ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UN SERVIDOR PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y DE EVENTOS, INTEGRADO CON LA INFRAESTRUCTURA DE UNA EMPRESA IMPORTADORA Y COMERCIALIZADORA DE SUMINISTROS ELÉCTRICOS Y SERVICIOS ESPECIALIZADOS, COMO SALVAGUARDA DEL PLAN DE RIESGOS INFORMÁTICOS"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

ALEX JAVIER ARANA NORTHIA

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Agradezco a Dios que es la fuerza, la guía que hace posible las cosas, a mis padres que son los ángeles de la guarda que están siempre a mi lado brindándome su inmenso amor, a mis hermanos por todo su apoyo, por ser las manos extras cuando las necesite, a mis familiares y amigos que de una u otra manera me han ayudado a lo largo del camino, finalmente a todos los maestros que tuve, por sus valiosas enseñanzas de vida.

DEDICATORIA

A todas esas personas que no se dan por vencidas y me han inspirado a seguir luchando. Ama y has lo que quieras dijo San Agustín, con la inspiración de ese amor finalmente le dedico este trabajo a mis padres y mis hermanos.

TRIBUNAL DE SUSTENTACIÓN

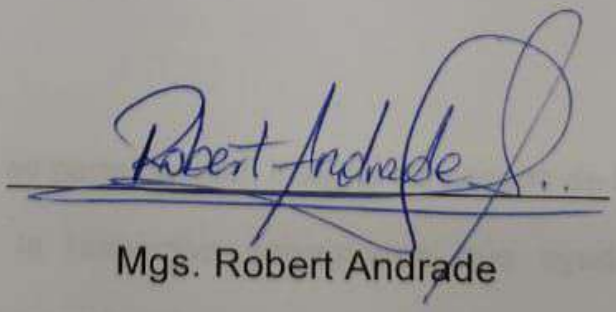
Ing. Lenin Freire

DIRECTOR MSIA

Mgs. Néstor Arreaga

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



Mgs. Robert Andrade

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El presente trabajo pretende demostrar la importancia de la seguridad de la información, así como dejar una base de solido conocimiento para el público interesado en el tema.

Los aspectos que abarca están relacionados con la evaluación de riesgos informáticos, donde se analizaran conceptos del mismo, se definirán activos de la información que serán evaluados, sus amenazas, el impactos de estas, es decir la degradación de afectación del activo si se materializa alguna amenaza, las probabilidades que esto suceda y como resultado los niveles de riesgo presentes.

Todo este análisis es parte del plan integral de riesgos de la empresa, donde quedara aplicada la respectiva salvaguarda que ayudara a mejorar la seguridad de la información.

Finalmente se llevara a cabo la implementación de una herramienta SIEM de licencia GPL, donde se mostrara los requerimientos mínimos del sistema, las recomendaciones de su instalación, la configuración de acuerdo a la política de seguridad de la información de la empresa y su puesta en marcha.
También se analizara los beneficios de su implementación y para culminar se entregaran unas conclusiones y recomendaciones sobre este trabajo.

Este trabajo está basado en la realidad actual y se deja abierta la posibilidad de implementarlo; al final se declaran las conclusiones y recomendaciones que se deben seguir para el éxito de este proyecto.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

ISO	Organización Internacional de Normalización
ISO 27000	Estándar de Seguridad de la Información
ISO 27002	Mejores prácticas de la Seguridad de la Información
GPL	Licencia Pública General
OSSIM	Open Source Security Information and Event Management
SGSI	Sistema de Gestión de Seguridad Informática
SIEM	Gestión de la Seguridad de la Información y Eventos

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad la sociedad es testigo de un factor crece a una velocidad impresionante, las Tecnologías de la Información.

Estas han cambiado la forma y los medios como nos comunicamos, hacemos negocios así como sus formas de pago, como aprendemos y en donde podemos hacerlo, de qué manera podemos socializar, y demás cambios en nuestra forma de vivir.

Pero con toda esta oleada de cambios vienen también nuevos desafíos y problemas que aparecen. Lo que más le preocupa a las organizaciones de Gobierno y a los empresarios es la seguridad de la información, que es uno de los pilares fundamentales dentro de las Tecnologías.

Nos vemos expuestos a un sin número de amenazas que aparecen a diario, por ejemplo la empresa Kaspersky Lab encuentra un programa malicioso nuevo cada dos minutos, un mismo reporte de esta empresa revelo que un

programa malicioso llamado Carbanak ocasiono perdidas en el sector financiero por más de mil millones de dólares.

Los sistemas de procesamiento de información no son del todo seguros de ahí nuestros esfuerzos por ir buscando soluciones a estos problemas de carácter mundial y reforzar la seguridad de las comunicaciones, la infraestructura además de concientizar al personal.

El inconveniente se da cuando no disponemos de la suficiente capacidad de inversión como las corporaciones, organizaciones de gobiernos, bancos o grupos financieros. Enfrentarlos en estas condiciones se vuelve complicado y ante esta situación tenemos que buscar soluciones de manera inteligente y eficiente, como el alinearnos a las mejores prácticas de seguridad de la información ISO27002, revisando las exigencias del estándar ISO27001, aplicando metodologías de libre distribución como la es MAGERIT, para la evaluación y tratamiento de riesgos informáticos, instalando aplicaciones y sistemas de licencia GPL o software libre de seguridad informática.

CAPÍTULO 1

1. GENERALIDADES

1.1. DESCRIPCIÓN DEL PROBLEMA

La empresa importadora y comercializadora de suministros eléctricos y servicios especializados tienes algunas deficiencias relacionadas a la seguridad de la información, al manejar pagos transaccionales comerciales, información confidencial propia, de sus clientes y proveedores, así como los servicios brindados.

La productos que maneja la empresa, satisface parte de la demanda que tienen las empresas el sector industrial, el de la construcción y el de alimentos, que compran sus productos y utilizan sus servicios.

La información que se genera como parte de la dinámica comercial propia del negocio tiene que estar debidamente protegida, disponible e integra. Pero en la actual situación organizacional, se aprecia la falta de sistemas de seguridad de la Información y controles de seguridad en los procesos informáticos.

