UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

Trabajo de fin de carrera titulado:

DISEÑO DE UN PLAN DE SEGURIDAD PARA LA RED DE DATOS DE LA EMPRESA NEUMAC S.A.

Realizado por:

RAISA SAMARA GRUEZO VÉLEZ

Como requisito para la obtención del título de:
INGENIERO EN SISTEMAS EN TELECOMUNICACIONES

QUITO, SEPTIEMBRE DE 2010

DECLARACIÓN JURAMENTADA

Yo Raisa Samara Gruezo Vélez, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

……

Raisa Samara Gruezo Vélez.

DECLARATORIA

El presente trabajo de investigación de fin de carrera titulado

DISEÑO DE UN PLAN DE SEGURIDAD PARA LA RED DE DATOS DE LA EMPRESA NEUMAC S.A.

Realizado por el alumno

RAISA SAMARA GRUEZO VÉLEZ

Como requisito para la obtención del título de

INGENIERO EN SISTEMAS EN TELECOMUNICACIONES

Ha sido dirigido por el profesor

ING. FRANKIE ERIKSON CATOTA

quien considera que constituye un trabajo original de su autor.

……..

DIRECTOR

Los profesores informantes

Ing. VIVIANA GUERRÓN SIERRA, e

Ing. ADRIANA ABAD

después de revisar el trabajo escrito presentado,

lo han calificado como apto para su defensa oral ante el tribunal examinador.

…….. ……

Ing. VIVIANA GUERRÓN S. Ing. ADRIANA ABAD

Quito, a 17 de Septiembre de 2010

Dedicatoria y Agradecimiento

El desarrollo y finalización de este proyecto de tesis, no hubiese sido posible sin la ayuda e intervención de las personas que citaré a continuación:

A DIOS, mi señor y salvador por ser mi guía y fortaleza en cada batalla, por permitirme lograr una más de mis metas trazadas, y no dejarme decaer o perder la fe.

A mis padres, por todo su amor, comprensión, apoyo, dedicación y ejemplo, los cuales me sostienen y me ayudan a continuar creciendo y adquiriendo experiencia en cada paso dado.

A mi hermana por creer en mí, por su cariño y admiración, por ser mi guía, llenando de inspiración y alegrías mi vida.

A ti, mi razón, mi fuerza, el ser que con amor llena de motivos mi vida, aceptándome como soy, sin dejarme sola en mis errores y apoyándome en cada una de mis decisiones.

Un agradecimiento especial a mi tutor, por su tiempo y esfuerzo empleado, y por cada uno de sus consejos y recomendaciones, los cuales permitieron desarrollar satisfactoriamente este proyecto de tesis.

A todos mis profesores y maestros por los conocimientos impartidos durante los cinco años de carrera universitaria.

A mis amigos y resto de familiares, por su apoyo y cariño sincero, razón para seguir adelante.

Abstracto

El presente trabaja está estructurado en cinco capítulos. Cada capítulo describe el proceso de desarrollo que se cumplió para la culminación del mismo. Además, se ha incluido una sección de anexos, relacionados con algunos capítulos, donde se puede encontrar información más detallada, que ayude a comprender mejor el contenido de algunas partes de la tesis.

El Capítulo 1, contiene la introducción general, la descripción y justificación de problema, objetivos generales y específicos de la tesis que son la base para el desarrollo de la misma, adicionalmente este capítulo indica el alcance del proyecto y el diseño metodológico a emplear. El Capítulo 2, encierra todos los conceptos básicos e importantes que formarán parte de la investigación como un marco de referencia para las demás personas no involucras en el trabajo de tesis. El Capítulo 3, abarca el análisis de la red de datos de la empresa, a través de un levantamiento exhaustivo de los activos de información que posee, categorizados en ocho grupos: hardware, software, comunicaciones, servicios de red, información, personas, procesos y red, haciendo hincapié en este último, a detalle en su arquitectura, topología, y extensión. El Capítulo 4, contiene un inventario consolidado de todos los ítems de activos de información que dispone la empresa, una estimación del riesgo de cada grupo de activo en base al grado de confidencialidad, integridad y disponibilidad, y la búsqueda de vulnerabilidades que presenta la red de datos de la empresa. Finalmente el Capítulo 5, comprende ocho dominios o áreas de gestión de seguridad basadas en la norma ISO/IEC 27002:2005, que contienen medidas que se deberán emplear para conseguir seguridad en la información y elementos informáticos de la compañía, y así conseguir reducir el riesgo.

