerta de enlace

Figura 5.9 Establecimiento de usuario y contraseña

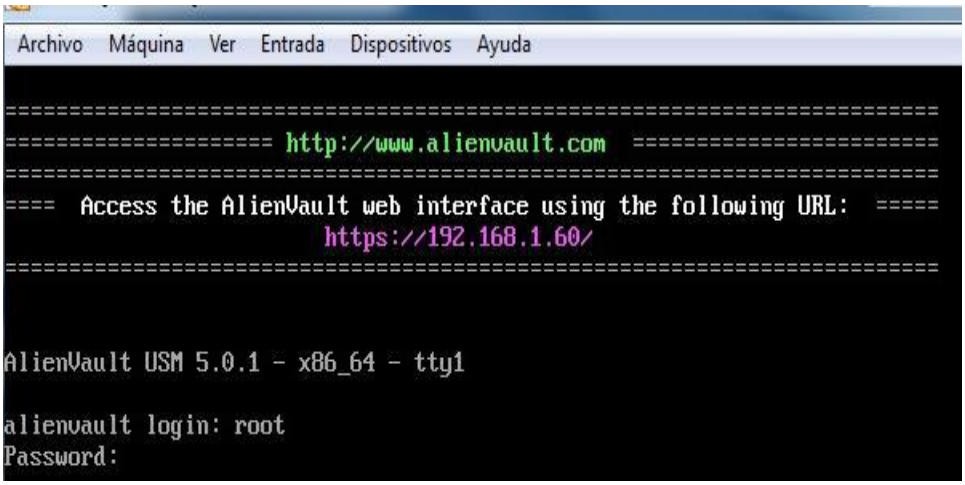


Figura 5.10 Pantalla de login al sistema

5.4.2 Configuración de Servidor OSSIM

Una vez estableció el usuario y la contraseña se debe configurar los principales componentes de OSSIM, se puede ingresar a la interfaz web con la url https://192.168.100.60, donde se ingresa con el mismo usuario y clave que se configuro, nos ayuda a verificar los descubrimientos y los logs recolectados de los equipos que tiene configurado.

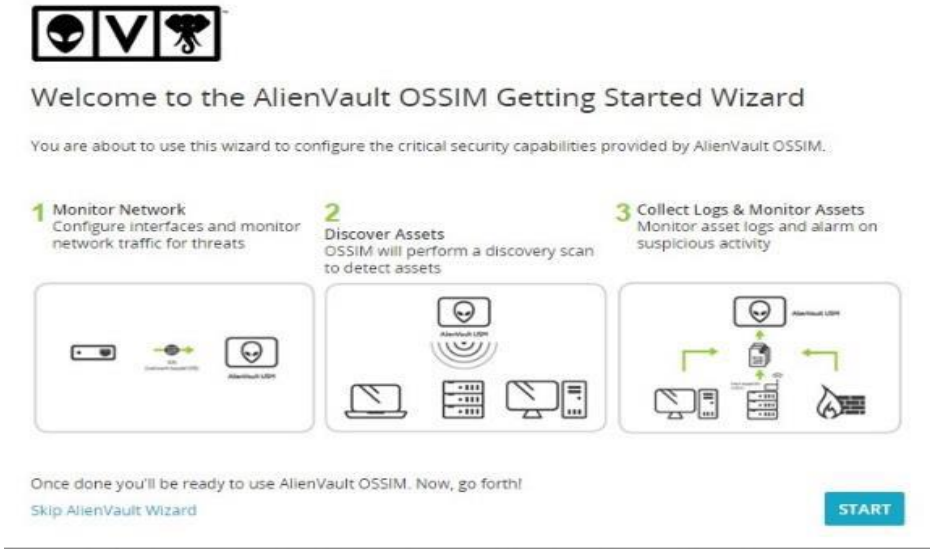


Figura 5.11 Pantalla de Bienvenida de configuración de OSSIM

Se utilizó cono ejemplo la opción de descubrimiento de equipos, lo que podrá recolectar eventos y logs de forma automática. De acuerdo al escaneo de la red interna. En el escaneo puede detectar equipos de la red interna.

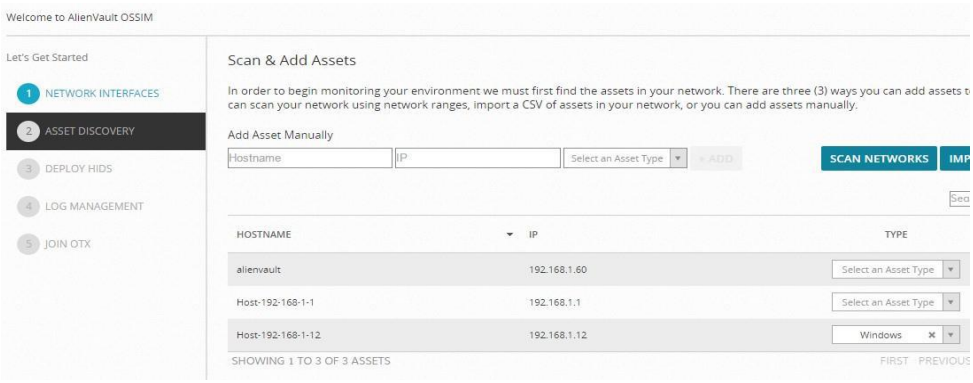


Figura 5.12 Escaneo de equipos de la red interna

Después de haber hecho el análisis de la red tal como se muestra en la figura 524, la aplicación refleja opciones varias opciones como es el Dashboard, el cual permite tener una visualización global de estado del sistema, cuenta control general de los eventos, análisis, reportes, configuración entre otras opciones para una administración completa de la aplicación.

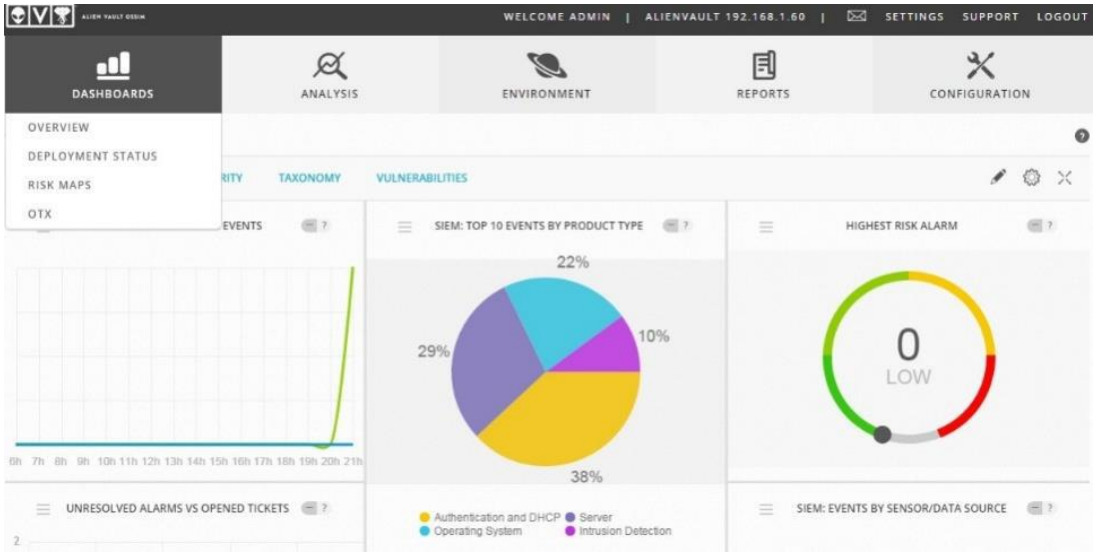


Figura 5.13 Dashboard del sistema de gestión de eventos

5.5 Instalación y Configuración de Fuentes de Eventos

La configuración del agente se realiza una vez detecta las maquinas en la red interna, luego se realiza la instalación del agente, se activa el registro de log de seguridad. Posterior se detallan los pasos de relación de e integración de la base de datos con el servidor OSSIM.

5.5.1 Instalación y configuración Servidor Base de Datos

Para este ejemplo hemos instalado una base de datos de prueba, se inicia instalando el Mysql-Server con el comando apt-get, se define usuario y contraseña como se muestra en la figura 5.14, se lo realiza con el fin de facilitar la creación de la base de datos.