Esta situación actual da lugar a diferentes problemas como son:

- Perdida de información del negocio.
- Mal uso de los recursos.
- La variedad de procedimientos de control de acceso que se ejecutan sin el debido monitoreo.
- Sistemas vulnerables.
- Falta Control en el tráfico sobre la red.

Dentro de la empresa se ha podido observar que:

- Existen configuraciones predeterminas en varios equipos. Dando espacios a agujeros de seguridad.

- Existen diferentes tecnologías funcionado sobre la infraestructura.
- Existen varios servidores sin enviar notificaciones de eventos sobre posibles incidentes de seguridad.
- No existe un monitoreo de la red orientado a detección de intrusos y fuga de información.
- No se analizan los log de las actividades de los hosts de la red.

1.2. SOLUCIÓN PROPUESTA

Para solucionar de la manera más eficiente estos problemas de seguridad informática que tiene la empresa, se propone implementar un servidor con una herramienta SIEM en pruebas para la gestión de seguridad de la información y eventos de seguridad, integrado con la plataforma tecnológica operativa.

La implementación de esta solución será con la herramienta OSSIM, que beneficiara de manera general la seguridad de la información.

Brindará una consola integral donde se podrá estudiar de manera no solo reactiva sino pro activa los posibles incidentes de seguridad de la información presentes sobre la plataforma tecnológica actual, a través

del análisis de los diferentes datos recogidos de los diferentes equipos de comunicación, hosts y servidores.

Con la cual se desarrollaran las siguientes actividades:

- Definir los equipos de comunicación a integrar.
- Seleccionar la herramienta informática para la gestión de seguridad de la información y eventos de seguridad, de acuerdo a las necesidades del negocio.
- Implementar OSSIM.
- Integración de la plataforma tecnológica operativa al OSSIM.
- Definir reglas de operación del OSSIM, según las necesidades del negocio.
- Evaluación de riesgos de los activos afectados por el sistema SIEM.

Los beneficios a obtener serán:

- Un conocimiento formal de cuáles las vulnerabilidades, amenazas presentes, así como su impacto.

- Una plataforma integral para la gestión de seguridad de la información y eventos de Seguridad.
- Tener controles sobre la información que administra la empresa, dentro de la Infraestructura aplicaciones y comunicaciones.
- Alinearse a las mejores prácticas de la ISO 27002.
- Fortalecer procedimientos para brindar una mayor seguridad.
- Evitar la dependencia de uno o varios funcionarios; la delegación y la distribución de actividades y roles ayudara a la dinámica del área.
- Mejorar los niveles de servicios brindados.
- Usar los recursos informáticos de manera eficiente.

CAPÍTULO 2

2. METODOLOGÍA Y DESARROLLO DE LA SOLUCIÓN

2.1. PLAN DE GESTIÓN DE RIESGOS

La gestión de riesgo es fundamental para la empresa, donde el plan no solo ayudara a controlar los riesgos presentes, sino que también a tomar mejores decisiones fundamentadas en el conocimiento que tenemos a partir de esta recopilación de datos y también definir los beneficios, riesgos, amenazas, impactos, salvaguardas de las nuevas decisiones tomadas en relación al negocio.

Como primera parte de la implementación de un plan integral de riesgos se realizara un análisis de riesgo sobre los activos de información que la empresa ha considerado como relevantes para su operación y luego

de esto la aplicación de la salvaguarda seleccionada, que consiste en la implementación de la herramienta OSSIM.

El plan de Riesgo tendrá una estructura de PHVA, de planificar, hacer, verificar y actuar[1]. Adicionalmente esto servirá para que la empresa se comience a familiarizar con los procesos de auditorías.

Figura 2.1 Ciclo de Mejora Continua

2.2. ANÁLISIS DE RIESGOS

Estableceremos la valoración de los activos, de acuerdo a sus dimensiones de confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad; así como el tipo de activo del estudio, su propietario que es quien lo genera o crea, su responsable quien es quien lo utiliza o custodia.

[1] NORMA ISO 27001:2005

Las amenazas valoradas son aquellas que presenten afectación sobre los activos de información, es decir, cual es la degradación y su probabilidad de ocurrencia. Como resultado de esta evaluación obtendremos los niveles de riesgo.[2]

Figura 2.2 Proceso de Análisis de Riesgos

[2] Consejo Superior de Administración Electrónica, http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VbmzOPI_Oko,2015

Se realizara el análisis a través de tablas con múltiples elementos que serán combinados y ordenados por importancia donde se manejaran escalas de Bajo, Medio, Alto, Muy Alto, Extremo.

El modelo de estudio que se aplico es cualitativo donde buscaremos saber cuáles son la propiedades relevantes de los activos dentro de todos los aspectos posibles del análisis en las siguientes ilustraciones se muestran los activos de información clasificados por tipo, propietarios y responsables con sus niveles porcentuales presentes.

