UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de:

Ingeniería de sistemas con mención en Telemática

TEMA:

"Análisis para la integración de un
Sistema de Gestión de Seguridad de Información (SGSI)
ISO-27001 Utilizando OSSIM para empresa Industrial"

AUTORES:

Claudia Yagual Del Valle

Leslie Chilán Rodríguez

DIRECTOR:

Msig. Nelson Mora

GUAYAQUIL, DICIEMBRE 2014

DECLARACIÓN EXPRESADA

La responsabilidad del contenido de este Proyecto de Grado, corresponde exclusivamente a los autores; y el patrimonio intelectual de la misma a la Universidad Politécnica Salesiana.

Guayaquil, 15 de Diciembre del 2014

_____ _____

Claudia Yagual Del valle **Leslie Chilán Rodríguez**

DEDICATORIA

A mi familia quienes son de gran motivación en mi vida para salir adelante junto con ellos en la carrera de la vida.

Claudia Yagual Del valle

AGRADECIMIENTO

Agradezco a mi Soberano Padre Celestial Jehová por permitirme avanzar hasta donde he llegado, una vez más cumpliendo un objetivo importante en mi vida, porque sin Él nada es posible.

Agradezco a mis amados Padres Máximo y Alexandra, quienes han sido de mucho apoyo a lo largo de esta meta, en especial a mi querida hermana Odalys quien nunca dejó de darme fuerzas en todo momento.

A mi querido novio Mauricio quien siempre estuvo dándome aliento, motivación, apoyo y ejemplo de no desfallecer en el camino.

A mis amigos y hermanas de la iglesia quien siempre estuvieron pendientes de este proyecto.

A la Ing. Lilia Saltos, Jefa de TI de la empresa Industrial donde se realizó esta tesis, puesto que nos permitió desarrollar este proyecto y habernos contribuido su experiencia con su ayuda con la elaboración del mismo.

Y un sincero agradecimiento a nuestro director de tesis Msig. Nelson Mora quien nos ha brindado su ayuda y guía para la realización del presente trabajo.

Claudia Yagual Del valle

DEDICATORIA

A mi abuelita Bélgica Díaz y a mis padres Judith Rodríguez y Genner Chilán, por su apoyo incondicional por haberme inculcado valores que me han servido y los he puesto en práctica a lo largo de mi vida.

Por enseñarme que con constancia, dedicación y amor todo es posible.

En especial a mi mamá que aunque ya no está físicamente conmigo es la luz que me guía en cada etapa de mi vida.

Leslie Chilán Rodríguez

AGRADECIMIENTO

En primer lugar agradecerle a Dios por darme las fuerzas necesarias para cumplir mis objetivos y ayudarme a enfrentar de manera positiva cualquier adversidad.

A mis padres, a cada uno de mis familiares, amigos y jefes por confiar en mí, por estar siempre pendientes de este proceso y darme las palabras de ánimo cuando más las necesitaba. Gracias por su apoyo incondicional ya que esto me permitió seguir adelante para alcanzar la meta.

Agradezco a todos los docentes que conocí a lo largo de la carrera por impartir sus conocimientos con mucha dedicación, paciencia y compartir sus experiencias.

En especial a la Ing. Lili Saltos por su apoyo y respaldo para la realización de esta tesis. A mi tutor el Msig. Nelson Mora por guiarnos a lo largo de este proceso y darnos las recomendaciones necesarias.

Leslie Chilán Rodríguez

RESUMEN

El presente trabajo se basa en la identificación de amenazas y vulnerabilidades hacia los activos más críticos de una empresa industrial para los cuales, ya sabiendo que tan vulnerables pueden materializarse, se recomendarán los controles adecuados basándose en la norma ISO 27001, de tal manera que la empresa pueda minimizar sus riesgos. Además, se deja un plan de contingencias sobre los riesgos a las que se encuentra expuesto el centro de cómputo y servicios informáticos de la empresa.

Para este caso de estudio se usó el método de investigación de riesgos llamado "Magerit", la cual nos guio con la realización de una matriz de evaluación y riesgos para cada proceso de la empresa, determinando que tan expuesto se encontraba un activo hacia alguna vulnerabilidad.

La norma ISO 27001 también propone un Sistema de Gestión de Seguridad de la Información (SGSI, incluida en esta tesis) en la cual se plantean las diferentes políticas que podrían regularizarse dentro de la empresa y, a su vez, ser conocidas por el personal, llegando así a tener una mejor práctica de seguridad de la información.

OSSIM es una plataforma Open Source que permite integrar 22 herramientas de seguridad para detectar patrones y vulnerabilidades. Monitoriza anomalías y analiza el tráfico, beneficiando a la empresa al aumentar la seguridad en la red. Su objetivo principal es centralizar, clasificar y priorizar los distintos eventos que generan sus herramientas, facilitando al administrador la gestión para la toma de decisiones y la visión en tiempo real del estado de la red.

Uno de los componentes principales de OSSIM, OpenVas, fue de gran utilidad dentro de este proyecto debido a que, mientras se realizó el escaneo de la red, se pudo comprobar que al recibir un evento el componente fue capaz de revisar el plug-in y determinar con un test si era o no un falso positivo de vulnerabilidad. Como resultado del mencionado escaneo no se detectaron vulnerabilidades dentro de la organización.

ABSTRACT

This work is based on the identification of threats and vulnerabilities to the most critical assets of an industrial enterprise for which, and knowing how vulnerable it can become, based on the ISO 27001 standard appropriate controls will be recommended so the company can minimize the risks. In addition, a contingency plan is left to deal on the hazards that the data center and Informatics services are exposed.

For this use case study research method called risk "Magerit" which guided us in conducting a risk assessment matrix and for each business process, determining how an asset was exposed to a vulnerability .

The ISO 27001 standard also proposes an Information Security Management System (ISMS included in this thesis) which present the various policies that could be regularized within the company and, in turn, be known by the enterprise staff, thus leading to a better practice of Information Security.

OSSIM is an Open Source system that integrates 22 security tools to detect patterns and vulnerabilities. This platform monitors and analyzes traffic anomalies, benefiting the company while increasing network security. Its main purpose is to centralize, classify and prioritize the different events their tools generate, providing an easy management for decision-making and a real-time view of the network status to the administrator.

One of the OSSIM's main components, OpenVas, was very suitable in this project because, while the network scan was performed, it was found that when receiving an event, the component was able to check the plugin and, by a test, determine whether it was a false positive or not for a vulnerability. As a result, no vulnerabilities within the organization were detected.

ÍNDICE DEL CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FÍGURAS

INTRODUCCIÓN

Actualmente las organizaciones gastan una gran cantidad de dinero comprando firewalls o dispositivos de seguridad, pero muchas veces esta inversión no es en su totalidad segura porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad "Las personas que administran los equipos".

La norma ISO 27001 permite regular, gestionar y mitigar al máximo los riesgos a los que se encuentran expuestos los activos de una empresa; tales como pérdida de información, disponibilidad de servicios entre otros.

Para esto se realizó la evaluación de activos por procesos considerados como críticos de la empresa; puesto que el área de TI brinda sus servicios informáticos, equipos, diferentes tipos de hardware, entre otros, a diferentes áreas de la organización, entonces se vio la necesidad de realizar la evaluación sobre los procesos de la empresa para que el área de TI conociera cuáles son sus activos que afectarían a algún proceso del negocio, si estos no estuvieran disponibles, íntegros o no se conociera una medida de confidencialidad sobre el activo.

Se realiza una matriz de evaluación y riesgos, para cada proceso de la empresa y el resumen de los resultados se detallan en el capítulo cuatro del presente proyecto.

Con OSSIM se expone que con una sola tecnología como la que brinda AlienVault se puede llegar a obtener una mejor visibilidad de todos los eventos que se presentan en el sistema y todos con un mismo formato enfocados en un mismo punto priorizando cada evento y permitiendo aumentar la capacidad de detección, ahorrando a su vez dinero ya que como es de código abierto se llega a realizar modificaciones por los propios administradores de red.

CAPÍTULO 1

1 PLANTEAMIENTO DEL PROBLEMA

Luego de analizar la infraestructura del departamento de TI de la empresa industrial a la que llamaremos "Yanez", es notable el crecimiento experimentado con el paso de los años. Esto ha provocado que los controles a nivel de seguridad de la información no sean los adecuados para garantizar la disponibilidad, integridad, y confidencialidad de la información, razón por la cual es necesario sean revisados y mejorados.

La norma ISO 27001 permite, regular, gestionar y mitigar al máximo los riesgos a los que está expuesto el departamento de TI tales como incidentes de seguridad, pérdida de información, disponibilidad de servicios entre otros. A la vez se ha encontrado un mecanismo de control que permita al administrador de seguridad establecer una estructura completamente centralizada la cual le permite visualizar y analizar los eventos relevantes que ocurren en una infraestructura de TI, para esto se utilizara como herramienta la consola de seguridad OSSIM.

La capacidad de la consola OSSIM permitirá obtener información completa y selecta, de los diferentes eventos que reportan otras herramientas en el departamento de TI, así les permite ser una herramienta muy útil a los administradores de red, eligiendo el procedimiento que regirá la seguridad en el sistema de información, pudiendo así, detectar amenazas rápidamente y disponiendo de un nivel adecuado de protección para la información y equipos que permiten la comunicación dentro de la red.

1.1 Formulación del problema

¿Cómo puede la organización contar con un excelente nivel de seguridad de la información, detectando a su vez actividades o procesos que realicen individuos o sistemas no autorizados sobre elementos de la red?

1.2 Sistematización del problema

¿Cómo puede mejorarse la seguridad de la información en la empresa?
¿Cómo saber que procesos son los que requieren mayor nivel de prioridad?
¿Cómo evitar el acceso no autorizado a la información de los sistemas y servicios?
¿Cómo gestionar de manera segura las comunicaciones y operaciones informáticas?

1.3 Objetivos

1.3.1 Objetivo general

Minimizar los riesgos de seguridad de la información mediante el análisis previo a la implementación de la norma ISO 27001 combinando las herramientas de seguridad que ofrece OSSIM logrando así el fortalecimiento de un sistema de gestión de control eficiente para el área de Tecnología de información.

1.3.2 Objetivos específicos

- Proponer políticas y objetivos para la seguridad de la información.
- Identificar los activos más críticos de los diferentes procesos de la empresa.
- Aplicar controles adecuados previniendo riesgos encontrados.
- Permitir la visualización de análisis de eventos de vulnerabilidad que pudieran presentarse dentro de la infraestructura de la empresa mediante la consola de aplicación OSSIM.

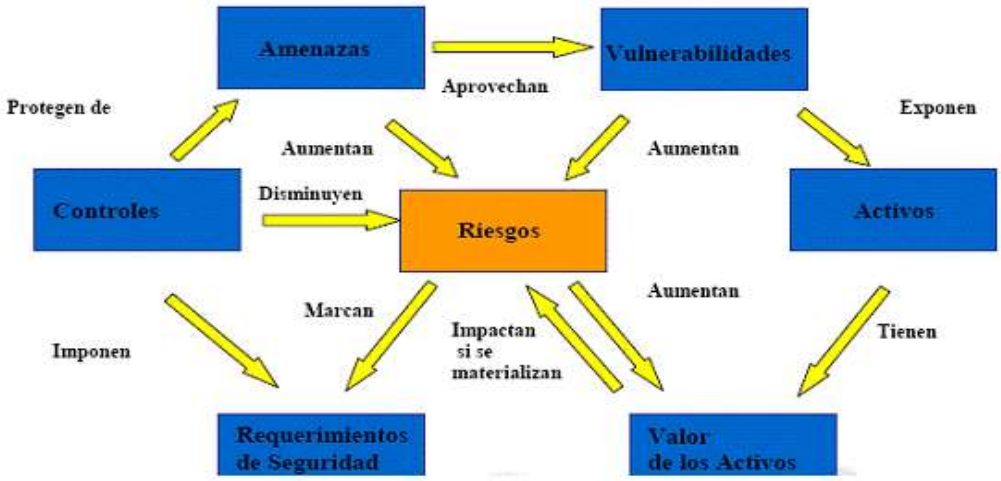
1.4 Justificación

Debido a que cada vez existen más organizaciones y sistemas expuestos a los diferentes tipos de amenazas que aprovechando cualquiera de las vulnerabilidades existentes, pueden llegar a someter a los activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente por personal de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

La protección adecuada de la información siendo este considerado como el activo más importante de la empresa, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de la empresa.

Figura 1.1 Debilidades en la información



Fuente: http://www.gestion-calidad.com/seguridad-informacion.html

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos. El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo.

En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayudará a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. (DestacaDos SGSI, 2005)

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

La competitividad es otro de los factores en el cual se encuentra muy interesada la empresa.

En un mercado cada vez más competitivo, a veces es muy difícil encontrar algo que lo diferencie ante la percepción de sus clientes. La norma ISO 27001 puede ser un verdadero punto a favor, especialmente si se administra información sensible de los clientes.

CAPÍTULO 2

2 MARCO TEÓRICO

2.1 ISO/IEC 27001

El estándar para la seguridad de la información ISO/IEC 27001, fue aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Este especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) definiendo los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). (López Neira & Ruiz Spohr, 2012)

2.1.1. Antecedentes del estándar ISO 27001

Hace algunos años no existía la tendencia de certificar procesos, o sistemas de gestión, por ello, ISO 9000 vino a redefinir en el año 2000 la certificación de los sistemas de gestión de calidad, mediante la norma ISO 9001:2000.

Pero aún en el 2005, no existía una norma ISO que permitiera certificar, por alguna organización en cuanto a sus prácticas de seguridad informática y las alternativas, en esos momentos se certificaba en normas inglesas (BS) o españolas (UNE).

Hasta 2005, el estándar más conocido en el entorno de seguridad informática era el ISO 17799, pero con la limitación de ser un "código de prácticas" (Information technology– Security techniques– Code of practice for information security management), en el momento que se publica su última revisión, se anuncia el desarrollo de una serie de estándares ISO 27000, dedicada exclusivamente a la seguridad informática. Con esto se le da un nuevo alcance a la seguridad, porque no sólo es llevar un código de mejores prácticas sino establecer un estándar certificable de forma similar al ISO 9000 (el primero de esa serie en publicarse fue el ISO 27001). (Logisman, 2011)

Las certificaciones han pasado a ser necesidad para demostrar la existencia de sistemas de gestión, con objeto de asegurar procesos consistentes. En el campo de la seguridad informática se tenían certificaciones por parte de estándares británicos y españoles pero, hace pocos años, la ISO emitió los estándares por los sistemas de gestión de seguridad informática con objeto de certificar que las recomendaciones y buenas prácticas brinden una ventaja competitiva a las organizaciones, y no dejar descubiertos todos los sistemas de información que día con día cobran una mayor importancia para sustentar la toma de decisiones y salvaguardar el activo más importante de una organización: la información.

2.1.2 Objetivos de la seguridad

Entre los objetivos de la seguridad tenemos:

Disponibilidad y accesibilidad de los sistemas y datos: "Solo para uso autorizado, es un requisito necesario que garantiza que el sistema trabaje puntualmente, con prontitud y que no se deniegue el servicio a ningún usuario autorizado." (Areitio Bertolín, 2008)

Integridad: "Se encarga de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados mientras se almacena, procesan o transmiten así evitando la perdida de consistencia." (Areitio Bertolín, 2008)

Confidencialidad de datos: "Es el requisito que intenta que la información privada o secreta no se revele a individuos no autorizados. La protección de la confidencialidad se aplica a los datos almacenados durante su procesamiento, mientras se transmiten y se encuentran en tránsito." (Areitio Bertolín, 2008)

Asimismo, existen otros objetivos más generales tenemos:

- Conocer todos los riesgos de seguridad asociados a la organización.
- Establecer un conjunto equilibrado de requisitos de seguridad de acuerdo con los riesgos identificados, para satisfacer las necesidades de un determinado proceso de negocio.

Al tener claro estos objetivos lo primero que se debe realizar es una lista de todos los activos de cada departamento con su respectivo análisis de riesgo.

La gestión del riesgo es una parte importante de la gestión de la seguridad y se define como el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado.

La valoración de riesgos es el proceso consistente en identificar los problemas antes de que aparezcan.

En la gestión de riesgos, existe un factor de incertidumbre asociado con la probabilidad de que aparezcan las amenazas, que sea diferente, dependiendo de cada situación. Cada amenaza se puede predecir dentro de ciertos límites.

Un incidente no deseado presenta tres componentes: amenazas, vulnerabilidad e impacto. La vulnerabilidad indica la debilidad del activo que puede ser explotada por una amenaza. Los riesgos disminuyen con controles o medidas. (Areitio Bertolín, 2008)

2.2 Elementos de gestión de la seguridad de los sistemas de información

Entre los elementos involucrados están:

- Identificación de todos los activos
- Identificación de amenazas a los activos
- Identificación de vulnerabilidades
- Identificación de impactos
- Identificación de riesgos
- Aplicación de controles

2.2.1. Identificación de los activos del sistema

Los activos son aquellos elementos relacionados con el entorno, como son el personal, los edificios, las instalaciones, los equipos, o los suministros; los relacionados con los sistemas de TIC (Tecnologías de la Información y la Comunicación), como los equipos hardware, el software, los componentes de comunicaciones de datos; los relacionados con la información, los relacionados con las funcionalidades de la organización, como la capacidad de proporcionar un servicio, crear un producto. (Areitio Bertolín, 2008)

2.2.2 Identificación de riesgos

El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio es decir un conjunto de activos o en toda la organización.

Este impacto se puede producir debido a que una amenaza explote vulnerabilidades para causar pérdidas o daños.

El riesgo se caracteriza por una combinación de dos factores: la probabilidad de que ocurra el incidente no deseado y su impacto. (Areitio Bertolín, 2008)

Figura 2.2 Análisis de riesgos

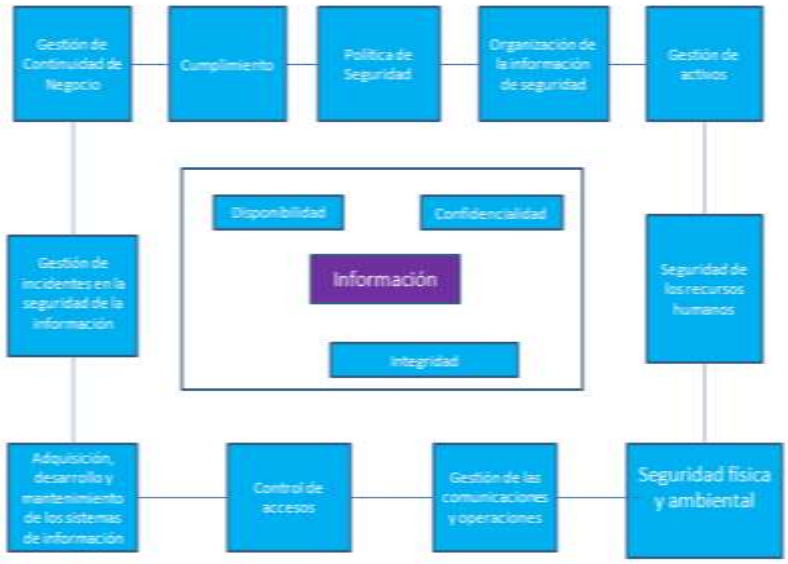
Fuente: (Areitio Bertolín, 2008)

2.2.3 Aplicación de controles y su descripción

Los controles que el anexo A de esta norma propone quedan agrupados y numerados de la siguiente forma:

A.5 Política de seguridad.
A.6 Organización de la información de seguridad.
A.7 Gestión de activos.
A.8 Seguridad del recurso humano.
A.9 Seguridad física y ambiental.
A.10 Gestión de las comunicaciones y operaciones.
A.11 Control de accesos.
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información.
A.13 Gestión de incidentes en la seguridad de la información.
A.14 Gestión de la continuidad de negocio.
A.15 Cumplimiento (legales, de estándares, técnicas y auditorías).

Figura 2.3 Controles de la norma ISO 27001



Fuente: (ISO 27001 Security)

Política de seguridad: Es donde se estipulan las políticas con respecto a la seguridad de la información. (Seguridad de la Información)

Organización de la seguridad: Gestiona la seguridad de la información dentro de la empresa. (Roles, compromisos, autorizaciones, acuerdos, manejo con terceros). (Seguridad de la Información)

Gestión de activos: Se relaciona con el mantenimiento y protección apropiados de todos los activos de información. (Seguridad de la Información)

Seguridad del recurso humano: Busca asegurar que empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles a desempeñar minimizando los riesgos relacionados con personal. (Seguridad de la Información)

Seguridad física y del entorno: Busca prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones de la empresa y a su información. (Seguridad de la Información)

Gestión de comunicaciones y operaciones: Se busca asegurar la correcta y segura operación de las áreas de procesamiento de información (actividades operativas y concernientes a la plataforma tecnológica). (Seguridad de la Información)

Control de acceso: Se realiza el control físico o lógico de los accesos a los activos de la información. (Seguridad de la Información)

Adquisición, desarrollo y mantenimiento de sistemas de información: Asegurar la inclusión de todos los controles de seguridad en los sistemas de información (infraestructura, aplicaciones, servicios, etc.). (Seguridad de la Información)

Gestión de incidentes de seguridad: Permitir que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicados

de tal manera que se tome una acción correctiva adecuada y en el momento indicado. (Seguridad de la Información)

Gestión de la continuidad del negocio: Enfocado en reaccionar en contra de interrupciones a las actividades del negocio y en proteger los procesos críticos contra fallas mayores en los sistemas de información o desastres, y por otro lado, asegurar que se recuperen a tiempo. (Seguridad de la Información)

Cumplimiento: Busca prevenir el incumplimiento total o parcial de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad. (Seguridad de la Información)

2.3 Metodología de evaluación de riesgos

En este proyecto se aplicará el método de investigación de riesgos denominado Magerit, la cual recomendará las medidas apropiadas para controlar los activos. (Amutio Gómez, 2012)

La metodología Magerit evalúa y determina si los activos de la organización están expuestos a vulnerabilidades ya que muestra el grado de protección que tienen, permitiendo establecer controles para mejorar y disminuir factores maliciosos y que puedan presentarse como un riesgo.

Magerit identifica el riesgo luego determina la vulnerabilidad a la que está expuesto el activo y recomienda el control para reducir el daño.

Está compuesta de cuatro etapas, que aclara la forma de trabajar en este ámbito, que son:

- La planificación: Se considera como el comienzo del proyecto y es donde se define lo que se va a cumplir.
- En el análisis de riesgos: Se identifican y se cuantifica los activos, obteniendo una estimación deseable que se pueda controlar.
- La gestión de riesgos: Identifica las funciones y servicios de salvaguardas o controles

- Seleccionar las salvaguardas (controles)

2.3.1 Beneficios para la empresa del uso de la metodología

- **Ventajas a nivel interno**

  Mayor seguridad informática al aplicar y conocer los controles que se pueden aplicar para los posibles riesgos a la que se encuentra expuesta la información.

- **Ventajas a nivel externo**

  Derivadas de la imagen positiva que puede ofrecer la empresa a sus clientes habituales o potenciales, de control, eficacia y seguridad de sus datos personales, reforzando el resto de actividades de la empresa frente a sus competidores.

2.4 SGSI

SGSI como sus siglas lo indican se refiere a un Sistema de Gestión de la Seguridad de la Información, una herramienta de mucha utilidad y de importante ayuda para la gestión de las empresas. Es el concepto central sobre el que se construye la norma ISO 27001.

Proteger la información que se encuentra expuesta a las diferentes amenazas, es necesario conocer y afrontar de manera ordenada los riesgos a los que está sometida la información. (Concepto de un SGSI, 2002)

También, adopta el modelo de procesos "Plan-Do-Check-Act" (PDCA) que significa "Planificar-Hacer-Controlar-Actuar" que se aplica para estructurar todos los procesos del SGSI. (DestacaDos SGSI, 2005)

- **Plan *(planificar)*:** Es la fase de diseño del SGSI, donde se realiza la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- **Do *(hacer)*:** En esta fase envuelve la implantación y utilización de los controles.

- **Check *(controlar)*:** Es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- **Act *(actuar)*:** En esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

2.4.1 Política de seguridad

La política de seguridad debe conformar un conjunto de normas y recomendaciones sobre cómo se manejaran los siguientes temas:

- Organización de la seguridad: Establecer un marco gerencial para controlar su implementación.
- Seguridad del personal: Reducir riesgos de error humano
- Seguridad física y ambiental: Impedir accesos no autorizados
- Gestión de las comunicaciones y las operaciones: Garantizar el funcionamiento correcto y seguro de las instalaciones de telecomunicaciones.
- Control de acceso: Controlar el acceso lógico a la información.
- Desarrollo y mantenimiento de los sistemas: Medidas de seguridad en los sistemas de información.
- Administración de la continuidad del negocio: Proteger los procesos críticos
- Cumplimiento: Impedir infracciones y violaciones de las normas internas y externas.

2.4.2 Alcances y responsables

Para cada punto mencionado en los literales anteriores la empresa deberá definir su alcance donde deberán quedar definidas las actividades de la organización, las ubicaciones físicas que van a verse involucradas, la tecnología de la organización y las áreas que quedarán excluidas en la implantación del sistema.

Además deberá crearse un comité directivo que estará formado por los directivos de la empresa y que tendrá las máximas responsabilidades y aprobará las decisiones de alto nivel relativas al sistema.

Y por último, el Comité de Gestión, que controlará y gestionará las acciones de la implantación del sistema colaborando muy estrechamente con el responsable de seguridad de la entidad. Este comité tendrá potestad para asumir decisiones de seguridad y estará formado por personal de los diferentes departamentos involucrados en la implantación del sistema.