Al final del documento se proporcionan conclusiones y recomendaciones obtenidas durante el desarrollo del trabajo.

Abstract

This work is structured in five chapters. Each chapter describes the development process was accomplished for the completion of it. In addition, we have included a section of appendices relating to certain chapters, where you can find more detailed information that will help to better understand the content of some parts of the thesis.

Chapter 1 contains a general introduction, description and justification of the problem, general and specific objectives of the thesis, whose are the basis for the development of it, this chapter suggests further the project scope and design methodology to be used. Chapter 2 contains all the basic and important concepts that will be part of the research as a framework for the other person not involved in the thesis. Chapter 3 covers the analysis of the data network of the company, through a comprehensive survey of information assets they have, categorized into eight groups: hardware, software, communications, network services, information, people, processes and network with emphasis on the latter, in detail in its architecture, topology, and extension. Chapter 4 contains a consolidated inventory of all items of information assets available to the company, the estimated risk of each asset group based on degree of confidentiality, integrity and availability, and the search for vulnerabilities that the network Company data presents. Finally, Chapter 5, comprises eight domains or areas of safety management based on ISO / IEC 27002:2005, which contain measures to be used to allow information security and computer elements of the company, and thus reduced the risk.

At the end of the document provides conclusions and recommendations obtained during the course of work.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

Capítulo 1

1. DISEÑO CONCEPTUAL DE LA INVESTIGACIÓN

1.1 DEFINICIÓN DEL TEMA

Diseño de un Plan de Seguridad para la red de datos de la empresa Neumac S.A.

1.2 ANTECEDENTES Y DEFINICIÓN DEL PROBLEMA

Neumac S.A., se constituyó el 13 de Agosto de 1994, en una empresa dedicada a servir la industria en general, con maquinaria de equipo móvil, para la construcción, y agrícola. Ubicada en la Av. Eloy Alfaro S/N y calle Enrique portilla, cuenta con sucursales en USA, Colombia, Panamá, Perú, siendo la matriz en Ecuador.

La importación, reconstrucción, venta y servicio de unidades e instrumentos hidráulicos y neumáticos, constituyen la misión de la empresa; dichas actividades se las realiza a través de catálogos, mostrador, portal web, y vía e-mails. Debido a la gran cantidad de información que maneja la empresa, y la gran exposición al público de este recurso, ha sido víctima de ataques a su red, produciendo problemas de pérdidas de información o de intrusión.

La ausencia de un nivel de seguridad de información efectivo dentro de la empresa, provoca que sus TICs no sean confiables, además de carencias en la protección para el hardware y la autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Es notable, que no es un tema de máxima prioridad para esta compañía. Por ello es necesario, crear una cultura informática, para que tanto directivos y empleados de la empresa, sean responsables de los datos e información del negocio, contando con un sistema de seguridad y respaldo.

Existen varios paradigmas sobre el uso de seguridad dentro de las redes, habitualmente se creé que los procedimientos de seguridad son responsabilidad del personal de los departamentos de sistemas y telecomunicaciones, pero se debe cambiar este paradigma y conocer que estas son responsabilidades del usuario y de la organización en general.

De esta forma, es conveniente diseñar un plan de seguridad para proteger la red de datos de la empresa, una vez definido el grado de riesgo de cada activo, se debe elaborar una lista de las tecnologías de información y comunicación con las medidas preventivas que se deben tomar y las correctivas si se presenta un ataque, señalando la prioridad de cada uno.