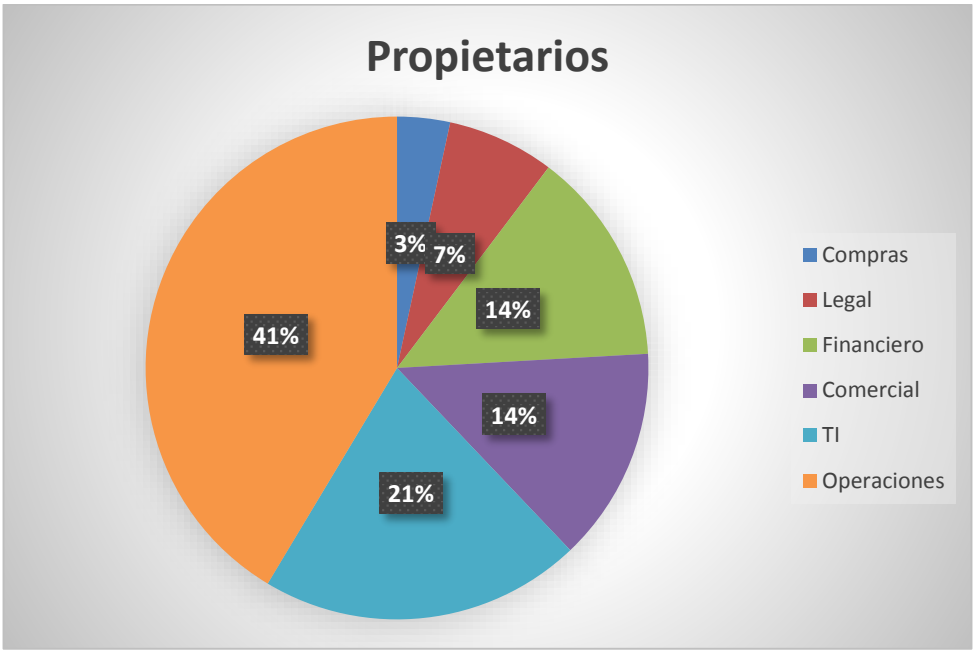


Figura 2.3 Propietarios de los Activos de Información

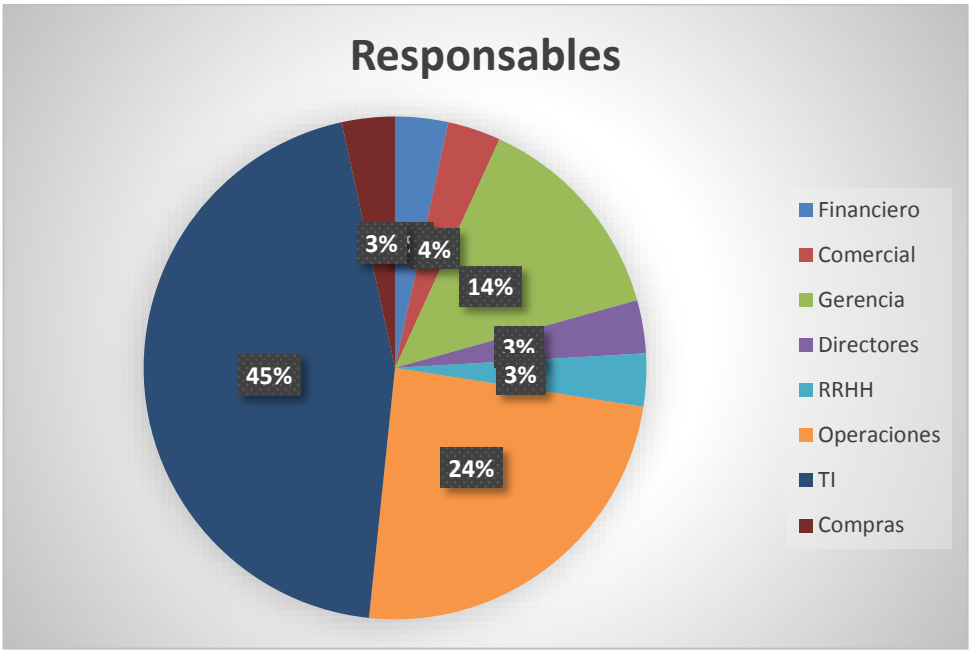


Figura 2.4 Responsables de los Activos de Información

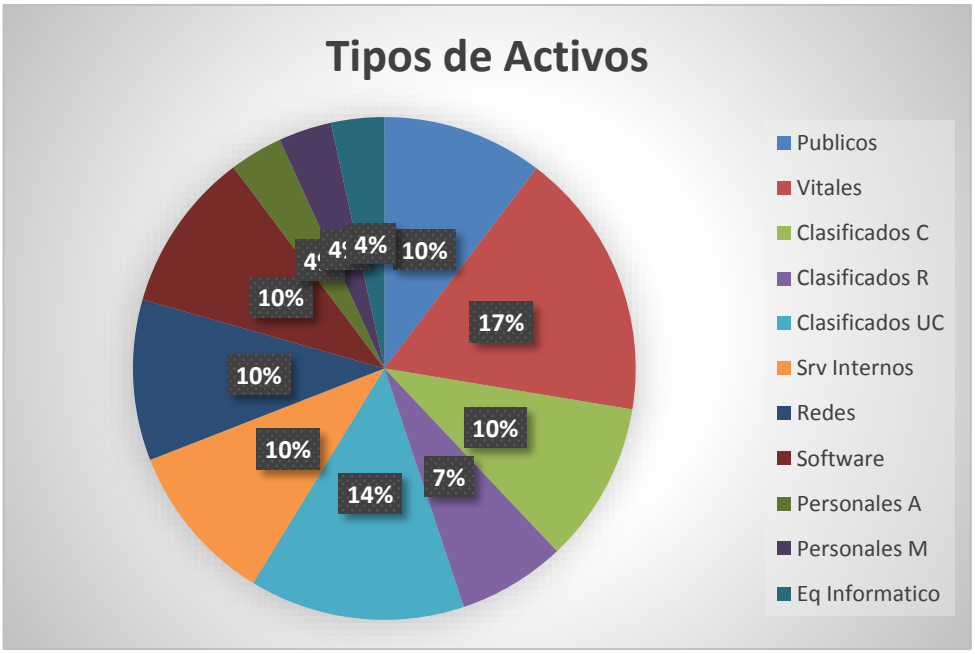


Figura 2.5 Tipos de Activos de Información

VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN.

En el siguiente cuadro veremos a los activos de información sobre las dimensiones de valor de la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad. Como resultado podemos ver que existen varios activos que necesitan de una alta integridad en sus datos, así como la autenticidad de sus fuentes o quien envía el mensaje, también llevar un registro para su trazabilidad. La confidencialidad no es una prioridad pero tampoco deja de ser importante y la disponibilidad se mantiene un valor medio alto dentro de los activos.