Figura 5.14 Instalación del paquete MySQL

A continuación, se crea la base de datos en este ejemplo se va crea tres tablas un registro de usuarios, usuario_sistemas y otra de auditora, conoce muestra en la figura 526.

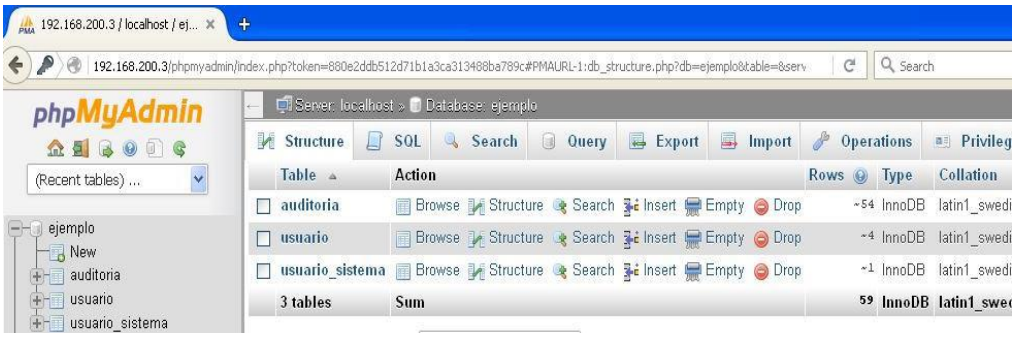


Figura 5.15 Creación de la base de datos de Ejemplo

5.5.2 Agente OSSIM en el servidor de base de datos

Posterior a la instalación de la base de datos se procede a la configuración del agente de eventos de seguridad del servidor. A través del agente OSSIM.

5.5.3 Instalación del agente OSSIM

La instalación del agente del OSSIM, se encarga de recolectar y enviar al servidor OSSIM a través de la red interna, en las figuras 526 a 529 se muestra la instalación del agente.

Figura 5.16 Instalación del agente

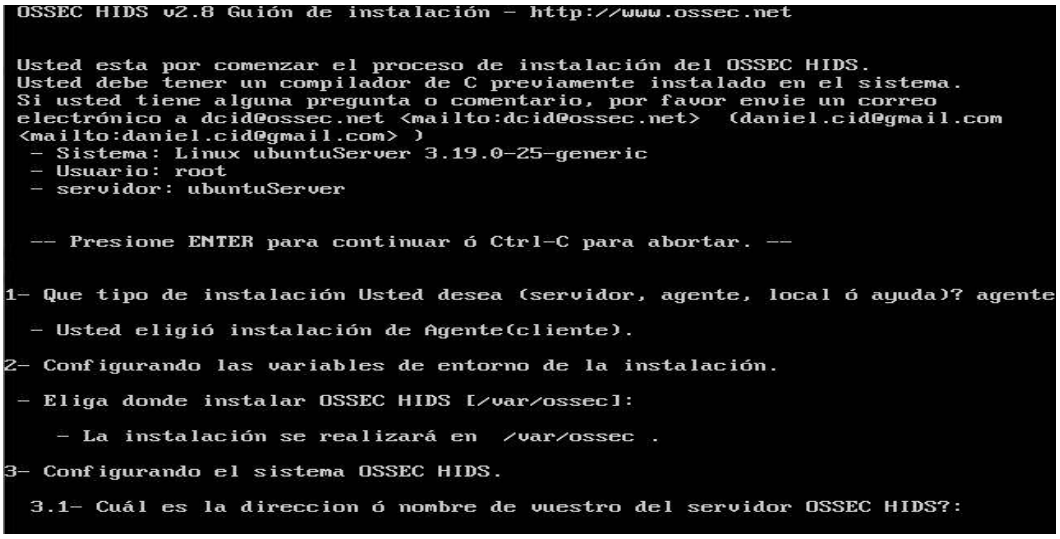


Figura 5.17 Proceso de instalación agente

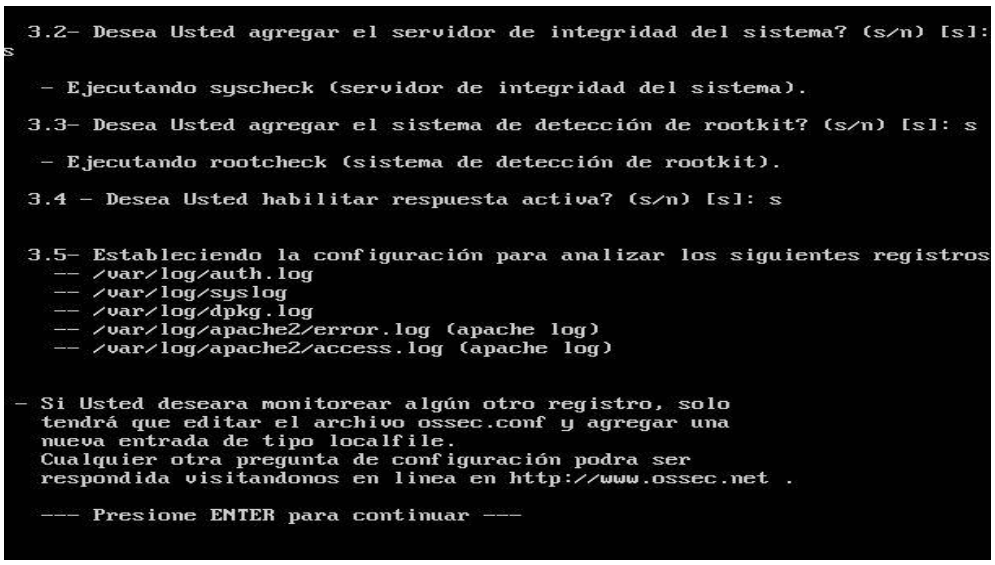


Figura 5.18 Selección de opciones para agente

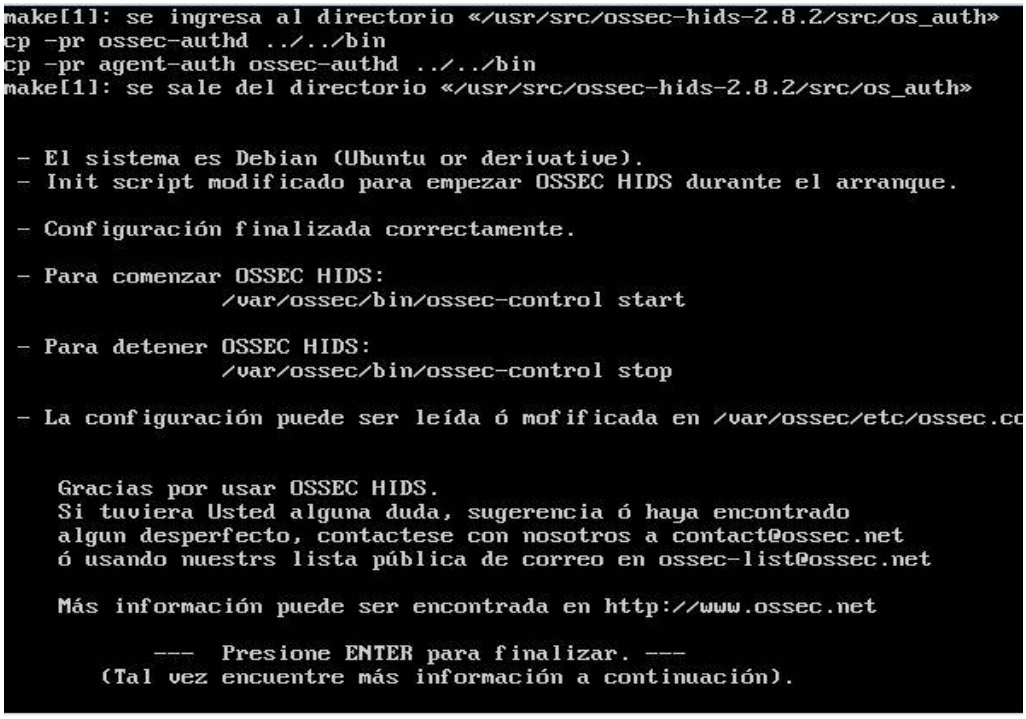


Figura 5.19 Instalación Finalizada

5.5.4 Integración del agente con en el servidor OSSIM

El último paso es la integración del agente con el servidor OSSIM, se crea un agente, pero dentro del módulo Detección, el estado del agente cambia una vez activado esto se lo puede ver en la sección Status. En las figuras 531 a 533 se muestra la instalación del agente.

