Informe Final Practica Académica
Modalidad Práctica Empresarial

UNIVERSIDAD DE ANTIOQUIA
1803
FACULTAD DE INGENIEIRÍA

Identificación del estudiante

Nombres y apellidos.	Edwin Alejandro Agudelo Roldan
Documento de identidad.	
Teléfono.	
Semestre académico.	2015-2
E-mail.	

Identificación del asesor interno (U. de A.)

Nombres y apellidos.	Jeysson Pérez
Teléfono.	
Oficina.	Biblioteca Carlos Gaviria Díaz 3er Piso
E-mail.	

Identificación del asesor externo (empresa)

Nombres y apellidos.	Jaime Andrés Agudelo Roldan
Teléfono.	
Dirección.	
E-mail.	
Cargo.	Gerente General

Identificación de la empresa

Nombre de la empresa.	Optimalsoft
Dirección.	
Ciudad.	
Teléfono.	
Actividad económica.	Análisis y Desarrollo de sistemas informáticos

Auditoria de seguridad de redes para la empresa OPTIMALSOFT SAS.

Resumen

La seguridad informática es una disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas que están orientados a ejercer las mejores prácticas de confidencialidad, integridad y disponibilidad. Debido al incremento constante de internet cada vez más empresas crean servicios disponibles en la web, por lo tanto es necesario tomar medidas de seguridad para la protección de la información.
Es de gran importancia que las empresas tengan el conocimiento de ciertas métricas de seguridad, y además las empresas donde contienen código fuente en repositorios, estas deben tener un cuidado aún más especial. En el proceso que se llevó a cabo en la empresa Optimalsoft se intervinieron credenciales de autenticación, certificados de seguridad a sitios web, restricción de accesos, mantenimiento y control de repositorios de código fuente, actualización y versionamiento de sistemas operativos, control y gestión de inventarios de aplicativos, configuración de alarmas de acceso físico, control e inventario de sistema virtualizados, configuración de puntos de acceso a internet. Con la auditoria a las redes de la empresa se estandariza y fortalece la seguridad de la información, y se logra métricas de confidencialidad, integridad y disponibilidad de la información.

Introducción

Optimalsoft SAS es una empresa dedicada al análisis y desarrollo de soluciones informáticas, su finalidad de brindar a sus clientes servicios y de esta manera automatizar sus procesos operativos y proyectarlos al mundo mediante el uso de Internet. La misión de la empresa es ofrecer un excelente servicio optimizando los procesos y productos informáticos contemplando estándares de calidad y con un personal excelentemente capacitado para que los clientes obtengan productos de calidad. La empresa ha participado principalmente en proyectos privados, durante el proceso de evolución y crecimiento Optimalsoft SAS ha especializado su oferta en brindar servicios de migración de tecnologías.

En vista de que la organización carece de antecedentes en estudios previos sobre la seguridad de la información, se ha decidido realizar el siguiente estudio cuyo fin es establecer la situación actual de la empresa con respecto a la seguridad, y sugerir los correctivos necesarios.
La información es el activo más importante que tiene una empresa, es de gran importancia protegerla, esto conlleva a que la empresa tenga credibilidad. Para realizar buenas prácticas de seguridad se deben acoplar una serie de metodologías que implementen un estándar que garanticen las mejoras en todos los procesos que involucran la seguridad. Una de las metodologías más usadas en la actualidad es la metodología MAGERIT, esta permite hacer el estudio de los riesgos que soporta un sistema de información y el entorno asociado a él, para ello propone realizar la

evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados. Ministerio de Hacienda y Administraciones Públicas (2012, Noviembre) “Los resultados del proceso de análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios”.

Objetivos

Objetivo general

Gestionar un sistema de seguridad informático que permita planear, organizar, dirigir, controlar y garantizar la integridad de los recursos informáticos de la empresa Optimalsoft S.A.S, elaborando un estudio de gestión de seguridad con herramientas open source.

Objetivos específicos.

1. Identificar, clasificar y diagnosticar los activos de información presentes en la empresa Optimalsoft S.A.S
2. Aplicar la metodología Magerit de evaluación de riesgos para definir las vulnerabilidades y amenazas de seguridad existentes.
3. Sugerir mecanismos de control y gestión que mitiguen las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado.
4. Diseñar e implementar un informe de las acciones que se realizaron para la mitigación de los riesgos analizados.

Planteamiento del Problema

En la actualidad es imposible garantizar que un sistema sea completamente seguro, independientemente de que el sistema esté o no expuesto a internet, hace pocos días expertos en seguridad probaron que se puede acceder a un equipo desde cuartos aledaños mediante ondas, esto es una muestra de que no hay posibilidad de proteger un sistema al 100%. Para minimizar el riesgo es necesario diseñar un sistema de gestión de seguridad que permita identificar las vulnerabilidades, riesgos y amenazas las cuales pueden comprometer los activos de la organización.

¿Cómo identificar y tratar los riesgos que afecten la seguridad de la información de la empresa Optimalsoft, con el fin de definir e implementar a futuro un sistema de gestión de seguridad de la Información y salvaguardar los activos de la empresa mediante el análisis de riesgos?.

Marco Teórico

La seguridad de la información se encarga de mantener la Confidencialidad, integridad y disponibilidad, en general es la capacidad de salvaguardar la información en sistemas informáticos. López, E.(s.f) "el servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados, el principio de confidencialidad también puede verse como la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él". La Integridad garantiza que la información no sea alterada sin autorización, incluyendo su creación y eliminación, el problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales. La disponibilidad responde a un servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerido. Un sistema seguro debe mantener la información disponible para los usuarios. El sistema, tanto hardware como software, debe mantenerse funcionando eficientemente y ser capaz de recuperarse rápidamente en caso de fallo. En el libro Magerit v3 (2012, Noviembre p.7) se define Magerit "es una metodología de análisis y gestión de riesgos de los sistemas de información, con esta metodología se lleva a la creación de un marco de trabajo para la gestión de riesgos, mediante aproximaciones al problema de analizar los riesgos, los cuales son los siguientes: mandato y compromiso, diseño del marco de trabajo, implementación de la gestión de riesgos, seguimiento y revisión del marco y mejora continua del marco".