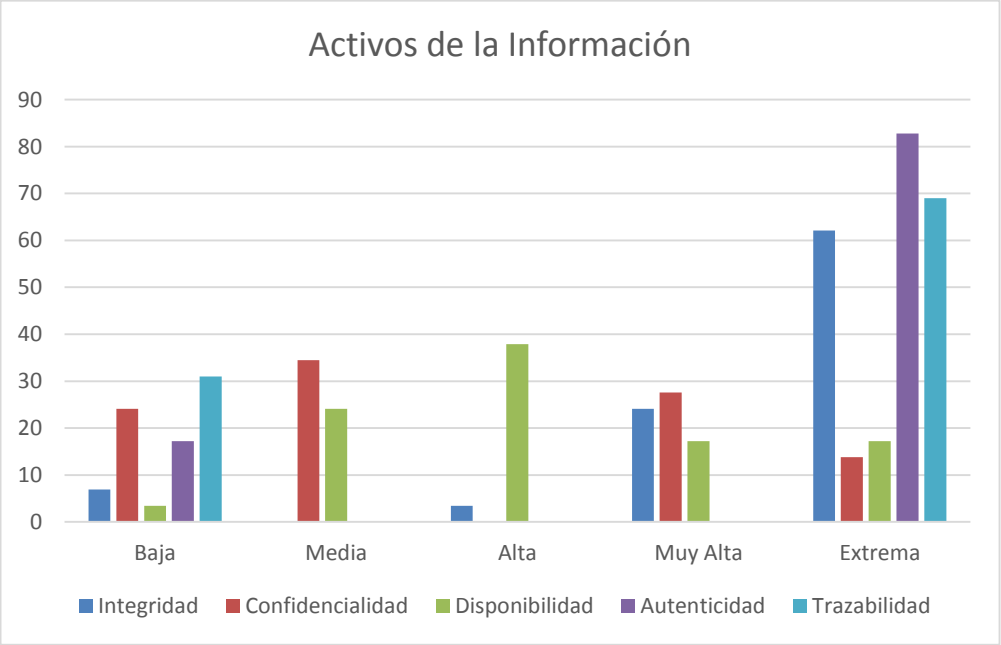


Figura 2.6 Valor de los Activos de Información.

VALORACIÓN DE AMENAZAS.

Según la metodología que aplicamos tenemos diferentes categorías de amenazas como Desastres Naturales, De origen Industrial, Errores y fallos no intencionados, ataques intencionados[3]. Nuestra valoración se centrara en las dos últimas categorías, correlacionadas entre sí en la siguiente tabla:

Tabla 1 Valoración de Amenazas

ID	AMENAZAS	IMPACTO	PROBABILIDADES
1	Errores y fallos de usuarios	2	4
2	Errores del Administrador	4	2
3	Difusión de Software Malicioso	5	5
4	Destrucción de la Información	4	3
5	Fuga de Información	3	2
6	Vulnerabilidades de los Programas	4	4
7	Manipulación de los registros de actividad	2	2
8	Manipulación en la Configuración	5	3

[3] Mclure, S.; Scambray, J.; Kurtz, G., Hacking exposed 7: Network Security Secrets & Solutions, McGrawHill 7th Ed, 2012

9	Suplantación de Identidad del Usuario	4	3
10	Abuso de Privilegio de Accesos	3	3
11	Acceso no Autorizado	4	3
12	Análisis de Trafico	2	2
13	Repudio	3	3
14	Intercepción de la Información	4	3
15	Modificación de la Información	5	3
16	Denegación de servicio	4	1

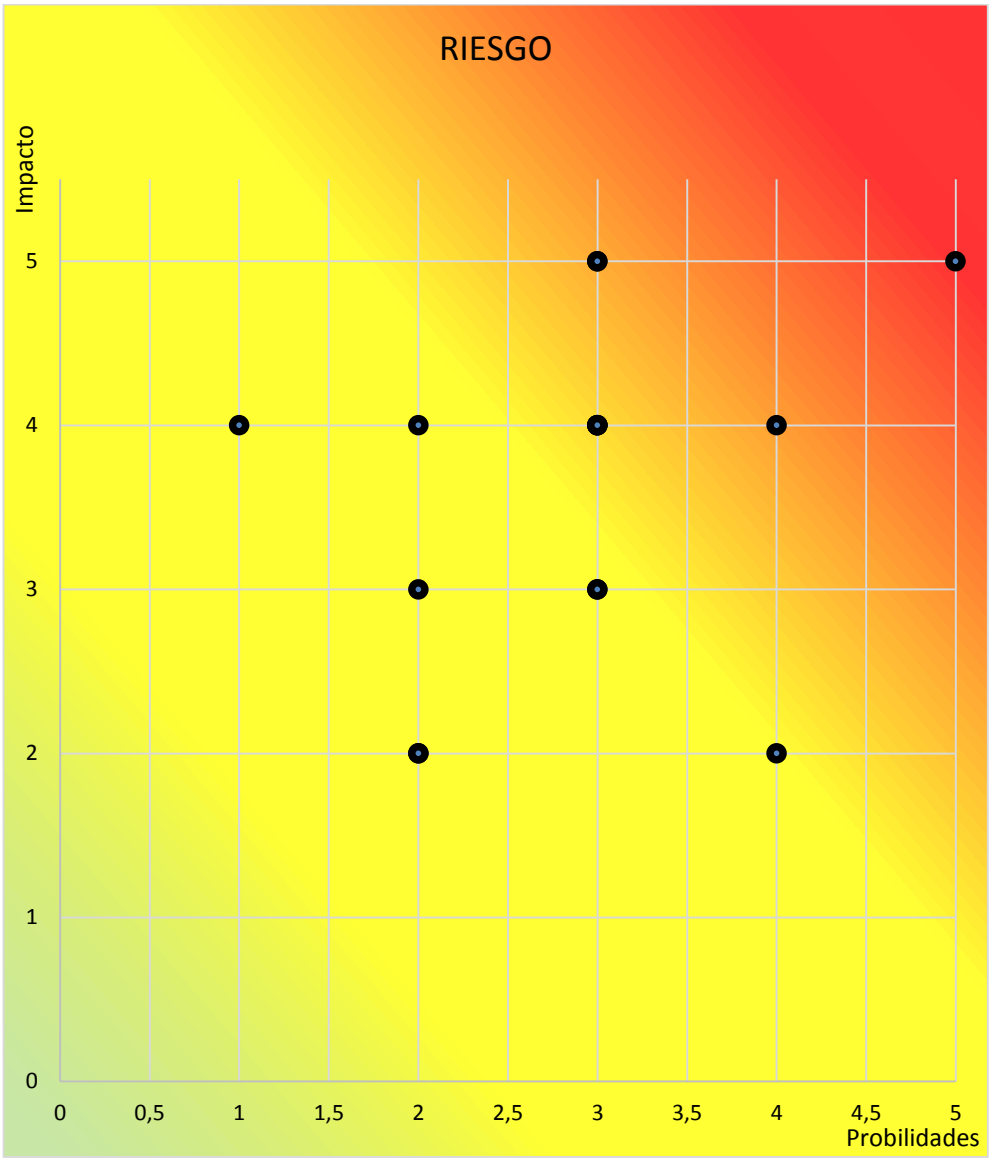


Figura 2.7 Mapa de Riesgos

Las amenazas que se encuentran hacia la zona roja tienen un carácter de muy probables y de alto impacto. Podemos decir que esta son las que representan un riesgo crítico para la empresa.