1.2. JUSTIFICACIÓN E IMPORTANCIA DEL PROBLEMA

La información es hoy en día uno de los activos más importantes con los que cuenta cualquier organización pública y privada; un activo que no siempre tiene la consideración e importancia necesaria dentro de algunas empresas. Entre mayor es el flujo de información que maneja determinada entidad, mayor es el interés de mantener la seguridad en la red, por lo tanto, es relevante la seguridad de la información.

Con los adelantos tecnológicos actuales, sobre todo en las tecnologías de información y comunicación, es casi imposible que una empresa no haga uso de la información para el desarrollo de sus actividades cotidianas. Antiguamente toda la información era almacenada en papel, por lo que toda su seguridad se limitaba a una seguridad física, sin embargo actualmente existen multitud de dispositivos en los que se puede almacenar la información, por lo tanto la forma de evitar accesos a esa información ha cambiado.

La seguridad no es solamente el implementar usuarios y contraseñas, es el implementar políticas que garanticen la seguridad tanto física como lógica de la información. Dentro del entorno de la red se debe asegurar la privacidad de la información y de proteger las operaciones de daños no intencionados como deliberados.

La planificación de la seguridad, en el diseño de la red, es de suma importancia ya que de esto depende el buen desempeño de la misma. Es necesario concienciar a las empresas, sobre la importancia que tiene la seguridad de su información dentro de los procesos de negocio,

puesto que una pérdida de información puede comprometer datos que en algunos casos podrían llegar a evidenciarse como pérdidas millonarias para las empresas.

En ocasiones el tema de seguridad es presentado como fuera de presupuesto y de prioridad baja, por lo que es fundamental asumir una cultura informática en las organizaciones, de esta manera permitir condiciones necesarias para que la red de datos logre los objetivos de la empresa.

Por estas razones, la empresa NEUMAC S.A – Ecuador, tomo la decisión de diseñar un plan de seguridad para su red de datos, estableciendo políticas y medidas de seguridad para sus activos, dando énfasis a la información, y manteniendo un seguimiento continuo del desarrollo del mismo.

1.3 OBJETIVOS

1.3.1 General

Diseñar un Plan de Seguridad para la red de datos de la empresa NEUMAC S.A. - Ecuador; que permita proteger la confidencialidad, integridad, y disponibilidad de la información durante su procesamiento, distribución y almacenamiento.

1.3.2 Específicos

- Diagnosticar el estado de funcionamiento actual de la red de información de la empresa.
- Realizar un levantamiento de los activos de información de la red.
- Identificar y estimar los riesgos de los activos de la red de datos, en base a criterios de confidencialidad, integridad y disponibilidad.
- Establecer amenazas tecnológicas y humanas a las que se expone la información.
- Identificar vulnerabilidades en los activos de información dentro de la organización.
- Aplicar ocho dominios de seguridad de la norma ISO/IEC 27002:2005.
- Diseñar un plan de seguridad desglosado en tres etapas en base a las vulnerabilidades encontradas en la red de la empresa, categorizadas en altas, medias y bajas.
- Plantear políticas de seguridad que se encuentre alineadas a los objetivos del negocio.
- Estructurar procedimientos y normas de seguridad para proteger cada uno de los activos de la organización.

1.4 DELIMITACIÓN DEL TEMA

El diseño del plan de seguridad, se limitará al análisis de la red de datos de la empresa NEUMAC S.A. – matriz Ecuador, ubicada en la ciudad de Quito; incluyendo hardware, software, comunicaciones, red, personas, procesos, servicios de red e información que posea.

El plan de seguridad, basará su estructura en políticas, controles y medidas de prevención y corrección de posibles riesgos a los activos de la empresa; además de proteger la confidencialidad, disponibilidad e integridad de la información y datos que maneja la compañía.