2.4.3 Aspectos organizativos de la seguridad de la información

Se deberá crear un Comité de Seguridad de la Información, integrado por representantes de cada área relacionada con la seguridad de la información en los que estén:

- Directivos y administrador de seguridad
- Personal

Sus funciones deberían ser:

- Revisar y proponer a la máxima autoridad del organismo para su aprobación, la política y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.

2.5 OSSIM

Es un acrónimo para Open Source Security Information Management, en español podría traducirse como: Herramienta de Código Abierto para la Gestión de Seguridad de la Información. OSSIM no es tan sólo una herramienta, sino una combinación de herramientas, todas de código libre, que construyen una infraestructura de monitorización de la seguridad.

Obtiene información completa y selecta, de los miles de eventos que reportan otras herramientas, logrando ser muy útil.

A los administradores de red, les permite elegir el procedimiento que regirá la seguridad en el sistema de información, pudiendo así, detectar amenazas rápidamente y disponer de un nivel adecuado de protección para la información y equipos que permiten la comunicación dentro de la red. Al Considerar que en muchas ocasiones se presenta grandes cantidades de alertas, de las cuales no todas son confiables, en los últimos años se han generado importancia para la seguridad de los sistemas de información. (Torres Manrique & Villegas Oliveros , 2010)

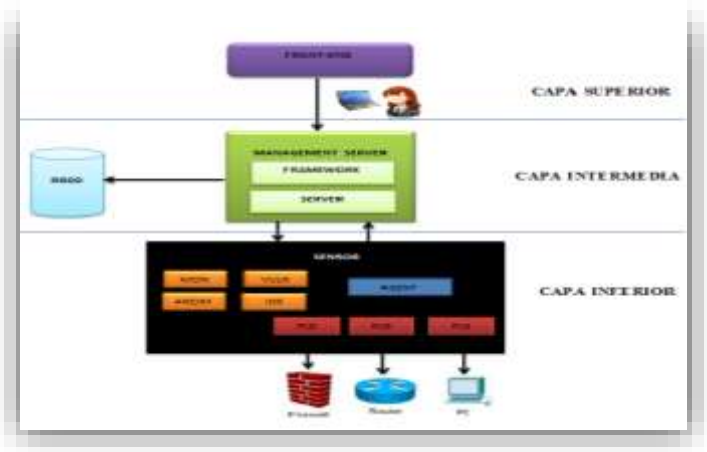
2.5.1 Capas de OSSIM

OSSIM tiene como finalidad aprovechar todas las herramientas con las que trabaja para mejorar la seguridad de la red. Proporciona al administrador una vista detallada y comprensiva de los datos entregados por las diferentes aplicaciones de monitoreo y mostrarlos a través de una interfaz web.

Se divide en tres capas:

- Capa Superior
- Capa Intermedia
- Capa Inferior

Figura 2.4 Capas de OSSIM



Fuente: (García , Cerquera , & Bedoya , 2013)

Capa Inferior.- También denominado "Preprocesado". En esta capa se obtiene toda la información que recogen los detectores, monitores (sensores) y es enviada al sistema central donde se realiza la colección y la correlación de los diferentes eventos que ocurren en la red. (García , Cerquera , & Bedoya , 2013)

Entre los preprocesadores dispersos en la red tenemos:

- IDS (Detectores de patrones).
- Detectores de anomalías.
- Cortafuegos (Firewall).
- Monitores.

Capa Intermedia.- Es el nivel intermedio o nombrado el "Postprocesado". OSSIM desarrolla un proceso de abstracción de los eventos incompresibles que suceden en los sistemas y los convierte en alarmas comprensibles para los administradores de la red, este proceso se lleva a cabo principalmente en el motor de correlación, donde el administrador crea directivas de correlación para unir diferentes eventos de bajo nivel en una única alarma de alto nivel, cuyo objetivo es aumentar la sensibilidad y la fiabilidad de la red. (García , Cerquera , & Bedoya , 2013)

Los principales métodos de OSSIM son los siguientes:

- Normalización
- Correlación
- Priorización
- Valoración de Riesgos

Capa Superior.- Conocido como "Front-end", en este nivel se ubica una herramienta de gestión, capaz de configurar y visualizar tanto los módulos externos como los propios del framework, permitiendo crear la topología de la red, inventariar activos, crear las políticas de seguridad, definir las reglas de correlación y enlazar las diferentes herramientas integradas.

La visualización es mediante la consola web. (García , Cerquera , & Bedoya , 2013)

2.5.2 Administrador del servidor

OSSIM-SERVER.- Es un demonio que se ejecuta en segundo plano y se conecta con la base de datos para recuperar e introducir los datos desde los agentes y el framework. (It Freek Zone , 2010)

El propósito principal es:

- Recoger datos de los agentes y otros servidores
- Priorizar los eventos recibidos
- Correlacionar los eventos recibidos de diferentes fuentes
- Realizar la evaluación de riesgos y genera alarmas
- Almacenar eventos en la base de datos

El servidor OSSIM puede recibir:

- Información de eventos de los agentes, el servidor recibe el estado de los plugins conectados a cada agente.
- Colección de datos de los eventos de agentes y servidores.
- Consultas de datos de otros servidores.
- Pedidos emitidos desde framework o un servidor maestro.

El servidor OSSIM puede enviar datos a otros lugares:

- SQL Database todos los eventos se almacenan como cierta información, como alarmas, números de eventos por sensor o diferentes funciones del servidor.
- Otro servidor un servidor puede enviar datos a otro servidor.
- Framework el servidor envía todas las alarmas de framework para permitir al usuario configurar y utilizar la acción o respuestas.

2.5.3 Proceso de detección

Consiste en el descubrimiento de anomalías, vulnerabilidades mediante el uso de técnicas de recopilación de datos provenientes de los detectores y monitores de la red.

2.5.3.1 La capacidad de detección

Reforzar la seguridad de la red dependerá de los dispositivos que se utilicen y la capacidad de detección que tengan estos para detectar los ataques o amenazas.

La capacidad de un detector se define mediante 2 variables:

- Sensibilidad: Definida como la capacidad de análisis que posee el detector al momento de localizar un posible ataque.
- Fiabilidad: Definida como el grado de certeza que ofrece el detector ante el aviso de un posible evento.

2.5.3.2 La incapacidad de detección

Los detectores en la actualidad tienen 2 principales problemáticas:

- Falsos Positivos: La falta de fiabilidad en los detectores es el causante del mayor problema actual, es decir alertas que realmente no corresponden con ataques reales.
- Falsos Negativos: La incapacidad de detección implicaría que un ataque es pasado por alto.

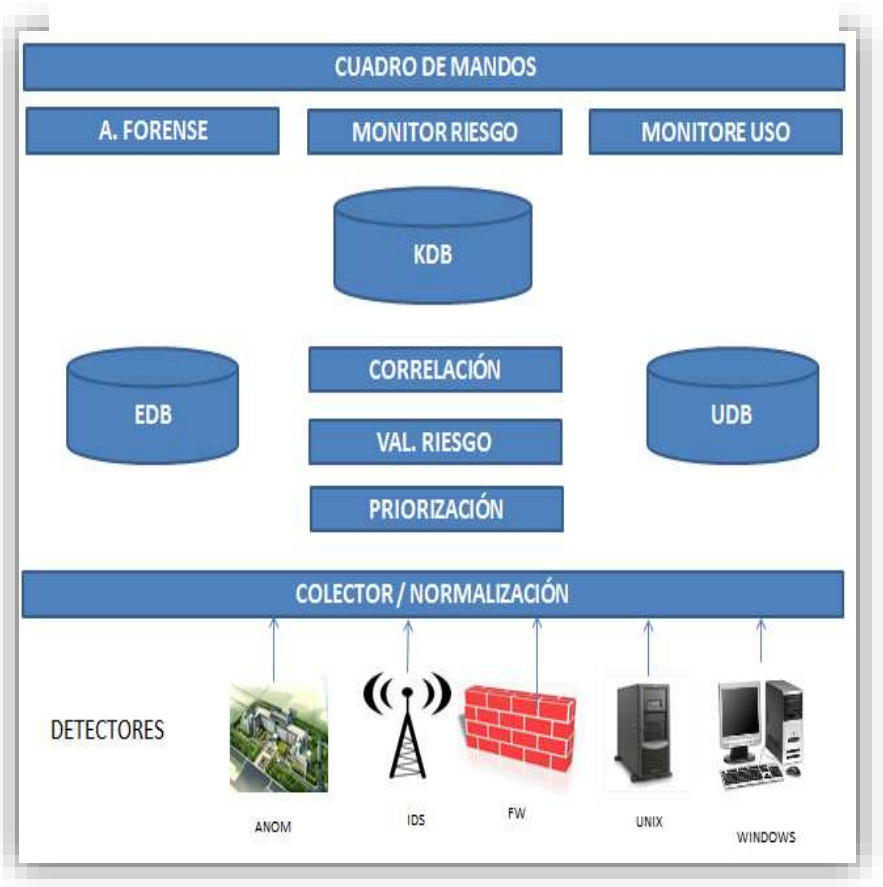
2.5.4 Arquitectura

OSSIM utiliza tres bases de datos heterogéneas para los distintos tipos de datos almacenados:

- EDB Base de datos de eventos, la más voluminosa pues almacena todos los eventos recibidos desde los detectores y monitores.

- KDB Base de datos del framework, en la cual se almacena toda la información referente a la red y la definición de la política de seguridad.
- UDB Base de datos de perfiles, almacena todos los datos aprendidos por el monitor de perfiles.

Figura 2.5 Arquitectura de OSSIM

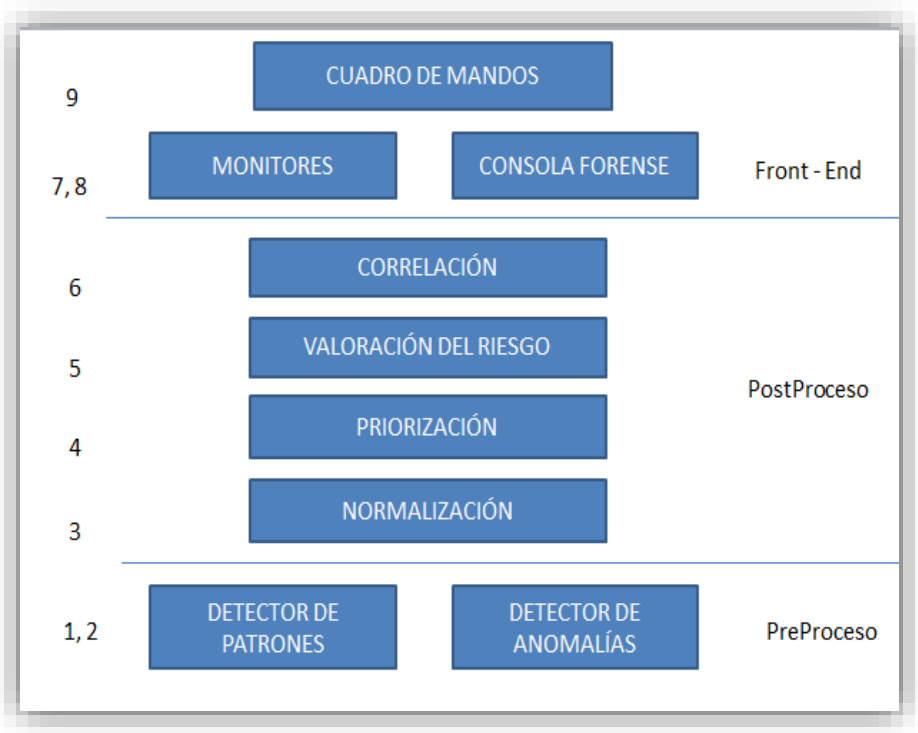


Fuente: http://radio.gnu.org.ve/wiki/Ossim

2.5.5 Funcionalidad

Al conocer que OSSIM consta de tres capas se debe especificar que cada una de ellas se descompone en niveles y en total son 9 niveles.

Figura 2.6 Representación niveles OSSIM



Fuente: http://radio.gnu.org.ve/wiki/Ossim

2.5.5.1 Detector de patrones

Es todo dispositivo o elemento de la red capaz de monitorear y detectar patrones sospechosos basándose en firmas o reglas previamente definidas produciendo eventos de seguridad.

Entre los elementos más comunes se encuentra el IDS (Sistema de Detección de Intrusos) capaz de escuchar y analizar todo el tráfico de la red e identificar posibles ataques.

Existen otros detectores incluidos en dispositivos como los routers o firewalls, tienen la capacidad de detectar patrones en la red como escaneos de puertos o ataques por fragmentación y estos a su vez poseen un log de seguridad que alerta el posible problema.

OSSIM integra varios detectores de patrones de código abierto. El detector más común el Snort (NIDS, Network Intrusión Detection System).

2.5.5.2 Detectores de anomalías.

Para detectar anomalías primero hay que considerar ¿Cómo es el comportamiento normal de un sistema? Este modelo de detección conoce lo que es "normal" en la red o los equipos mediante dos grandes premisas:

- Aprender por sí mismo y alertar cuando un comportamiento difiere del comportamiento normal.
- Especificar al sistema el comportamiento normal mediante un conjunto de reglas.

Entre las funcionalidades detecta:

- Nuevos ataques que aún no están registrados por los detectores de patrones.
- Cuando un gusano es introducido desde la red interna o exista un ataque de spam, que pueden generar conexiones anómalas.
- Uso de servicios con origen y destino anormales.
- El uso de activos en horarios anormales.
- Exceso de tráfico o de conexiones.

OSSIM integra los siguientes detectores de anomalías:

- Aberrant Behaviour plugin para Ntop aprende el uso de parámetros y alerta cuando dichos parámetros se salen de los valores esperados.
- ArpWatch utilizado para detectar cambios de MAC.
- Pof utilizado para detección de cambios de sistema operativo.
- Pads y Nmap utilizado para detectar anomalías en los servicios de red.

2.5.5.3 Sistema de colección y normalización.

El sistema de colección y normalización proporciona unificación de todos los eventos de seguridad provenientes de las herramientas en una sola consola y formato.

La colección de datos se puede hacer de dos formas en el sensor:

- Enviando los datos desde el equipo analizado usando protocolos nativos del equipo al sensor que actúa como concentrador.
- Instalando agentes en el equipo analizado que recopilan la información en el host y la envía inmediatamente al sensor.

La normalización implica la existencia de un intérprete que conozca los tipos de formatos de alertas de los diferentes detectores, capaz de estandarizar el tratamiento y almacenar todos los eventos de seguridad en una única base de datos "EDB". Para luego visualizar en la misma pantalla y con el mismo formato los eventos de seguridad de un momento específico ya sean del Router, firewall, IDS o de cualquier host.

2.5.5.4 Políticas de priorización.

Definir la prioridad para una alarma dependerá de la topología de la red, inventario de cada máquina y del rol que estas desempeñan en la empresa.

Valorar la importancia de una alerta depende del escenario de la red. Este escenario esta descrito en una base de conocimientos sobre la red formada por:

- Inventario de Máquinas y Redes (IP, MAC, Sistema Operativo, Servicios, etc).
- Políticas de Acceso (Conocer que está permitido o prohibido).

KDB es la base de datos que OSSIM utiliza para parametrizar el Framework, en ella se pueden configurar las siguientes características:

- Política de seguridad
- Inventario de las máquinas de la red.
- Valoración de activos.
- Valoración de amenazas.
- Valoración de fiabilidad de cada alerta.
- Definición de alarmas.

2.5.5.5 Motor de correlación

El motor de correlación en OSSIM comprueba cada uno de los eventos recibidos y busca evidencias que prueben si es un ataque o un falso positivo.

También tiene la capacidad de:

- Desarrollar patrones específicos para detectar lo conocido y detectable.
- Desarrollar patrones ambiguos para detectar lo desconocido y no detectable.
- Poseer una máquina de inferencia configurable a través de reglas relacionadas entre sí capaz de describir patrones más complejos.
- Permitir enlazar detectores y monitores de forma recursiva.

El motor de correlación de OSSIM se alimenta de dos elementos claves en la red de datos, como son:

- Los monitores proporcionan indicadores del estado.
- Los detectores proporcionan alertas.

Existen 3 maneras diferentes de correlación:

- **Correlación Cruzada.-** Permite priorizar o dar de baja a eventos mediante la información que proviene de los detectores. La correlación cruzada se realiza con eventos que tienen dirección IP de destino para comprobar si el destino del evento

tiene alguna vulnerabilidad definida en la base de datos. También permite modificar la confiabilidad de un evento.

- **Correlación de Inventario.-** El objetivo es reducir el número de falsos positivos, comprueba si el ataque tuvo como ingresar a través del sistema operativo o algún servicio.

- **Correlación Lógica.-** Genera alarmas sin conocer el tipo de ataque específico, reduce falsos positivos ya que visualiza datos específicos de los eventos tratados.

2.5.5.6 Monitores

OSSIM realiza una monitorización de la red ayudando al administrador de seguridad a reconocer si un evento está presentando alguna actividad anómala de la normal.

Tipos de monitorización:

- **Monitor de Uso.-** Ofrece datos generales de la máquina, como el número de bytes que transmite al día.

- **Monitor de Perfiles.-** Ofrece datos específicos del uso realizado por el usuario y permite establecer un perfil, (uso de correo, pop y http, perfil de usuario normal), estos datos se obtienen de la base de datos de perfiles "UDB".

- **Monitor de Sesión.-** Permite ver en tiempo real las sesiones que está realizando el usuario.

- **Monitor de Caminos.-** Entrega una representación en tiempo real de los caminos trazados en la red entre las diferentes máquinas que interactúan entre ellas en un intervalo de tiempo. Obtiene sus datos del monitor de sesión y el monitor de riesgos.

- **Monitor de Disponibilidad.-** La información de disponibilidad es importante para detectar ataques de denegación de servicios.

- **Monitorización Personalizada.-** Existe un plugin que permite crear monitores personalizados, que extraen cualquier parámetro que se quiera recopilar, filtrar y enviar al motor de correlación para ser procesado.

2.5.5.7 Consola forense

La consola forense permite la consulta de toda la información almacenada en un frontal web.

Esta consola es un buscador de la base de datos de eventos "EDB" y permite al administrador analizar de una forma centralizada los eventos de seguridad de todos los elementos críticos de la red. Profundiza cada detalle de los eventos ocurridos en el sistema.

2.5.5.8 Cuadro de mandos

El cuadro de mandos monitorizará una serie de indicadores definidos que medirán el estado de seguridad de la organización, definiendo umbrales que debe cumplir la organización. A través de estos cuadros se enlazan cada una de las herramientas de monitorización para profundizar sobre cualquier problema localizado.

Como ejemplo se podrían visualizar los siguientes datos:

- Monitorización permanente de los niveles de riesgo de las principales redes de la organización.
- Monitorización de las máquinas o subredes que superen el umbral de seguridad.
- Monitorización de perfiles que superen los umbrales por:

    - Uso de tráfico.
    - Uso de servicios críticos.
    - Cambios en configuración.

- Uso de servicios anómalos.

- Monitorización de aquellos parámetros de la red o niveles de servicio que superen el umbral establecido:

  - Número de correos, virus, accesos externos.
  - Latencia de servicios, uso de tráfico por servicios.

2.6 Herramientas de OSSIM

OSSIM construye una infraestructura de monitorización de seguridad integrando productos Open Sources.

Tabla 2.1 Herramientas IDS integradas en OSSIM

Sistema de Detección de Intrusos	
SNORT	Sistema de detección de intrusos en una Red (NIDS)
OSSEC	Sistema de detección de intrusos basado en los logs (LIDS).
OSIRIS	Sistema de detección de intrusos a nivel de Host (HIDS).

Elaborado por: Los autores

Entre los Sistemas de Detección de Intrusos tenemos:

2.6.1 SNORT

Detector de intrusos basado en red (NIDS) o analizador de paquetes. Implementa un motor de detecciones de ataques y barrido de puertos que permite detectar y alertar las anomalías. Analiza el tráfico de red, inspeccionando el contenido de los paquetes con las reglas previamente establecidas para emitir alertas, o incluso, realizar algún tipo de acción cuando detecta tráfico sospechoso. Snort implementa un lenguaje de creación de reglas, flexible, potente y sencilla. (Alfon, 2003)

2.6.2 OSSEC

Conocido también como el sistema de detección de intrusos basado en host (HIDS). Analiza logs de las máquinas monitorizadas para conocer si existe algún tipo de ataque. Reconoce y traduce gran cantidad de tipos de logs y tiene un motor de reglas con capacidad de correlación. Los IDS basados en análisis de logs son llamados LIDS porque detectan errores o ataques usando logs como su fuente de información.

OSSEC, está formado por un administrador central de monitoreo, que recibe información desde agentes, syslog y bases de datos. (Info Seguridad , 2010)

2.6.3 OSIRIS

Es un sistema de detección de intrusos basado en host (HIDS). Supervisa cambios en la red de hosts en un tiempo determinado e informa al administrador. Osiris captura imágenes periódicas del filesystem y los almacena en una base de datos.

Estas bases de datos, así como las configuraciones y los logs, son almacenados en un host de administración central. También monitorea listas de usuarios, listas de grupos, y módulos del kernel o extensiones. (Info Seguridad , 2010)

Tabla 2.2 Detectores integrados en OSSIM

Detectores	
PADS	Detección de anomalías en servicios.
SPADE	Detección de anomalías en paquetes.
ARPWATCH	Detección de anomalías en direcciones MAC.
P0f	Detección del sistema operativo y la versión de las máquinas conectadas en la red.

Elaborado por: Los autores

2.6.4 PADS

Es un motor de detección basada en firmas para localizar pasivamente activos de la red. Su funcionamiento es sencillo, monitoriza la red y a través de firmas va detectando servicios y hosts que se ejecutan, e identifica lo que detecta. De esta forma se puede hacer una descripción de la red sin generar tráfico. (Info Seguridad , 2010)

2.6.5 SPADE

Es un preprocesador se basa en un motor de estadísticas de paquetes para detección de anomalías. Revisa los paquetes recibidos por Snort y es usado para conocer ataques sin firma. (Info Seguridad , 2010)

2.6.6 ARPWATCH

Detección de anomalías en direcciones MAC. Arpwatch mantiene archivos con IP y su respectiva MAC que están asociadas a la red, genera notificaciones cuando existen cambios entre IP-MAC. (Info Seguridad , 2010)

2.6.7 P0f

P0f es una herramienta de identificación pasiva de sistema operativo, permite detectar el sistema y la versión de las máquinas conectadas a la red. No genera tráfico y es posible identificar el sistema de equipos que estén detrás de un cortafuego que el escáner habitual no podría llegar. (Info Seguridad , 2010)

Tabla 2.3 Monitores integrados en OSSIM

Monitores	
NTOP	Monitorización del tráfico de red.
TCPTRACK	Sniffer utilizado para conocer información de las sesiones.
NAGIOS	Monitorización de la disponibilidad de host y servicios.

Elaborado por: Los autores

2.6.8 NTOP

Permite controlar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red. (Info Seguridad , 2010)

Características de Ntop:

- Su interfaz es web y muy intuitivo.
- Dispone de gran variedad de informes: informes globales de carga de red, de tráfico entre elementos, de sesiones activas de cada elemento, etc.
- Detecta posibles paquetes dañinos.
- Es capaz de analizar datos proporcionados por dispositivos de red que soporten NetFlow y sFlow.

2.6.9 TCPTRACK

Es un analizador de paquetes muestra información sobre las conexiones TCP de una interfaz de la red. Su función es observar de forma pasiva las conexiones TCP, realizando un seguimiento de su estado y mostrando la lista de conexiones. Muestra las direcciones de origen, destino, puertos, el estado de conexión, el tiempo de inactividad, y el uso de ancho de banda. (Info Seguridad , 2010)

2.6.10 NAGIOS

Sistema de monitorización de redes, vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no es normal. Nagios permite al administrador tener una visión central del estado de los hosts de la red, enviando alertas en caso de fallas.

Los datos provenientes de los plugins son almacenados en una base de datos. No incluye mecanismos de control de estado de hosts y servicios, deja este trabajo a los plugins,

simplemente se limita a ejecutar los plugins, recibir los resultados, procesar los resultados y ejecutar las acciones necesarias. (Info Seguridad , 2010)

Tabla 2.4 Scanners integrados en OSSIM

Scanners	
NESSUS	Escáner de vulnerabilidades en la red.
NMAP	Inventario de sistemas activos.
OPENVAS	Escaneo y análisis de vulnerabilidad en la red

Elaborado por: Los autores

2.6.11 NESSUS

Es un programa de escaneo de vulnerabilidades. Su función es escanear los hosts que el usuario desea, detectando primero los puertos que tienen abiertos y luego enviando un test para comprobar qué hosts son vulnerables. A partir de los resultados obtenidos, Nessus arma un detallado informe con las vulnerabilidades de cada host, describiendo cada vulnerabilidad, el nivel de riesgo que representa y las posibles formas de mitigarla. (Info Seguridad , 2010)

2.6.12 NMAP

Es una herramienta para la exploración de redes. Escanea puertos de las máquinas que se encuentran en la red de la organización y establece si un puerto está abierto, cerrado o protegido por cortafuegos. Así, es capaz de identificar máquinas dentro de una red, determinar qué servicios utiliza dicha máquina, definir cuál es su sistema operativo e incluso devolver cierta información sobre el hardware de la máquina. (Info Seguridad , 2010)

Tiene como función enviar paquetes o realizando una llamada de conexión, luego de esto es capaz de distinguir entre seis estados diferentes para cada puerto:

- Abierto (open): Una aplicación está aceptando conexiones TCP, datagramas UDP o asociaciones SCTP en el puerto.
- Cerrado (closed): El puerto es accesible pero no existe ninguna aplicación escuchando en él.
- Filtrado (filtered): El paquete que se ha enviado ha sido filtrado por un firewall y Nmap no puede determinar si está abierto o no.
- Sin filtrar (unfiltered): El puerto es accesible pero Nmap no es capaz de determinar si está abierto o cerrado.
- Open|filtered – Closed|filtered: Nmap no es capaz de definir si el puerto está abierto/cerrado o filtrado. Esto sucede cuando los puertos abiertos no generan alguna respuesta.