2.3. BUENAS PRACTICAS ISO 27002

Lo que establece el estándar son guías de aplicación en los diferentes aspectos relacionados a la seguridad de la información por medio de objetos de control y controles.

Dentro de estos objetivos de control tenemos el de Gestión de Incidentes de Seguridad con los controles que reportes de eventos y debilidades de la información, que responde a la exigencia del Control A.13 del Estándar de Auditoria ISO 27001.

La ISO 27002 tiene medidas que responden a estas exigencias, dentro de las guías de buenas prácticas de seguridad de la información se propone el un procedimiento formal para los reportes de eventos y el procedimiento de respuesta de:

- La pérdida del servicio
- Errores humanos
- Modificaciones no controladas en el sistema
- Mal funcionamientos de las Aplicaciones
- Violaciones de Acceso

Monitorear el sistema, alertas y las vulnerabilidades. Usar esta información de la evaluación de la seguridad e identificar problemas recurrentes o de alto impacto[4].

Recoger y organizar la información como evidencias para acciones disciplinarias o legales.

2.4. HERRAMIENTAS SIEM

Son un conjunto de tecnologías diseñadas para brindar una visión clara y precisa de la seguridad de la información en la empresa, beneficiando el trabajo de los administradores y los analistas de Seguridad.

Una de las fortalezas de esta solución es la correlación de eventos, que ofrece un alto nivel de inteligencia y compresión de los incidentes, no se analizaran eventos de forma aislada y de acuerdo a esto tomar una acción o no, en cambio tendremos una vista amplia y completa de todo el problema, al estar relacionados todos los eventos de las diferentes capas que genero el incidente y tomaremos los ajustes necesarios y correctos, es decir se implementaran las correspondientes salvaguardas dependiendo del caso[5].

[4] NORMA ISO/IEC 17799:2005

[5] Miller, D.; Harris, S.; Harper, A.; VanDyke, S.; Blask, C.; Security Information and Event Management (SIEM) Information, Network Pro Library 1 st Ed, 2010

La oferta de productos que tenemos en el mercado es variada, comerciales tenemos CiscoMARS, ArcSight ESM, Tenable, Alien Vault; en el sector de software libre no existen muchas ofertas pero esta OSSIM, que ha demostrado ante la comunidad especializada en seguridad de la información ser una solución excelente contra los productos de comerciales.

2.5. IMPLEMENTACIÓN DE OSSIM

La implementación del servidor que alojara OSSIM, tendrá las siguientes características de procesamiento, memoria y almacenamiento:

- CPU Intel Xeon E5620, Memoria de 2GB, HDD 1 TB

También es mejor trabajar con OSSIM manteniendo una arquitectura de 64 bits para mejorar su desempeño al igual de tener la suficiente capacidad de transmisión en la red, un ancho de banda acorde al rendimiento que exige la red.

El diagrama de red quedara de la siguiente manera:

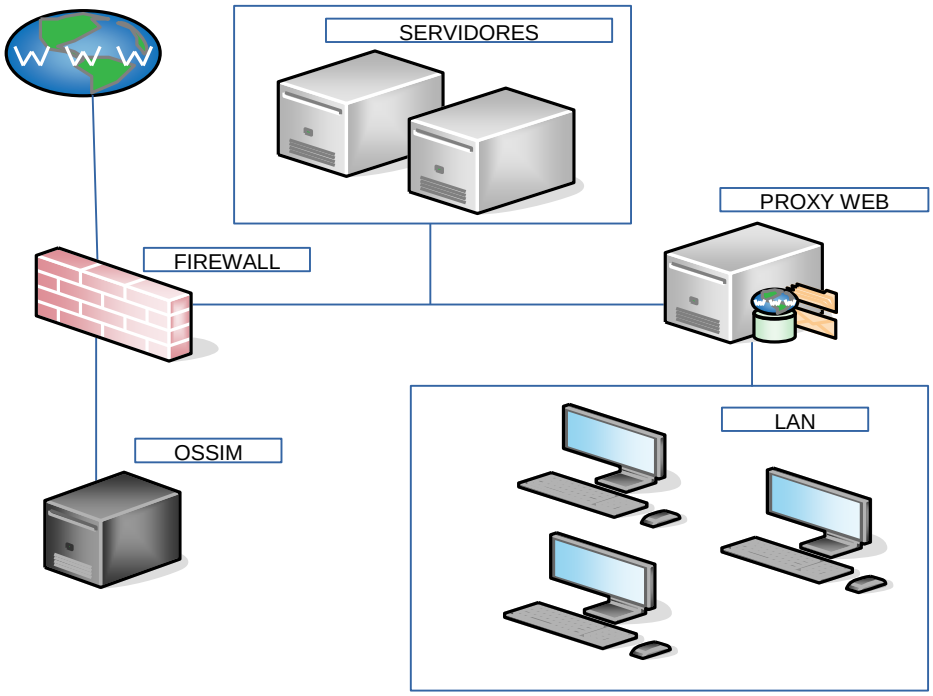


Figura 2.8 Diagrama de Red

2.6. CONFIGURACIÓN DE OSSIM.

La configuración de OSSIM no es complicada luego de realizar la instalación, que es sencilla, es necesario configurar la interfaz de red sobre la cual va a trabajar OSSIM, es decir definir su direccionamiento IP, que en nuestro caso fue la red privada 192.168.1.7 en la subred 255.255.255.240, con el propósito de trabajar en un ambiente aislado y controlado para pruebas. Es importante indicar que la tarjeta de red tiene que estar en modo promiscuo.