1.5 MARCO TEÓRICO

1.5.1 Análisis del estado actual de la red de la empresa

La infraestructura de una red de datos, es la parte más importante de toda la operación y control de un administrador, dado que si la estructura de medio de transporte es débil y vulnerable, nuestra red de datos no puede tener un nivel alto de confiabilidad, y esto repercute en la marcha normal del negocio y ejecución de actividades relevantes para su óptimo crecimiento en el mercado.

1.6.1.1 Arquitectura

La arquitectura de red es el medio más efectivo para desarrollar e implementar un conjunto de productos que se puedan interconectar. Es el plan con el que se conectan los protocolos y otros programas de software, por ende es necesario que sea útil tanto para los usuarios de la red como para los proveedores de hardware y software.

1.6.1.2 Topología de Red

La topología de red, es la forma de tender el cable hacia las diferentes estaciones de trabajo; por muros, suelos y techos del edificio. Determina únicamente la configuración de las conexiones entre nodos, por ende la distancia entre nodos, interconexiones físicas, tasas de transmisión y/o los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.

1.5.1.1 Extensión

Las redes de área local, son la interconexión de varias computadoras y periféricos, limitando su extensión físicamente a un edificio o a un entorno de 200 metros. Este tipo de redes se

emplean para conectar computadoras personales y estaciones de trabajo en oficinas, fábricas, etc., y a la vez compartir recursos e intercambiar datos y aplicaciones. [1]

1.5.1.2 Levantamiento de los activos de información de la Red

Se entiende por activos de información, al conjunto de elementos con valor informático, que contienen datos de diferentes tipos con los que una organización desarrolla su actividad y que son vitales para el avance óptimo y efectivo del negocio de la organización. Es por ello que la seguridad informática tiene como objetivo proteger las principales propiedades de la información, confidencialidad, disponibilidad e integridad.

Definir una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

- **Confidencialidad.** Asegurar que únicamente personal autorizado tenga acceso a la información.
- **Integridad.** Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
- **Disponibilidad.** Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

[1] Monografía, autor Jhonathan Cueto, http://www.monografias.com/trabajos44/redes-ambito-mundial/redes-ambito-mundial2.shtml.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación. El objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad.

1.5.2 Análisis de riesgos de la información

Es el proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos la red de datos así como su probabilidad de ocurrencia y el impacto de las mismas. Además es una evaluación del tipo, alcance y naturaleza de los incidentes o acciones que pueden resultar en consecuencias adversas.

1.5.2.1 Amenazas

Son circunstancias o incidentes que tienen la probabilidad de ocasionar daño a un recurso de información al explotar las vulnerabilidades en el sistema. El análisis de amenazas consiste en la identificación de las amenazas que existen contra los activos de información y la tecnología de información. El análisis de amenazas suele definir también el nivel de la amenaza y la probabilidad de que esta se materialice.

1.5.2.1.1 Humanas

La proyección de las posibles amenazas que resultan de la interacción entre el ser humano y la compañía, es un factor decisivo en cuanto a la estabilidad y calidad del negocio e influye directamente sobre el beneficio y la sustentabilidad que brinda a los usuarios o clientes. Ejemplos son: descuido, operación inadecuada, administración ineficiente, sabotaje y otros.

1.5.2.1.2 Tecnológicas

Hoy en día, las compañías necesitan protegerse contra una serie de amenazas cada vez más diversas, rápidas y sofisticadas que provienen tanto del interior como del exterior. Ejemplos son: malware, phishing, spam, redes sociales y otros.

1.5.2.2 Vulnerabilidades

El análisis de riesgos y vulnerabilidades se basa en la evaluación integral de la empresa. Una vulnerabilidad se define como el conjunto de fallas e irregularidades dentro de la infraestructura de la empresa o provenientes de los productos suministrados por terceras personas, de forma administrativa y tecnológica. La mayor parte de las intrusiones a los sistemas que se producen en la actualidad, deben a la explotación de vulnerabilidades, por ello es de vital importancia todas aquellas susceptibles de ser aprovechadas por una amenaza, para evitar que está llegue a materializarse.