Figura 5.20 Creación agente en el Server

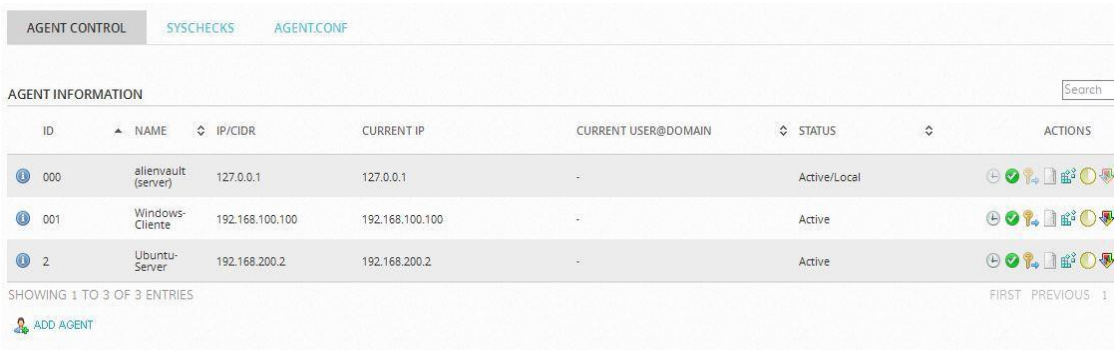


Figura 5.21 Agente Activado

Para comprobar el funcionamiento del agente con el servidor, se deber realizar el reinicio del servicio, para poder visualizar el estado tal como lo muestra la figura 5.22.

EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP
ossec: Login session opened.	0	ossec-authentication_success	alienvault	Ubuntu-Server
ossec: SSHD authentication success.	0	ossec-authentication_success	alienvault	192.168.200.1:39818
ossec: SSHD authentication failed.	0	ossec-authentication_failed	alienvault	192.168.200.1:39816
ossec: User login failed.	0	ossec-authentication_failed	alienvault	Ubuntu-Server

Figura 5.22 Recolección en tiempo real de logs.

5.6 Creación y Configuración de Directivas

A continuación, se detalla el conjunto de paso para la creación de directivas de seguridad, que nos ayudara a generar alarmas según las reglas definidas por el administrador. Las reglas serán definidas y se configura según el evento que se

desea monitorear o de acuerdo al evento anormal que se registre en la red. Como propósito de ejemplo se realizará un ingreso a la base que será registrado en la plataforma, por lo cual se creará una directiva para el registro de log.

La configuración de reglas ayuda brindar ejemplos de casos específicos de eventos que pasan en nuestra red, Se recomienda la creación de reglas, análisis de los log de la red, que deseamos monitorea y generar alertas.

Escenario: El usuario se conecta a la base de datos.

Nombre de la Directiva: Acceso- Database -Exitoso

LOG GENERADO:

Tabla 13 Directiva de acceso a la base de datos

Fecha	Nombre de evento	Riesgo	Generador	Sensor	Ip Fuente	Ip Destino
2018-04-11-16:40:15	Database authentication	0	autentication_ susccess	alienvault	Server BD	OSSIM -Server

Se detalla la configuración de la regla “Conexión-BaseDatos-Exitosa” se ilustra en las Figuras 5.23 a la 5.27.

Figura 5.23 Configuración de la regla / Selección de Prioridad

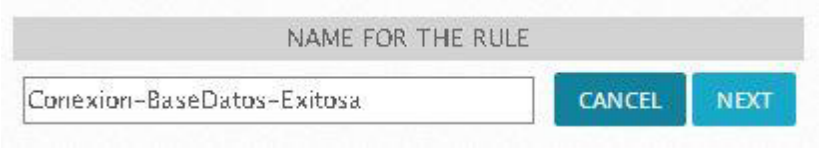


Figura 5.24 Establecer nombre Regla Conexión Base de Datos Exitosa

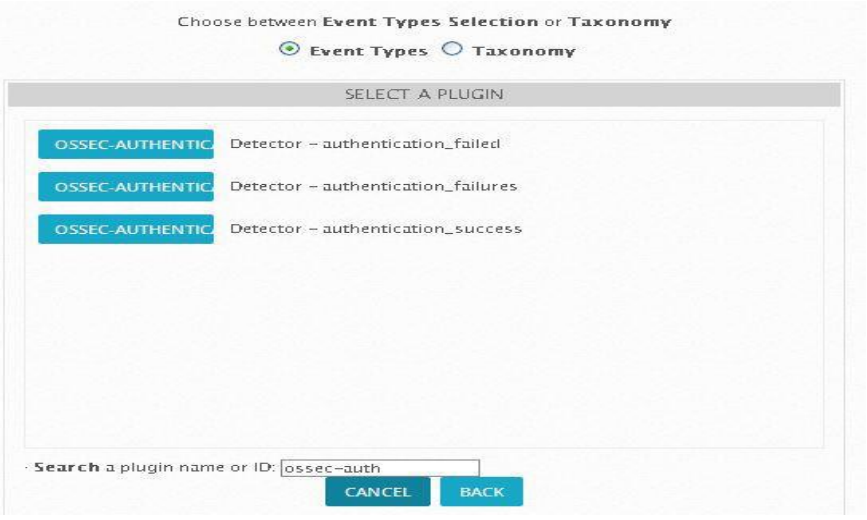


Figura 5.25 Selección de agente

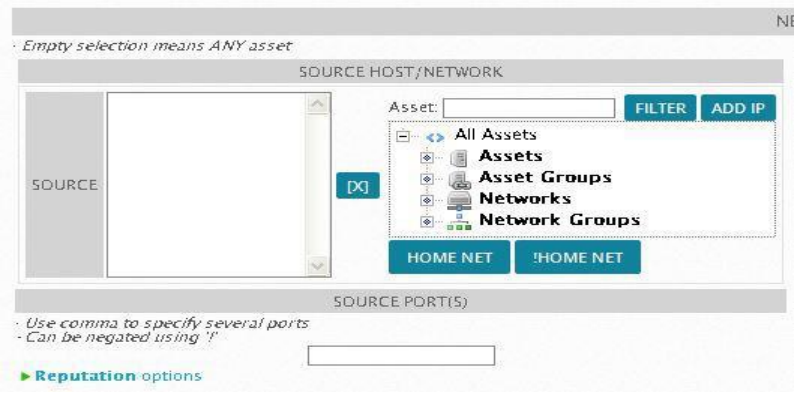


Figura 5.26 Selección de Host Origen

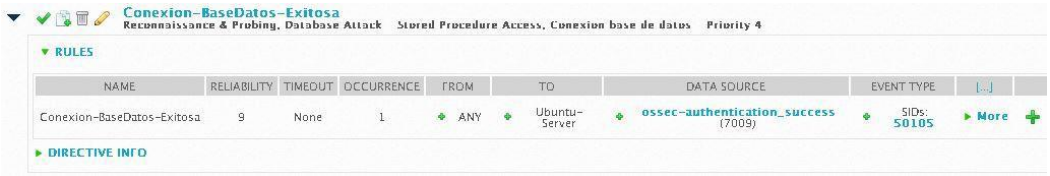


Figura 5.27 Directiva creada

Para ilustrar el funcionamiento de la regla se va proceder a modificar el valor de un registro, la figura 5.28 ilustra se demuestra.