Luego en el menú podemos definir otras opciones como los DNS, la configuración proxy de tenerla, las VPN, etc.

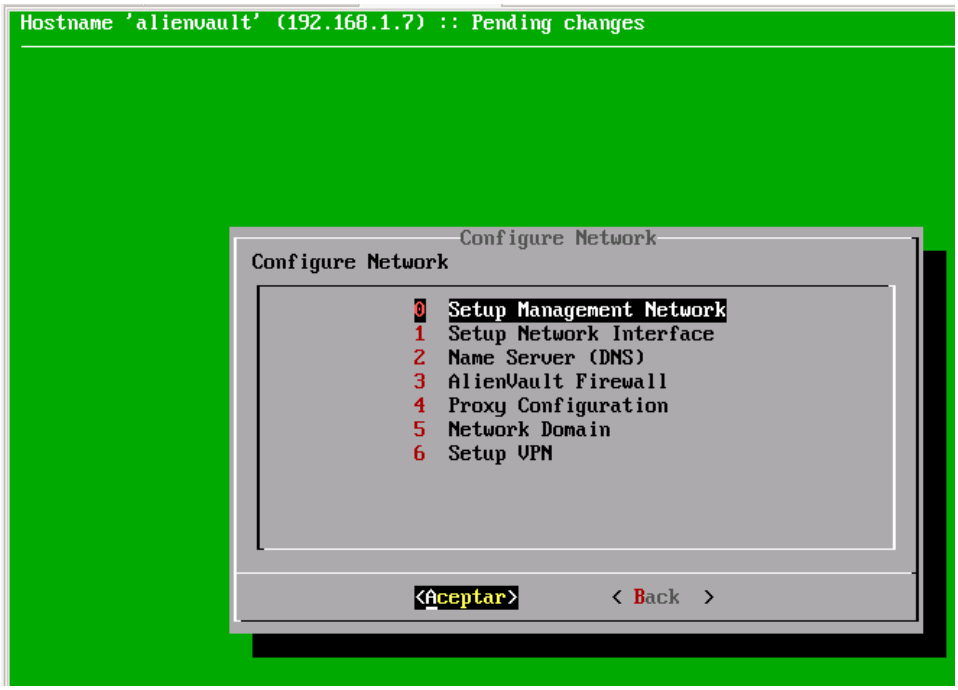


Figura 2.9 Pantalla de Configuración de OSSIM.

2.7. INTEGRACIÓN DE OSSIM Y LA PLATAFORMA TECNOLÓGICA.

OSSIM nos permite escanear los host vivos de la red o importarlos de un archivo de texto CSV, también a través de la instalación de plugins para dispositivos especiales, se recolectara la información de eventos de los hosts y los dispositivos. También podemos definir varios segmentos de red a monitorear.

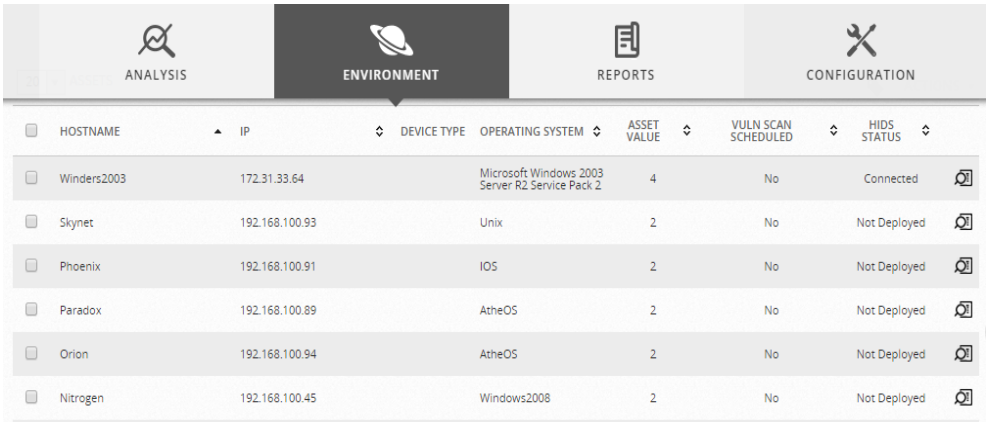


Figura 2.10 Interfaz de OSSIM, Hosts y Dispositivos de Red.

2.8. POLÍTICAS APLICADAS A OSSIM.

Dentro de la plataforma de OSSIM podemos no solo ver el análisis de las amenazas y los eventos de seguridad, otra forma de trabajar es usando las políticas, para construir reglas sobre los eventos si estamos detectando algún comportamiento sospechoso de algún host o si vemos comunicaciones extrañas hacia un destino.

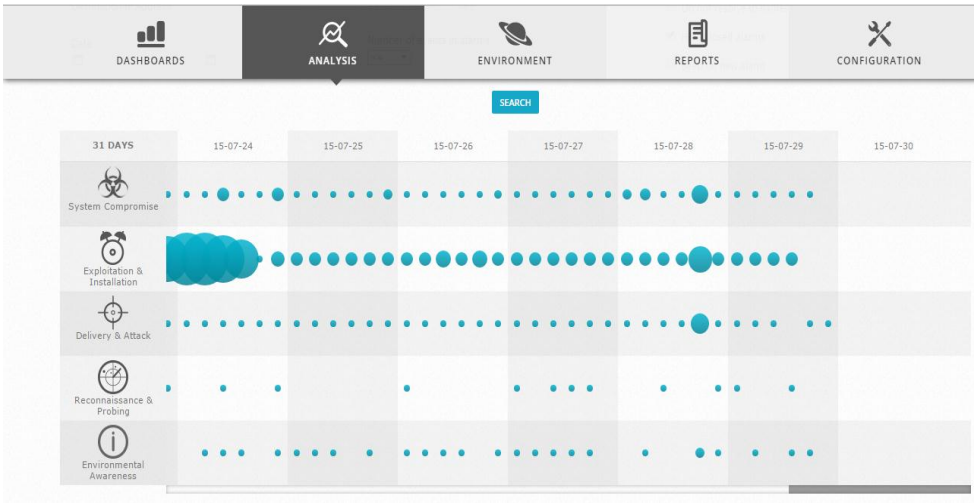


Figura 2.11 Interfaz de OSSIM Amenazas.