2.6.13 OPENVAS

OpenVas no solo es un software para escanear puertos, en si integra un conjunto de herramientas que permiten gestionar desde un portal web y de manera centralizada las vulnerabilidades detectadas. OSSIM utiliza OpenVas para la evaluación de las vulnerabilidades y el control de acceso e intrusiones. Al analizar los equipos realiza informes sobre las vulnerabilidades detectadas y trabaja con un motor de correlación con el cual compara todo lo que se ha detectado y buscar soluciones asociadas. (Info Seguridad , 2010)

OpenVas funciona con 3 servicios:

- Servicio de escaneo (scanner) encargado de realizar el análisis de las vulnerabilidades
- Servicio cliente (interfaz gráfica web) utilizado por el usuario para configurar y presentar los resultados obtenidos (informes)
- Servicio manager que mediante el OMP (OpenVas Management Protocol) es el encargado de interactuar con servicios scanner, cliente.

Tabla 2.5 Syslogs integrados en OSSIM

Syslogs	
NTSYSLOG	Analizador de logs para Windows
SYSLOG	Analizador de logs en Linux
SNAREWINDOWS	Trabaja como un manejador de logs y reporte de incidentes

Elaborado por: Los autores

Tabla 2.6 Firewall del sistema OSSIM

Firewall	
CISCO PIX	Controla el tráfico entre la red interna y externa.
IPTABLES	Filtra el tráfico, recolecta los eventos de las IPtables.

Elaborado por: Los autores

Tabla 2.7 Servidores Web del sistema OSSIM

Servidores Web	
IIS COLECTOR	Servidor de páginas Web de Microsoft, registra los eventos del servidor, peticiones y errores.
APACHE COLECTOR	Servidor HTTP de código abierto, registra la actividad, rendimiento y los problemas que puedan ocurrir en el servidor HTTP.

Elaborado por: Los autores

2.7 MARCO CONCEPTUAL

Acceso.- Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal. (Instituto Nacional de Estadística e Informática, 1997)

Agente.- Es un programa de computación que actúa para un usuario u otro programa en una relación de entidad, la cual deriva del Latin *agere* (hacer): un acuerdo para actuar en nombre propio. Tal "acción en nombre de" implica la autoridad para decidir cuál acción, si existe, es adecuada. (Agente Software, 2013)

Amenaza.- Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados. (Instituto Nacional de Estadística e Informática, 1997)

Ataque.- Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora. (Instituto Nacional de Estadística e Informática, 1997)

AlienVault SIEM.- Se basa en la tecnología SIEM ofrece las mismas funciones pero AlienVault es capaz de monitorear los millones de datos que son enviados por los diferentes sensores. (Barraco , 2014)

AlienVault Sensor.- Recoge los logs de los diferentes dispositivos electrónicos y aplicaciones de seguridad, que son normalizados y enviados al management server para su correlación. Reúne una serie de productos integrados para la detección y monitorización de alarmas y amenazas en tiempo real que dan visibilidad de toda la infraestructura del cliente. (Barraco , 2014)

Incorpora entre otras herramientas de:

- Inventariado automático y gestión de activos
- Escaneo de vulnerabilidades
- Operación como IDS, Wireless IDS y Host IDS
- Descubrimiento de tráfico anómalo
- Monitorización de red y disponibilidad

AlienVault Logger.- Recoge y almacena archivos (logs) en una base de datos de forma masiva en su estado original añadiendo las medidas de seguridad oportunas para asegurar la integridad de los eventos tratados. (Barraco , 2014)

Base de Datos.- Es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan. También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos. (Data Base Management System - DBMS).

Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación. (Instituto Nacional de Estadística e Informática, 1997)

Consola.- Es una terminal de línea de comandos o ventana en donde interactúa el usuario y el sistema operativo. Permite ingresar comandos y ejecutar programas. (WordPress.com., 2009)

Datos.- Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc. (Instituto Nacional de Estadística e Informática, 1997)

Demonio.- Los daemons (o demonios) no son más que un proceso que se ejecuta en segundo plano. Estos demonios ejecutan diferentes funciones y proporcionan ciertos servicios, pero

sin la interacción del usuario; son procesos de los que no "notamos" su ejecución.

Los demonios pueden ser iniciados al arrancar el sistema, al entrar en un runlevel (nivel de ejecución) determinado, o simplemente cuando nosotros los iniciemos. Veremos entonces de qué modo podemos controlar nosotros mismos los demonios (iniciarlos, pararlos, etc.) y cómo podemos hacer que se inicien automáticamente. (Nacx, 2014)

Dimensión.- Es una faceta o aspecto de un activo, independiente de otras. Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado con respecto a dicho aspecto.

DNS.- Sistema de nombres de dominio adopta una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominios en internet. Se encarga de traducir y resolver nombres de dominio de computadoras conectadas a internet con una IP. (del Barrio)

DHCP.- Protocolo de configuración de host dinámico, es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración en forma dinámica. Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP y una máscara de subred de manera independiente. (Primo Guijarro, 2011)

FTP.- Protocolo de transferencia de archivos, método muy común para transferir uno o más ficheros de una maquina a otra a través del internet. (Wikipedia, 2014)

HTTP.- Protocolo de transferencia de hipertexto basado en el modelo cliente-servidor, en donde un cliente HTTP (navegador) abre una conexión y realizar una solicitud al servidor.

Este responde a la petición con un recurso (texto, gráficos, etc.) o un mensaje de error, y finalmente se cierra la conexión. (Urrutia Fuentealba , 2013)

ICMP.- El Protocolo de mensajes de control y error de internet, controla si un paquete no puede alcanzar su destino, si su TTL ha expirado, si el encabezamiento lleva un valor no

permitido, si es un paquete de eco o respuesta, etc. Emite un mensaje de error o control a la fuente que emitió los datos para que corrija el problema, solo informa no toma decisiones. (Kioskea ES)

IGMP.- Protocolo de administración de grupos de Internet, es un método los routers utilizan para comunicarse unos con otros al enviar y recibir datos a través de Internet. Cuando se conecta a Internet con un router, el router busca e identifica otros routers cerca de la zona en función de sus direcciones IP. Esto hace que sea más fácil para enviar y recibir datos a través de Internet, ya IGMP ayuda a encontrar el camino más corto posible entre su red de routers. (IGMP Protocolos)

Incidente.- Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido. (Instituto Nacional de Estadística e Informática, 1997)

Integridad.- Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos. (Instituto Nacional de Estadística e Informática, 1997)

Interfaz gráfica.- Es un software donde se comunica el usuario y la computadora de forma visual por medio de iconos, botones, menús etc. (Wikipedia , 2014)

Log.- Es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le va añadiendo líneas a medida que se realizan acciones sobre el sistema. Los sistemas operativos también suelen trabajar con logs, por ejemplo para guardar incidencias, errores, accesos de usuarios, etc. A través de los log se puede encontrar información para detectar posibles problemas en caso de que no funcione algún sistema como debiera o se haya producido una incidencia de seguridad. (Los logs, 2011)

Plugin.- El plug-in es un complemento que añade un servicio específico al principal. (Edukavital)

Privacidad.- Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros. (Instituto Nacional de Estadística e Informática, 1997)

Proxy.- Los servidores Proxy permiten dar seguridad y mejorar el acceso a páginas web, conservándolas en la caché. Así, cuando un usuario envía una petición para acceder a una página web que está almacenada en la caché, la respuesta y el tiempo de visualización es más rápido. Aumentan la seguridad ya que pueden filtrar cierto contenido web y programas maliciosos. (Valbuena, 2013)

Seguridad.- Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados. En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos. El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos. (Instituto Nacional de Estadística e Informática, 1997)

SIEM.- Seguridad de información y gestión de eventos, son un grupo de herramientas que trabajan en conjunto dentro de la red. Tienen como función recoger, analizar y priorizar en tiempo real los eventos que son generados por el software y hardware de la red. Entre los beneficios tenemos generar informes, alertas, reglas de correlación. (Benjumea Gómez, 2009)

Sistema de detección de intrusos.- En una empresa siempre es necesario tener un software que te permita examinar la red en la que se está trabajando para prevenir y actuar frente a los ataques o abusos al sistema. La detección de intrusos tiene como objetivo mantener la integridad, confidencialidad o disponibilidad de la información. Tiene un funcionamiento

sencillo ya que al monitorear la red y al detectar un comportamiento sospechoso o acceso no autorizado envía dicho evento para ser analizado basándose en políticas previamente configuradas, actúa y envía una alarma indicando lo que está sucediendo. (Ramírez Martínez, 2004)

Sistema operativo.- Para que el usuario se pueda comunicar con la computadora existe un intermediario y ese es el sistema operativo. En un sistema de computación podemos situar al sistema operativo por debajo del programa de aplicación, controlado y coordinando el soporte físico, para realizar acciones que establece el usuario a través de su programa. (Martinez Cobo, Cabello Requema, & Díaz Martín, 1997)

TCP.- Protocolo de control de transmisión, permite la conexión entre varias máquinas (cliente-servidor) accediendo a una comunicación segura, la transferencia de datos es en ambas direcciones. Envía los datos sin errores y en el mismo orden que se transmitieron. (Kioskea ES, 2014)

UDP.- Protocolo de datagrama de usuario, este protocolo es muy simple ya que no proporciona detección de errores no es un protocolo orientado a conexión, es decir cuando una maquina A envía paquetes de datos a una maquina B, el flujo es unidireccional. La transferencia de datos es realizada sin haber realizado previamente una conexión con la máquina B, y el destinatario recibirá los datos sin enviar una confirmación a la maquina A.

No existe confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros. (El protocolo UDP, 2009)

Usuario.- Persona que tiene permisos para acceder a la documentación e información y recursos. (Instituto Nacional de Estadística e Informática, 1997)

2.8 Formulación de la hipótesis y variables

2.8.1 Hipótesis general

Se conseguirá mantener y mejorar las medidas de seguridad y protección de los activos más relevantes para la empresa basado en un Sistema de gestión de seguridad de la información (SGSI) ISO 27001

2.8.2 Hipótesis específica

- Reducir los riesgos de pérdida y corrupción de la información.
- Se buscara mantener un conjunto estructurado documentado y definir tratamiento de los riesgos encontrados.
- Reducir los niveles de riesgo detectados a un nivel aceptable.
- Mejorar el nivel de seguridad de la red y facilitar la presentación de los informes.

2.8.3 Variables e indicadores

2.8.3.1 Variables independientes

Sistema de gestión de seguridad de información

2.8.3.2 Variables dependientes

Herramientas de gestión

2.8.3.3 Indicadores

Amenazas

- Criminalidad (Robo/ hurto, virus, sabotaje).

- Sucesos de origen físico (Incendio, inundación, sismo, polvo, sobrecarga eléctrica).
- Negligencia y decisiones institucionales (Tráfico sobrecargado, falta de actualizaciones, falta de reglas, falta de capacitación, mal manejo de contraseñas).

Vulnerabilidades

- Por deficiencias en la seguridad por parte de los recursos humanos, puede suscitarse por falta de capacitación en el personal en lo relacionado a seguridad carencia de concientización, tener personal no capacitado.
- Por deficientes controles de acceso, puede originarse por deficiente configuración de contraseñas, falta de monitoreo de acceso concedidos a usuarios.
- Por deficiente seguridad física y ambiental, suele suceder cuando se tiene centros de cómputos sin restricciones de acceso a terceros, que además se encuentren ubicadas en áreas propensas a inundaciones, carencia de aire acondicionado y falta de mantenimiento a los equipos.
- Por mala gestión de operaciones y comunicación, acontece cuando se tiene mecanismos inseguros de envío y recepción de mensajes, falta de protección en las redes, fallos en la obtención de respaldos de información.
- Por mala gestión en el mantenimiento, adquisición y desarrollo en los sistemas de información ocurren por la falta de adecuada gestión de cambios en aplicaciones y bases de datos, deficiencia en revisiones de código.

Al detectar las vulnerabilidades se debe evaluar la posibilidad de que esta no se convierta en amenaza y poder establecer los controles que se deben asignar para que este incidente no se convierta en un daño potencial.

2.9 Matriz causa y efecto

Tabla 2.8 Matriz causa y efecto

Problema General	Objetivo General	Hipótesis General
¿Cómo puede la organización contar con un excelente nivel de seguridad de la información, detectando a su vez actividades o procesos que realicen individuos o sistemas no autorizados sobre elementos de la red?	Minimizar los riesgos de seguridad de la información mediante el análisis previo a la implementación de la Norma ISO 27001 combinando las herramientas de seguridad que ofrece OSSIM logrando así el fortalecimiento de un sistema de gestión de control eficiente para el área de Tecnologías de información.	Se conseguirá mantener y mejorar las medidas de seguridad y protección de los activos más relevantes para la empresa basado en un Sistema de gestión de seguridad de la información (SGSI) ISO 27001
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Específicas**
¿Cómo puede mejorarse la seguridad de la información en la empresa?	Proponer políticas y objetivos para la seguridad de la información.	Reducir los riesgos de pérdida y corrupción de la información.
¿Cómo saber que procesos son los que requieren mayor nivel de prioridad?	Identificar los activos más críticos de los diferentes procesos de la empresa.	Se buscara mantener un conjunto estructurado documentado y definir tratamiento de los riesgos encontrados.
¿Cómo evitar el acceso no autorizado a la información de los sistemas y servicios?	Aplicar controles adecuados previniendo riesgos encontrados.	Reducir los niveles de riesgo detectados a un nivel aceptable.
¿Cómo gestionar de manera segura las comunicaciones y operaciones informáticas?	Permitir la visualización de análisis de eventos de vulnerabilidad que pudieran presentarse dentro de la infraestructura de la empresa mediante la consola de aplicación OSSIM.	Mejorar el nivel de seguridad de la red y facilitar la presentación de los informes.

Elaborado por: Los autores

CAPÍTULO 3

3. MARCO METODOLÓGICO

En primera instancia se realiza un levantamiento de información de los activos más críticos de la empresa a nivel de procesos. La empresa ya tiene identificado sus procesos críticos, por lo que se realizan entrevistas con el personal encargado para cada proceso y se valoriza sus activos conforme a su nivel de criticidad. Esta información recolectada es muy valiosa para la realización de las matrices de evaluación y riesgos. Dentro de la matriz de evaluación y riesgos (detallada en el Anexo A) se realiza el cálculo de riesgos. Para cada riesgo encontrado en un rango alto o medio se procede a la asignación de controles sugeridos por la norma ISO 27001 para así poder minimizar el riesgo. Se plantea a la empresa el Sistema de Gestión de Seguridad de la Información (SGSI) detallando para que pueda ser aplicado por la empresa industrial donde se realiza el proyecto .Además se deja plan de contingencia para el área de Tecnología de la Información (TI). El Alcance para este plan de contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y sistemas de información. Corresponde aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de todo tipo. También se muestra la instalación y configuración de OSSIM (Anexo B).

3.1 Tipos de estudio

- **Estudio exploratorio**

  Su propósito es encontrar lo suficiente acerca de un problema para formular hipótesis útiles. Este tipo de estudio se realiza ante la falta de información o de organización del problema que se quiere investigar.

  La idea principal de este estudio es obtener un conocimiento más amplio respecto al problema planteado.

Un estudio cualitativo es un muy buen ejemplo de estudio exploratorio, ya que se puede obtener un análisis preliminar de la situación. Entre los métodos más usados tenemos: observación y la entrevista. (Namakforoosh, 2005)

Se utiliza este método para obtener toda la información que permita aumentar el conocimiento y conocer cuáles son los problemas y tipos de riesgo, incidentes, amenazas etc. que ocurren en la empresa.

- **Estudio cualitativo**

Se dedican a los aspectos objetivos y reservados de la cuantificación de los datos recolectados. Esta investigación denota en sus estudios procesos de tipo generativo, constructivo y subjetivo.

El estudio cualitativo comienza con la recolección de datos mediante la observación empírica o mediciones de cualquier clase. Su finalidad es encontrar una teoría con la que se pueda probar, con razones convincentes, la efectividad de los datos. (Landeau, 2007)

Al utilizar este tipo de estudio podremos conocer como las personas que laboran en el departamento actúan al encontrar algún tipo de riesgo o incidencia en la información. Saber qué es lo primero que hacen, conocer si las herramientas que usan son las adecuadas para la prevención de dicho riesgo.

- **Estudio analítico**

En este tipo de estudio se desea encontrar los factores que contribuyen al problema, la razón del mismo y como sucedió esta situación para evitarla en el futuro. (Ruiz Limón , 2006)

Una vez identificados los eventos que ocurren para el daño de la información se podrá mejorar el plan de contingencia que mantiene la empresa o establecer otro.

3.2 Métodos de investigación

El método que utilizaremos será el inductivo ya que partimos de la observación y luego realizaremos una serie de investigaciones para llegar a una conclusión generalizada. Es decir método inductivo establece como son los fenómenos, sus causas y efectos de forma concreta.

- **El método inductivo**

  Todas las cosas y sus cambios, todos los hechos y sus consecuencias, todo aquello que afecta a nuestros sentidos son fenómenos.

  El modo de proceder de nuestro conocimiento del mundo exterior, que nos lleva de la observación de los fenómenos particulares a la formulación de una regla, de una ley, de una teoría, recibe el nombre de método inductivo y puede esquematizarse de la manera siguiente:

  A través de los sentidos:

  - Mundo exterior Ü memoria Ü razón
  - Fenómeno Ü información Ü ley, regla

La ley es una tentativa del hombre de explicar el mundo y lo que en él sucede físicamente. En unos casos, la ley expresa cómo sucede un fenómeno. En otros, es un intento de explicar el porqué de un fenómeno, sus causas naturales.

Un conjunto orgánico y unitario de leyes, reglas, proposiciones o conceptos que procuran hallar explicación a una serie de fenómenos naturales recibe el nombre de teoría.

Las leyes y las teorías no son veraces en sentido absoluto, sino en relación con los conocimientos de cada época. Se hallan, por ello, ligadas al ambiente y a la época histórica en la que vieron la luz, al científico que las formuló y a sus esquemas mentales. Más tarde serán modificadas y perfeccionadas en virtud del progreso del conocimiento científico. (Moreno, 2010)

3.3 Fuentes y técnicas

3.3.1 Fuentes

- **Fuentes Primarias.-** Se obtiene información por contacto directo con el sujeto de estudio; por medio de observación, cuestionarios, entrevista, etc. Es aquella que el investigador recoge directamente a través de un contacto inmediato con su objeto de análisis. (Gutierrez Cervantes)

- **Fuentes Secundarios.-** Es aquella que el investigador recoge a partir de investigaciones ya hechas por otros investigadores con propósitos diferentes.

  La información secundaria existe antes de que el investigador plantee su hipótesis, y por lo general, nunca se entra en contacto directo con el objeto de estudio.

  Información obtenida desde documentos; libros, expedientes, estadísticas, datos, censo, base de datos. (Gutierrez Cervantes)

3.3.2 Técnicas

- **La entrevista.-** Recoge los datos que se necesitan para la investigación, una conversación orientada con una o varias personas. Dicho diálogo cuenta con un propósito profesional y, por tanto se desarrolla en relación con cierto asunto o cuestión específica. (Zapata, 2005)

Se utiliza esta técnica para conocer cuál es el rol del personal que labora en la empresa cuales son los activos y herramientas que utilizan.

- **La encuesta.-** Puede definirse como un conjunto de técnicas destinadas a reunir, de manera sistemática, datos sobre determinado tema, a través de contactos directos o indirectos con los individuos que integran la población estudiada. (Zapata, 2005)

  Se realizara encuestas para recabar toda la información que sea posible del departamento a realizar el análisis. Conocer las opiniones, actitudes que tomen los encuestados.

- **La observación.-** Es un procedimiento que utiliza el investigador para presenciar directamente el fenómeno que estudia, sin actuar sobre el esto es, sin modificar o realizar cualquier tipo de operación que permita manipularlo. (Zapata, 2005)

  Con la observación de cómo trabajan las personas del departamento vamos a poder obtener el mayor número de datos para su posterior análisis. Vamos a poder medir las variables de una manera uniforme.

3.3.2.1 Cuestionario de preguntas

La siguiente encuesta fue realizada al jefe o personal encargado de los diferentes procesos críticos de la empresa industrial.

En el capítulo 4 se detalla los nombres de los procesos críticos, los nombres de los diferentes tipos de amenazas y vulnerabilidades sobre las cuales fueron evaluados los activos.

Las respuestas de cada proceso se encuentran en el anexo A presente proyecto.

1.- ¿Culés son los activos más importantes (críticos) para el proceso (nombre del proceso) que necesita respaldarse?

2.- Para este activo crítico que Ud. considera, ¿Cuál sería su valor de disponibilidad?, Considerando lo siguiente:

1 como "bajo"
2 como "medio"
3 como "alto"

3.- Para este activo crítico que Ud. considera, ¿Cuál sería su valor de integridad?, Considerando lo siguiente:

1 como "No Necesaria"
2 como "Necesaria"
3 como Alto "Importante"

4.- Para este activo critico que Ud. considera, ¿Cuál sería su valor de confidencialidad?, Considerando lo siguiente:

1 como "Pública"
2 como "Uso Interno"
3 como Alto "Secreto o Privado"

5.- Para el tipo de amenaza "X", ¿Cuál sería su probabilidad de ocurrencia sobre este activo? Considerando lo siguiente:

1 como "bajo"
2 como "medio"
3 como "alto"

6.- ¿Qué tan vulnerable se encuentra expuesto el activo, para el tipo de vulnerabilidad "X"

1 como "bajo"
2 como "medio"
3 como "alto"

CAPÍTULO 4

4. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1 Resultados de las entrevistas

Para la identificación de los activos se realizaron entrevistas con cada jefe encargado de los procesos críticos y procesos de apoyo identificados por la empresa. Los mismos fueron clasificados de la siguiente manera:

- **Activos de información:** Bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad.
- **Documentos impresos:** Documentos impresos, contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes del negocio.
- **Activos físicos:** Equipos de comunicación y computación, medios magnéticos, otros equipos técnicos.
- **Personas:** Personal, clientes, suscriptores.
- **Servicios:** Servicios de computación y comunicación, otros servicios técnicos.

Tabla 4.9 Plantilla de identificación de activos

CÓDIGO	ACTIVO	DESCRIPCIÓN	CLASE DE ACTIVO	PROPIETARIO	DEPARTAMENTO
Codificación con que se identificara el activo.	Nombre del activo.	Describir para que esta siendo usado el activo.	La clasificación indicada en la parte superior.	Nombre de la persona responsable del activo.	Nombre del Departamento donde está ubicado el activo.

Elaborado por: Los autores

4.2 Dimensiones de valoración

Son las características o atributos que hacen valioso un activo.

- **Dimensión.-** Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado con respecto a dicho aspecto

- **Disponibilidad.-** La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

- **Integridad.-** Mantenimiento de las características de completitud y corrección de los datos. La integridad afecta directamente al correcto desempeño de las funciones de una organización.

- **Confidencialidad.-** Que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados.

4.3 Criterios de valoración

Para valorar los activos, la siguiente escala de valores nos ofrece los siguientes aspectos:

- Escala común para todas las dimensiones, permitiendo comparar riesgos.
- Escala logarítmica, centrada en diferencias relativas de valor.
- Criterio homogéneo que permita comparar análisis realizados por separado.

Se ha elegido una escala detallada de tres valores, clasificados de la siguiente manera:

Tabla 4.10 Estándares para confidencialidad

Activos de información (Confidencialidad)	CLASE	DESCRIPCIÓN
1	Pública	Puede ser revelado y proporcionado a terceras partes. Si el contenido fuera revelado, hubiera pequeños efectos en las operaciones de la empresa.
2	Uso interno	Puede solo ser revelada y proporcionado en la empresa (no disponible a terceras partes). Si el contenido fuera revelado, no hubiera mucho efecto en las operaciones de la empresa.
3	Secreto	Puede ser solo revelado y proporcionado a partes específicas y departamentos. Si el contenido fuera revelado, hubiera un gran efecto en las operaciones de la empresa.

Elaborado por: Los autores

Tabla 4.11 Estándares para integridad

Activos de información (Integridad)	CLASE	DESCRIPCIÓN
1	No necesaria	Usado solo para consulta. No tiene posibles problemas.
2	Necesaria	Si el contenido fuera falsificado, hubiera problemas, pero estos no afectarían mucho las operaciones de la empresa.
3	Importante	Si la integridad se perdiera, hubiera un efecto fatal en las operaciones de la empresa.

Elaborado por: Los autores

Tabla 4.12 Estándares para disponibilidad

Activos de información (Disponibilidad)	CLASE	DESCRIPCIÓN
1	Bajo	Si la información no llegara a estar disponible, no hubiera efectos en las operaciones de la empresa.