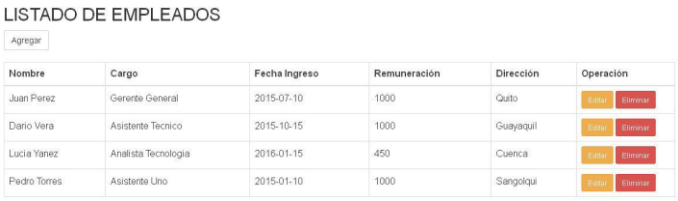


Figura 5.28 Ingreso a Base de Datos

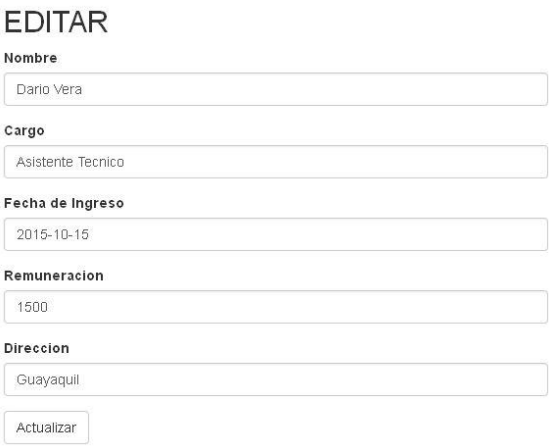


Figura 5.29 Modificación de Datos

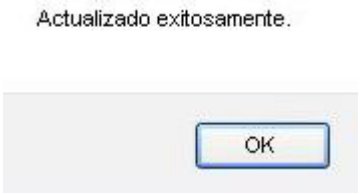


Figura 5.30 Actualizo exitosamente

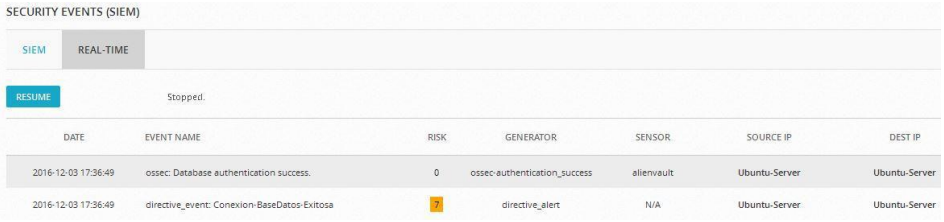


Figura 5.31 Directiva generada

5.7 RESULTADO DE LAS PRUEBAS DE CONCEPTO

Una vez configurado la regla y la alarma en el servidor OSSIM, se procede ejecutar el escenario de prueba a manera de simulación de acciones, que se realiza en un lapso de un minuto. Se menciona en este punto que el sistema OSSIM debe recolectar mayor log para una correcta detención temprana de un ataque. En las figuras se ilustra el acceso a la base de datos.

ESUME Stopped.

DATE	EVENT NAME	RISK	GENERATOR	SENSOR	SOURCE IP	DEST IP
2016-12-03 17:48:50	ossec: Database authentication success.	0	ossec-authentication_success	alienvault	Ubuntu-Server	Ubuntu-Server
2016-12-03 17:48:50	directive_event: Conexion-BaseDatos-Exitosa	7	directive_alert	N/A	Ubuntu-Server	Ubuntu-Server
2016-12-03 17:48:48	ossec: Database authentication success.	0	ossec-authentication_success	alienvault	Ubuntu-Server	Ubuntu-Server
2016-12-03 17:48:48	directive_event: Conexion-BaseDatos-Exitosa	7	directive_alert	N/A	Ubuntu-Server	Ubuntu-Server
2016-12-03 17:48:46	ossec: Database authentication success.	0	ossec-authentication_success	alienvault	Ubuntu-Server	Ubuntu-Server
2016-12-03 17:48:46	directive_event: Conexion-BaseDatos-Exitosa	7	directive_alert	N/A	Ubuntu-Server	Ubuntu-Server
2016-12-03 17:48:43	ossec: Windows Logon Success.	0	ossec-authentication_success	alienvault	Windows-Cliente:2080	Windows-Server
2016-12-03 17:48:43	directive_event: Acceso-Windows-Exitoso	10	directive_alert	N/A	Windows-Cliente:2080	Windows-Server
2016-12-03 17:48:42	ossec: Database authentication success.	0	ossec-authentication_success	alienvault	Ubuntu-Server	Ubuntu-Server
2016-12-03 17:48:42	directive_event: Conexion-BaseDatos-Exitosa	7	directive_alert	N/A	Ubuntu-Server	Ubuntu-Server
2016-12-03 17:48:34	directive_event: Conexion-UbuntuServerWeb-Exitoso	2	directive_alert	N/A	Windows-Cliente	Ubuntu-Server

Figura 5.32 Resultados del acceso a la base de datos

5.7.1 Alarmas Generadas

Como vemos en la figura anterior, el sistema OSSIM permite alarmar en tiempo real, la misma se encuentra almacenada en el servidor OSSIM para su posterior análisis, así como eventos de seguridad. La información es almacenada de manera que se pueda visualizar de

una forma fácil para el usuario, para ver el análisis se debe ingresar en la sesión de análisis como muestra la figura 5.33.

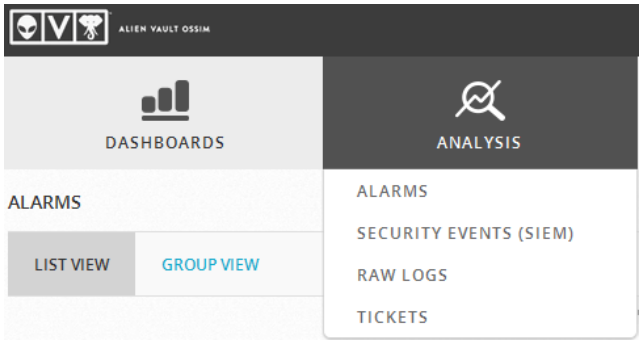


Figura 5.33 Ingreso a Sección Alarmas

Para visitar de manera gráfica las alarmas existe una opción llamada List View, el cual se visualiza de manera histórica los eventos y alarmas generadas se presenta de manera circular; mientras el círculo aumente su tamaño es que se generaron más cantidad de alerta.

Figura 5.34 Vista General de Alarmas

5.7.2 Análisis alarma de Base de datos

La siguiente Figura muestra el número de acceso a la base de datos, el cual genero muchos y eventos, estos son capturados por el agente OSSIM.

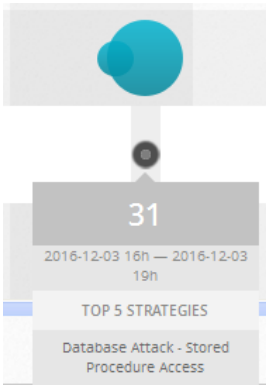


Figura 5.35 Número de Eventos

En la siguiente figura 5.36 se muestra las alarmas generadas por la alerta.

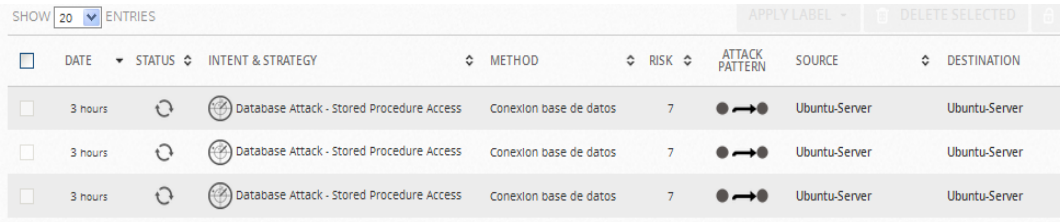


Figura 5.36 - Alarmas Generadas

Para tener más información de la alerta se debe hacer doble clic sobre el icono, la información se presenta detallada e intuitiva para el usuario. Se muestra en la figura 5.37.