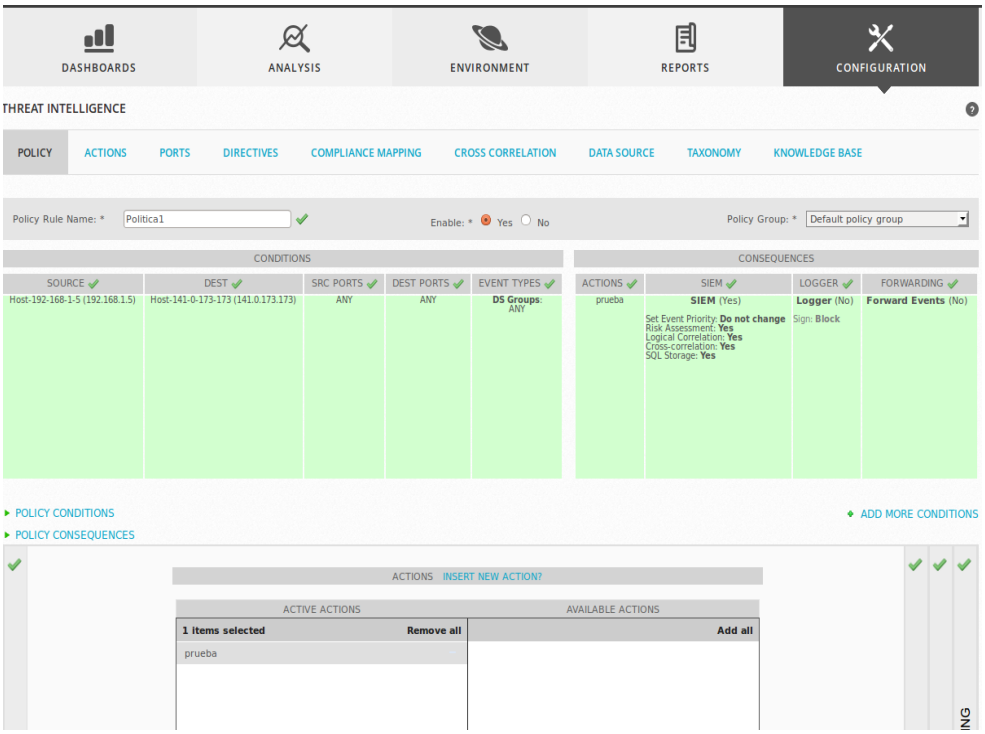


Figura 2.12 Interfaz de OSSIM Políticas

2.9. PRUEBAS Y MONITOREO DE OSSIM

Las pruebas y lo referente al monitoreo de todos lo que registra y correlaciona OSSIM, lo tenemos a la mano en el DASHBOARD, donde tendremos eventos de alarmas de seguridad, categorías de eventos, el intercambio de amenazas, los host que generan más eventos entre otros.

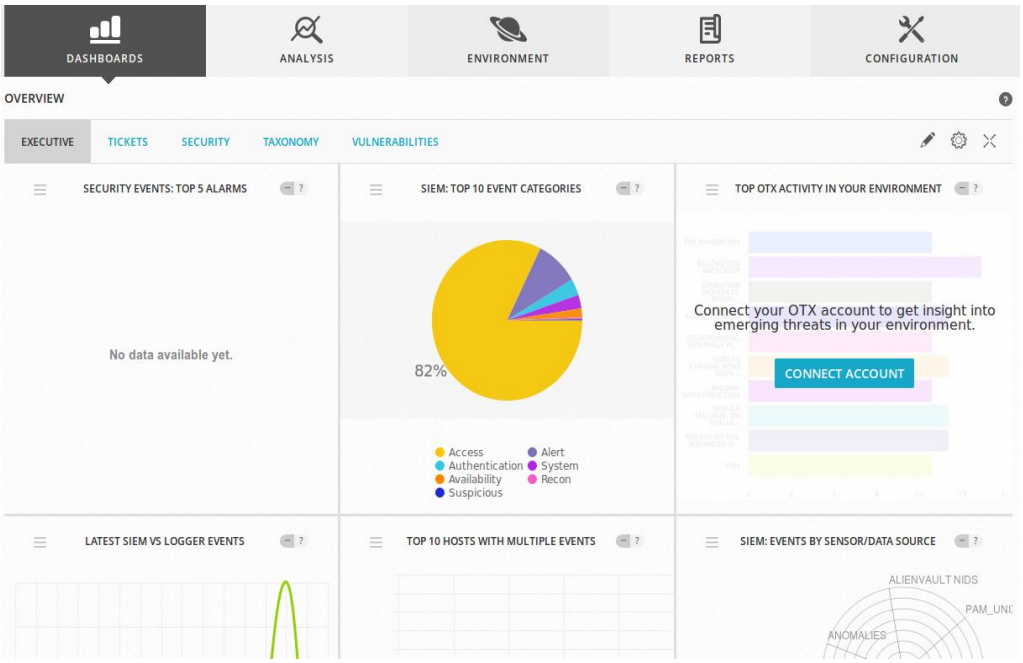


Figura 2.13 Interfaz del Dashboard

CAPÍTULO 3

3. ANÁLISIS DE RESULTADOS

3.1. ANÁLISIS DE COSTO BENEFICIO DE LA IMPLEMENTACIÓN DEL SIEM

El despliegue de OSSIM ha afectado de manera positiva los activos vitales de la información, ayudando a reducir los niveles de riesgo. Tenemos un mayor control, una mayor visión de los que se necesita en la empresa para irnos alineado a las guías de la ISO 27002.

En la siguiente ilustración vemos como se disminuyeron los niveles de riesgos luego de aplicar la salvaguarda de gestión de seguridad de la información y eventos.