2	Mediano	Si la información no llegara a estar disponible, hubiera algún efecto en las operaciones de la empresa. Sin embargo, métodos alternativos pudieran ser usados para las operaciones, o los procesos podrían ser demorados hasta que la información esté disponible.
3	Alto	Si la información no estuviera disponible cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones de la empresa.

Elaborado por: Los autores

La frecuencia de ocurrencia de las amenazas debe ser evaluada. A partir de la lista de amenazas, las amenazas deben ser revisadas basadas en la experiencia de operaciones y datos estadísticos que han sido ya coleccionados.

Las amenazas son típicamente divididas en tres categorías: “Baja”,”Media”,”Alta”.

Tabla 4.13 Criterios para determinar las categorías de las amenazas

AMENAZAS		
PROBABILIDAD DE OCURRENCIA	**CLASE**	**DESCRIPCIÓN**
1	Bajo	Hay una baja probabilidad. La frecuencia de ocurrencia es una vez al año o menos.
2	Medio	Hay una moderada probabilidad. La frecuencia de ocurrencia es una vez cada medio año o menos.
3	Alto	Hay una alta probabilidad. La frecuencia de ocurrencia es una vez al mes o más.

Elaborado por: Los autores

Tabla 4.14 Criterios para determinar las categorías de las vulnerabilidades

VULNERABILIDADES		
PROBABILIDAD DE OCURRENCIA	**CLASE**	**DESCRIPCIÓN**
1	Bajo	Se tiene controles de seguridad muy débiles o no se tiene ningún control de seguridad, de tal manera que esta vulnerabilidad es susceptible de ser explotada fácilmente.
2	Medio	Hay un moderado control de seguridad.
3	Alto	Si en el activo se tiene los controles de seguridad adecuados, de tal manera que sea muy difícil explotar esta vulnerabilidad.

Elaborado por: Los autores

4.4 Identificación de amenazas y vulnerabilidades

El objetivo es identificar las amenazas a las que se exponen los activos dentro del alcance del SGSI y las vulnerabilidades que pueden ser explotadas por las amenazas. A continuación detallamos las amenazas principales acorde al origen de la misma.

Tabla 4.15 Amenazas de origen natural

1.-Desastres Naturales.-Sucesos que pueden ocurrir sin intervención humana	
Amenaza:	**Activo:**
Fuego	Activos físicos
Daños por agua	Servicios de comunicación, Energía
Desastres naturales	Documentación y registros
Afecta: Disponibilidad del servicio, Integridad, Trazabilidad del servicio, Trazabilidad de los datos	

Elaborado por: Los autores

Tabla 4.16 Amenazas de origen industrial

2.-De origen industrial.- Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	
Amenaza:	**Activo:**
Corte de suministro eléctrico	Activos físicos
Degradación en el hardware	Servicios de comunicación, Energía
Condiciones inadecuadas de temperatura y/o humedad	Documentación y registros
Afecta: Disponibilidad, Confidencialidad, Integridad, Trazabilidad del servicio, Trazabilidad de los datos, Funcionamiento y procesamiento correcto de los datos.	
Elaborado por: Los autores	

Tabla 4.17 Amenazas de origen industrial

3.-Ataques intencionales.- Fallos deliberados causados por las personas.	
Amenaza:	**Activo:**
Instalación no autorizada o cambios de SW	Activos físicos
Manipulación de la configuración	Servicios de comunicación, Energía
Brechas de seguridad no detectadas	Documentación y registros
Suplantación de la identidad del usuario	Software
Uso no previsto	
Abuso de privilegios de acceso	
Acceso no autorizado	
Análisis de tráfico	
Negación de servicio	
Robo	
Ataque destructivo	
Ingeniería social	
No autorización de copia de SW o información	
Virus de computación, Fuerza bruta y ataques de diccionario	

Afecta: Disponibilidad del servicio, Confidencialidad, Integridad, Autenticidad de los usuarios del servicio, Autenticidad del origen de datos, Cumplimiento con regulaciones de seguridad, Trazabilidad del servicio, Trazabilidad de los datos, Plan de contingencia.

Elaborado por: Los autores

4.4.1 Amenazas y vulnerabilidades consideradas para la evaluación de procesos de la empresa

En la siguiente tabla se detallan las vulnerabilidades que se presentan en cada uno de los activos, y las amenazas que pueden explotar dichas amenazas las cuales fueron analizadas en conjunto con la Jefa de Tecnología de la información conocida también el área como TI.

Tabla 4.18 Amenazas y vulnerabilidades - Tipo de activo "Archivos"

ACTIVO	AMENAZA	VULNERABILIDAD
Archivos	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastre natural	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Pérdida de la información	Errores de los empleados/ Almacenamiento no protegido
	Divulgación de información de clientes	Almacenamiento no protegido
	Incumplimiento de leyes en cuanto a la información de clientes o empleados	Falta de conocimiento de los empleados
	Contratos incompletos	Falta de control para el establecimiento de contratos
	Incapacidad de restauración	Falta de planes de continuidad del negocio

	Modificación no autorizada de la información	Insuficiente entrenamiento de empleados

Elaborado por: Los autores

Tabla 4.19 Amenazas y vulnerabilidades - Tipo de activo "Documentos"

ACTIVO	AMENAZA	VULNERABILIDAD
Documentos	Fuego.	Falta de protección contra fuego.
	Daños por agua.	Falta de protección física adecuada.
	Desastre natural.	Condiciones locales donde los recursos son fácilmente afectados por desastres.
	Pérdida de la información.	Errores de los empleados/ Almacenamiento no protegido.
	Divulgación de información de clientes.	Almacenamiento no protegido.
	Incumplimiento de leyes en cuanto a la información de clientes o empleados.	Falta de conocimiento de los empleados.
	Contratos incompletos.	Falta de control para el establecimiento de contratos.
	Incapacidad de restauración.	Falta de planes de continuidad del negocio.
	Modificación no autorizada de la información.	Insuficiente entrenamiento de empleados.

Elaborado por: Los autores

Tabla 4.20 Amenazas y vulnerabilidades - Tipo de activo "Equipos"

ACTIVOS	AMENAZA	VULNERABILIDAD
EQUIPOS	Fuego.	Falta de protección contra fuego.
	Daños por agua.	Condiciones locales en mal estado.
	Desastre natural.	Condiciones locales donde los recursos son fácilmente afectados por desastres.
	Degradación o falla de HW.	Falta de mantenimiento.
	Uso no previsto.	Falta de políticas de control de acceso.
	Corte de suministro eléctrico o falla de aire acondicionado.	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado.
	Instalación no autorizada o cambios de software.	Falta de control de acceso.
	Ataque destructivo.	Áreas físicas en mal estado.
	Robo.	Falta de controles de acceso de personas externas dentro de la organización.

Elaborado por: Los autores

Tabla 4.21 Amenazas y vulnerabilidades - Tipo de activo "Servicios"

ACTIVOS	AMENZAS	VULNERABILIDAD
SERVICIOS	Negación del servicio.	Capacidad insuficiente de los recursos.
	Errores de configuraciones del servicio.	Falta de capacitación del administrador.
	Virus de computación.	Falta de protección actualizada.
	Falta de capacidad de restauración.	Falta de copias de backups continúas.
	Pérdida del servicio.	Actualizaciones incorrectas.
	Alteración no autorizada de la	Falta de control de acceso.

configuración.	
Manipulación en la configuración.	Falta de políticas de seguridad.
Modificación no autorizada.	Falta de procedimientos para cambios.
Negación del servicio.	Capacidad insuficiente de los recursos.

Elaborado por: Los autores

Para el activo "servicios", cabe recalcar que este es evaluado solo con el proceso de TI, puesto que este es el departamento responsable de los servicios críticos que ofrece la empresa y son utilizados por el resto de procesos de la organización.

Para cada proceso crítico evaluado se consultó cuáles eran los servicios más indispensables para su operatividad, y así el área de TI tenga conocimiento de esto, es decir que si algún momento un servicio que ofrece TI no se encontrase disponible, el área de TI sabría a qué proceso estaría afectando en ese momento.

A continuación se presenta el modelo en el cual fueron evaluados el resto de procesos críticos conociendo cuál sería su servicio indispensable. Se presenta un ejemplo:

Tabla 4.22 Servicios indispensables

CÓDIGO	ACTIVO	DESCRIPCIÓN	PROPIETARIO	DEPARTAMENTO RESPONSABLE	PROCESO TESORERÍA
001	Telefonía fija	Telefonía fija: Soporte técnico Telefonía fija (análoga/digital/IP).	Técnico	TI	
003	CCTV	CCTV: Soporte técnico Sistema de	Técnico	TI	

	vigilancia y seguridad electrónica (análoga/digital/IP).

Elaborado por: Los autores

4.5 Exposición del riesgo

Se analizará la probabilidad de que pueda ocurrir cada amenaza y el nivel de vulnerabilidad, teniendo como resultado el nivel de exposición de riesgo de cada activo de la empresa.

Valoración:

Amenaza= probabilidad de ocurrencia de la amenaza, en base a los registros de los últimos 2 años.

Vulnerabilidad = probabilidad de ocurrencia

4.6 Selección de opciones para el tratamiento del riesgo

Cuando los riesgos han sido identificados y evaluados, la organización debería identificar y evaluar la acción más apropiada para tratar los riesgos, lo que se conoce como el Plan de Tratamiento de Riesgos (PTR), que es un documento o conjunto de ellos, de vital importancia para el SGSI. El objetivo fundamental es describir de forma bien clara las actualizaciones que se van a realizar para disminuir los riesgos a niveles aceptables, qué recursos van a asignarse para la realización de cada una de estas actualizaciones, las responsabilidades asociadas y las posibles prioridades en la ejecución de las actualizaciones. (Areitio Bertolín, 2008)

Para el tratamiento del riesgo existen cuatro estrategias:

Reducción del riesgo

Para los riesgos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente identificados por la empresa.

Al identificar los controles a ser establecidos es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como las vulnerabilidades y las amenazas previamente identificadas.

Los controles pueden reducir los riesgos valorados en varias maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionando o recuperándose de ellos.

La elección de cualquiera de estas maneras para controlar los riesgos dependerá de una serie de factores, tales como: requerimientos comerciales de la organización, el ambiente, y las circunstancias en que la empresa requiere operar.

Un aspecto muy importante que se debe tomar en cuenta si la empresa opta por este método para el tratamiento del riesgo, es el económico.

Aceptación del riesgo

Es probable que a la empresa se le presente situaciones donde no se pueden encontrar controles ni tampoco es viable diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.

En el caso en que la empresa no pueda manejar el riesgo debido al costo de la implantación de los controles y las consecuencias son devastadoras, se deben visualizar las opciones de "Transferencia del riesgo" o la de "Evitar el riesgo".

Transferencia del riesgo

La transferencia del riesgo, es una opción para la empresa, cuando es muy difícil, tanto técnica como económicamente para la organización llevar al riesgo a un nivel aceptable. En

estas circunstancias podría ser económicamente factible, transferir el riesgo a una aseguradora.

Hay que tomar en cuenta, que con las empresas aseguradoras existe un riesgo residual. La transferencia del riesgo por lo tanto, debe ser muy bien analizada para así poder identificar con precisión, cuánto del riesgo actual está siendo transferido.

Otra posibilidad es la de utilizar a terceras partes para el manejo de activos o procesos considerados críticos. En la medida en que la empresa tercerizadoras esté preparada para asumir dicha responsabilidad.

Evitar el riesgo

La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

Las maneras habituales para implementar esta opción son:

- Dejar de conducir ciertas actividades.
- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información si no se consigue la protección adecuada.

La decisión por la opción de "evitar el riesgo" debe ser balanceada contra las necesidades financieras y comerciales de la empresa.

4.7 Selección de controles para reducir los riesgos a un nivel aceptable.

La selección de controles debe ser sustentada por los resultados de la evaluación del riesgo.

Las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida y qué forma debe tener.

Cuando se seleccionan controles para la implementación, un número de factores deben ser considerados:

- Uso de controles.
- Transparencia del usuario.
- Ayuda otorgada a los usuarios para desempeñar su función.
- Relativa fuerza de controles.
- Tipos de funciones desempeñadas.

4.8 Implementación del plan de tratamiento de riesgo

El objetivo de este punto es tomar la acción más apropiada de tratamiento para cada uno de los riesgos identificados.

Tabla 4.23 Ejemplo del PTR (Plan de tratamiento de riesgo)

ACTIVO	AMENAZA	VULNERABILIDAD	PTR
EQUIPOS	Fuego.	Falta de protección contra fuego.	Reducir
	Daños por agua.	Condiciones locales en mal estado.	Reducir
	Desastre natural.	Condiciones locales donde los recursos son fácilmente afectados por desastres.	Reducir
	Degradación o falla de HW.	Falta de mantenimiento.	Reducir
	Uso no previsto.	Falta de políticas de control de acceso.	Reducir
	Corte de Suministro eléctrico o falla de aire acondicionado.	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado.	Aceptado

	Instalación no autorizada o cambios de software.	Falta de control de acceso.	Reducir
	Ataque destructivo.	Áreas físicas en mal estado.	Reducir
	Robo.	Falta de controles de acceso de personas externas dentro de la organización.	Reducir

Elaborado por: Los autores

4.9 Valoración de riesgos

La valoración de riesgos es ejecutada una vez que ya se ha creado un inventario de activos de información y determinando las categorías de importancia de los activos de información y el criterio para la evaluación de amenazas y vulnerabilidades.

El valor de un riesgo puede ser calculado usando la siguiente fórmula y los valores para el "valor de los activos de información", "escala de las amenazas" y "nivel de vulnerabilidad".

C: Valor del riesgo por la confidencialidad

I: Valor del riesgo por la integridad

D: Valor del riesgo por la disponibilidad

Valor del riesgo = "Valor del activo" **x** "Amenazas" **x** "Vulnerabilidades"

EJEMPLO:

Elementos de activo de información	Valor de Activos
C: Confidencialidad	3
I: Integridad	2
D: Disponibilidad	1

Amenaza	3
Vulnerabilidad	3

El valor del riesgo para este caso en calculado de la siguiente manera:

Valor del Riesgo por la Confidencialidad: 3*3*3=27
Valor del Riesgo por la Integridad: 2*3*3=18
Valor del Riesgo por la Disponibilidad: 1*3*3=9

En base a la información obtenida se puede realizar este cálculo y determinar el valor de riesgo de cada activo.

Una vez que tenemos la valoración de los riesgos debemos tomar la decisión de aceptar el riesgo o reducirlo. Se llega a un acuerdo con la jefa de TI, en qué consiste que todos los valores de riesgo menores o igual a 3 serán considerados como riesgo aceptado.

A continuación un ejemplo de una parte de la matriz de evaluación y riesgos mostrando como resultado que el riesgo es aceptado. Si observamos el valor total fue 3 en cada riesgo tanto para confidencialidad, integridad y disponibilidad.

Tabla 4.24 Opción de tratamiento del riesgo.

VALOR DEL RIESGO				
CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD		OPCIÓN DEL TRATAMIENTO DEL RIESGO
3	3	3	BAJO	ACEPTADO

Elaborado por: Los autores

4.10 Matrices por procesos

Una vez teniendo en cuenta cómo se procederá a evaluar la matriz de evaluación y riesgos, la empresa clasifica los siguientes procesos como críticos:

- Cobranzas.
- Comercio Exterior.
- Facturación.
- Tesorería.
- Colada Continua
- Ventas.
- Procesamiento Materia Prima.
- Asesoría Jurídica.
- Fundición.
- Laminación en caliente.
- Laminación en frío.
- Mantenimiento Electrónico.
- Captación de Materia Prima.
- Control y Calidad.
- Despacho.
- Talento Humano.
- Tecnología de la información (TI).

4.11 Resumen de riesgos detectados en la empresa y sus controles seleccionados

A continuación se detalla en los siguientes cuadros el resumen de los riesgos encontrados afectando a los diferentes procesos de la empresa, esta información se resume del resultado de las matrices de evaluación y riesgos detalladas en el anexo A.

De cada riesgo se asignan los diferentes controles a seguir, controles escogidos de la norma ISO 27001.

Se detalla en cuadros cual es el objetivo del control según la norma y el control respectivo que debería considerar la empresa para evitar el posible riesgo.

Los cuadros se encuentran clasificados por los diferentes tipos de riesgos que se encontraron en la empresa con criticidad en nivel medio o alto, los riesgos con criticidad en nivel bajo, no se consideró que se tomen acciones con algún tipo de control sobre estas, puesto que el nivel evaluado indicó una baja posibilidad de ocurrencia en el riesgo encontrado.

4.11.1 Procesos críticos resumen de riesgos detectados en la empresa y sus controles seleccionados

4.11.1.1 Procesos críticos

Tabla 4.25 Riesgo: Pérdida de la información

Riesgo: Pérdida de la información	
Activo - Documentos	
Procesos afectados	Criticidad
Cobranzas	Alta
Comercio Exterior	Alta
Acciones - Control	
A.5.1 Políticas de seguridad de la información	Objetivo: Proporcionar dirección gerencial y apoyo a la seguridad
A.5.1.1 Documentar política de seguridad de la información	Control: La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes
A.6.1 Organización interna	Objetivo: Manejar la seguridad de la información dentro de la organización
A.6.1.3 Asignación de responsabilidades de la seguridad de la información	Control: Se deben definir claramente las responsabilidades de la seguridad de la información
A.13.Gestión de incidentes en la seguridad de la información	Objetivo: Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una decisión correctiva oportuna

A.13.1 Reportes de los eventos y debilidades de seguridad de la información	Control: Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.2. Gestión de incidentes y mejoras en la seguridad de la información	Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información
A.13.2.1 Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

Elaborado por: Los autores

Tabla 4.26 Riesgo: Incapacidad de restauración

Riesgo: Incapacidad de restauración	
Activo - Documentos	
Proceso afectado	Criticidad
Facturación	Alta
Acciones - Control	
A.9.1 Áreas seguras	Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información
A.9.1.4 Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial	Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres asegurando su reanudación oportuna.
A.14.1.3 Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información	Control: Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos

Elaborado por: Los autores

Tabla 4.27 Riesgo: Divulgación de información a clientes

Riesgo: Divulgación de información a clientes	
Activos - Documentos	
Procesos afectados	Criticidad
Tesorería	Media
Colada Continua	Alta
Laminación en frío	Alta
Cobranzas	Media
Acciones - Control	
A.9.1 Áreas seguras	Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información
A.9.1.3 Seguridad de oficinas, recintos e instalaciones	Control: Se debe diseñar y aplicar seguridad física en las oficinas, salones y medios
A.11.1 Requerimiento comercial para el control de acceso	Objetivo: Controlar el acceso a la información
A.11.1.1 Política de control de acceso	Control: Se debe establecer, documentar y revisar la política de control de acceso en la base a los requerimientos de seguridad y comerciales
A.15.1 Cumplimiento con requerimientos legales	Objetivo: Evitar violaciones de cualquier ley, obligación, reguladora o contractual y de cualquier requerimiento de seguridad
A. 15.1.3 Protección de los registros organizacionales	Control: Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.

Elaborado por: Los autores

Tabla 4.28 Riesgo: Divulgación de información a clientes

Riesgo: Degradación o falla de hardware	
Activo - Equipos	
Procesos afectados	Nivel de Criticidad
Tesorería	Alta
Facturación	Alta
Comercio Exterior	Alta
Ventas	Alta
TI	Media
Captación de Materia Prima	Alta

Acciones - Control	
A.9.2 Seguridad de los equipos	Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
A.9.2.4 Mantenimiento del equipo	Control: El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad

Elaborado por: Los autores

Tabla 4.29 Riesgo: Corte de suministro eléctrico

Riesgo: Corte de suministro eléctrico	
Activos - Equipos	
Procesos afectados	Nivel de Criticidad
Tesorería	Media
Facturación	Alta
Colada Continua	Media
Procesamiento Materia Prima	Media
Asesoría Jurídica	Media
Fundición	Media
Laminación en frío	Media
Laminación en caliente	Media
Comercio Exterior	Media
Mantenimiento Electrónico	Media
Ventas	Media
Cobranzas	Media
Captación de Materia Prima	Media
Control y Calidad	Media
Despacho	Media
Acciones - Control	
A.9.2 Seguridad de los equipos	Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
A.9.2.4 Mantenimiento del equipo	Control: El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad
A.9.2.2 Servicios públicos	Control: El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos

Elaborado por: Los autores

Tabla 4.30 Riesgo: Uso no previsto

Riesgo: Uso no previsto	
Activos - Equipos	
Procesos afectados	Criticidad
Tesorería	Alta
Facturación	Alta
Talento Humano	Alta
Mantenimiento Electrónico	Alta
Cobranzas	Alta
Control y Calidad	Alta
Despacho	Alta
Acciones - Control	
A.6.1 Organización interna	Objetivo: Manejar la seguridad de la información dentro de la organización
A.6.1.1 Compromiso de la gerencia con la seguridad de la información	Control: La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información
A.8.1 Antes de la contratación laboral	Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios
A.8.1.1 Roles y responsabilidades	Control: Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización
A.8.2.Durante el empleo	Objetivo: Asegurar que todos los empleados, contratistas estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal y reducir de los riesgos de error humano.
A.8.2.3 Proceso disciplinario	Control: Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.

A.11.3 Responsabilidades del usuario	Objetivo: Evitar el acceso de usuarios no autorizados y el compromiso o robo de la información y los medios de procesamiento de la información
A.11.3.1 Uso de las claves secretas	Control: Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.1 Requerimiento comercial para el control de acceso	Objetivo: Controlar el acceso a la información
A.11.1.1 Política de control de acceso	Control: Se debe establecer, documentar y revisar la política de control de acceso en la base a los requerimientos de seguridad y comerciales

Elaborado por: Los autores

Tabla 4.31 Riesgo: Fuego

Riesgo: Fuego	
Activos - Equipos	
Proceso afectado	Criticidad
Proceso de Control y Calidad	Alta
Acciones - Control	
A.9.1 Áreas seguras	Objetivo: Evitar el daño a la empresa y la información de la organización
A.9.1.4 Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
Riesgo :	En el área existen extintores de humo como en toda la empresa, pero el riesgo existe por las pequeñas explosiones que suelen ocurrir anualmente es decir por la actividad a la que se dedica el área

Elaborado por: Los autores

Tabla 4.32 Riesgo: Errores de los empleados y acciones

Riesgo: Errores de los empleados y acciones	
Activo - Personas	
Proceso afectado	Criticidad
Asesoría Jurídica	Alta
Acciones - Control	

A.13.2. Gestión de incidentes y mejoras en la seguridad de la información	Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información
A.13.2.1 Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información

Elaborado por: Los autores

Tabla 4.33 Riesgo: Insuficiente personal

Riesgo: Insuficiente personal	
Activos - Personas	
Procesos afectados	Criticidad
TI	Media
Asesoría Jurídica	Media
Captación de Materia Prima	Media
Acciones - Control	
A.6.1 Organización de seguridad de la información	Objetivo: Manejar la seguridad de la información dentro de la organización
A.6.1.3 Asignación de responsabilidades	Control: Se deben definir claramente las responsabilidades de la seguridad de la información.

Elaborado por: Los autores

Tabla 4.34 Riesgo: Divulgación de información confidencial

Riesgo: Divulgación de información confidencial	
Activos - Personas	
Proceso afectado	Criticidad
Asesoría Jurídica	Media
Acciones - Control	
A.6.1 Organización interna	Objetivo: Manejar la seguridad de la información dentro de la organización
A.6.1.5 Acuerdos de confidencialidad	Control: Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información

Elaborado por: Los autores

Tabla 4.35 Riesgo: Alteración no autorizada de la configuración

Riesgo: Alteración no autorizada de la configuración	
Activo	Servicios
Servicio afectado	Telefonía móvil
Procesos afectados	Criticidad
Ventas	Media
Cobranzas	Media
Acciones - Control	
A.11.2 Gestión del acceso del usuario	Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información
A.11.2.1 Inscripción del usuario	Control: Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios.

Elaborado por: Los autores

Tabla 4.36 Riesgo: Manipulación en la configuración

Riesgo: Manipulación en la configuración	
Activo	Servicios
Servicios afectados	Telefonía móvil, CCTV, Relojes biométricos, Cableado estructurado, Networking (Wlan, Wireless, Lan), Networking (VPN, Acceso remoto), Qlikview (Aplicación)
Procesos afectados	Criticidad
Ventas, Cobranzas, Talento Humano, Mantenimiento Electrónico, Captación de Materia Prima, Laminación en caliente	Media
Acciones - Control	
A.11.4 Control de acceso a redes	Objetivo: Evitar el acceso no autorizado a los servicios en red.
11.4.1 Política sobre el uso de servicios en red	Control: Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.

Elaborado por: Los autores

Tabla 4.37 Riesgo: Falta de capacidad de restauración

Riesgo: Falta de capacidad de restauración	
Activo	Servicios
Servicio afectado	QlikView (Aplicación)
Procesos afectados	Criticidad
Laminación en caliente	Media
Acciones - Control	
A.10.5.1 Respaldo	Objetivo: Mantener la integridad del software y la información
A.10.2.1.Backup o respaldo de la información	Control: Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente.