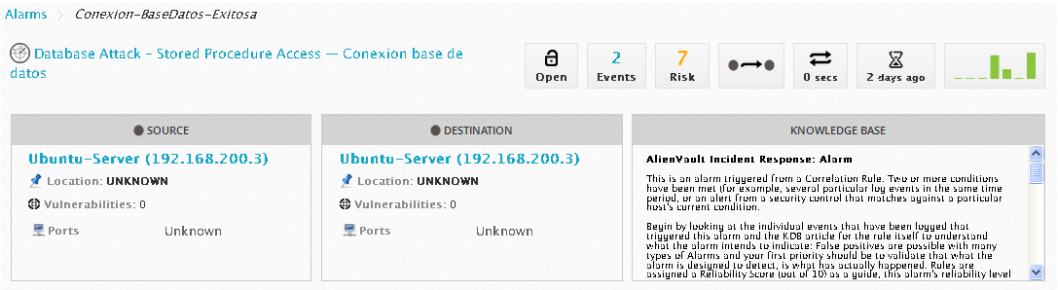


Figura 5.37 Detalle de Alarma

En la siguiente figura 5.38, se muestra las alarmas agrupadas esto se lo realizo con la opción Group View.

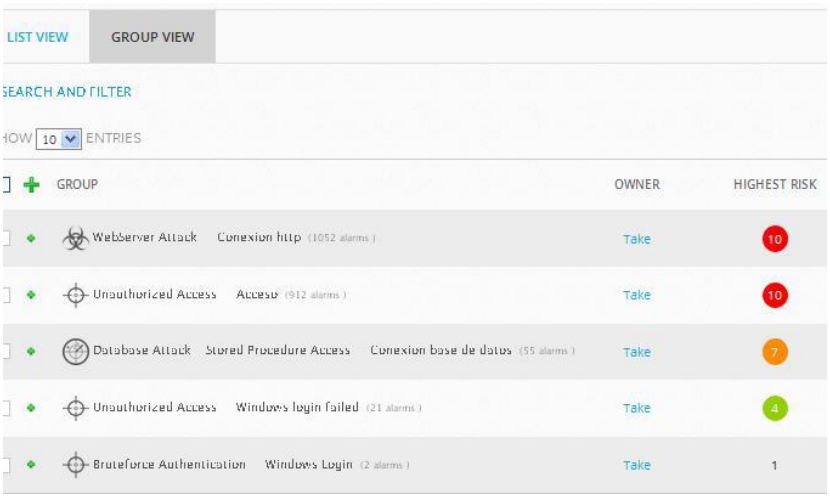


Figura 5.38 Alarmas en grupo

El usuario que administre la herramienta es el responsable de la gestión de evento de seguridad podrá ser uso las múltiples opciones para análisis y revisión de los logs, así como dispondrá de variedades de reporte de incidentes que pueden ser descargado desde la aplicación.

5.7.3 Reportes de alarmas

La opción de reportaría es una herramienta muy útil para el administrador se encuentra en el menú de Reportes, como se indica en la figura 5.39.

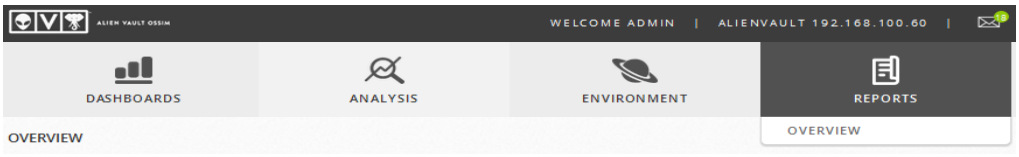


Figura 5.39 Sección Reportes

A continuación, selecciones la opción de reporte de alerta como se indica en la figura 5.40.

Figura 5.40 Generación de Reportes

A continuación, generamos el reporte seleccionando un rango de fechas, este reporte puede descargado en formato pdf, como se visualiza en la Figura 5.41, de las principales alarmas que en este escenario fueron detectadas.

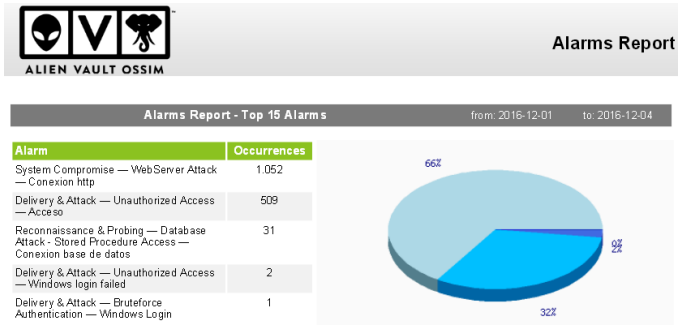


Figura 5.41 Generación de Reportes

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 ANÁLISIS DE RESULTADO ESPERADOS

En este capítulo se llevará a cabo una prueba de concepto en un ambiente controlado de seguridad informática mediante un análisis de vulnerabilidades de la red interna de la institución, mediante la selección y utilización de herramientas de análisis de seguridad no intrusivos en los sistemas. Se realizarán actividades de reconocimiento pasivo con la finalidad de identificar información disponible del objetivo o equipo analizado.

El escaneo de la red se realizó sobre los sistemas activos a nivel de infraestructura y de aplicaciones web con el propósito de que los activos o servidores atacados, generen eventos o logs, que permita al sistema OSSIM detectarlos, disparar alarmas, reportes, estadísticas, entre otros, para una gestión integral. El principal objetivo es mostrar las bondades que tiene OSSIM

como software libre y que permite contar con un sistema de gestión integral de seguridad, permitiendo a las organizaciones disminuir costos en la adquisición de equipos sofisticados de seguridad con licencia, soporte de mantenimiento, etc.

Finalmente, los resultados esperados era la integración de eventos al OSSIM, la evaluación de riesgos de red tomando como referencia Acuerdo Ministerial Nro. 166 basado ISO 27002, lo cual permitirá tener un visión amplia y general de lo que sucede en la red desde el punto de vista técnico y de gestión. Cabe señalar que no se detallarán las vulnerabilidades técnicas halladas por las herramientas de seguridad, pero si se analizarán los eventos o logs, así como las reglas de correlación definidas por el usuario.

6.2 ANÁLISIS DE RESULTADO OPTENIDOS

Los resultados de la auditoría brindaron una visión global de las sentencias y carga generada sobre las bases de datos de Preproducción. Los logs de auditoría entregan mucha información valiosa, entre la que se destaca:

- Usuario de base de datos y SO
- IP fuente y destino
- Sentencia SQL ejecutada
- # de registros consultados o actualizados
- Tamaño y tiempo de respuesta de la sentencia SQL

- Operaciones y su tipo, objetos y su tipo
- Esquema y base de datos
- Hits, query hits, hits privilegiados e hits de data sensible
- Logins y logouts
- Tipo de evento y hora exacta del evento (evento es cualquier sentencia sobre la base de datos)

Se pudo evidenciar la facilidad en la navegación sobre la información de auditoría a detalle y además certificó en vivo el uso de los reportes predefinidos que permiten una visión completa del comportamiento y rendimiento del servidor de base de datos protegido. Los reportes que pueden ayudar al DBA y demás interesados en las tareas de administración y afinamiento de la base de datos. Se pueden mencionar:

- Rendimiento de los servidores de base de datos
- Análisis por usuario de base de datos y por usuario de SO
- Análisis por IP, host y aplicación origen
- Sentencias SQL por análisis de carga, tipo, # de registros, data sensible accedida
- Sentencias DDL, DCL y sentencias privilegiadas
- Cambios a esquemas, tablas y procedimientos almacenados
- Errores SQL y logins fallidos

Además, se realizó un escaneo de vulnerabilidades se pudo evidenciar intentos ataques los cuales fueron contabilizaron y presentados en la siguiente tabla:

Tabla 14. Porcentaje de ataques detectados

	Tipo de ataque					
	Escaneo de Puertos	SQL Injection	Denegación de Servicio	Comando Injection	Intentos de logins	Fuerza Bruta
Porcentaje de ataques	20	10	30	50	100	2