Tabla 2 Reducción de Impacto y Probabilidad

AMENAZAS TIPOS	RIESGO NIVELES DE CRITICIDAD	SALVAGUARDA OSSIM
Software Malicioso	5,5	4,3
Vulnerabilidad Programas	4,4	3,3
Manipulación de Configuración	5,3	4,3
Acceso no Autorizado	4,3	4,1
Intercepción de Información	4,3	4,2
Modificación de la Información	5,3	4,2

El costo de inversión sobre la implementación de la salvaguarda se ha trabajado de forma inteligente, en vez de invertir en una solución comercial, donde no solo se compra el producto, si no que se necesita pagar por el soporte o adquirir algún appliance dedicado, que representan una buena alternativa si tenemos los recursos, pero si estamos limitados y tenemos que distribuir de mejor forma estos recursos con la instalación de una herramienta OSSIM, se ha apostado por las soluciones de software libre y el talento humano, capacitándolo en materia de seguridad esto se verá reinvertido cuando el personal

comience a detectar agujeros de seguridad, falta de controles, mejoras en la política, se transformara en actores activos de la seguridad en la organización. En la siguiente tabla veremos como el costo de la implementación de esta solución se vuelve no solo rentable si no estratégica para la toma de futuras decisiones empresariales.

Tabla 3 Degradación del activo implementando OSSIM

AMENAZAS	DEGRADACIÓN DEL ACTIVO	SALVAGUARDA	RECUPERACIÓN DEL ACTIVO
Software Malicioso	80%	60%	20%
Vulnerabilidad Programas	60%	40%	20%
Manipulación de Configuración	70%	50%	20%
Acceso no Autorizado	60%	40%	20%
Intercepción de Información	60%	40%	20%
Modificación de la Información	60%	40%	20%

3.2. ACEPTACIÓN DEL RIESGO RESIDUAL

El valor del riesgo residual esta expresado sobre los valores de los activos que hemos definido usando el nuevo impacto y la nueva probabilidad de las amenazas. Donde se ha evaluado la nueva situación de la seguridad de la Información de la empresa donde el Riesgo de los Activos Vitales a los cuales se les implemento la salvaguarda se redujo en 20%. Dejando un nuevo riesgo residual por niveles de entre el 50% y 60% promedio sobre los activos vitales.

3.3. INFORME FINAL DEL ESTADO

En la siguiente tabla veremos las nuevas probabilidades e impacto de todas las amenazas analizadas, luego de la operación de OSSIM en la plataforma tecnológica.

Tabla 4 Valor de las Amenazas bajo los nuevos valores

ID	AMENAZAS	IMPACTO	PROBABILIDADES
1	Errores y fallos de usuarios	1	4
2	Errores del Administrador	3	2
3	Difusión de Software Malicioso	4	3
4	Destrucción de la Información	3	3

5	Fuga de Información	3	2
6	Vulnerabilidades de los Programas	3	3
7	Manipulación de los registros de actividad	1	2
8	Manipulación en la Configuración	4	3
9	Suplantación de Identidad del Usuario	3	2
10	Abuso de Privilegio de Accesos	3	3
11	Acceso no Autorizado	4	1
12	Análisis de Trafico	2	2
13	Repudio	2	2
14	Intercepción de la Información	4	2
15	Modificación de la Información	4	2
16	Denegación de servicio	4	1

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Las tecnologías de la información necesitan de sistemas, aplicaciones, normas o políticas y personal especializado que trabaje por la seguridad de la información.

2. El plan de gestión de riesgos es medular dentro de las operaciones de una empresa y necesita ser gestionado.

3. El análisis y evaluación de riesgos puede ser cualitativo o cuantitativo pero debe estar siempre ajustado a todas las dimensiones que influyen sobre los activos, el impacto de las amenazas y su probabilidad

4. La salvaguarda seleccionada e implementada está justificada en el análisis y evaluación de riesgo. Revisando la capacidad de inversión

empresarial se tomó la decisión de ir por las soluciones de software libre.

5. La herramienta OSSIM está basada en el sistema operativo Linux, es liviana, estable, y existe una gran gama de documentación sobre sus bondades y soluciones a problemas presentados.

6. El despliegue completo del servidor OSSIM, quedo a discreción de los directivos de la empresa, luego de revisar los beneficios de esta y su incidencia en las operaciones.

7. La herramienta OSSIM es una muy buena alternativa para las medianas y pequeñas empresas para la gestión de seguridad de la información y eventos.

RECOMENDACIONES

1. Recomendamos que el proceso de Gestión de Riesgos sea una actividad continua por la importancia que tiene.

2. Definir los responsables y sus roles en relación a la seguridad de la información de la empresa.

3. Una campaña de concientización y formación de los colaboradores sobre lo que es la seguridad de la información.

4. Seguir utilizando la Herramienta OSSIM, para ir madurando en su uso.

5. Recomendamos seguir trabajando con la norma ISO 27000, para ir diseñando procesos y controles alineados al estándar.

6. Es necesario que los directivos de la empresa se comprometan con el desarrollo de los procesos y las políticas de seguridad de la información.

7. Se recomienda que al buscar aplicaciones que nos ayuden en un determinado proceso, analicemos no solo los programas las comerciales sino su contraparte en software libre.

BIBLIOGRAFÍA

[1]. Norma ISO 27001:2005, Tecnología de Información - Técnicas de Seguridad - Sistema de gestión de seguridad de Información – Requerisitos.

[2]. Norma ISO/IEC 17799:2005 – Tecnologia de la Informacion – Tecnicas de Seguridad – Codigo para la practica de la gestion de la seguriad de la Informacion.

[3]. Mclure, S.; Scambray, J.; Kurtz,G, Hacking exposed 7: Network Security Secrets & Solutions, McGrawHill 7th Ed, 2012.

[4]. Consejo Superior de Administración Electrónica, Metodología de Análisis y gestión de Riesgos de los Sistemas de Información, http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VbmzOPl_Oko, fecha de consulta julio 2015.

[5]. Miller,D.; Harris,S.; Harper,A.; VanDyke,S.; Blask,C., Security Information and Event Management (SIEM) Information, Network Pro Library 1st Ed, 2010.