Elaborado por: Los autores

Tabla 4.38 Riesgo: Modificación no autorizada

Riesgo: Modificación no autorizada	
Activo	Servicios
Servicios afectados	CCTV, Relojes biométricos, Cableado Estructurado, Networking: Switching y Routing: Administración de ACLs Networking: WLAN - Wireless LAN, Networking: Enlaces de Comunicaciones Datos e internet Networking: VPN - Acceso Remoto Soporte Bann (ERP), RIB -Reporteador Integrado BAAN (RIB VFL: Ventas - Finanzas - Logística), Aplicativos Internos (Aplicativos Internos: Ventas - Finanzas - Logística), Aplicativos Externos (Strategylink), QLIKVIEW (tableros gerenciales), RIB -Reporteador Integrado BAAN (RIB: Laminación - Materia Prima - Planificación), Correo Electrónico, Internet, Dominio - Active Directory, Base de Datos,FileServer - Servidor de Archivos
Procesos afectados	Criticidad
Laminación en caliente	Media
Acciones - Control	
A.10.1 Procedimientos y responsabilidades operaciones	Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.

A.10.1.1 Procedimientos de operación documentados	Control: Se deben documentar y mantener los procedimientos de operación y se deben poner a disposición de todos los usuarios que los necesiten.

Elaborado por: Los autores

Tabla 4.39 Riesgo: Negación del servicio

Riesgo: Negación del servicio	
Activo	Servicios
Servicios afectados	Relojes biométricos, Soporte Baan
Procesos críticos afectados	Criticidad
Talento Humano, Laminación en caliente, Materia prima	Media
Acciones - Control	
A.11.4.1 Política sobre el uso de servicios en la red	Control: Solo los usuarios deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
A.10.1 Procedimientos y responsabilidades operaciones	Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.
A.10.1.1 Procedimientos de operación documentados	Control: Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.

Elaborado por: Los autores

Tabla 4.40 Riesgo: Pérdida del servicio

Riesgo: Pérdida del servicio	
Activo	Servicios
Servicio afectado	Soporte BAAN, Soporte ADAM Personal, Aplicativos Internos (Aplicativos Internos: Ventas - Finanzas - Logística), Aplicativos Externos (Strategylink), Aplicativos Externos (9000 DOC), Aplicativos Externos (PDA's), Soporte BAAN.
Procesos afectados	Criticidad

Tesorería, Comercio Exterior, Ventas, Cobranzas, Despacho, Procesamiento Materia Prima, Laminación en frío, Laminación en caliente, Mantenimiento Electrónico, Captación de Prima, Control y Calidad.	Media
Acciones - Control	
A.10.1 Procedimientos y responsabilidades operaciones	Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.
A.10.1.1 Procedimientos de operación documentados	Control: Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
A.10.1.2 Gestión del cambio	Control: Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.

Elaborado por: Los autores

Tabla 4.41 Riesgo: Negación del servicio afectando procesos definidos

Riesgo: Negación del servicio	
Activo	Servicios
Contingencia	Negación del servicio
Servicios afectados	Telefonía fija, Telefonía Móvil, Networking: Switching y Routing: Administración de ACLs, Networking: Enlaces de comunicaciones datos e internet, Networking: VPN - Acceso Remoto, Soporte BAAN (Baan VFL: Soporte técnico Ventas - Finanzas - Logística), Soporte ADAM PERSONAL, RIB -Reporteador Integrado BAAN (RIB VFL: Ventas - Finanzas - Logística), Aplicativos Internos (Aplicativos Internos: Ventas - Finanzas - Logística), Aplicativos Externos (Strategylink), Aplicativos Externos (9000 doc), Aplicativos Externos (PDA´s), QLIKVIEW - Tableros gerenciales
Procesos afectados	Criticidad

Tesorería, Ventas, Cobranzas, Facturación, Despacho.	Media
Acciones - Control	
A.10.1 Procedimientos y responsabilidades operaciones	Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.
A.10.1.1 Procedimientos de operación documentados	Control: Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.

Elaborado por: Los autores

4.12 Definición de políticas de seguridad

4.12.1 Seguridad física y ambiental

Política

- **Perímetro de seguridad física**

  - La protección física comprende la creación de diversas barreras o medidas de control físicas alrededor de las oficinas de la empresa y de las instalaciones de procesamiento de información.
  - Se deberá utilizar perímetros de seguridad para proteger las áreas que contienen activos importantes como switchs, routers, suministro de energía eléctrica, aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.
  - Un perímetro de seguridad se refiere por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas.

- **Controles de acceso físico**

  - Llevar un registro de los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso.
  - Controlar y limitar el acceso a la información clasificada y a instalaciones dónde se encuentren activos importantes. El acceso se otorga exclusivamente las personas autorizadas.

  - Implementar el uso de una identificación visible para todo el personal del área.
  - Definir un periodo para la revisión de los derechos de acceso para áreas protegidas, esto debería ser documentado para posteriores actualizaciones.
  - Revisar los registros de acceso a las áreas protegidas.

- **Protección de oficinas, recintos e instalaciones**

  - Reconocer la posibilidad de daño producido por incendio, inundación, explosión, y otras formas de desastres naturales o provocados por el hombre.

- **Mantenimiento de equipos**

  - Someter el equipamiento a tareas de mantenimiento preventivo, con períodos establecidos, especificaciones recomendados por proveedores y con la autorización formal del Jefe Técnico.
  - Se debe mantener un inventario actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
  - Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
  - Llevar un registro y generar un informe de todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

- **Seguridad de los equipos fuera de las instalaciones**

    - El uso de equipamiento, fuera de las instalaciones de la empresa, será autorizado por el encargado de bodega.
    - Se respetarán las instrucciones del fabricante respecto al cuidado del equipamiento.

4.12.2 Gestión de comunicaciones y operaciones

Política

- **Documentación de los procedimientos operativos**

    - Instrucciones para el manejo de errores u otras condiciones que puedan darse durante la ejecución de tareas.
    - Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
    - Reinicio del sistema y procedimientos de recuperación en caso de producirse falla en el sistema.
    - Instalación y mantenimiento de equipos destinados a las comunicaciones.
    - Monitoreo del procesamiento y las comunicaciones.
    - Gestión de servicios.
    - Resguardo de información.
    - Gestión de incidentes de seguridad en las áreas donde se desarrollan actividades del negocio.

- **Procedimientos de manejo de incidentes**

    - Definir todos los posibles incidentes relativos a la seguridad.
    - Comunicar los incidentes tan pronto como sea posible a las personas encargadas.

- Implementar controles detallados y formalizados de las acciones de recuperación.
- Respecto de las violaciones de la seguridad y de corrección de fallas en los casos en los que se considere necesario, se solicitará la participación del Jefe técnico o supervisores en el tratamiento de incidentes de seguridad ocurridos.

➢ **Política de correo electrónico**

- Protección contra ataques al correo electrónico.
- Protección de archivos adjuntos de correo electrónico.
- Uso de técnicas criptográficas para proteger dimensiones de seguridad controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados. Definir para qué actividades será el uso del correo electrónico por parte del personal de la empresa.
- Potestad de la empresa para auditar los mensajes recibidos o emitidos por el personal, lo cual se debería de incluir en un compromiso de confidencialidad con el personal.

4.12.3 Control de accesos

Política

➢ **Reglas de control de acceso**

- Indicar expresamente si las reglas son obligatorias u optativas.
- Establecer reglas sobre protección y acceso a la información.
- Controlar los cambios en los permisos de usuario.
- Controlar las reglas que requieren la aprobación del administrador, y aquellas que no requieren aprobación.

- **Administración de accesos de usuarios**

    - Otorgar derechos de acceso a los sistemas, datos y servicios de información mediante procedimientos.

- **Registro de usuarios**

    - Utilizar identificadores de usuario únicos, con el fin de que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
    - Verificar que el nivel de acceso otorgado es adecuado para el rol que cumple el usuario y es coherente con la política de seguridad de la empresa.
    - Entregar a los usuarios un documento que indique sus derechos de acceso.
    - Entregar un documento para que los usuarios lo firmen y acepten las condiciones de acceso.
    - Mantener un registro formal de todas las personas que utilizan el servicio.
    - Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización o salieron de la empresa.
    - Efectuar revisiones en periodos establecidos.
    - Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal intenta accesos no autorizados.

- **Administración de privilegios**

    - Mantener un registro de todos los privilegios asignados.
    - Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
    - Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el responsable de Seguridad Informática.

- **Administración de contraseñas de usuario**

    - Generar contraseñas temporales seguras para otorgar a los usuarios.
    - Almacenar las contraseñas sólo en sistemas protegidos.
    - Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica, verificación de firma, uso de autenticadores de hardware.

4.12.4 Control de acceso a la red

Política

- **Utilización de los servicios de red**

    - Controlar el acceso a los servicios de red tanto internos como externos.
    - El Jefe Técnico deberá tener a cargo el otorgamiento del acceso a los servicios y recursos de red.

- **Autenticación de usuarios para conexiones externas.**

    - Un método de autenticación físico (por ejemplo tokens de hardware).
    - Un protocolo de autenticación desafío / respuesta.
    - También pueden utilizarse líneas VPN's o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

- **Registro y revisión de eventos**

    - Se deberá implementar un procedimiento de revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados. La frecuencia de estas revisiones será definida por los propietarios de la información y el responsable de Seguridad Informática.

4.12.5 Gestión de la continuidad del negocio

Política

- **Proceso de la administración de la continuidad del organismo**

    - Identificar y dar prioridad a los procesos críticos de la empresa.
    - Asegurar que todo el personal de la empresa comprenda los riesgos que la misma enfrenta, en relación con la probabilidad de ocurrencia e impacto de las posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de negocio.
    - Elaborar y documentar una estrategia de continuidad de las actividades de la empresa conforme a los objetivos y prioridades acordados.
    - Plantear planes de continuidad de las actividades de la empresa.
    - Crear conjuntamente con el representante de cada área un cronograma de pruebas de cada uno de los planes de contingencia asignando funciones para su cumplimiento.
    - Diseñar actualizaciones periódicas de los planes y procesos implementados.

- **Continuidad de las actividades y análisis de los impacto**

    - Identificar los eventos o amenazas que puedan ocasionar interrupciones en los procesos de las actividades de la empresa.
    - Realizar una evaluación de riesgos para de esta manera poder determinar el impacto que causarían estas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.
    - Determinar controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y demás sistemas que puedan mitigar los daños.

- **Elaboración e implementación de los planes de continuidad de las actividades del organismo**

    - Definir las acciones correctivas que se deban implementar.
    - Diseñar e implementar procedimientos de emergencia para de esta forma garantizar la recuperación y restablecimiento según un cronograma establecido.
    - Llevar una documentación los procedimientos y procesos.
    - Capacitar al personal sobre procedimientos y procesos de emergencia acordados.
    - Instruir al personal involucrado en los procedimientos de reanudación y recuperación.

- **Marco para la planificación de la continuidad de las actividades del organismo**

    - Especificar cuáles son las condiciones de implementación para los planes que describan el proceso a seguir.
    - Describir los procedimientos de emergencia que indiquen qué medidas tomar una vez ocurrido un incidente que ponga en peligro las operaciones de la empresa.
    - Definir los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la empresa.
    - Definir un cronograma de mantenimiento donde conste por escrito cómo y cuándo será probado el plan.
    - Realizar la concientización e instrucción al personal, con el objetivo de que todos comprendan los procesos de continuidad de sus actividades y de esta forma garantizar de que los procesos van a seguir siendo eficaces.

4.12.6 Cumplimiento de la política de seguridad

Política

- Los responsables de cada una de las áreas de la empresa, serán los encargados de la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área.
- El responsable de la seguridad informática, deberá realizar las revisiones periódicas de todas las áreas de la empresa para garantizar el cumplimiento de la política, normas y procedimientos de seguridad.

- **Sanciones previstas por incumplimiento**

  - Se sancionará administrativamente a todo aquel que viole lo dispuesto en la política de seguridad conforme a lo dispuesto por las normas que rigen al personal.
  - Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga según las políticas de la empresa existentes referente a incumplimientos y demás normativas específicas aplicables.

4.13 Plan de contingencia departamento de TI

El presente trabajo de plan de contingencias de TI ha sido elaborado de acuerdo con los estándares generales y con las condiciones propias de la empresa, tratando de prevenir las situaciones por las cuales se pudiera presentar un siniestro que signifique una paralización de las operaciones informáticas, con sus consecuentes pérdidas. Implica un análisis de los posibles riesgos a cuales pueden estar expuestos los equipos de cómputo y sistemas de información. Corresponde aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de tipos.

El propósito de este plan de contingencias de TI es minimizar los riesgos causados por el suceso de contingencias e interrupciones en la operación de los sistemas de información computacionales de la empresa.

El plan de contingencia está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, de tal manera de establecer medidas destinadas para salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. La información como uno de los activos más importantes de la organización, es el fundamento más importante de este plan de contingencia.

Al existir siempre la posibilidad de desastre, pese a todas nuestras medidas de seguridad, se incluya el plan de recuperación de desastres con el único objetivo de restaurar el servicio informático en forma rápida, eficiente, con el menor costo y pérdidas posibles.

Las consecuencias de las interrupciones o contingencias pueden ser:

- Incapacidad temporal o permanente de continuar el flujo normal de las operaciones de la empresa.
- Pérdida de la ventaja competitiva que puede haberle dado a la empresa el uso de los sistemas de información computacionales.
- Disminución de ingresos debido a causas directas o indirectas.
- Impacto en la eficacia y/o eficiencia de los procesos.
- Impacto en la calidad de trabajo de los empleados.
- Impacto en la calidad de vida de los empleados.

Prevención, detección, recuperación: estos son los elementos claves de la seguridad en un centro de cómputo. La seguridad física es prerrequisito para cualquier seguridad. Cualquier medida de seguridad debe basarse en la probabilidad de ocurrencia, costo de protección, valor de lo que se está protegiendo y el probable costo si una pérdida llegara a ocurrir.

Hay que considerar que la implantación de los distintos métodos planteados en este plan, de prevención y detección de posibles siniestros puede ser costosa y llevar tiempo. Es de gran importancia hacer evaluaciones previas, realistas y pragmáticas.

- **Definición de desastre en el ámbito informático**

  - Inoperabilidad del servidor de producción por más de 1 día.
  - Inoperabilidad del servidor NT (correo electrónico) por más de 1 día.
  - Inoperabilidad del servidor de desarrollo por más de 15 días.
  - Inoperabilidad del computador personal de un usuario por más de 1 semana.
  - Inoperabilidad de las comunicaciones de datos internas con cada servidor, por el mismo tiempo.
  - Inoperabilidad de las comunicaciones con Quito por más de 1 día.
  - Inoperabilidad de las comunicaciones con el proveedor de internet por más de 1 día.

- **Margen de no operabilidad de las aplicaciones de la empresa**

Tabla 4.42 Margen de No operabilidad de las aplicaciones de la empresa

SUBSISTEMA	MÓDULOS	MARGEN DE NO OPERABILIDAD
Baan	• Planificación • Ventas • Finanzas • Logística •Producción • Servicios	2 horas
Adam	•Personal • Nómina •Salud Ocupacional • Evaluación de Personal	1día 1 día 1 semana 1 mes
Presupuesto	• Presupuesto	1 semana
Administración	• Manejo de Documentos Legales	1 semana
QilkView	• Gerencia General • Ventas • Producción • Talento Humano	2 horas 2 horas 2 horas 2 horas

StrategyLink	• BSC	1 día
Reporteadores	• Planificación • Ventas • Finanzas • Logística •Producción • Servicios	1 día 2 horas 1 día 2 horas 2 horas 1 día

Elaborado por: Los autores

La tabla descrita nos indica cual es tiempo máximo que los subsistemas de la empresa pudieran estar sin operabilidad sin causar afectación alguna.

Análisis de riesgos

A continuación se realiza un análisis de todos los elementos de riesgos a los cuales está expuesto el conjunto de equipos informáticos y la información procesada, y que deben ser protegidos. Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectados a riesgos:

a) Personal.
b) Hardware.
c) Software y utilitarios.
d) Datos e información.
e) Documentación.
f) Suministro de energía eléctrica.
g) Suministro de telecomunicaciones.

- **Daños**

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones, naturales o humanas.

b) Imposibilidad de acceso a los recursos informáticos, sean estos por cambios involuntarios o intencionales, tales como cambios de claves de acceso, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

c) Divulgación de información a instancias fuera de la empresa industrial y que afecte su patrimonio estratégico, sea mediante robo o infidencia.

- **Fuentes de daño**

Las posibles fuentes de daño que pueden causar la no operación normal de la empresa son:

- Acceso no autorizado
- Ruptura de las claves de acceso a los sistemas computacionales
- Desastres naturales:
  a) Movimientos telúricos.
  b) Inundaciones.
  c) Fallas en los equipos de soporte (causadas por el ambiente, la red de energía eléctrica, no acondicionamiento atmosférico necesario).

- **Fallas de personal clave: por los siguientes inconvenientes:**

a) Enfermedad
b) Accidentes
c) Renuncias
d) Abandono de sus puestos de trabajo
e) Otros.

- **Fallas de Hardware:**

a) Falla en los Servidores (Hw).
b) Falla en el hardware de red (Switches, Cableado de la red, Router, Firewall).

- **Incendios**

Objetivos

- Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información.
- Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

Importancia

- Garantiza la seguridad física, la integridad de los activos humanos, lógicos y materiales de la empresa.
- Permite realizar un conjunto de acciones con el fin de evitar el fallo, o en su caso, disminuir las consecuencias que de él se puedan derivar.
- Permite realizar un análisis de riesgos, respaldo de los datos y su posterior recuperación de los datos. En general, cualquier desastre es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de la empresa.
- La probabilidad de que ocurra un desastre es muy baja, aunque se diera, el impacto podría ser tan grande que resultaría fatal para la organización.
- Permite definir contratos de seguros, que vienen a compensar, en mayor o menor medida las pérdidas, gastos o responsabilidades.

Seguridad física

La integridad física del centro de cómputo radica en la existencia de condiciones indispensables de seguridad. El departamento debe contar con un ambiente separado para la ubicación de los servidores.

El personal que es parte del centro de cómputo debe considerarse facilidad de evacuación, ruido, temperatura, iluminación, mobiliario, etc. Los riesgos existentes en cuanto a seguridad física son:

Riesgo: Falta de suministro eléctrico

Descripción del riesgo:

Cortes de energía eléctrica, ocasionados internamente o por la Empresa Eléctrica.

Prevención

Se debe considerar los siguientes aspectos:

- Incluir equipos de suministro eléctrico de emergencia: UPS's, plantas de emergencia.
- Se instalarán UPS´s en los servidores y en cada estación de usuario. Así mismo se instalará 1 UPS en cada rack de comunicaciones.
- A nivel de servidores de producción y de correo electrónico, además del UPS se debe instalar bancos de baterías de respaldo con energía suficiente para 4 horas
- A nivel de estaciones de usuario, el UPS proporciona respaldo de energía durante diez minutos, tiempo suficiente para grabar cambios en los archivos y apagar adecuadamente las computadoras.
- Se deberá instalar luces de emergencia a baterías en cada ambiente del centro de cómputo. Se deben revisar periódicamente estos dispositivos a fin de asegurar su buen funcionamiento.

Situación actual

Actualmente los servidores de producción y correo electrónico cuentan con sus respectivos UPS y bancos de baterías para 4 horas (servidor de datos) y 8 horas (servidor de correos racks de comunicaciones y las principales estaciones de trabajo cuentan con UPS individuales, con respaldo para aproximadamente 15 minutos.

Riesgo: Polvo, humo, gases en el ambiente

Descripción del riesgo:

- Contaminación por gases, humo y otros.
- Presencia de polvo en el ambiente.

Prevención

Se deben considerar los siguientes aspectos:

- Cubrir los computadores con cobertores, durante el tiempo en que no se utiliza el computador.
- Cubrir los teclados con cobertores flexibles adecuados.
- Contrato de mantenimiento preventivo.

Recuperación

- **De equipos:**
    - Contrato de mantenimiento preventivo - correctivo.
    - Póliza de seguro.
    - Equipo alterno de respaldo.
    - Equipo de reemplazo proporcionado por el proveedor del contrato de mantenimiento.
- **De datos:**
    - Cintas de respaldo
    - Disquetes de respaldo

Situación actual

Se ha provisto a un 60 por ciento de los usuarios, de cobertores para sus equipos, mismos que son utilizados para cubrirlos fuera de horas de trabajo. Además, en las áreas en las que el ambiente se encuentra más contaminado (bodegas, despachos), se ha provisto de protectores permanentes de teclado.

Riesgo: Incendio o fuego

Descripción del riesgo:

En el centro de cómputo, la causa más común de incendio es un cortocircuito. Cuando se provoca un cortocircuito que origina fuego en un equipo, el fuego puede extenderse si encuentra alrededor elementos combustibles.
De acuerdo a NEPA (National fire prevention agency) los equipos se clasifican en:

Tipo 1: El equipo no se incendia
Tipo 2: El equipo se incendia dentro de su gabinete
Tipo 3: El equipo se incendia con su gabinete.

Debe identificarse en cada caso el tipo de equipo según esta clasificación, a fin de tomar las debidas precauciones de aislamiento. Si el equipo dispone de interruptor propio ofrece mayor seguridad, y si incluye mecanismo de protección es mejor.

Un incendio también puede ser causado por sobrecalentamiento de equipos en contacto con material combustible, por fumar en el área o intencionadamente.

Prevención

Precauciones en el ambiente físico:

- Evitar el uso o almacenamiento de materiales combustibles.

- Almacenar los papeles en un gabinete de metal o en un área contigua físicamente independiente.
- Los recipientes de basura deben ser de material no combustible y deben evacuarse oportunamente.
- Las alfombras o cortinas deben ser de material no combustible y, en caso de entrar en contacto con el fuego, no producir gases corrosivos ni tóxicos.
- Los gabinetes y muebles debes ser metálicos preferiblemente.
- No fumar en las instalaciones.
- Conservar limpio el ambiente, libre de papel de desperdicio; realizar limpieza diaria de las superficies de trabajo y de pisos.
- Los interruptores maestros deben ser ubicados estratégicamente a fin de permitir acciones de emergencia sin riesgos para el personal.
- Establecer procedimientos de apagado de los equipos
- La ubicación de las tomas de aire debe minimizar la captación de llamas, humo y gases tóxicos externos.
- Los ductos de acondicionamiento de aire deben ser metálicos, con aislamiento exterior.
- Se debe revisar periódicamente los cables e instalaciones eléctricas.

Prevención de daños al soporte lógico:

- Los archivos de datos y de programas sólo deben estar en la sala de equipos cuando se los vaya a utilizar. Normalmente deben estar en las bóvedas, cajas fuertes o en muebles metálicos.
- Para su almacenamiento es muy recomendable el uso de bóvedas de seguridad y cajas fuertes resistentes al fuego y equipadas con detección automática de incendios. Estas bóvedas pueden ser principales o remotas; las principales contienen respaldo magnético de archivos útiles e importantes; las bóvedas remotas deben contener archivos magnéticos vitales y respaldo de ciertos archivos importantes.
- Las bóvedas deben estar separadas de la sala de equipos por una instalación que sea capaz de resistir al menos dos horas la propagación de un incendio; deben tener dos

puertas de acceso para permitir acciones de neutralización del fuego y poseer ventilación de emergencia para extraer humo, vapores y gases.

Detección

Existen varios tipos de detectores, entre ellos los de humo, de temperatura y de ionización. Estos detectores deben activar alarmas audibles, cortar el suministro eléctrico de los equipos y activar los sistemas de extinción de incendios.

Los detectores ópticos de humo son activados cuando el humo disminuye la intensidad del rayo de luz que llega al detector; son muy sensibles y no necesitan la presencia de llama para activarse.

Los detectores de temperatura son sensibles a incrementos muy rápidos de temperatura; los de ionización detectan productos de combustión en el aire.

Estos detectores deben instalarse en la sala de equipos y en las tomas de aire del acondicionador de aire así como en los ductos de retorno de aire. Se debe escoger adecuadamente el equipo de detección de incendios.

Los sistemas de alarma asociados a los detectores deben transmitir las señales a un punto que sea supervisado las 24 horas.

Extinción

Debe efectuarse utilizando extintores de compuestos aleganados de contacto seco (gas halón) o CO2 (éste no debe aplicarse directamente sobre los equipos de cómputo). El gas halón es efectivo en áreas totalmente cerradas. Es preferible no utilizar agua como elemento principal de extinción.

Las salidas del gas extintor deben ubicarse en el piso y techo falsos y en las paredes. Estas salidas deben estar diseñadas para soportar altas temperaturas. Debe existir una toma de agua y mangueras como elemento secundario de extinción.

El activamiento debe ser automático disparado por cualquiera de los detectores. Es conveniente que haya pre activamiento: la presencia de humo y calor activa alarmas audibles, luego si la temperatura sube definitivamente se activa el sistema de extinción (activamiento de los extintores y corte del suministro eléctrico a los equipos y a los acondicionadores de aire). Es prudente un tiempo de espera de 30 segundos entre las dos etapas.

Deben diseñarse procedimientos de emergencia ampliamente difundidos y ensayados, de manera que cada persona sepa lo que debe hacer.

Es importante que en todos los ambientes del centro de cómputo existan extintores manuales; hacerlos accesibles a las personas que trabajan en la sala, señalar su ubicación y vigilar su carga periódicamente de acuerdo a las normas técnicas del proveedor.

Recuperación

- **De equipos:**

    - Contrato de mantenimiento preventivo - correctivo
    - Póliza de seguro
    - Equipo alterno de respaldo
    - Equipo de reemplazo proporcionado por el proveedor del contrato de mantenimiento

- **De datos:**

    - Cintas de respaldo
    - Disquetes de respaldo

Situación actual

El departamento de Seguridad Industrial mantiene los extintores de incendios.

Estos son recargados periódicamente para asegurar su idoneidad. En el área de TI se encuentra instalado 1 extintor. Se ha solicitado la instalación de un extintor adicional en las oficinas de TI en el bloque B y un extintor en la oficina de TI del bloque A.