Perafan, J. (2014) "La seguridad de la información protege a una organización que la adopte como parte de su visión y misión de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los posibles daños y maximizar el retorno de las inversiones y sus las oportunidades".

Después de hacer un reconocimiento de los activos de la empresa, se imponen unas prácticas para reconocimiento de la infraestructura como tal de la empresa para saber cuáles son los medios tecnológicos para la realización de las actividades empresariales.
El reconocimiento de activos se llevó a cabo mediante reconocimiento de la empresa, viendo su visión, alcance y reglamentos internos. Magerit permitió obtener este reconocimiento bajo una serie de fases, las cuales son:

1. Captación de información.

En esta fase se hace recolección de documentación e información relevante tales como manuales de configuración, documentos de fabricantes, gestión de accesos a

dispositivos, manuales creados por agentes de la organización, documentos de estudios o contrataciones relacionadas con seguridad de la información, manuales de usuario, manuales de operación de sistemas de información propios o de externos, procesos o procedimientos diseñados para respuestas a incidencias.

Se identifican los activos relevantes mediante un plan para obtener datos sobre el nivel de seguridad de los servicios tanto software como hardware, procesos y procedimientos. Se obtiene información accediendo a los sitios físicos evaluando tuberías, plantas eléctricas, sitios de almacenamientos, con esto se logra evidenciar las condiciones que se encuentran las instalaciones. Se realizan solicitudes de cuentas de acceso para para ingreso a servidores, hardware, equipos de comunicación, todo esto con el fin de evidenciar configuraciones de los dispositivos en general.
Después de obtener credenciales a los dispositivos en general se desea determinar las posibles vulnerabilidades mediante un escenario de pruebas basado en herramientas de pentesting para detectar falencias a niveles de servicios, protocolos, puertos. Pruebas a nivel de fuerza bruta para contraseñas blandas para esquematizar la seguridad de acceso restringido. Se realiza una selección de herramientas y entornos para la realización de pruebas de pentesting con estas se procede a esquematizar los puertos abiertos, los servicios activos, las aplicaciones expuestas a posibles ataques, se hacen ataques de denegación de servicios a los servidores expuestos. Con los datos obtenidos se hace un análisis y clasificación de amenazas para sugerir salvaguardas para minimizar el impacto que podría ser muy grave donde no se tuvieran en cuenta posibles incidencias.

Se hace valoración de los activos mediante la identificación del grado de vulnerabilidad de cada activo a las amenazas que le afectan.
Se hace un reconocimiento de activos clasificándolos como: Activos esenciales los cuales en un sistema de información hay dos tipos y son la información que se maneja y los servicios que prestan. Activos de arquitectura del sistema estos se tratan de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior. Activos de Datos e información estos son el corazón que permite a la organización prestar sus servicios.
Activos de claves estos emplean claves criptográficas para guardar secretamente o para autenticar a las partes. Activos de servicios estos satisfacen una necesidad del cliente final. Activos de software estos son herramientas que han sido automatizadas para un desempeño por medio de un equipo informático. Activos de hardware estos son los medios materiales, físicos destinados a soportar directa o indirectamente los servicios prestados por la organización. Activos de redes de comunicación estos incluyen tanto instalaciones dedicadas como servicios de telecomunicaciones contratadas. Activos de media estos son dispositivos físicos que almacenan información permanente, básicamente almacenamiento auxiliar.

Terminada la clasificación de los activos se generó un plan de trabajo donde se estableció un plazo de tiempo mediante la creación de un cronograma de actividades donde se limita el tiempo por tareas para desarrollar el proyecto de seguridad.

Después de tener reconocidos y clasificados los activos, identificamos los riesgos existentes, procedemos a realizar procesos técnicos para identificación de vulnerabilidades tanto en sistemas de información, como en estructura física.

Básicamente utilizaremos Kali Linux, este es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad. Kali es una completa re-construcción de BackTrack Linux desde la base hacia arriba, y se adhiere completamente a los estándares de desarrollo de Debian. La distribución contiene más de 300 herramientas de pruebas de penetración, El equipo de Kali Linux está compuesto por un pequeño grupo de personas de confianza que sólo puede comprometer e interactuar con los paquetes de los repositorios, haciendo uso de múltiples protocolos seguros. Kali Linux, al igual que su predecesor Backtrack, es completamente gratis. Para el análisis de puertos utilizamos nmap, herramienta integrada en la distribución Kali Linux, esta aplicación es de código abierto sirve para efectuar rastreo de puertos, con esta identificamos cada servicio disponible en los computadores, sistema operativo, versiones de aplicaciones disponibles, este es un primer paso para reconocimiento, como complemento utilizamos metasploit y armitage, el primero es un framework de seguridad informática, el cual cuenta con una base de datos de vulnerabilidades y sus exploits para atacar y un objetivo y poder llevar a cabo un ataque, este contempla opciones para ataques automatizados. Armitage es una herramienta e colaboración en equipo que permite el uso de Scripts para Metasploit que permite visualizar objetivos, recomienda exploits y expone las características avanzadas de post-explotación que tiene el framework. Con Armitage pude visualizar las maquinas disponibles en la red empresarial, facilitándome ataques independientes en tiempo real, esta herramienta cuenta con tres paneles principales que son modulos, objetivos y fichas. Los modulos permiten lanzar opciones auxiliares de metasploit, lanzar un exploit, generar una carga útil, y ejecutar un módulo de post-explotación. La vista de objetivos permite visualizar la lista de target (objetivos) que podrán ser atacados. Las fichas son un espacio tipo consola para visualizar los ataques y resultados obtenidos tras la selección de objetivos y modules de ataque.