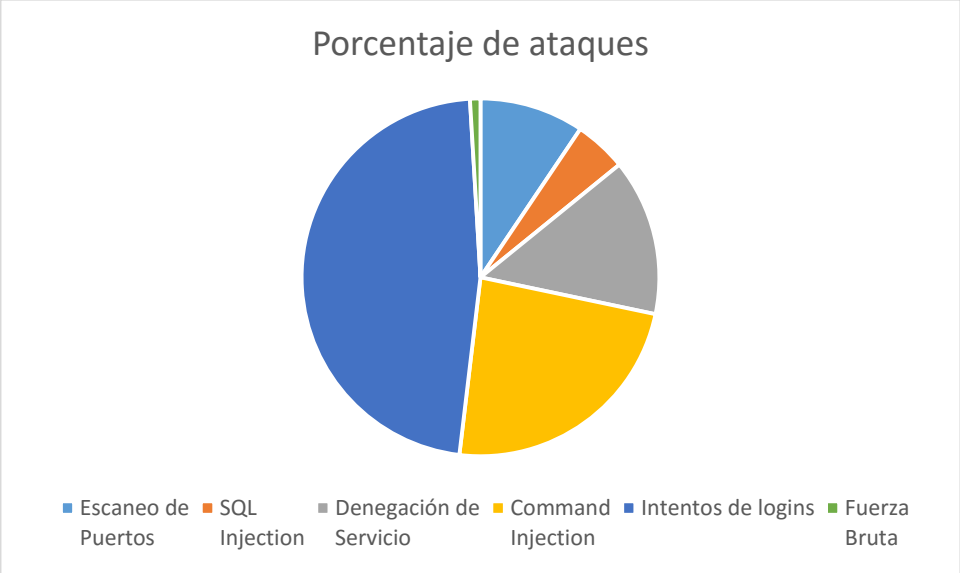


Figura 6.1 Porcentaje de ataques

6.3 VISUALIZACIÓN DE RESULTADOS

La herramienta de gestión de eventos de seguridad OSSIM, ofrece una consola gráfica muy completa que permite una visión general de los eventos producidos en la red interna. El dashboard muestra las estadísticas de los eventos y reglas de seguridad que se están generando en tiempo de ejecución la red de la institución.

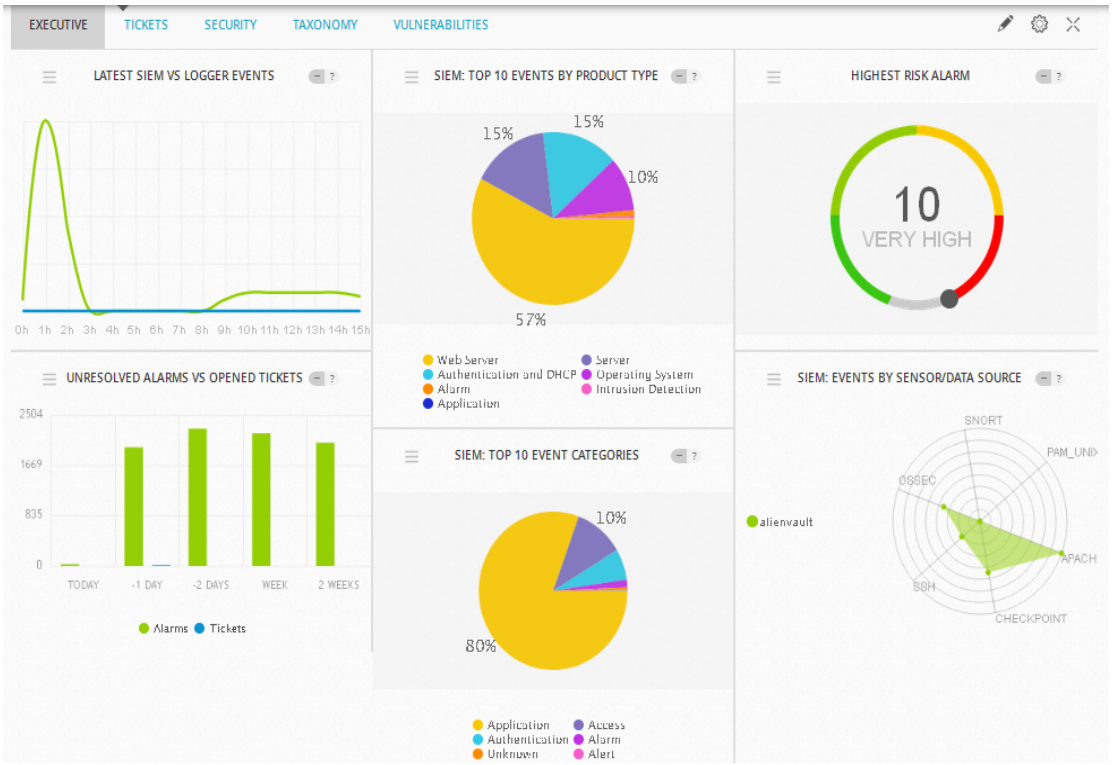


Figura 6.2 Dashboard OSSIM - Tableros de Control

El dashboard es editable según las necesidades del administrador, cada una de las gráficas mostradas en la figura 6.2 nos da información de los eventos

generados en el sistema de gestión de seguridad. A continuación, se muestra la descripción de cada gráfico:

6.3.1 Evento de log

En esta figura 6.3 se muestra los logs que son generados en los dispositivos de la red interna de las últimas 24 horas. El evento se compone de login, acceso a los dispositivos, el componente debe estar habilitado para que la herramienta comience a producir información.

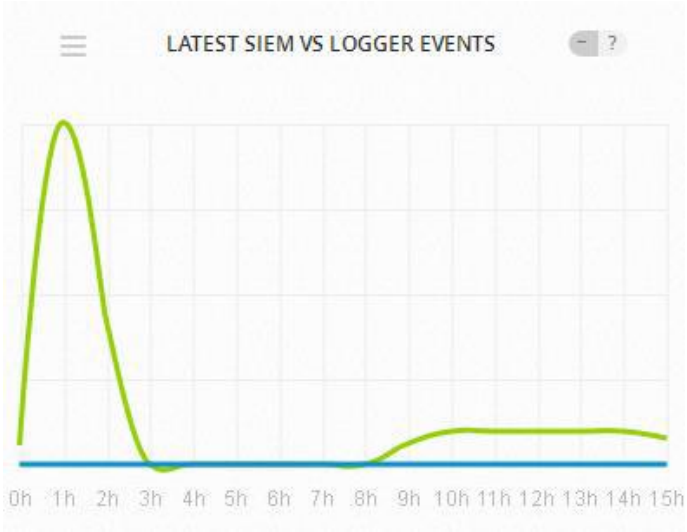


Figura 6.3 Evento de acceso

6.3.2 TOP 10 de Eventos por productos

En la figura 6.4 se muestra los eventos de seguridad agrupados en los 10 más importantes eventos de seguridad, divididos por tipo. Al dar al clic presenta el registro histórico, el detalle de los registros histórico son presentado con Fecha, Ip Origen y Destino.

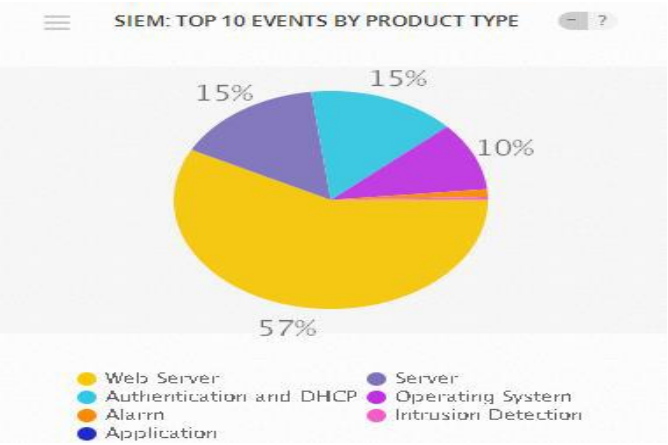


Figura 6.4 TOP 10 de Eventos por productos

6.3.3 Alarma de alto riesgo.

En la Figura 6.56 se muestra un gráfico estadístico que muestra la alarma de mayor riesgo, muestra un valor entero entre de 0 a 10 que se basa en el mayor riesgo de todas las alarmas abiertas que fueron encontradas en el sistema, el riesgo de un evento se calcula a través de la fórmula Riesgo = (Valor del activo * Prioridad del evento * Fiabilidad del evento) / 25. OSSIM en base al resultado obtenido de la fórmula de riesgo asignar las siguientes categorías de riesgo:

En la figura 56, se muestra el gráfico estadístico de los eventos con alto riesgo, lo muestra con una escala de 0 a 10, se basa en la alarma con mayor riesgo para determinarlo la herramienta se base en una formula.

$$RIESGO = \frac{Valor\ de\ activo * Prioridad\ de\ eveto * Fiabilidad\ del\ evento}{25}$$

[6.1] Formula de valoración de riesgo

Valor activo: El valor del activo lo establece en función de su criticidad en la red.