Capacitación del personal de TI en el uso del extintor de incendios.

Todo el personal de la empresa ha sido entrenado por el Departamento de Seguridad Industrial en el uso del extintor de incendios ubicado en cada área. Esto incluye al personal de TI.
El centro de cómputo no cuenta actualmente con un sistema automático de detección y extinción de incendios. Debe realizarse un estudio de factibilidad para instalarlo.

Riesgo: Temperatura inadecuada

Descripción del riesgo:

El aire acondicionado está relacionado con el control de temperatura, humedad y contenido de polvo y partículas contaminantes. La excesiva temperatura puede provocar daños permanentes en los equipos así como interrumpir su normal operación.

La humedad excesiva deteriora los elementos y, si se suma a ella la salinidad del ambiente de Guayaquil, se tiene como resultado un factor altamente corrosivo que disminuirá la vida útil de los equipos.

Debido a la naturaleza del proceso de la empresa industrial, altamente contaminante del aire, toda el área de la empresa se encuentra expuesta a la presencia de partículas contaminantes (humo, hollín, polvo). Las áreas cercanas al horno de fundición se encuentran especialmente expuestas a esta contaminación.

Prevención

Los sistemas de aire acondicionado deben contener filtros y se recomienda limpiarlos cada quince días. Se debe contar con un equipo auxiliar de aire acondicionado que deberá ser sometido a revisión periódica.

Temperatura

Se debe mantener un control estricto de la temperatura en el ambiente donde se encuentran ubicados los servidores y se debe tener extrema precaución para que no se susciten cambios bruscos.

La temperatura está influenciada por:

- Calor disipado por los equipos y el alumbrado
- Calor disipado por las personas (alrededor de 100 W por persona)
- Calor transferido a través de suelos, paredes y techo.

El diseño de la mayoría de sistemas de aire acondicionado impone un límite máximo de personas que pueden estar presentes en el medio controlado sin ocasionar variación en la temperatura ambiente.

Cualquier acontecimiento que origine sobrepasar estos máximos, por ejemplo, la admisión de un grupo de visitantes, debe ser de duración tan corta como sea razonable.

Sin perjuicio de las recomendaciones del fabricante de ciertos equipos particulares, las recomendaciones para la temperatura en el ambiente de servidores deben ser:

Equipos en operación.- Mínimo: 10°C
Máximo: 40°C
Recomendada: 20°C
Equipos en operación.- Mínimo: 10°C

Máximo: 50°C
Recomendada: 26°C

Humedad

Se debe mantener un control de humedad, especialmente en el ambiente donde se encuentran los servidores, para evitar los efectos de corrosión.

Sin perjuicio de las recomendaciones del fabricante de ciertos equipos particulares, la humedad relativa debe controlarse de acuerdo a los siguientes parámetros.

Humedad relativa mínima:	8%
Humedad relativa máxima:	60%
Humedad relativa recomendada:	32%

Aire Contaminado

- Se debe proveer a todos los usuarios de cobertores para monitor, CPU, teclado, para que cubran sus equipos cuando no lo utilicen. Para las áreas de bodegas, acería, despachos, naves, mantenimiento automotor, se debe proveer de protectores permanentes de teclado.
- Se debe realizar periódicamente mantenimiento preventivo que incluya una limpieza exhaustiva de todas las partes de los equipos. Para las áreas más expuestas el mantenimiento deberá ser más frecuente.

Recuperación

- **De equipos:**

    - Contrato de mantenimiento preventivo - correctivo
    - Póliza de seguro
    - Equipo alterno de respaldo

- Equipo de reemplazo proporcionado por el proveedor del contrato de mantenimiento

- **De datos:**

  - Cintas de respaldo
  - Disquetes de respaldo

Situación actual

Todas las oficinas de la empresa se encuentran climatizadas por equipos de acondicionamiento de aire, lo cual garantiza que los equipos de los usuarios sean enfriados adecuadamente mientras están encendidos. El área en la cual se encuentran ubicados los servidores de datos posee un sistema adicional de acondicionamiento de aire, que garantiza que durante las 24 horas del día dichos equipos se encuentren a la temperatura recomendada por el fabricante.

La sala donde se encuentra el servidor de datos se encuentra provista de un equipo de aire acondicionado mini-split y un aire acondicionado doméstico de reserva.

Para las áreas de mayor exposición al aire contaminado, se ha provisto de protectores permanentes de teclado. A todos los usuarios se los ha provisto de cobertores para monitores y CPU.

La empresa mantiene desde 1996, con un proveedor de servicios de computación, un contrato de mantenimiento preventivo - correctivo sin repuestos. En virtud de ese contrato, se realiza trimestralmente un mantenimiento preventivo exhaustivo de todos los computadores.

Riesgo: Rotura de un tramo de fibra óptica

Descripción del riesgo: Rotura accidental o malintencionada de un tramo de fibra óptica, aérea o subterránea.

La rotura de un tramo de fibra ocasionaría el aislamiento de un bloque de computadoras del resto de la red. El problema es más crítico para los usuarios cuyas computadoras se encuentran en un segmento en el cual no están los servidores, pues esos usuarios no podrían acceder a las aplicaciones, a la base de datos ni al correo electrónico.

Prevención

Coordinación con el responsable de la ejecución de obras civiles, a fin de evitar trabajos que pudieran poner en riesgo la integridad de la fibra.

Recuperación

- Póliza de seguro
- Fibra de backup (configuración en anillo)

Riesgo: Interferencias

Descripción del riesgo: Interferencias electromagnéticas sobre las líneas de comunicación de la red interna de datos.

Estas interferencias pueden ser ocasionadas por:

- Armónicas introducidas a causa de la cercanía con motores y otros elementos eléctricos
- Campos eléctricos y magnéticos creados por líneas de alta tensión.

Las interferencias pueden causar pérdida de datos, disminución del rendimiento del sistema de comunicaciones, interrupción de las comunicaciones, etc.

Prevención

Se debe independizar la toma de corriente eléctrica a la que está conectado el equipo de computación. El circuito independiente debe ser debidamente protegido de interferencias.

Se debe cuidar de que los cables de datos estén lo suficientemente alejados de los cables que conducen energía eléctrica, a fin de evitar los campos electromagnéticos generados por la conducción de energía eléctrica.

Recuperación

- **De equipos:**
    - Contrato de mantenimiento preventivo – correctivo
    - Póliza de seguro
    - Equipo alterno de respaldo
    - Equipo de reemplazo proporcionado por el proveedor del contrato de mantenimiento

- **De datos:**

    - Cintas de respaldo
    - Disquetes de respaldo

Riesgo: Robo

Descripción del riesgo:

Introducción subrepticia de personas en horarios en los que no se encuentra el personal del departamento, con presencia de fractura de cerraduras, puertas, ventanas, techos, etc.

Prevención

El propósito de los controles de acceso físico es proteger los recursos del departamento de datos, el que incluye información sensitiva y confidencial así como de inversiones de la organización, previniendo acceso no autorizado a ellos. Los controles de acceso físico deben diseñarse para permitir acceso a personal autorizado solamente y negar acceso a cualquier otro personal.

Esencialmente se tienen los siguientes niveles de controles de acceso:

- Controles de perímetros
- Controles de acceso al departamento de procesamiento de datos
- Controles de acceso dentro del departamento de procesamiento de datos

Detección

Debe instalarse en el centro de cómputo un sistema de alarma que envíe señales a Seguridad en caso de producirse un ingreso no autorizado al área de TI.

Recuperación

- **De equipos:**
    - Póliza de seguro
    - Equipo alterno de respaldo
- **De datos:**
    - Cintas de respaldo
    - Disquetes de respaldo

Situación actual

- Las instalaciones del Complejo están protegidas por altos muros.
- La seguridad física está garantizada por una empresa de seguridad que vigila permanentemente las áreas y protege los activos de la compañía.
- Todas las oficinas tienen cerraduras con llave. Las llaves están en custodia de los funcionarios del área y de la empresa que presta los servicios de seguridad.

Riesgo: Vibraciones del terreno

Descripción del riesgo:

Vibraciones causadas por prensas, maquinaria pesada, circulación de vehículos, temblores, terremotos, etc.

Prevención

- Ubicación de los equipos en un lugar firme y no en extremos de mesas o escritorios.
- Ubicación de amortiguadores de vibración entre los equipos y el piso.

Recuperación

- **De equipos:**

    - Contrato de mantenimiento preventivo – correctivo
    - Póliza de seguro
    - Equipo alterno de respaldo
    - Equipo de reemplazo proporcionado por el proveedor del contrato de mantenimiento

- **De datos:**

    - Cintas de respaldo
    - Disquetes de respaldo

Seguridad de datos

Se describen algunos conceptos y normas para prevenir errores, omisiones, cambios no autorizados en programas y/o archivos, accesos indebidos que pudieran causar daños al software o alteración indebida de datos.

Riesgo: Pérdida de datos por virus

Descripción del riesgo:

Introducción de virus informáticos en una o más computadoras de la red.

Las vías de entrada de virus en una computadora pueden ser varias, entre ellas, las más comunes son:

- Correo electrónico de internet.
- Correo electrónico de la intranet.
- Lectura de disquetes o CD infectados.
- Archivos bajados de la web.

Los virus, cuya variedad actualmente se cuenta por decenas de miles, actúan de forma diferente para causar daño, pero generalmente el resultado es la pérdida de información en la computadora infectada.

Prevención

El uso de programas antivirus disminuye el riesgo de infección y ayuda a eliminar virus ya instalados en una computadora.

Se debe establecer como política empresarial, para minimizar el riesgo de infección, la prohibición de introducir disquetes y CD's a la empresa, a menos que el departamento de TI lo autorice y verifique la ausencia de virus en esos medios.

Se debe inducir a los usuarios hacia la cultura de respaldos de su información.

Se debe instalar, en toda la red, un programa antivirus que permita detectar la mayor cantidad posible de virus, desinfectar los archivos que los contienen y notificar al administrador la presencia de virus.

Detección

Se debe instalar, en toda la red, un programa antivirus que permita detectar la mayor cantidad posible de virus, desinfectar los archivos que los contienen y notificar al administrador la presencia de virus.

Recuperación

- **De datos:**

    - Discos de respaldo de datos de usuarios
    - CD de instalación de sistemas operativos y utilitarios

Situación actual

De acuerdo a políticas del área de TI, se ha capacitado a los usuarios en el manejo del sistema operativo para la obtención de respaldos en disquetes. Cada usuario es responsable de la seguridad de la información que se encuentra contenida en su computadora.

En caso de daños en la misma, el área de TI restaurará el sistema operativo Windows, las aplicaciones y los utilitarios, y ayudará al usuario a restaurar sus datos desde sus disquetes de respaldo. Si el usuario no tenía un respaldo, o tenía un respaldo muy antiguo, no es responsabilidad atribuible al área de TI.

El área de TI ha instalado en todas las computadoras un programa antivirus que chequea los archivos que se abren, los archivos que llegan adjuntos a un correo electrónico y otras áreas de los discos duros, a fin de prevenir y detectar infecciones por virus.

Cuando el programa antivirus detecta un virus en un correo electrónico, notifica de esta novedad al administrador.

Riesgo: Acceso no autorizado a la red de datos desde el exterior

Descripción del riesgo:

Debido a que, con el fin de utilizar los recursos de internet, la red interna de la empresa se encuentra enlazada con un ISP, se encuentra expuesta a intromisión externa por parte de hackers y crackers que pululan cada vez en mayor número en internet. Muchos de estos hackers y crackers buscan hacer daño, ya sea saturando las redes y los servidores, utilizando las computadoras de la red para saturar servidores ubicados en otros sitios, así como introduciendo programas dañinos o extrayendo información de la compañía.

Prevención

La única manera de prevenir estos accesos es mediante mecanismos de hardware o software denominados Firewalls (muros de fuego), que restringen el tráfico desde y hacia la red interna mediante reglas que autorizan específicamente a ciertas computadoras del exterior a conectarse a la red interna.

Recuperación

- **De datos:**

    - Discos de respaldo
    - Respaldo de datos de los usuarios (Servidor de archivos)
    - CD de instalación de sistemas operativos y utilitarios.

Situación actual

La red interna de datos se encuentra actualmente conectada al ISP Telconet mediante un canal de radio de tipo Spread Spectrum, en 2.4 GHz. El canal provee una conexión de 2 Mbps con el ISP y un ancho de banda de 64 Kb con internet.

Entre la red interna y la red de Telconet, se ha instalado un equipo Linux que mantiene operando permanentemente un firewall.

Riesgo: Acceso no autorizado a la base de datos u otros archivos de datos

Descripción del riesgo:

En el servidor de datos, el riesgo consiste en que una persona no autorizada posea las herramientas y conozca las contraseñas para ingresar al servidor y a la base de datos y pueda ocasionar:

- Fuga de información
- Infidencia de información
- Alteración no intencionada o malintencionada de datos
- Borrado de información

En las PC, el riesgo consiste en que una persona que no es el usuario a quien se ha asignado ese recurso, ingrese a la computadora y, sin estar autorizado, altere o borre información

contenida en la computadora, envíe correo electrónico a nombre del usuario, conozca información confidencial, etc.

Prevención

Servidores de datos

Cada miembro del área de TI tendrá su clave y nivel de acceso al sistema operativo del servidor y/o la base de datos, de acuerdo a las actividades que desempeña, según la política general de TI. Será responsabilidad de cada persona mantener en forma confidencial sus respectivas claves de acceso.

Computadoras personales

Cada usuario deberá configurar en su computadora los niveles de seguridad que considere necesarios para precautelar el acceso indebido a los mismos por personal no autorizado.

El nivel más bajo corresponde a la seguridad de encendido (clave mantenida como parte de la configuración en memoria CMOS). El siguiente nivel corresponde a la clave de acceso a la red. El tercer nivel corresponde a la clave establecida en el protector de pantalla.

Será responsabilidad de cada usuario mantener en forma confidencial sus respectivas claves de acceso. Las claves deben cambiarse periódicamente para prevenir accesos no autorizados por claves no confidenciales.

Recuperación

- **De datos:**

    - Discos de respaldo
    - Respaldo de datos de los usuarios (Servidor de archivos)
    - CD de instalación de sistemas operativos y utilitarios

Seguridad de soporte

Riesgo: Ausencia de documentación adecuada

Descripción del riesgo:

El riesgo consiste en que, en el momento en que se necesite información técnica correspondiente a la base de datos o a las aplicaciones, no se pueda contar con ella por inexistencia, pérdida, no localización o no disponibilidad de:

- Manuales técnicos.
- Manuales de usuario.
- Manuales de la base de datos.
- Manuales del sistema operativo.
- Modelos de datos de las aplicaciones.

Prevención

Se debe realizar un inventario de los manuales existentes a fin de determinar faltantes. Una vez establecidos los manuales faltantes, si se trata de manuales técnicos o de usuario de sistema operativo, base de datos o utilitarios, se procederá a adquirirlos. Si se trata de manuales técnicos y de usuario de aplicaciones, se procederá a elaborarlos y archivarlos de manera que puedan ser fácilmente localizados y que todo el personal del área de TI conozca su contenido y su ubicación.

Riesgo: Ausencia de personal de soporte

Descripción del riesgo:

- Indisponibilidad del personal de soporte por no encontrarse en la empresa (horas no laborables, domingos, feriados).
- Indisponibilidad del personal de soporte por vacaciones, enfermedad, capacitación, renuncia, etc.

Prevención

- Proveer de información a seguridad para localizar al personal de TI en cualquier momento.
- Capacitación de personal alterno en el conocimiento del soporte a las aplicaciones.
- Capacitación de personal alterno en la administración del sistema y de la base de datos.

Recuperación

- El personal de seguridad debe conocer una manera de localizar al personal de TI en cualquier momento.
- El usuario debe contactar con seguridad para que le proporcione un número telefónico donde localizar a una persona de TI.
- Todos los miembros del área de TI deben conocer la manera de contactar con el resto de personas del área, a fin de ayudar en su localización.
- La persona de TI que es requerida, una vez que se ha comunicado con el usuario y ha verificado la necesidad de soporte, si la situación así lo amerita, está en la obligación de trasladarse a la empresa a solucionar la novedad reportada.

Procesos orientados a la prevención

Obtención de respaldos de la base de datos

Servidor de producción.

Objetivo: Recuperación en caso de pérdida de equipo o disco duro o daño en la base de datos o los file systems. Los respaldos se obtendrán de la base de datos on-line y serán ubicados en cintas.

Frecuencia: Ver tabla.

Lugar de ubicación de los medios: Ver tabla

Responsable de la obtención del respaldo: Jefe de área de TI.

Tabla 4.43 Bitácora de respaldos.

	Descripción	Frecuencia	Hora
1	Respaldo diario de la Base de Datos	1 vez al día (lunes – sábado) 6 cintas (Reposan en caja fuerte de TI)	8H00
2	Respaldo semanal (Toda la Base de Datos, Cía. Empresa de Baan)	1 vez a la semana (dos copias) 8 cintas (reposan en caja fuerte de TI)	Lunes 8h00
3	Respaldo mensual (Toda la Base de Datos, Cía. Empresa de Baan)	1 vez al mes (dos copias) 24 cintas (reposan en caja fuerte de TI)	Primer día del mes 8h00
4	Respaldo anual (Toda la Base de Datos, Cía. Empresa de Baan)	1 vez al año (dos copias) 2 cintas (reposan en caja fuerte de TI)	Primer día del año 8h00

Elaborado por: Los autores

Se generarán duplicados de los respaldos semanal, mensual y anual, los cuales reposarán en la bóveda de seguridad de un banco local.
El Jefe de TI será el responsable de ubicar en la caja fuerte de TI y de depositar la segunda copia en la bóveda del banco, durante la mañana del día en que se obtienen los respaldos.

A fin de minimizar aún más el riesgo de pérdida de datos, se mantendrá permanentemente la base de datos en modo ARCHIVE, realizando cada mes (el primer día laborable del mes) un respaldo de todos los objetos de la base de datos off line a cinta. Esta cinta, generada por duplicado tendrá el mismo tratamiento que la cinta de respaldo mensual en cuanto a su archivo.

NOTA: Los archive logs generados por la base de datos deberán ubicarse en un file system diferente de los archivos que constituyen la base de datos.

Obtención de respaldos de la bitácora de transacciones (Log De Transacciones)

Servidor de Producción

Objetivo: Recuperación del log de transacciones, en caso de pérdida de equipo o disco duro o daño en la base de datos o los file systems.

Frecuencia: El primer día de cada mes.

Lugar de ubicación de los medios: Este respaldo se ubicará en las mismas cintas del respaldo mensual.

Responsable de la obtención del respaldo: Jefe de TI.

Las cintas deberán ser probada en su contenido (lectura) y etiquetadas adecuadamente.

Obtención de respaldos de programas fuente y objeto

PC´s de desarrollo

Objetivo: Recuperación en caso de pérdida de equipos de desarrollo o discos duros de esos equipo, o en caso de detectarse alteraciones no autorizadas o no deseadas a los programas. Los respaldos se obtendrán en CD.

Frecuencia: Primera vez y siempre que los programas sean modificados.

Número de copias: 2.

Lugar de ubicación de las copias:

- **Copia 1:** Oficina de Jefe de TI - caja fuerte.
- **Copia 2:** Bóveda de seguridad de un banco.

Responsable de la obtención del respaldo: Jefe de área de TI.

Responsable de ubicación de las copias: Jefe de área de TI.

Los CD's deberán ser probados en su contenido (lectura) y etiquetados adecuadamente.

La etiqueta debe permitir conocer:

- El contenido
- La fecha y hora del respaldo

Obtención de respaldos de Pc de usuarios

Objetivo: Recuperación en caso de pérdida de equipo o disco duro.

Frecuencia: Primera vez y siempre que los archivos sean modificados.

Número de copias: 1

Lugar de ubicación de las copias: Servidor de archivos

Responsable de la obtención del respaldo: Usuario.

El usuario será responsable de mantener todos sus archivos generados a partir de cualquier utilitario (Word, Excel, Power Point, etc.) dentro del directorio Mis documentos.

Periódicamente, al menos una vez por semana, el usuario deberá respaldar todo su directorio

Mis documentos en el servidor de archivos de la empresa.

Adicionalmente, para archivos críticos, el usuario deberá obtener una copia en disquetes.

Los disquetes deberán ser probados en su contenido (lectura) y etiquetados adecuadamente.

La etiqueta debe permitir conocer:

- El contenido
- La fecha del respaldo

Procesos orientados a la recuperación

Objetivo: Encontrar la solución apropiada y a tiempo, en el caso de tener algún problema en el funcionamiento en el funcionamiento del Servidor Baan.

Siniestro: Error no recuperable en un disco o en un File System del Servidor de datos, que no permita montar la base de datos a partir de su contenido actual.

Acciones a ejecutar:

- Notificar a los usuarios acerca del siniestro ocurrido, dándoles un tiempo estimado de recuperación.
- Recuperar el Sistema Operativo, si es que fue afectado.
- Recrear el o los file systems afectados.
- Restaurar la base de datos a partir del último respaldo off line.
- Regenerar las transacciones registradas a partir de ese respaldo, mediante el uso del archive log correspondiente.
- En caso de que este procedimiento fracasara por cualquier motivo, se deberá restaurar la base de datos a partir del último respaldo on line disponible.
- Puede ser el respaldo diario ubicado en la oficina del Jefe de TI, o puede que sea necesario acudir a los respaldos ubicados en la caja fuerte de TI o los respaldos ubicados en el casillero de seguridad del banco.
- En caso de ser necesario acudir a los respaldos ubicados en el casillero de seguridad del banco. El Jefe de TI deberá acudir al banco, retirar el respaldo, restaurarlo y volver a depositarlo.

Siniestro: Error no recuperable en el servidor de aplicaciones.

Acciones a ejecutar:

- Notificar a los usuarios acerca del siniestro ocurrido, dándoles un tiempo estimado de recuperación.
- Recuperar el Sistema Operativo, si es que fue afectado.
- Restaurar los objetos de las aplicaciones a partir del último respaldo.

Siniestro: Error no recuperable en un PC de desarrollo.

Acciones a ejecutar:

- Recuperar el Sistema Operativo, si es que fue afectado.
- Restaurar las fuentes y objetos de las aplicaciones a partir del último respaldo.

Siniestro: Pérdida total de un servidor, de un PC de desarrollo o de un PC de usuario.

Acciones a ejecutar:

- Notificar a los usuarios acerca del siniestro ocurrido, dándoles un tiempo estimado de recuperación.
- Proceder a la recuperación física del equipo, realizando el trámite de reclamo pertinente a la compañía de seguros.
- Para el caso de los servidores, montar el servidor de respaldo mientras se recupera físicamente el equipo original y restaurar en él los respaldos conforme se explica en los siniestros anteriores.

Siniestro: Rotura de tramo de fibra óptica subterráneo, TI – Gerencia General.

CASO 1: Rotura de 1 a 4 de los 6 hilos de fibra:

Acciones a ejecutar:

- Probar los hilos hasta detectar si 2 de ellos están operativos.
- Conectar los hilos operables.
- Notificar al seguro.
- Conectar el tramo alterno a los hubs.
- Proceder a reemplazar el tramo averiado, en coordinación con la compañía de seguros.

CASO 2: Rotura de más de 4 de los 6 hilos de fibra:

Acciones a ejecutar:

- Probar los hilos hasta detectar que no existen 2 de ellos operativos.
- Notificar al seguro.
- Conectar el tramo alterno a los hubs.
- Proceder a reemplazar el tramo averiado, en coordinación con la compañía de seguros.

Muchos de los aspectos de prevención y corrección están previstos en y cubiertos por un contrato de mantenimiento preventivo – correctivo sin repuestos, que contempla, entre otras cosas, el reemplazo del equipo dañado en un plazo máximo de:

- 1 semana calendario para el caso de los computadores personales y el servidor de desarrollo.
- 24 horas para el caso del servidor de producción.
- 24 horas para el caso de hubs.

Siniestro: Pérdida del servicio en la comunicación de datos entre las empresas general.

Acciones a ejecutar:

- Determinar si la funcionalidad del enlace de datos tiene problemas.
- Informar al responsable de redes y comunicaciones o a l especialista de comunicación
- Probar los hilos de la fibra hasta detectar si 2 de ellos están operativos.
- Conectar los hilos operables en los Equipos de Comunicaciones.
- Notificar a la empresa Telconet de lo acontecido.
- Proceder a solucionar el tramo averiado con la empresa Telconet.

Siniestro: Pérdida de la conexión con el servidor (IBMP5) de Baan

Acciones a ejecutar:

1. Determinar si la funcionalidad del equipo tiene problemas.
2. Comunicar al responsable de los equipos servidores (Especialista de Redes).
3. Determinar el daño del servidor: Si es la funcionalidad de Baan, si es la funcionalidad del sistema operativo. Si en la funcionalidad de Sistema Gestor de la Base de Datos Oracle. Si es la funcionalidad de la comunicación.
4. En caso de tener problemas en la funcionalidad de Baan y los usuarios no puedan ingresar al sistema.