Al realizar las pruebas de penetración las cuales se realizaron local y remotamente se reconocieron vulnerabilidades que permitieron evaluar los riesgos y estimar procedimientos de seguridad de la información, llevado a cabo esta actividad se procede a documentar las pruebas utilizando una matriz para resaltar los conceptos contemplados como lo son servidor, vulnerabilidad, nivel de la vulnerabilidad, identificación de la vulnerabilidad, y una solución a esta.

Metodología

Se plantearon una serie de actividades que dimensionaron y enfrentaron el problema de seguridad en general, esto se realizó para brindar al final del proyecto las posibilidades que tuvo la empresa para adoptar un plan de mejora de acuerdo a los resultados que se obtuvieron a partir del análisis de riesgos.

A continuación se listan las actividades realizadas:

Análisis de fuentes de datos y recopilación de información: Esta etapa busco recolectar la mayor cantidad de información posible con respecto al estado de la empresa en cuanto a información, estudios o proyectos que tuvieron relación con el análisis de riesgos y en general en materia de seguridad informática.

Recolección de documentos organizacionales: para realizar el análisis de riesgos fue importante conocer el entorno y contexto en el que se basa la empresa objeto de estudio, reconocimiento de su estructura organizacional.

Presentación de conceptos: Se presentó los conceptos informalmente. En particular se enmarcaron las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

Descripción de riesgos y su tratamiento: Se describió opciones y criterios de tratamiento de los riesgos y se formalizo las actividades de gestión de riesgos.

Centralización en los riesgos: Se centró en los proyectos de análisis de riesgos, proyectos en los que nos vimos inmersos para realizar el primer análisis de riesgos.

Reconocimiento de sistemas de información: Se centró en el desarrollo de sistemas de información y cómo el análisis de riesgos sirvió para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

Documentación: En paralelo a la generación del informe técnico, se realizó un resumen ejecutivo que muestra de una manera general y objetiva los resultados del proyecto.

Resultados y análisis

Se identificaron, clasificaron y diagnosticaron los activos de información presentes en la empresa Optimalsoft S.A.S mediante la alineación con los objetivos del negocio, construyendo un mapa de riesgos identificando las prioridades en el negocio, se diseñó un programa estratégico de seguridad de la información tomando como punto de partida los riesgos identificados. Se definieron políticas de seguridad donde se contemplan los sistemas y procedimientos de la empresa para la elaboración de ciertas actividades. Se capacitaron los miembros de la empresa respecto a amenazas y a la conveniencia de acatar políticas de protección para no abrir vulnerabilidades. Se llevó a cabo la creación de un equipo de seguridad para formalizar las funciones que se deben llevar a cabo por cada miembro del equipo. Se capacito para la creación de aplicativos seguros desde su origen, implementando soluciones tecnológicas encaminadas en la seguridad de la información. Medir el nivel de seguridad en la empresa como estrategia de protección para saber si los objetivos se están cumpliendo y si se encontró el nivel de conciencia de cada individuo para mitigar incidentes que puedan alterar los activos de la compañía.

Aplicando la metodología Magerit para evaluación de riesgos descubrimos la descripción de la organización, la misión, visión y objetivos. Seguido de esto nos enfocamos en la estructura tecnología, evaluando la situación inicial de los servicios tecnológicos prestados, pasando por la red física, red de datos, configuración de equipos tecnológicos, descripción de hardware y software, se determinan salvaguardas, luego de determinar estas debemos estimar el impacto, estimar los riesgos. Ejecutados los pasos anteriores se llevó una evaluación y tratamiento a los activos de la organización para mitigar riesgos existentes.

Mediante un diagrama de procesos de análisis y gestión de riesgos se sugiere mecanismos de control y gestión que mitiguen las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado.

En la terminología normativa Magerit implementa proceso de gestión de riesgo dentro del marco de trabajo, teniendo en cuenta los riesgos derivados del uso de tecnologías.

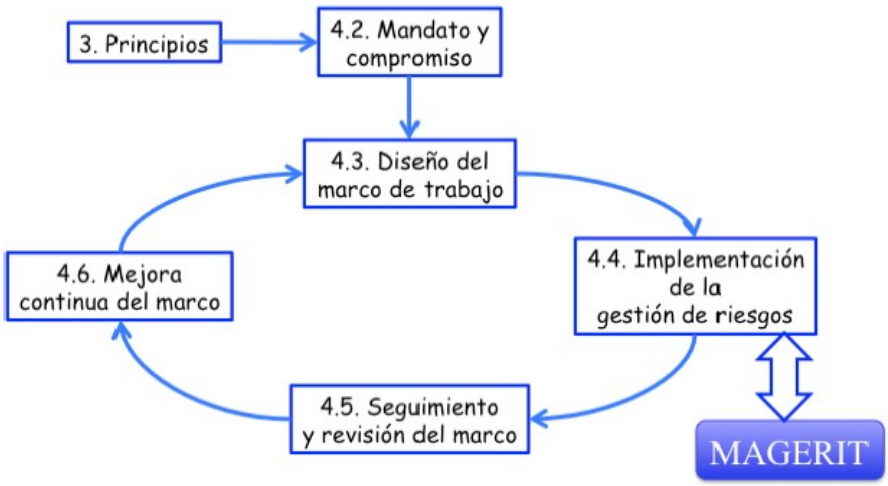

Figura 1. Marco de trabajo para la gestión de riesgos. (p.7), Por MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [2012].