Por ejemplo: Si es un equipo tiene un valor de 3 y el servidor tiene un valor de 5.

Prioridad de evento: Este valor lo establece el usuario.

Fiabilidad del evento: El valor de fiabilidad lo determina el servidor de acuerdo a su algoritmo determina si el log es fiable. Mediante el resultado de esta fórmula se asigna la categoría de riesgo.

Color/ Riesgo	Valor
Muy alto	9, 10
Alto	7,8
Elevado	5,6
Precaución	3,4
Bajo	0,1,2

Figura 6.5 Alarma de alto riesgo

6.3.4 Top 10 Eventos por categoría.

En la figura 655 se muestra los eventos de seguridad agrupados por la categoría del evento, divididos por categoría. Al dar al clic presenta el registro histórico, el detalle de los registros histórico son presentado con Fecha, Ip Origen y Destino.

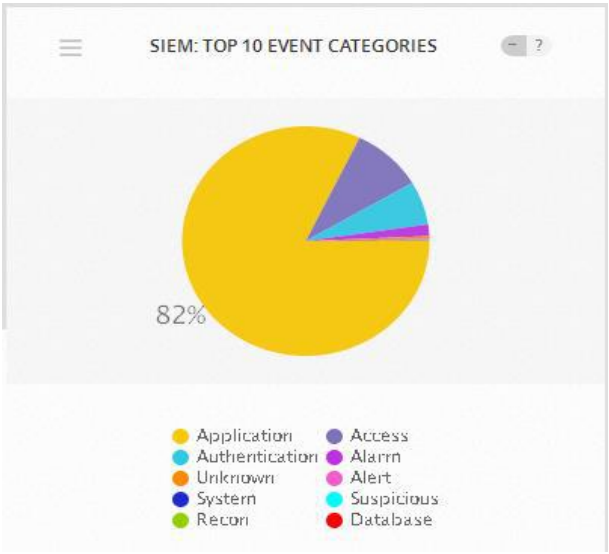


Figura 6.6 Top 10 Eventos por Categoría

6.4 DETECCIÓN Y ANÁLISIS DE EVENTOS

Las gráficas de detección y análisis de evento son muy útiles para observar la cantidad de alarmas generadas en los dispositivos y la criticidad que tiene, se debe ingresar haciendo clic a la gráfica tal como se puede visualizar en la figura 6.7, en este caso se analiza los ataque generados.

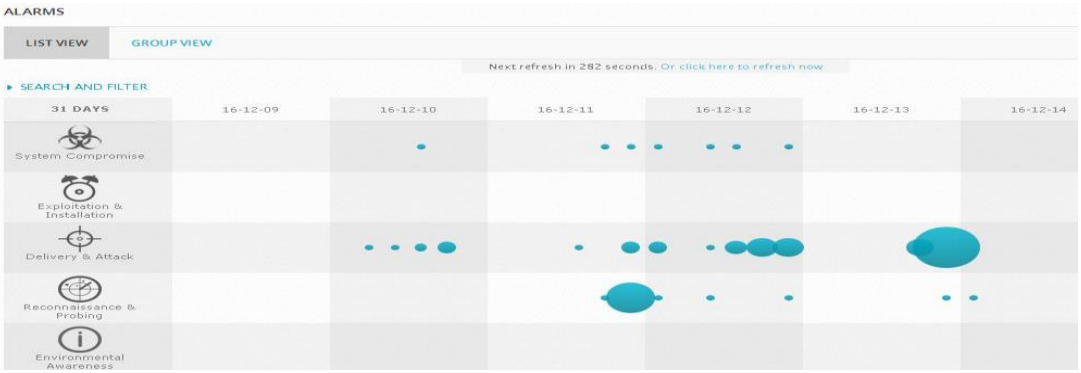


Figura 6.7 Vista de Alarmas reflejadas en el sistema

Selecciona la pestaña Group view como se muestra en la Figura 6.8:

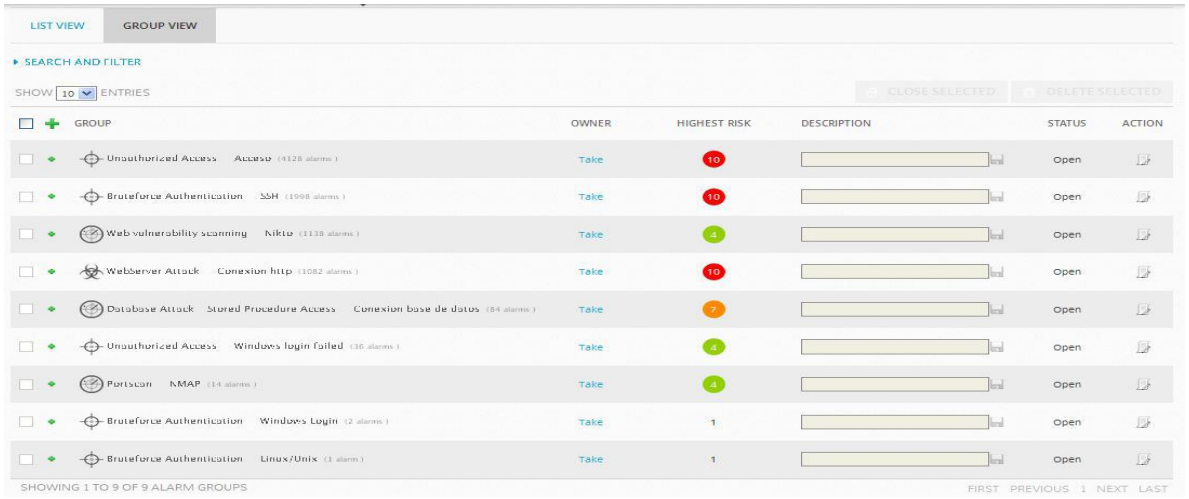


Figura 6.8 Vista de Alarmas Filtradas por Grupos

Se realiza el filtrado de la búsqueda mediante parámetro, colocamos los campos que nos interesan tal como se muestra la figura:

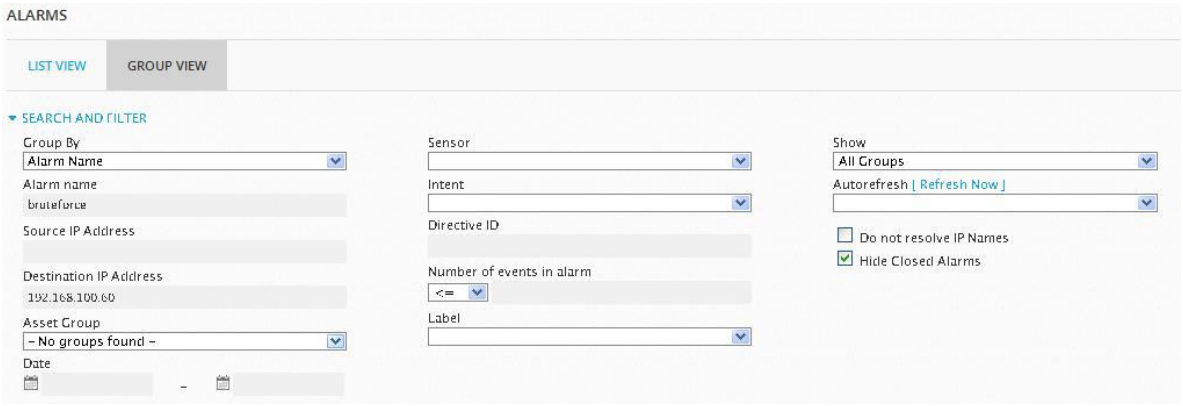


Figura 6.9 Campos de búsqueda de una alarma

Al ingresar de forma masiva a la base de datos, generaron eventos que a su vez alarmaron al sistema como se observa en la figura 6.10. De acuerdo al tipo de ingreso se activa la alarma.