5. Revisar que el usuario que está ingresando, este creado en el Sistema Baan.
6. Revisar que el usuario que está ingresando este creado en el sistema operativo AIX.
7. Realizar la vinculación del usuario en Baan.
8. Si persiste el problema de que no pueda ingresar, subir el servicio del Baan en el servidor (rc.start).
9. En el caso de tener problemas con el sistema operativo, bajar los servicios de Baan, Oracle, sistema operativo para reiniciar el equipo utilizando los respectivos comandos. Además se debe coordinar con la empresa Akros, que es la que da servicio de Help Desk y mantenimiento de los equipos.
10. En caso de tener problemas en la funcionalidad de la Base de Datos Oracle.
11. Subir el servicio de Oracle mediante los comandos que se indica en el punto 9

12. Revisar las configuraciones de instalación del Oracle, coordinando con la Jefe de TI y con el especialista de Base de datos.
13. En caso de tener problemas en la comunicación del servidor
14. Revisar si el cable UTP está en funcionamiento, sino esta proceder a cambiar el cable.
15. Revisar si el cable de comunicación que va desde el punto que se conecta el servidor hasta el Rack de Comunicaciones, si tiene averías proceder a cambiar el cable.
16. Revisar si está funcionando la tarjeta de red del equipo, si tiene problemas realizar el cambio de la tarjeta por otra de las mismas características.
17. Revisar la configuración de las comunicaciones en el servidor, si la IP está en el rango estipulado por el administrador de la red, si los servicios de comunicación se encuentran habilitados, esto se lo puede coordinar con el responsable de redes y comunicaciones, con el Jefe de TI.

4.14 Resultados obtenidos de OSSIM

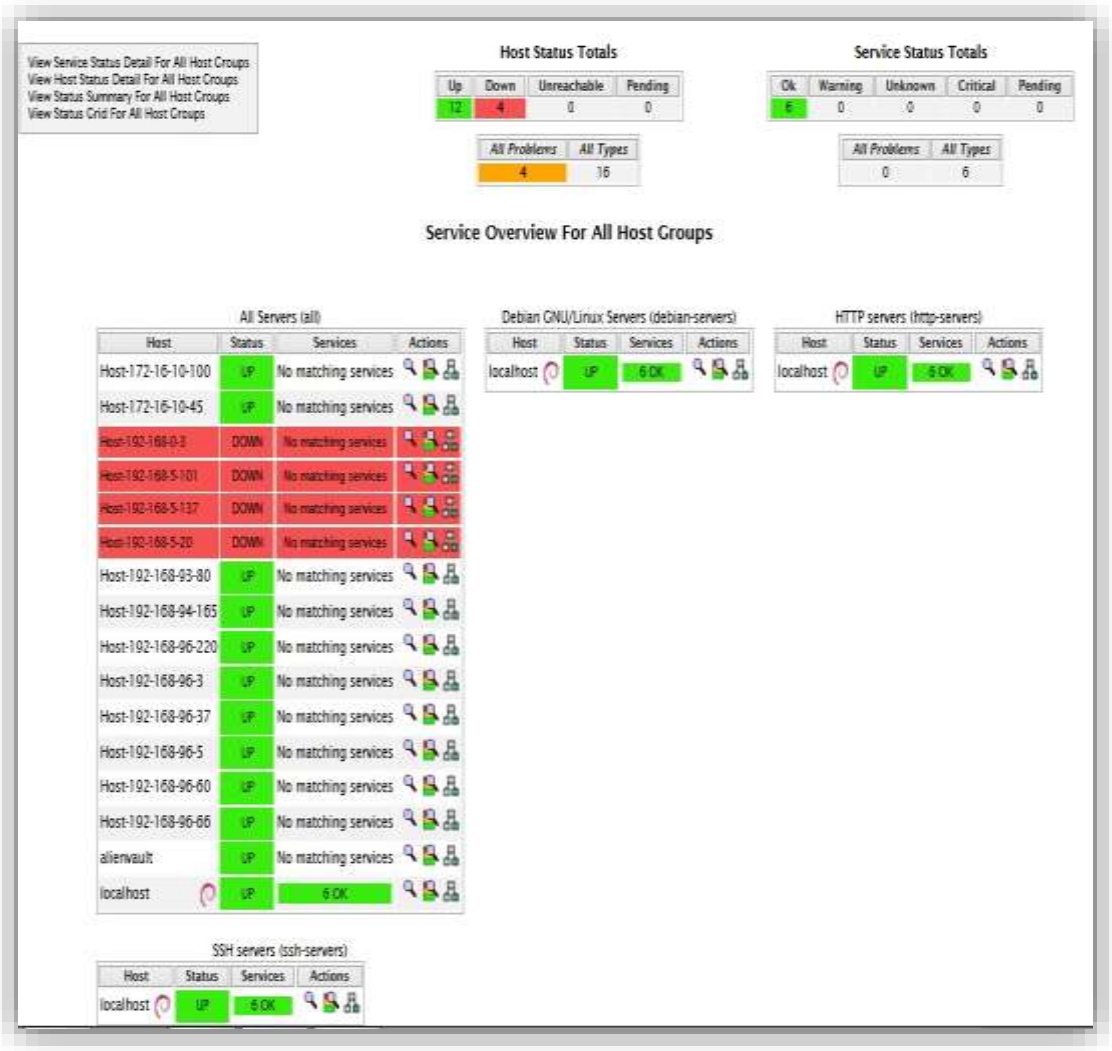
Monitores de servicios

Nagios se instala y configura automáticamente en OSSIM y esto permite ver la información básica de la red.

De los equipos y servicios de la red que se monitorizo presenta como resultado que de los 16 host analizados 4 se encuentran DOWN y es porque no estaban conectados a la red se encontraban apagados entre ellos eran laptops y pc del departamento de TI.

Los servicios HTTP, SSH y Debian GNU se encuentran UP. Si llegan a cambiar su status a DOWN y ponerse de color rojo es porque algún agente externo al servidor desactivo el servicio o existen intentos forzosos y se desactivo el servicio. Dependiendo de la configuración esto puede ser informado vía correo electrónico o envían mensajes al celular.

Figura 4.7 Consola administrativa de Nagios



Fuente: AlienVault OSSIM

NTOP

Permite visualizar todos los hosts con su respectiva información IP Address, MAC Address, nombre de equipo, protocolos que se está utilizando también muestra la cantidad de tráfico tanto de entrada como de salida y el destino de cada paquete.

Figura 4.8 Ntop - Información de host

Host Information

Traffic Unit: Bytes

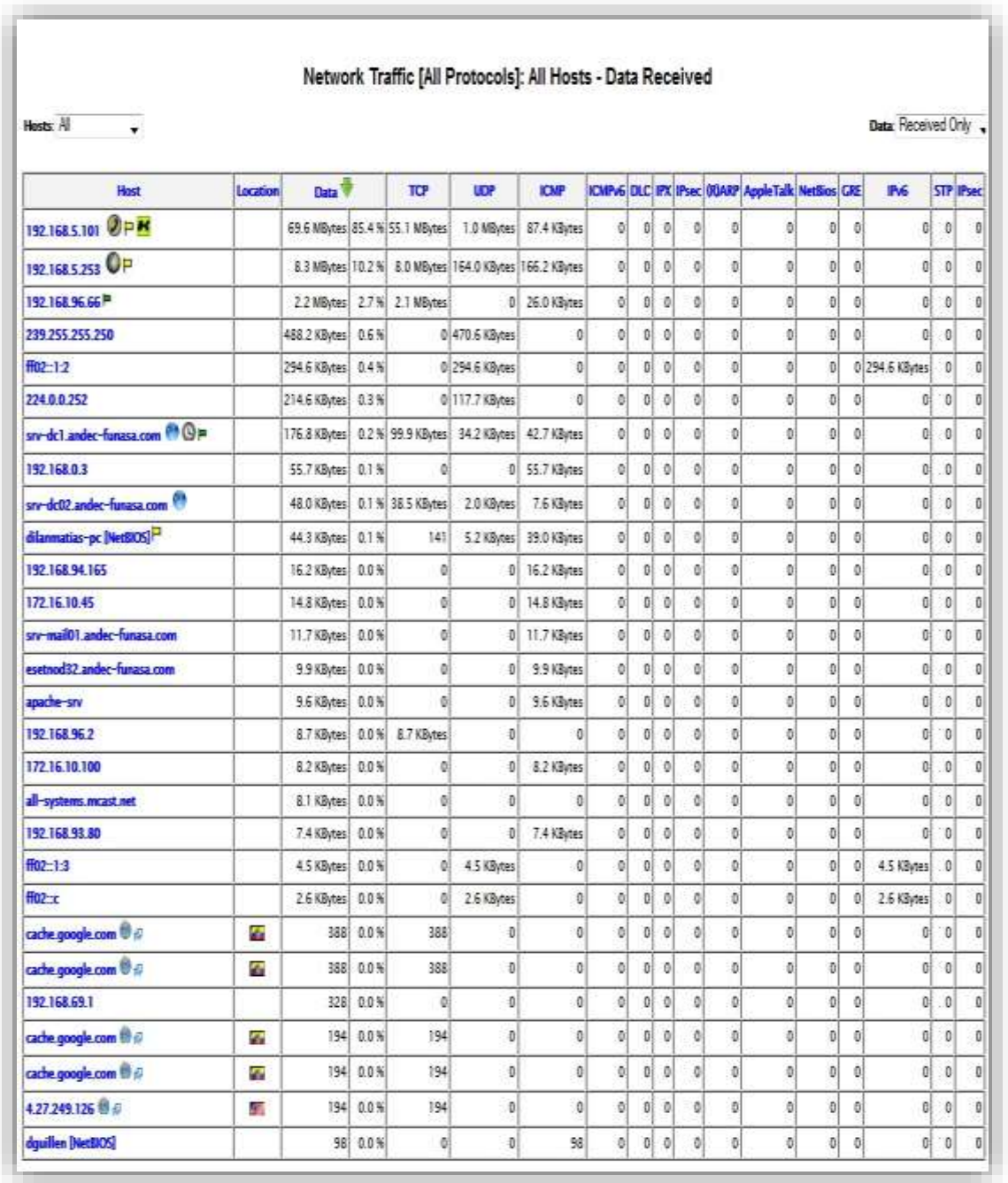
Subnet: All

Host	Location	IP Address	MAC Address	Community	Other Name(s)	Inbound vs Outbound	Nw Board Vendor	Hops Distance
192.168.5.101		192.168.5.101	2C:41:38:16:4C:16					
192.168.5.253		192.168.5.253	00:0C:29:26:81:24				VMware, Inc.	
192.168.96.66		192.168.96.66						1
239.255.255.250		239.255.255.250					LAA (Locally assigned address)	
ff02::1		ff02::1						
192.168.0.3		192.168.0.3						
ff02::2		ff02::2						
ff02::1:2		ff02::1:2						
ff02::1:3		ff02::1:3						
e_moya [NetBIOS]		192.168.5.22	00:24:E8:92:6B:4B		E_MOYA		Dell Inc.	
m_jaramillo.andec-funasa.com		192.168.5.56	2C:41:38:16:4C:ED		M_JARAMILLO			
dguillen [NetBIOS]		192.168.5.33	5C:26:0A:4A:B5:31		DGUILLEN			
dilanmatias-pc [NetBIOS]		192.168.5.137	78:2B:CB:CF:24:A9		DILANMATIAS-PC			
ff02::c		ff02::c						
ff02::16		ff02::16						
239.255.255.253		239.255.255.253					Multicast	
10.10.35.114		10.10.35.114						
all-systems.mcast.net		224.0.0.1					Multicast	
all-routers.mcast.net		224.0.0.2					LAA (Locally assigned address)	
224.0.0.252		224.0.0.252						
172.16.10.45		172.16.10.45						1
172.16.10.100		172.16.10.100						1
192.168.93.80		192.168.93.80						8
192.168.94.165		192.168.94.165						1
192.168.96.2		192.168.96.2						1
apache-srv		192.168.96.3						1
srv-dc1.andec-funasa.com		192.168.96.5						1
srv-dc02.andec-funasa.com		192.168.96.60						1
srv-mail01.andec-funasa.com		192.168.96.37						1
esetnod32.andec-funasa.com		192.168.96.220						1
ff02::1:ff19:4565		ff02::1:ff19:4565					XEROX CORPORATION	

Fuente: AlienVault OSSIM

En la sección “Data” muestra todo el tráfico de datos que reciben los hosts de la red. Descubre quien es el que consume más ancho de banda.

Figura 4.8 Ntop – Tráfico de datos recibidos



Network Traffic [All Protocols]: All Hosts - Data Received

Hosts: All

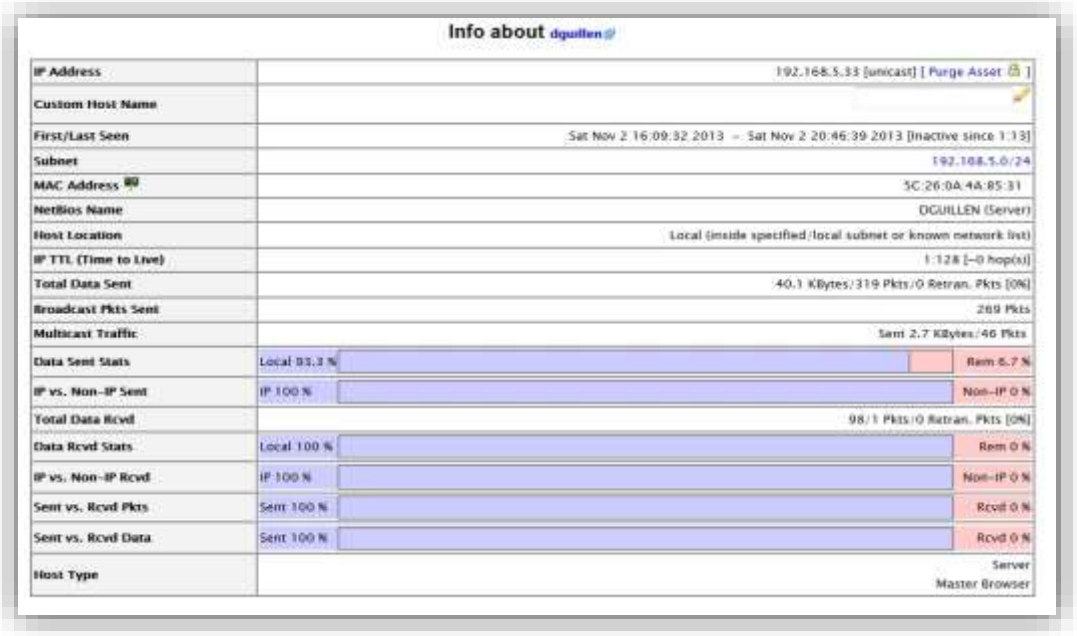
Data: Received Only

Host	Location	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	IPsec	(R)ARP	AppleTalk	NetBios	GRE	IPv6	STP	IPsec
192.168.5.101		69.6 MBytes	85.4 %	55.1 MBytes	1.0 MBytes	87.4 KBytes	0	0	0	0	0	0	0	0	0	0	0
192.168.5.253		8.3 MBytes	10.2 %	8.0 MBytes	164.0 KBytes	166.2 KBytes	0	0	0	0	0	0	0	0	0	0	0
192.168.96.66		2.2 MBytes	2.7 %	2.1 MBytes	0	26.0 KBytes	0	0	0	0	0	0	0	0	0	0	0
239.255.255.250		488.2 KBytes	0.6 %	0	470.6 KBytes	0	0	0	0	0	0	0	0	0	0	0	0
ff02::1:2		294.6 KBytes	0.4 %	0	294.6 KBytes	0	0	0	0	0	0	0	0	0	294.6 KBytes	0	0
224.0.0.252		214.6 KBytes	0.3 %	0	117.7 KBytes	0	0	0	0	0	0	0	0	0	0	0	0
srv-dc1.andec-funasa.com		176.8 KBytes	0.2 %	99.9 KBytes	34.2 KBytes	42.7 KBytes	0	0	0	0	0	0	0	0	0	0	0
192.168.0.3		55.7 KBytes	0.1 %	0	0	55.7 KBytes	0	0	0	0	0	0	0	0	0	0	0
srv-dc02.andec-funasa.com		48.0 KBytes	0.1 %	38.5 KBytes	2.0 KBytes	7.6 KBytes	0	0	0	0	0	0	0	0	0	0	0
dilanmatias-pc [NetBIOS]		44.3 KBytes	0.1 %	141	5.2 KBytes	39.0 KBytes	0	0	0	0	0	0	0	0	0	0	0
192.168.94.165		16.2 KBytes	0.0 %	0	0	16.2 KBytes	0	0	0	0	0	0	0	0	0	0	0
172.16.10.45		14.8 KBytes	0.0 %	0	0	14.8 KBytes	0	0	0	0	0	0	0	0	0	0	0
srv-mail01.andec-funasa.com		11.7 KBytes	0.0 %	0	0	11.7 KBytes	0	0	0	0	0	0	0	0	0	0	0
esetnod32.andec-funasa.com		9.9 KBytes	0.0 %	0	0	9.9 KBytes	0	0	0	0	0	0	0	0	0	0	0
apache-srv		9.6 KBytes	0.0 %	0	0	9.6 KBytes	0	0	0	0	0	0	0	0	0	0	0
192.168.96.2		8.7 KBytes	0.0 %	8.7 KBytes	0	0	0	0	0	0	0	0	0	0	0	0	0
172.16.10.100		8.2 KBytes	0.0 %	0	0	8.2 KBytes	0	0	0	0	0	0	0	0	0	0	0
all-systems.mcast.net		8.1 KBytes	0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.93.80		7.4 KBytes	0.0 %	0	0	7.4 KBytes	0	0	0	0	0	0	0	0	0	0	0
ff02::1:3		4.5 KBytes	0.0 %	0	4.5 KBytes	0	0	0	0	0	0	0	0	0	4.5 KBytes	0	0
ff02::c		2.6 KBytes	0.0 %	0	2.6 KBytes	0	0	0	0	0	0	0	0	0	2.6 KBytes	0	0
cache.google.com		388	0.0 %	388	0	0	0	0	0	0	0	0	0	0	0	0	0
cache.google.com		388	0.0 %	388	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.69.1		328	0.0 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0
cache.google.com		194	0.0 %	194	0	0	0	0	0	0	0	0	0	0	0	0	0
cache.google.com		194	0.0 %	194	0	0	0	0	0	0	0	0	0	0	0	0	0
4.27.249.126		194	0.0 %	194	0	0	0	0	0	0	0	0	0	0	0	0	0
dguillen [NetBIOS]		98	0.0 %	0	0	98	0	0	0	0	0	0	0	0	0	0	0

Fuente: AlientVault OSSIM

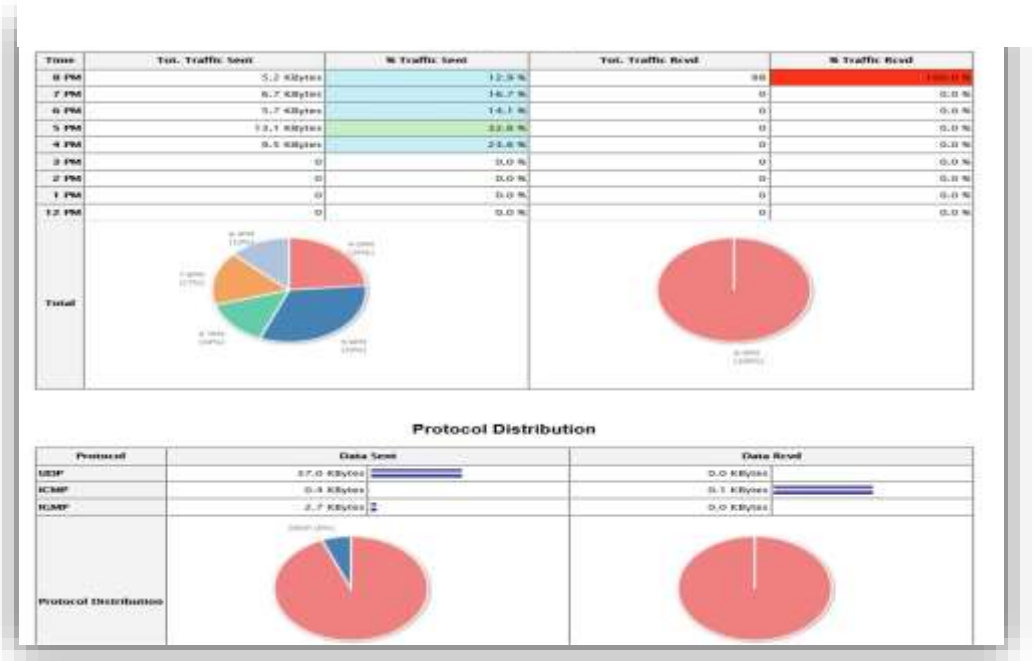
Se puede obtener las estadísticas detalladas de un host específico que Ntop ha recopilado.

Figura 4.9 Información recogida por Ntop de un host específico



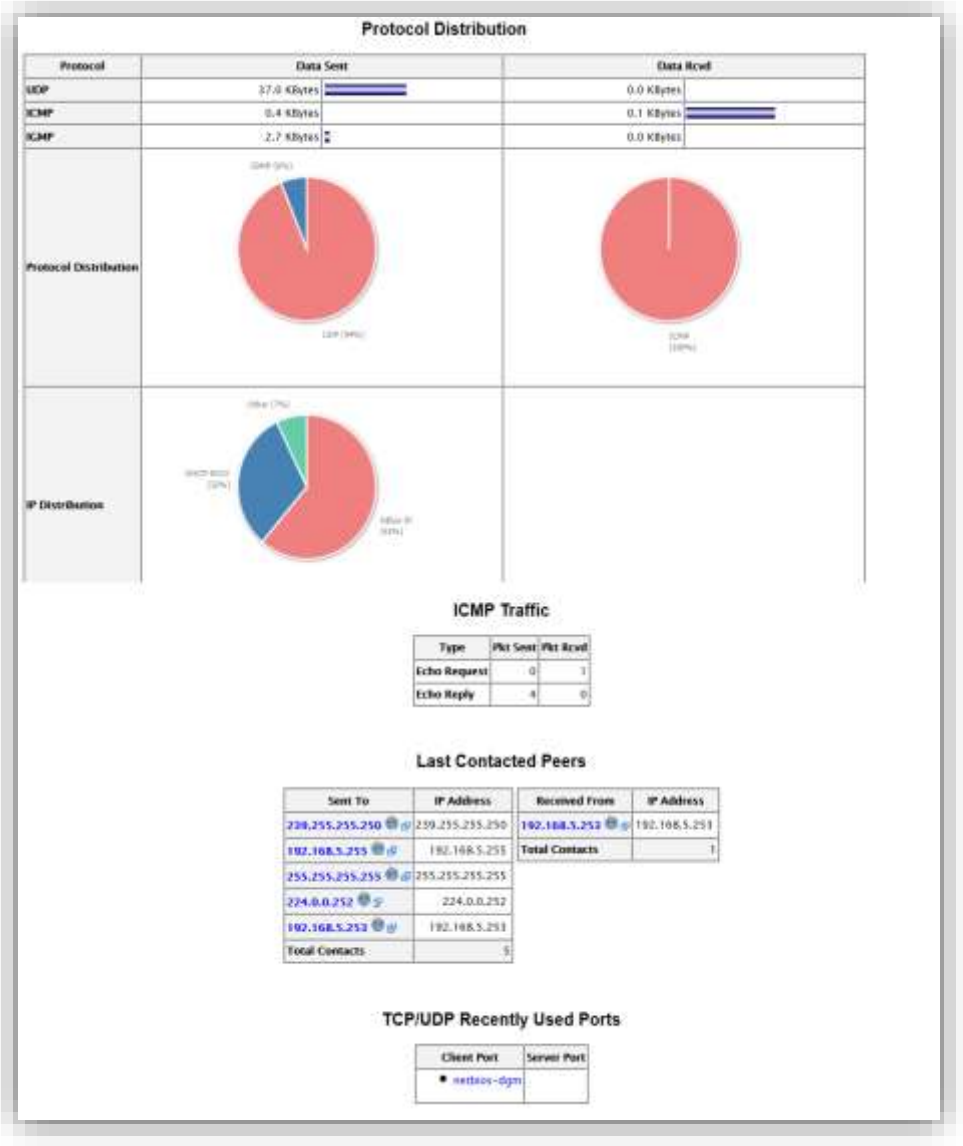
Fuente: AlienVault OSSIM

Figura 4.10 Estadísticas del Tráfico del Host



Fuente: AlienVault OSSIM

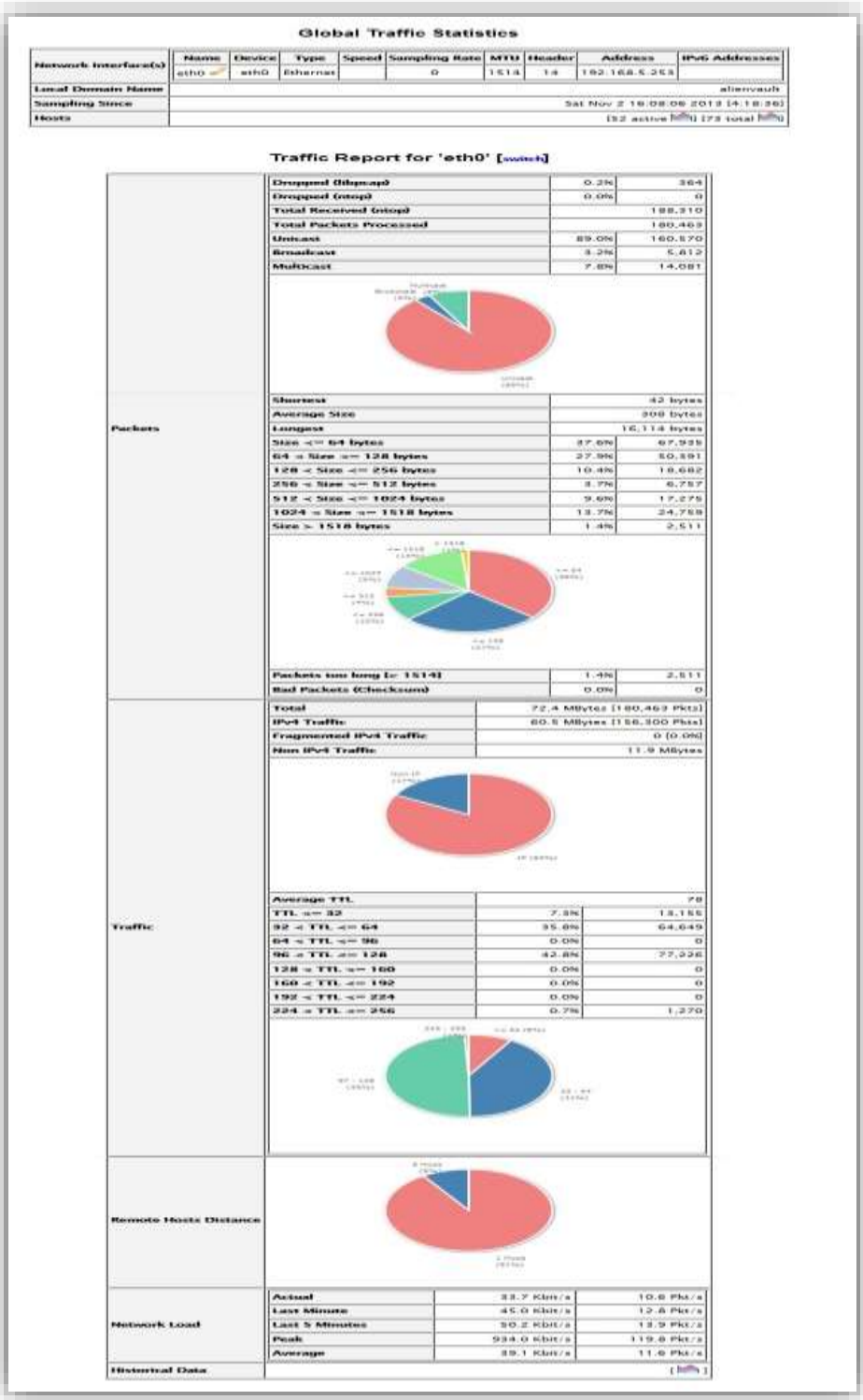
Figura 4.11 Cuadros estadísticos de los protocolos utilizados por el host específico