El ciclo de análisis y tratamiento de los riesgos permite identificar como es, cuanto vale, y como está protegido el sistema.

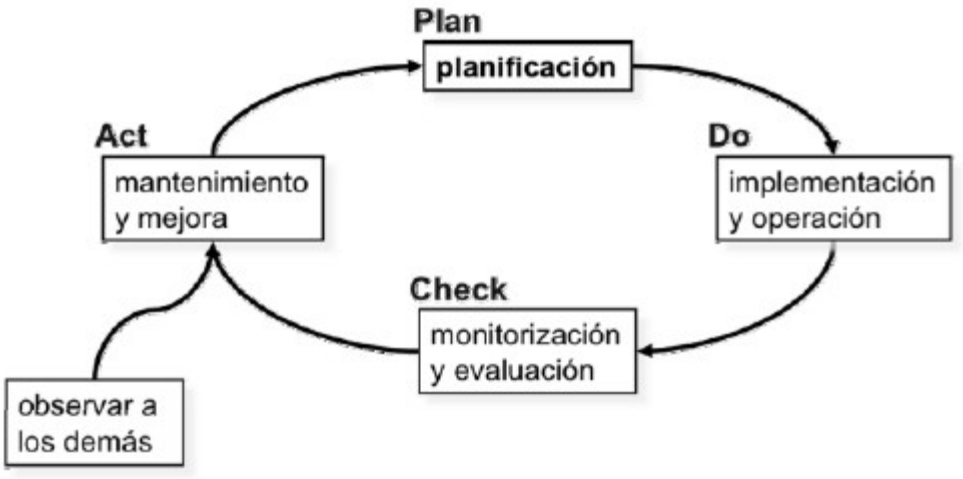

Figura 2. Ciclo de análisis y tratamiento de los riesgos en su contexto. (p.11), Por MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [2012].

En una auditoria puede contemplarse un análisis de riesgos que le permita saber que activos hay, saber a qué están expuestos y valorar las salvaguardas.

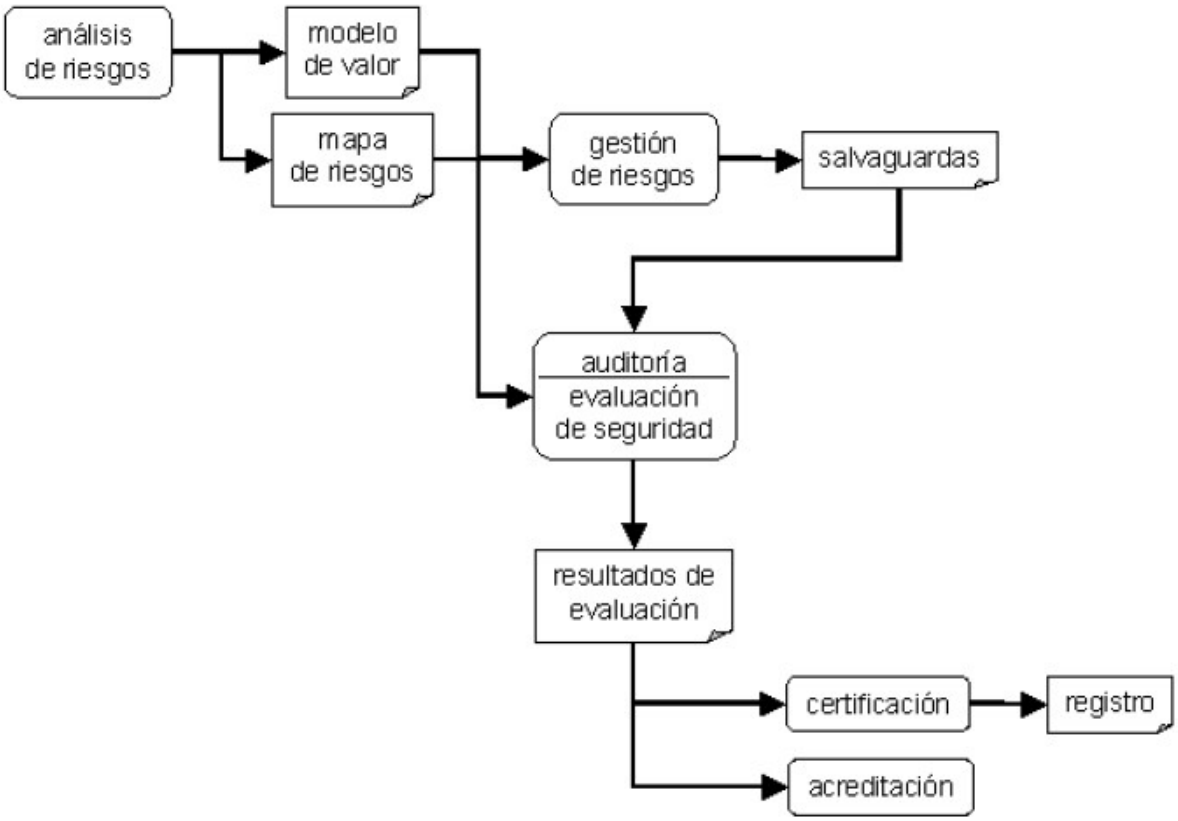

Figura 3. Contexto de certificación y acreditación de sistema de información. (p.15), Por MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [2012].

El análisis de riesgos es uno de los elementos fundamentales dentro de la implementación de un sistema de gestión de seguridad, debido a que en esta parte se cuantifica y clasifica la importación de los activos de la empresa.