6.5 INGRESO NO AUTORIZADO A LA BASE DE DATOS.

ALARM NAME	EVENTS	RISK	DURATION	SOURCE	DESTINATION	STATUS
Reconnaissance & Probing — Portscan — NMAP	2	4	1 sec	192.168.100.101	OSSIM	Open
Reconnaissance & Probing — Portscan — NMAP	2	4	1 sec	192.168.100.101	OSSIM	Open
Reconnaissance & Probing — Portscan — NMAP	2	4	2 secs	192.168.100.101	OSSIM	Open
Reconnaissance & Probing — Portscan — NMAP	2	4	1 sec	192.168.100.101	OSSIM	Open
Reconnaissance & Probing — Portscan — NMAP	2	4	0 secs	192.168.1.101	OSSIM	Open

Figura 6.10 Evento Generado

Se da clic en la alarma y se muestra el detalle como muestra la Figura 6.11:

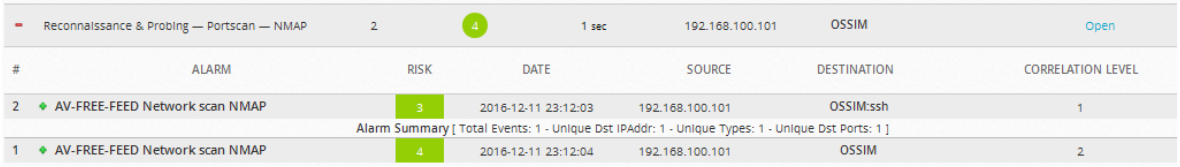


Figura 6.11 Detalle de Alarma

Dando clic en la pestaña de la izquierda se muestra la fuente donde se originó el evento de seguridad, para este caso se muestra la correlación de evento del SIEM de nivel 2 con prioridad 5 generado por el agente como se muestra en la Figura 6.12.

Para visualizar el código la regla se tiene que hacer clic en el evento:

:

```
directive_event: AV-FREE-FEED Login MYSQL, Priority: 5 Rule 1 [2018-04-12 04:12:03] [4003:10] [Rel: 8] 192.168.100.101:0 -> 192.168.100.60:22 Rule 2 [2018-04-12 04:12:04] [7014:5706] [Rel: 10] 192.168.100.101:0 -> 192.168.100.60:0
```

Figura 6.12 Detalle de la estructura de la regla.

La aplicación contiene una mesa de servicios, los tickets son abiertos a la interna de la institución para su revisión y resolución. Como se muestra la figura 6.13.

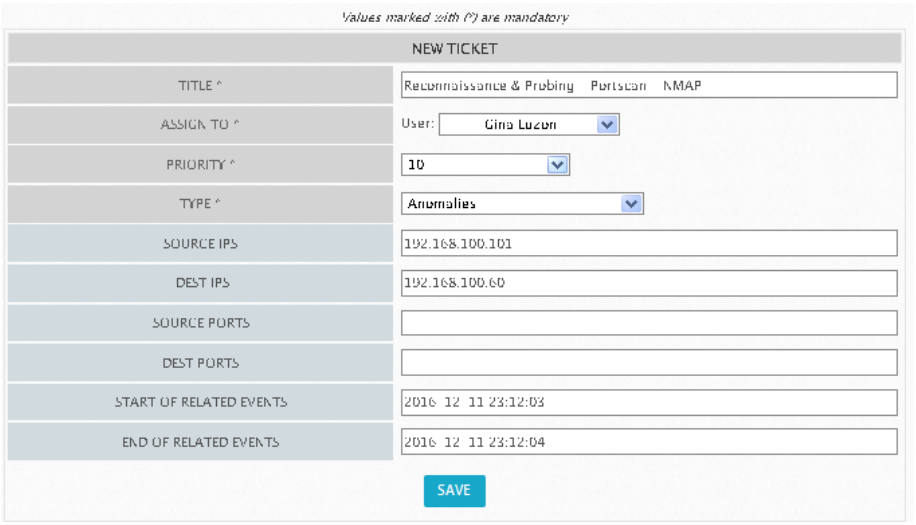


Figura 6.13 Creación del ticket

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La plataforma OSSIM trabajó sin problema durante el periodo de prueba de concepto. No se presentaron alertas respecto a la disponibilidad y/o rendimiento de la solución.
2. Los resultados obtenidos en la presente prueba de concepto están ajustados al periodo de licencia asignado, por tanto, no es posible visualizar y evidenciar las múltiples funcionalidades y beneficios adicionales que ofrece la solución, entre los que podríamos citar:
    - Monitoreo en tiempo real de transacciones en base de datos.
    - Descubrimiento de servidores y servicios de base de datos y aplicaciones.
    - Clasificación de la información en las bases de datos.

- Múltiples análisis de vulnerabilidades sobre distintos motores de bases de datos.
- Completa gestión de riesgos basándonos en vulnerabilidades de base de datos detectadas por la solución.
- Revisión y afinamiento del aprendizaje automático de la base de datos.
- Creación de políticas de auditoría y seguridad personalizadas de acuerdo a diversas necesidades de la institución.
- Creación de reportes personalizado basándonos en toda la información que monitorea y almacena la solución.
- Enriquecimiento de datos y cambio de texto.
- Configuración de alertas vía e-mail.
- Integración de la solución con LDAP (Active Directory).
- Administración de roles y usuarios en la solución.
- Análisis completo de performance de la solución

3. El análisis de vulnerabilidades ejecutado es suficiente evidencia la exposición al riesgo que tienen las bases de datos de institución.
4. Los reportes predefinidos para el análisis de tráfico monitoreado por la solución entregan información valiosa a los administradores de base

datos y demás interesados para el análisis de performance de las bases de datos de producción.

RECOMENDACIONES

1. Debido a lo criticidad de la información que maneja la institución, se recomienda la adquisición de soluciones especializadas que permitan monitorear y asegurar el tráfico SQL que se genera desde y hacia las bases de datos que administra la entidad.
2. Se debe monitorear la consola de administración para estar atentos ante cualquier novedad presentada. Además de mantener siempre la base actualizada, esto ayudaría en la protección de equipos y de la red.
3. Actualizar de manera periódica los equipos para evitar futuras anomalías en especial en equipos de comunicación, así como los switch, routers y servidores.
4. Realizar Auditorías a la seguridad informática de la compañía para tener un conocimiento de sus vulnerabilidades y que procedimientos seguir para minimizar los riesgos.

BIBLIOGRAFÍA

[1] Cristian Castillo Peñaherrera. ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI, septiembre 2013.

[2] Forecast, “Information Security, Worldwide, 2015-2021, 3Q17 Update, Noviembre 2017

[3] Muñoz, J. D. (2003). OSSIM (Open Source Security Information Management), Descripcion General del Sistema.

[4] TORRES, Juan Carlos. RONDÓN, Richard García. “Control, Administración E Integridad De Logs”. http://www.criptored.upm.es/guiateoria/gt_m248h.htm

[5] LONVICK, C., The BSD Syslog Protocol, RFC 3164, Agosto 2001. http://www.ietf.org/rfc/rfc3164.txt

[6] MOCKAPETRIS, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, Noviembre 1987.

[7] Alien Vault. OSSIM vs. USM A Comparison of Open Source vs. Commercial. Agosto 2015.

[8] Torres & Villegas, OSSIM (Open Source Security Information Management), Septiembre 2010.

[9] ALIENVAULT ACADEMY, S. (2014). AlienVault Certified Security Engineer, 1–134.

[10] Amrit T. Williams | Mark Nicolett, Improve IT Security With Vulnerability Management. May 2005.

[11] Kavanagh, K., & Rochford, O. Cuadrante Mágico de Seguridad de la Información y Gestión de Eventos. Gartner. Diciembre 2017.

[12] SNAP (Secretaria Nacional de Administración Publica), Acuerdo Ministerial 166, Septiembre 2013.

[13] Contraloría General del Estado del Ecuador, ACUERDO No. 013 - CG - 2016; Abril 2016.