Fuente: AlienVault OSSIM

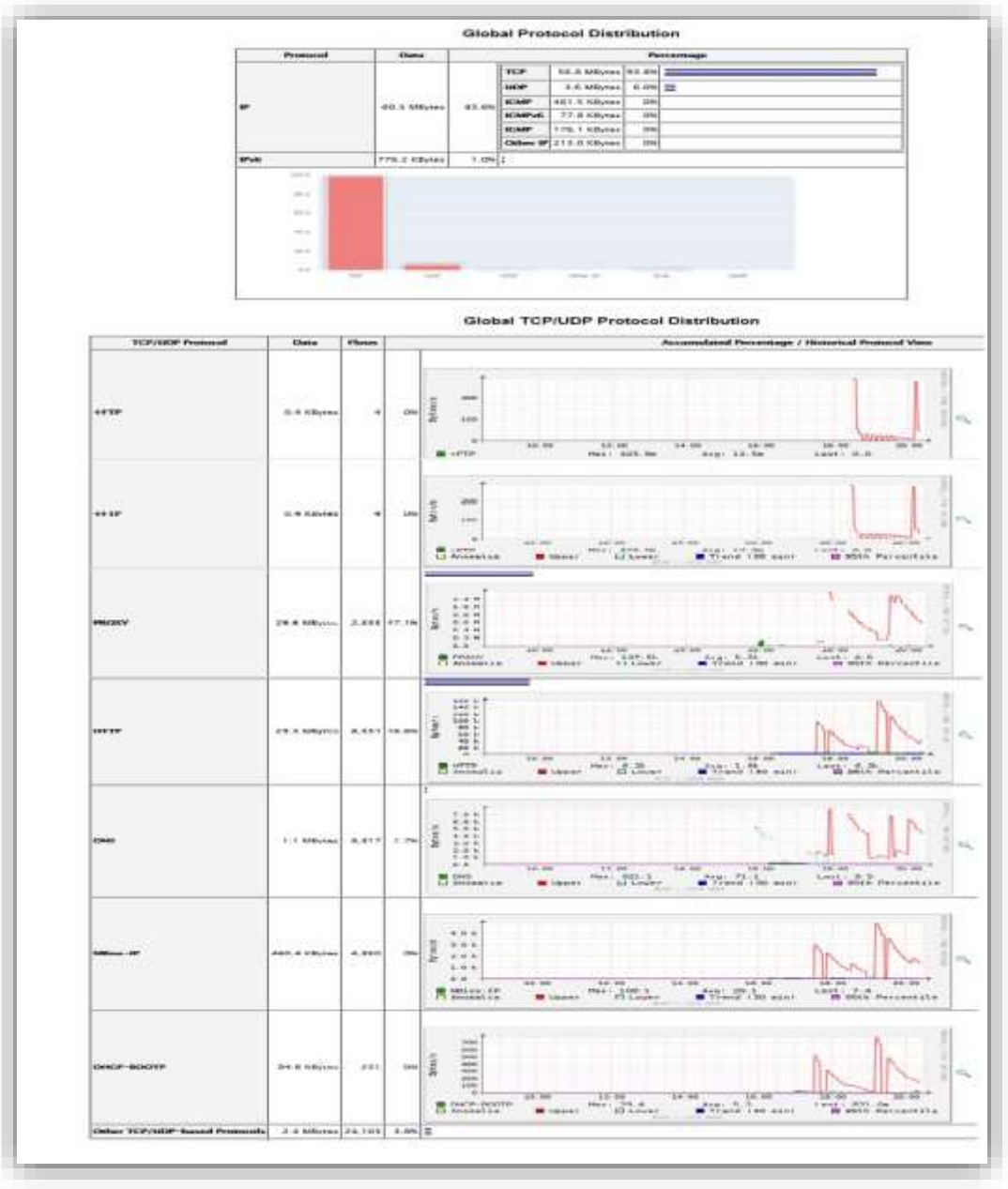
La consola de administración de Ntop se instala por defecto en cada uno de los sensores que componen el servidor AlienVault. En esta sección vemos que se analizan 52 hosts y están activos, el método de transmisión utilizado es el Unicast ya que él envió de datos se realiza desde un servidor a un grupo de host de la LAN. Muestra cuadros estadísticos de los tipos de protocolos que están.

Figura 4.12 Consola de administración de Ntop



Fuente: AlienVault OSSIM

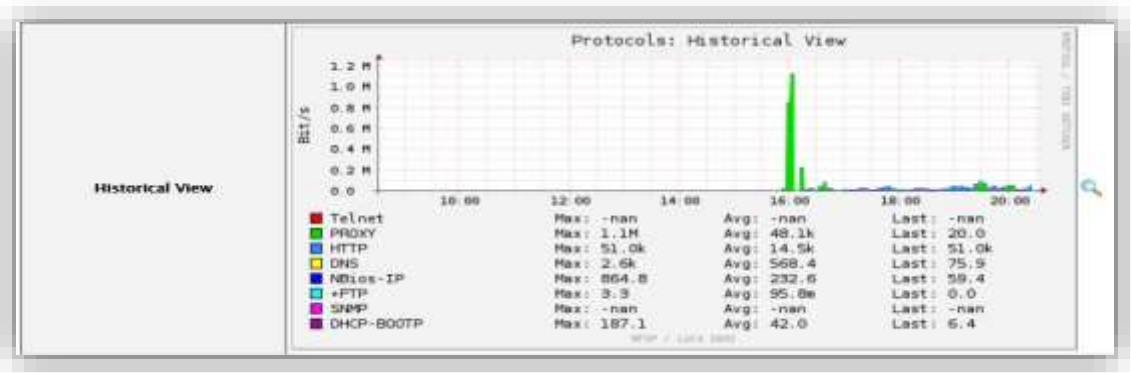
Figura 4.13 Distribución global de protocolo



Fuente: AlienVault OSSIM

Muestra el historial de tráfico de red de la empresa dividido por protocolo donde se visualiza que el más utilizado es el Proxy.

Figura 4. 14 Vista histórica del tráfico de red



Fuente: AlienVault OSSIM

Monitor de tráfico

En esta sección se observa el monitoreo en tiempo real de los protocolos TCP, UDP e ICMP que vienen por defecto en la instalación de OSSIM. La vista predeterminada proveniente de la herramienta Nfsen muestran el perfil por defecto (Live) y muestra el histórico de "flujos", "paquetes" y "bytes".Todos estos protocolos a partir de las 5:00 pm disminuyen en él envió de paquetes ya que muchos de los departamentos terminan sus actividades diarias.

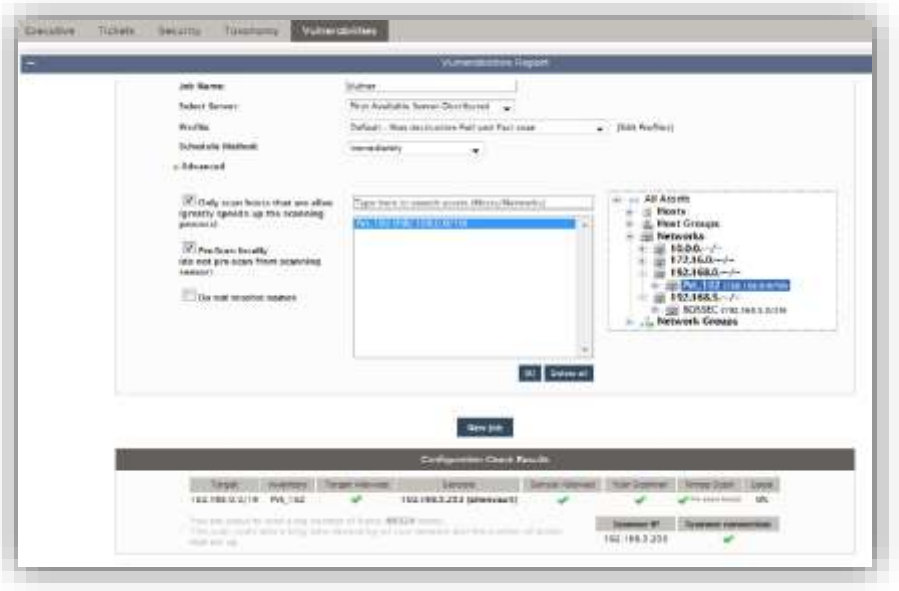
Figura 4. 15 Monitorización de tráfico en la red

Fuente: AlienVault OSSIM

Monitor de vulnerabilidad

Para realizar el análisis de vulnerabilidad con Openvas se escoge la red que se desea examinar luego aparece la configuración para realizar el escáner y presentar los resultados.

Figura 4. 16 Reporte de Vulnerabilidad Openvas

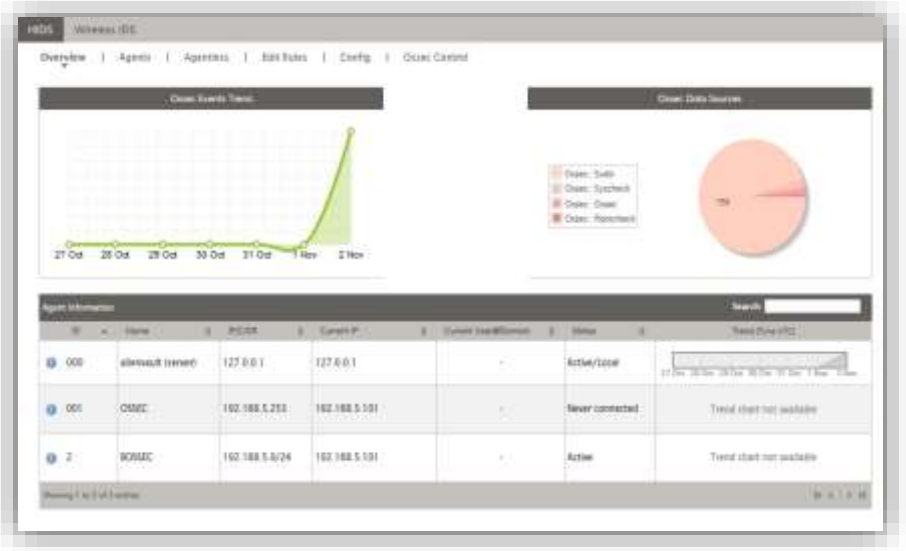


Fuente: AlienVault OSSIM

HIDS

Toda la información que es recogida por los sensores HIDS se muestra en la siguiente pantalla. El agente OSSEC se encuentra activo y listo para recoger los eventos que se generan, se observa que a partir de la instalación en cada equipo se genera una gráfica de forma ascendente de los eventos.

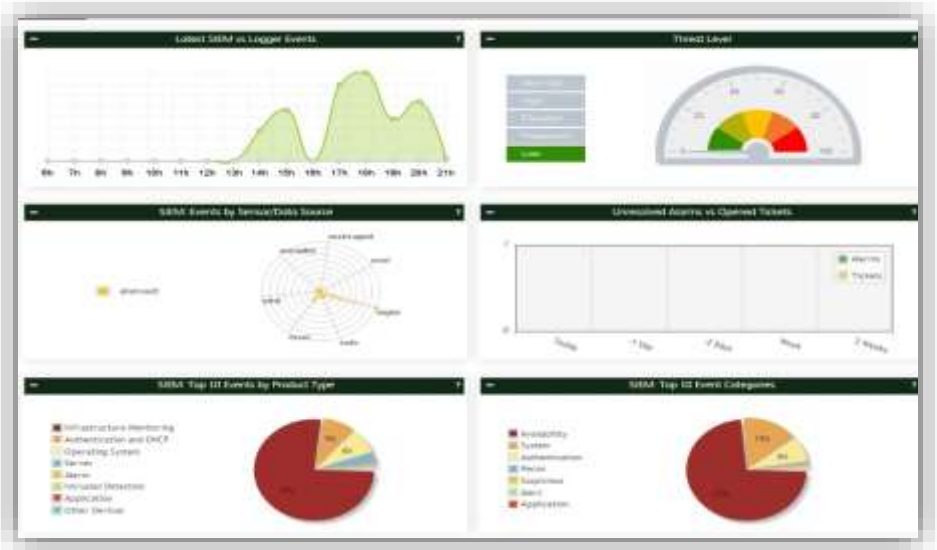
Figura 4.17 HIDS



Fuente: AlienVault OSSIM

En esta parte se muestra que sensores OSSEC y Nagios estan recogiendo la información, se observa que el 76% de la infraestructura está siendo analizada y con disponibilidad por ende su nivel de amenaza es bajo.

Figura 4.18 Interfaz Gráfica de OSSIM



Fuente: AlienVault OSSIM

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Se identificaron 15 diferentes riesgos de las cuales podrían afectar a 18 procesos críticos de la empresa. Para cada riesgo se seleccionaron los controles adecuados referentes a la norma IS0 27001, explicando su objetivo y el control a seguir.

Se propone un plan de contingencias para el área de TI tratando de prevenir las situaciones por las cuales se pudiera presentar un siniestro que signifique una paralización de las operaciones informáticas, con sus consecuentes pérdidas.

OSSIM provee un motor de correlación basado en el uso de directivas lógicas que ayudan a determinar el riesgo de un ataque en la red con detallados niveles de interfaces de visualización y generando reportes.

Al basarse en la tecnología SIEM, OSSIM aporta una serie de capacidades añadidas, como la monitorización y la detección de amenazas en tiempo real, de forma conjunta y en un único framework sin invertir mucho dinero.

Al no detectar vulnerabilidades en el tiempo que se realizó el escaneo se dejó un archivo en la empresa con la configuración y la explicación de todo el sistema de seguridad.

5.2 Recomendaciones

Para tener una mejor seguridad de la información, la empresa deberá aplicar los controles seleccionados para cada riesgo encontrado.
Así mismo la política SGSI que se propone deberá ser aplicada y regularizada por la empresa industrial, para que esta sea conocida por todo el personal, se obtendría así una robusta seguridad del activo más importante para la empresa “La información”

OSSIM por ser una plataforma muy compleja requiere como mínimo en una máquina 4 GB de RAM. Se aumenta la memoria RAM dependiendo del rendimiento de la red, el número de eventos que el servidor AlienVault procese y la cantidad de datos que se almacene en la base de datos. La versión de AlienVault profesional solo se ejecuta en procesadores de 64 bits.

Todas las configuraciones del sistema y políticas se deben realizar con la persona encargada de la seguridad de la red de la empresa o el administrador.

Bibliografía

Concepto de un SGSI. (2002). Obtenido de

http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Concepto_SGSI/

OSSIM. (10 de 21 de 2003). Obtenido de Descripción General del Sistema :

https://www.alienvault.com/docs/OSSIM-desc-es.pdf

DestacaDos SGSI. (2005). Obtenido de El portal de ISO 27001 en Español:

http://www.iso27000.es/sgsi.html

Canaima MetaDistribución GNU/LINUX. (17 de 11 de 2008). Obtenido de OSSIM:

http://radio.gnu.org.ve/wiki/Ossim

El protocolo UDP. (21 de 08 de 2009). Obtenido de

http://laclaveadsi.blogspot.com/2009/08/el-proctocolo-udp.html

Info Seguridad . (14 de 09 de 2010). Obtenido de OSSIM:

http://inforleon.blogspot.com/2010/09/ossim.html

It Freek Zone . (15 de 06 de 2010). Obtenido de Monitoreo de red: OSSIM Review Parte I (OSSIM, Snort y OSSEC): http://itfreekzone.blogspot.com/2010/06/monitoreo-de-red-ossim-review-parte-i.html

Los logs. (2011). Obtenido de http://www.desarrolloweb.com/faq/408.php

Agente Software. (11 de 12 de 2013). Obtenido de Fundación Wikimedia, Inc :

http://es.wikipedia.org/wiki/Agente_(software)

Comment Installer/ Configurer NTOP. (14 de 07 de 2013). Obtenido de

http://www.opendoc.net/solutions/comment-installer-configurer-ntop

AlienVault. (2014). Obtenido de OSSIM: http://www.alienvault.com/open-threat-exchange/projects

Alfon. (19 de 08 de 2003). *Sistema de detección de intrusos y Snort* . Obtenido de http://www.maestrosdelweb.com/snort/

Alvarez Orozco , J., Cuevaz, N., & Moyano, L. (28 de 08 de 2012). *Redes de computadoras*. Obtenido de Instalación y configuración de OSSIM: http://networkadmin.blogspot.es/

Amutio Gómez, M. (10 de 2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf

Areitio Bertolín, J. (2008). Seguridad de la Información Redes, informática y sistemas de información. Madrid .

Barraco , L. (13 de 03 de 2014). *AlienVault Technical Glossary*. Obtenido de https://alienvault.bloomfire.com/posts/672507-alienvault-technical-glossary/public

Benjumea Gómez, O. (10 de 2009). *Gestión de eventos de seguridad*. Obtenido de http://www.revistadintel.es/Revista/Numeros/Numero2/Empresarial/benjumea.pdf

Bowlig, J. (01 de 05 de 2010). *AlienVault: the Future of Security Information Management*. Obtenido de http://www.linuxjournal.com/magazine/alienvault-future-security-information-management

Cano, F. (2014). Obtenido de http://www.seinhe.com/blog/109-gestion-de-vulnerabilidades-de-seguridad-a-traves-de-openvas-y-ossim

del Barrio, D. (s.f.). *Aprende APACHE HTTP SERVER Y DNS (Bind) ejemplos 100%*. Obtenido de http://books.google.com.ec/books?id=tOyqFq8N_B8C&printsec=frontcover&dq=dns&hl=es&sa=X&ei=Tm45VNXoIe7LsATp9oJY&ved=0CCgQ6AEwAg#v=onepage&q&f=false

Edukavital. (s.f.). *Plugin su definicion y conceptos* . Obtenido de http://edukavital.blogspot.com/2013/05/plugin-definicion-de-plugin-concepto-de.html

Eumed.net. (s.f.). Obtenido de Introducción a la metodología de la investigación : http://www.eumed.net/libros/2006c/203/1t.htm

García , I., Cerquera , Y., & Bedoya , J. (24 de 10 de 2013). *Trabajo colaborativo OSSIM* . Obtenido de http://20101407tc1ossim.blogspot.com/

Gutierrez Cervantes, X. (s.f.). *Fuentes primarias y secundarias en un trabajo de investigación*. Obtenido de http://www.ehowenespanol.com/fuentes-primarias-secundarias-investigacion-info_354586/

IGMP Protocolos. (s.f.). Obtenido de http://ordenador.wingwit.com/Redes/internet-networking/68631.html#.VDnP3md5M08

Instituto Nacional de Estadística e Informática. (1997). Obtenido de ASPECTOS GENERALES DE LA SEGURIDAD DE LA INFORMACION: http://www.ongei.gob.pe/publica/metodologias/lib5007/21.htm

ISO 27001 Security . (s.f.). Obtenido de http://www.27001-online.com/

Kioskea ES. (10 de 2014). *Protocolo TCP*. Obtenido de http://es.kioskea.net/contents/281-protocolo-tcp

Kioskea ES. (s.f.). *El protocolo ICMP*. Obtenido de http://es.kioskea.net/contents/265-el-protocolo-icmp

Landeau, R. (2007). Elaboración de trabajos de investigación. Caracas: Alfa.

Logisman. (23 de 08 de 2011). *Familia ISO 27000: Seguridad de la Información*. Obtenido de Logisman: http://custodia-documental.com/familia-iso-27000-seguridad-de-la-informacion/

López Neira , A., & Ruiz Spohr, J. (2012). *El portal de ISO 27001 en Español*. Obtenido de ISO 27000.ES: http://www.iso27000.es/iso27000.html

MAGERIT . (s.f.). Obtenido de 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#.VBYDL8J5NCY

Martinez Cobo, P., Cabello Requema, M., & Díaz Martín, J. (1997). *Sistemas Operativos Teoría y Práctica.* Obtenido de http://books.google.com.ec/books?id=wXzwFPaVku0C&pg=PA1&dq=sistema+operativo&hl=es&sa=X&ei=YJhBVPLuBcfAggSl94DIDQ&ved=0CBoQ6AEwAA#v=onepage&q=sistema%20operativo&f=false

Moreno, L. (11 de 10 de 2010). *Métodos de Investigación*. Obtenido de Metodo Inductivo: http://luceromoreno.wikispaces.com/luceromoreno

Nacx. (2014). *Demonios*. Obtenido de http://www.adslayuda.com/Linux-demonios.html

Namakforoosh, M. N. (2005). Metodología de la investigación . Mexico: Limusa.

Primo Guijarro, Á. (20 de 10 de 2011). *DHCP*. Obtenido de http://alvaroprimoguijarro.files.wordpress.com/2011/10/dhcp.pdf

Ramírez Martínez, G. (11 de 2004). *Desempeño organizacional retos y enfoque contemporáneos*. Obtenido de http://books.google.com.ec/books?id=fpf7g2PhY6MC&pg=PA268&dq=sistema+de+deteccion+de+intrusos&hl=es&sa=X&ei=0hE-VLOAOcLIgwS7iYLQDQ&ved=0CBoQ6AEwAA#v=onepage&q=sistema%20de%20deteccion%20de%20intrusos&f=false

Ruiz Limón , R. (2006). *HISTORIA Y EVOLUCIÓN DEL PENSAMIENTO CIENTÍFICO*. Obtenido de Método Analítico: http://www.eumed.net/libros-gratis/2007a/257/7.1.htm

Seguridad de la Información . (s.f.). Obtenido de http://www.sisteseg.com/informatica.html

Tenorio Martinez, M. M. (14 de 08 de 2009). *MANUAL DE OSSIM*.

Torres Manrique, M., & Villegas Oliveros , D. (15 de 12 de 2010). *INTEGRACIÓN DE OSSIM Y UNTANGLE*. Obtenido de http://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/76599/1/integracion_ossim_untangle.pdf

Urrutia Fuentealba , G. (17 de 05 de 2013). *Protocolos HTTP, HTTPS y VPN*. Obtenido de http://prezi.com/jhsld65zlsft/untitled-prezi/

Valbuena, J. (31 de 05 de 2013). *Servidor Proxy*. Obtenido de http://prezi.com/ucjbkifmccqp/untitled-prezi/

Wikipedia . (24 de 08 de 2014). *Interfaz gráfica de usuario*. Obtenido de http://es.wikipedia.org/wiki/Interfaz_gr%C3%A1fica_de_usuario

Wikipedia. (26 de 09 de 2014). *Transferencia de archivos*. Obtenido de http://es.wikipedia.org/wiki/Transferencia_de_archivos

WordPress.com. (09 de 09 de 2009). *El Terminal, esa temida y desconocida herramienta.* Obtenido de http://macdrid.wordpress.com/2009/09/09/el-terminal-esa-temida-y-desconocida-herramienta/

Zapata, O. (2005). *Herramientas para elaborar tesis e investigaciones socieducativas*. Obtenido de http://books.google.com.ec/books?id=i339_F3C1RIC&pg=PA189&lpg=PA189&dq=como+un+conjunto+de+t%C3%A9cnicas+destinadas+a+reunirse,+de+manera+sistem%C3%A1tica,+datos+sobre+determinado+tema,+a+trav%C3%A9s+de+contactos+directos+o+indirectos+con+los+individuos+q

ANEXOS