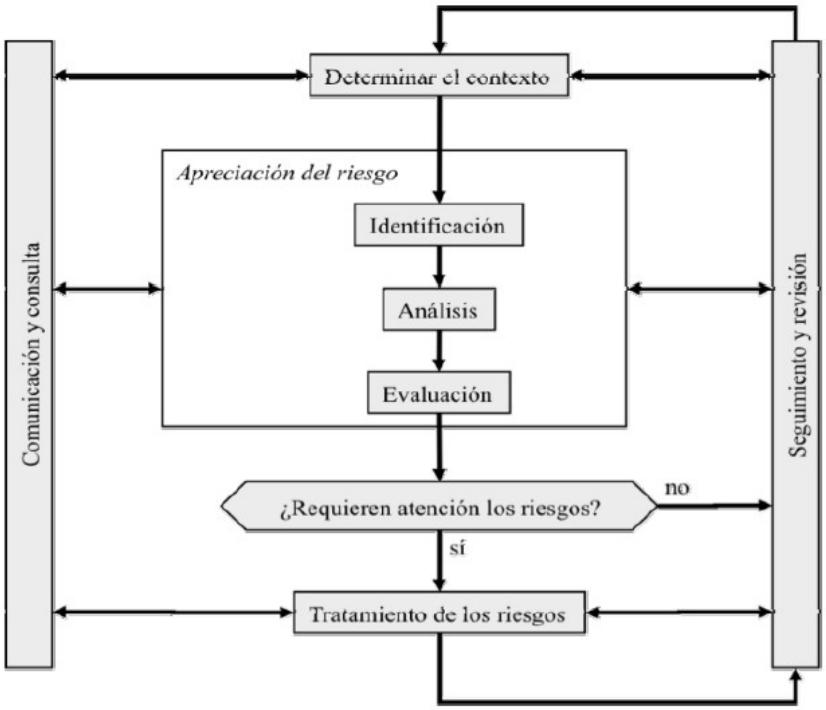

Figura 4. Proceso de gestión de riesgos. (p.20), Por MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [2012].

Después de determinar y clasificar los riesgos se determinan cuáles son los riesgos potenciales, es decir, los que afectan los activos más relevantes.

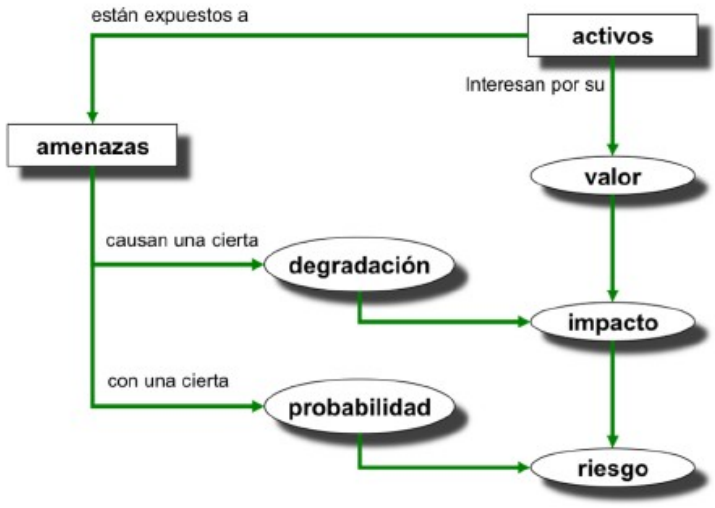

Figura 5. Elementos de análisis de riesgos potenciales. (p.22), Por MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [2012].

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse por zonas a tener en cuenta en el tratamiento de los riesgos.

Zona 1. Riesgos muy probables y de muy alto impacto. Zona 2. Cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo. Zona 3. Riesgos improbables y de bajo impacto. Zonta 4. Riesgos improbables pero de muy alto impacto.

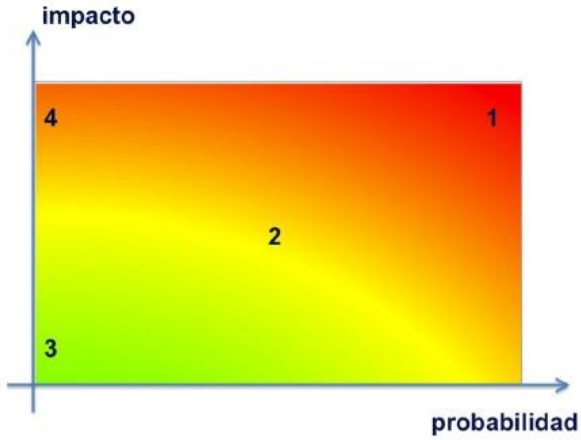

Figura 6. El riesgo en función del impacto y la probabilidad. (p.30), Por MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [2012].

Las salvaguardas entran en un cálculo de riesgo de dos formas, reduciendo la probabilidad de amenazas y limitando el daño causado.

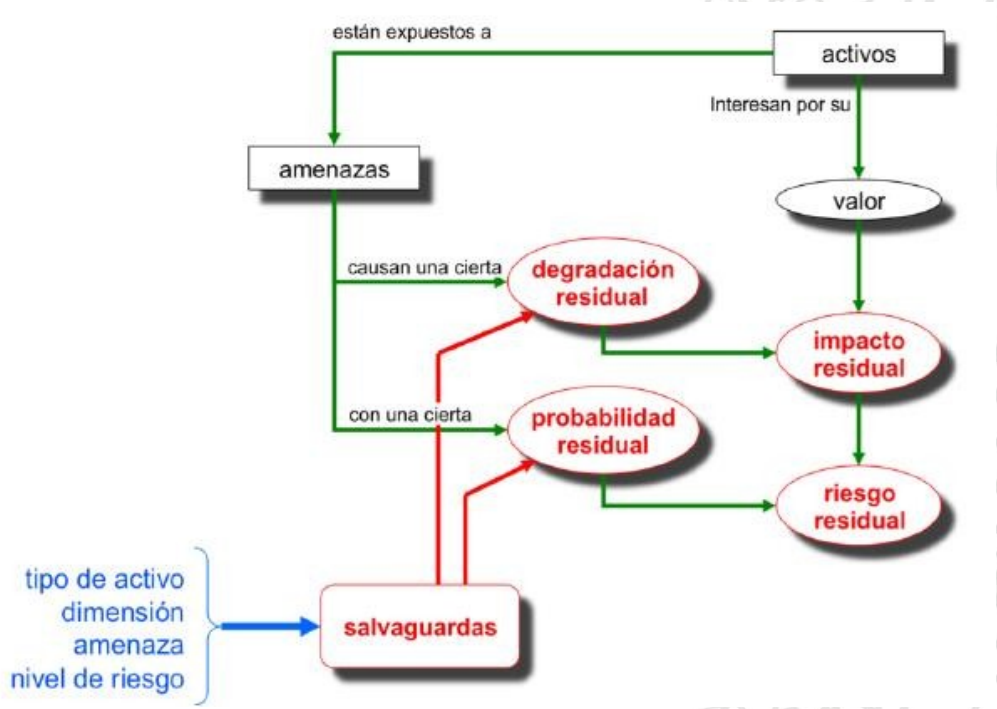

Figura 7. Elementos de análisis de riesgos residual. (p.32), Por MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [2012].

Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. El riesgo pondera la probabilidad de que ocurra. La siguiente figura resume las posibles decisiones que se pueden tomar tras haber estudiado los riesgos. La caja "estudio de los riesgos" pretende combinar el análisis con la evaluación.

Figura 8. Decisiones de tratamiento de los riesgos. (p.48), Por MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, [2012].

Dado por terminado el análisis de los riesgos y clasificación de los activos, procedemos a realizar técnicas de pentesting para encontrar vulnerabilidades en los sistemas de la empresa para posteriormente mitigarlas y proceder a la documentación que permita fomentar buenas prácticas de seguridad.

Se implementa escaneo de las redes corporativas para la identificación del sistema. Procedimos a realizar una serie de escaneo a todo el hardware conectado a las redes con herramientas gratuitas contenidas en la distribución Kali Linux.

Figura 9. Entorno grafico Kali Linux. Imagen propia.

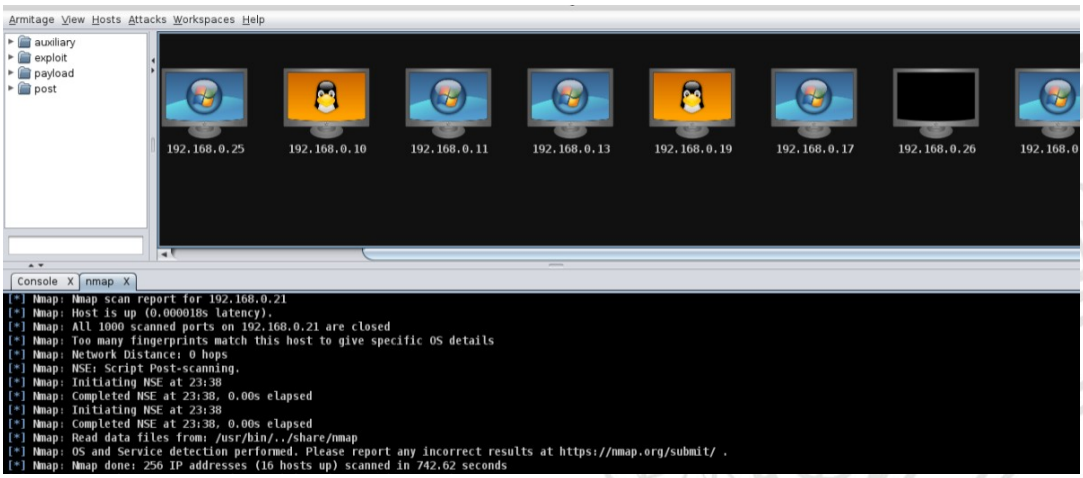

Figura 10. Escaneo de la red mediante herramienta armitage. Imagen propia.

Se prueban varios vectores de ataque contra las maquinas escaneadas, se encuentran vulnerabilidades.
Se testea aplicativo de información, alojado en tomcat, no se encuentran vulnerabilidades xxs ni sqlinjection. Se usaron las herramientas Vega, xxser, Grabber.

Mediante el navegador web se accede a sitio web, evidenciando la ausencia de certificados SSL, estos son los encargados de validar la identidad de tu sitio web y cifran la información que los visitantes envían a tu sitio o reciben del mismo. Esto evita que los ladrones espíen cualquier intercambio entre tú y tus compradores. Cuando tienes la protección de un Certificado SSL en tu sitio web, tus clientes pueden estar seguros de que la información que ingresan en cualquier página asegurada es privada y los estafadores cibernéticos no podrán verla. Se crearon llaves con la herramienta keytool de java, para la creación de llaves, las cuales deben ser intercambiadas con un proveedor de seguridad web, el cual se encargara de gestionar la autenticidad de nuestro sitio web.

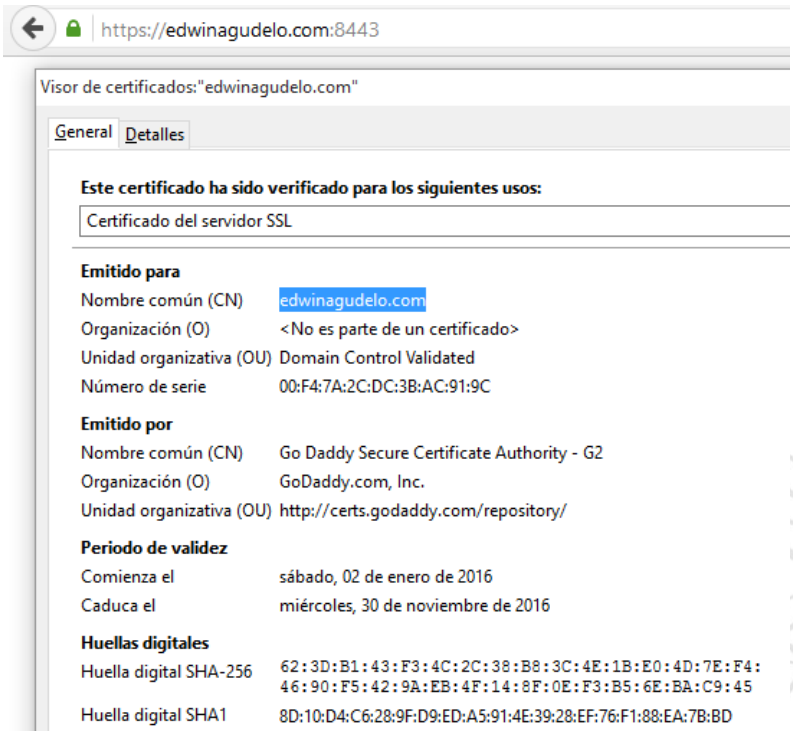

Figura 11. Sitio web certificado por Goddady marcado como sitio seguro. Imagen propia.

Reconocimiento de herramienta Apache Subversión (abreviado frecuentemente como SVN, por el comando *svn*) es una herramienta de control de versiones open source basada en un repositorio cuyo funcionamiento se asemeja enormemente al de un sistema de ficheros. Es software libre bajo una licencia de tipo Apache/BSD. Uno de los principales activos de una empresa de software es su código fuente, y con esté la gestión del mismo. Es de gran importancia realizar copias de seguridad y enviarla a otro servidor, para garantizar la disponibilidad, integridad del código fuente sin tener que depender del estado de salud del servidor principal.

```
sudo svnadmin dump codigo | gzip -9 > /home/usuario/$hoy/codigo.dump.gz
scp codigo.dump.gz usuariootroservidor@ipotroservidor:/home/usuariootroservidor/SEGURIDAD/$hoy/
```

Figura 12. Script copias de respaldo código fuente a servido remoto. Imagen propia.

Configuración de accesos wifi y enrutadores. Muchos administradores de tecnología se encargan que la empresas tengan un excelente internet, pero cuantos verifican el acceso a este?. Esta pregunta me la hago cada vez que ingreso a una red wifi. Todos sabemos que los proveedores de telecomunicaciones tratan de limitar el acceso a las configuraciones del router, esto para evitar el alto soporte que puede causar el acceso de personas que desconocen las funcionalidades de este. Voy a mostrar en breve, sabiendo la referencia del router para buscar con el fabricante las credenciales que nos corresponden. En la Puerta de enlace de nuestra red solemos

suele ser la que llevan asociados la mayoría de los routers ADSL, VDSL y FTTH del mercado. A través de ella podremos acceder a la configuración del equipo y podremos configurar por ejemplo la red WiFi, abrir los puertos, actualizar el firmware o modificar cualquier parámetro de la configuración. Normalmente suele ser 192.168.1.1 pero puede variar en el tercer bloque siendo 192.168.o.1 otra de las direcciones habituales más utilizadas por los equipos.

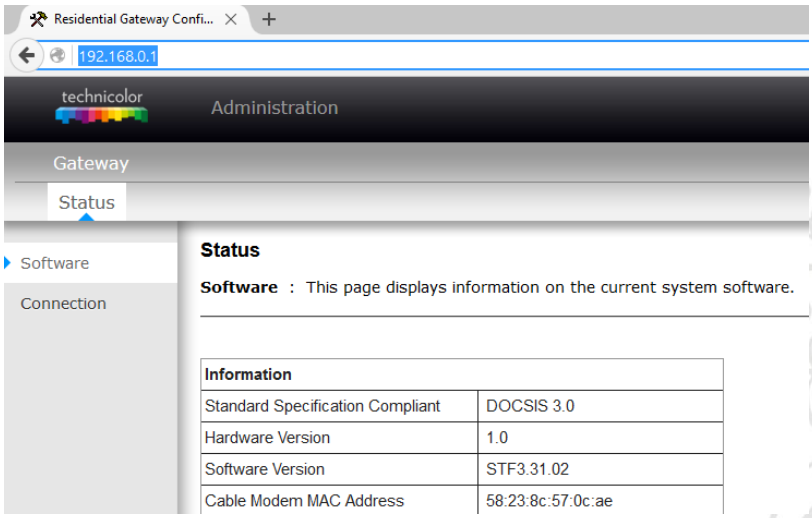

Figura 13. Enlace a puerta de enlace sin privilegios (Restricción de proveedor de internet). Imagen propia.

Ahora ingresamos con el navegador toor con la ip que nos suministra el proveedor de internet y nos saldrá una emergente pidiendo las credenciales suministrada por el fabricante del hardware.

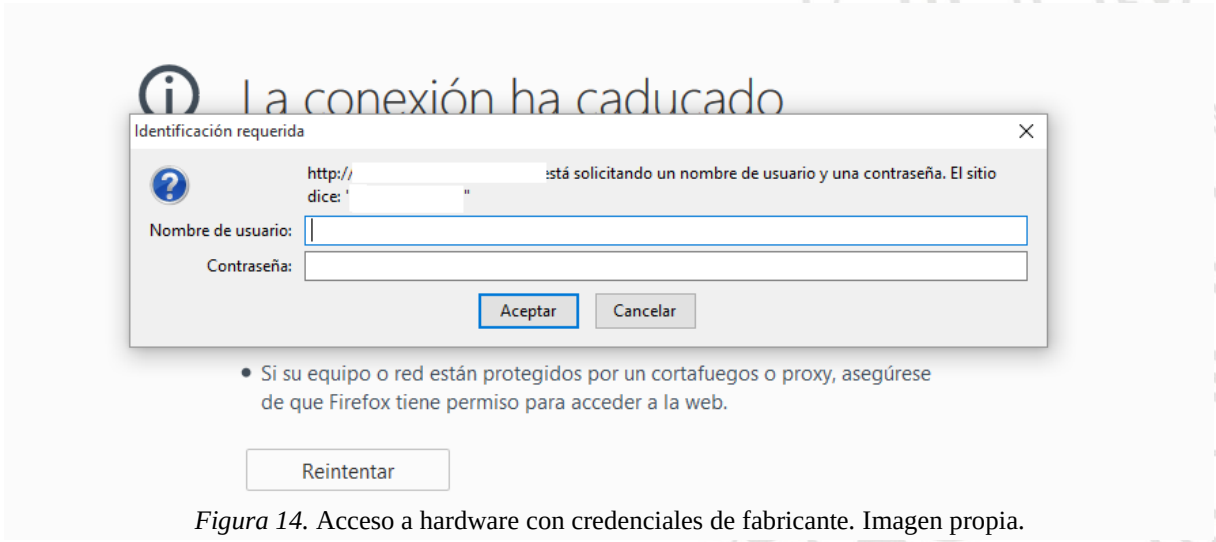

Figura 14. Acceso a hardware con credenciales de fabricante. Imagen propia.

Conclusiones

- Contar con una buena implementación de políticas de seguridad informática es un punto clave en toda organización para asegurar los activos de la empresa. Siempre se desea desarrollar con éxito un programa efectivo de seguridad de la información consistente e implementar las políticas, estándares y procedimientos de seguridad.

- La seguridad informática es importante porque las consecuencias de las explotaciones de vulnerabilidades pueden ser desastrosas. Las métricas de seguridad tienen que proteger a una máxima expresión los recursos y la información, para asegurarse que nadie pueda leer, copiar, descubrir o modificar la información sin autorización. Así como interceptar las comunicaciones o los mensajes entre entidades

- El estudio realizado me fue de gran importancia, este ayudo a mi crecimiento laboral, poniendo a prueba una serie de conceptos que no alcanzaba a manipular en la práctica además se logró concientizar a el personal de la empresa de vectores de ataque, independiente de las funciones desempeñadas en la empresa, desde la parte administrativa hasta el grupo de desarrolladores.

Referencias bibliográficas

Ben Collins-Sussman, Brian W. Fitzpatrick, and C. Michael Pilato. (2010). You are reading Version Control with Subversion. Consultado el día 9 de enero de 2016 de la World Wide Web: http://svnbook.red-bean.com/en/1.7/svn.ref.svnadmin.c.dump.html

Chema Alonso. (jueves, noviembre 01, 2007). Fortificando un Servidor Apache. Consultado el día 9 de diciembre de 2015 de la World Wide Web: http://www.elladodelmal.com/2007/11/fortificando-un-servidor-apache-iii-de.html

Chema Alonso. (lunes, noviembre 14, 2011). Una auditoría es como una caja de bombones: .svn/entries. Consultado el día 6 de enero de 2016 de la World Wide Web: http://www.elladodelmal.com/2011/11/una-auditoria-como-una-caja-de-bombones.html

Chema Alonso. (viernes, marzo 20, 2015). Un HASH MD5 en la password no sustituye a SSL. Consultado el día 8 de diciembre de 2015 de la World Wide Web: http://www.elladodelmal.com/2015/03/un-hash-md5-en-la-password-no-susituye.html

López, E.(s.f). Fundamentos de Seguridad Informática. Consultado el día 5 de diciembre 2015 de la World Wide Web: http://redyseguridad.fip.unam.mx/proyectos/seguridad/ServConfidencialidad.php

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (2012). Marco de trabajo para la gestión de riesgos. [Figura 1].

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (2012). Ciclo de análisis y tratamiento de los riesgos en su contexto. [Figura 2].

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (2012). Contexto de certificación y acreditación de sistema de información. [Figura 3].

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (2012). Proceso de gestión de riesgos. [Figura 4].

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (2012). Elementos de análisis de riesgos potenciales. [Figura 5].

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (2012). El riesgo en función del impacto y la probabilidad. [Figura 6].

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (2012). Elementos de análisis de riesgos residual. [Figura 7].

MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (2012). Decisiones de tratamiento de los riesgos. [Figura 8].

Ministerio de Hacienda y Administraciones Públicas (2012, Noviembre). MAGERIT versión 3. Consultado el día 6 de diciembre de 2015 de la World Wide Web: http://administracionelectronica.gob.es

Ministerio de Hacienda y Administraciones Públicas (2012, Noviembre). MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (Libro I método pp 7-9).

NETSIS. (24 junio, 2015). Distribuciones Linux Recomendadas para Pentesters. Consultado el día 9 de enero de 2016 de la World Wide Web: http://www.hackingpublico.net/10-distribuciones-linux-recomendadas-para-pentesters-en-el-2015-by-netsis/

Perafan, J. (2014). Análisis de Riesgos de la Seguridad de la Información para la Institución. Tesis de grado. Especialización en Seguridad Informática, Universitaria Colegio Mayor Del Cauca, Colombia.

Vicente Motos. (2016). Las 25 peores contraseñas del 2015 (y que nunca deberías utilizar). Consultado el día 7 de enero de 2016 de la World Wide Web: http://www.hackplayers.com/2016/01/las-25-peores-contrasenas-del-2015.html