1.5.2.2.1 Tecnologías de Información y Comunicación

Las tecnologías de la información y la comunicación (TICs) son un conjunto de técnicas, desarrollos y dispositivos avanzados que integran funcionalidades de almacenamiento, procesamiento y transmisión de datos. En las redes actuales, existen muchos componentes necesarios para que estas funcionen, cuantos más componentes, más probabilidad tenemos que algo falle.[2]

Estos problemas pueden ocurrir en servidores, fallos de discos, fuentes de alimentación, tarjetas de red, routers, switches, componentes de red, acceso a internet, aplicaciones y por debilidad en sus sistemas de seguridad.

1.5.2.2.2 Personas

En la organización pueden existir errores internos como externos. El personal que trabaja en la empresa puede provocar fallos en los sistemas de la compañía, pérdidas de información debido a falta de formación o de conocimiento. Igualmente si no existe una adecuada administración de RRHH dentro de la organización; ocasionará problemas en la selección, permanencia y despido del personal, convirtiéndose en un riesgo para la empresa y la información que manipula.

[2] Resumen, Jorge Rivera, http://www.gestiopolis.com/administracion-estrategia/terminos-del-derecho-de-internet-y-las-tecnologias-de-la-informacion.htm

En ocasiones, personas ajenas a la empresa pueden querer dañarla por algún motivo, por ende es necesario preparar a la organización para evitar ataques externos a sus TICs. Actualmente en las empresas públicas y privadas se ha experimentado la ingeniería social, que consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. El objetivo principal de esta técnica, es engañar a la gente para que revele contraseñas u otra información que comprometa la seguridad de la empresa u organización a la que pertenece.

1.5.2.2.3 Procesos

En una falla de proceso, la ejecución arroja un resultado incorrecto, los procesos provocan que el sistema se desvíe de las especificaciones y el proceso puede suspender su progreso. Entre los más comunes errores que causan la falla de los procesos están: los interbloqueos, tiempo expirado, violación de protección, error en la entrada provista por el usuario. [3] Dependiendo del tipo de error que cause que un proceso falle, este proceso puede ser abortado o reiniciado desde un estado anterior. Es necesario establecer y entender la estructura organizacional de los procesos dentro de la empresa y verificar que se encuentren alineados con los objetivos del negocio.

[3] Monografía, Autor Chevez Cruz Mileydi, http://www.itistmo.edu.mx/Pag%20Informatica/APUNTES_archivos/page0002.htm

1.5.3 DISEÑO PLAN DE SEGURIDAD

La infraestructura de telecomunicaciones actual se ha encargado de concebir nuevos y novedosos negocios, que han permitido la expansión y generación de mercados antes desconocidos. En esta medida la información que viaja a través de millones de tecnologías de información y comunicación, se ha convertido en uno de los recursos con mayor relevancia e importancia de las empresas, y en el motor de conocimiento para reconocer las fluctuaciones del entorno en el cual se encuentran. Por tanto, se hace necesario mantener y desarrollar posiciones y acciones claras y seguras frente a la información estratégica y relevante de la compañía.

Como definición un Plan de Seguridad, es la expresión utilizada para denominar al sistema de seguridad diseñado y el cual constituye el documento básico que establece los principios organizativos y funcionales de la actividad de seguridad de información en una entidad y agrupa claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

El objetivo de este diseño es establecer una metodología para la elaboración del Plan de Seguridad de la empresa NEUMAC S.A. - Ecuador, mediante la descripción de los controles de seguridad que deben ser implementados, de forma que permita la interpretación clara y precisa de las políticas, medidas y procedimientos que se definan en la misma, con el objetivo de alcanzar niveles aceptables de seguridad y evitar pérdidas y daños de activos.

El vigente mundo empresarial se enfrenta a un entorno cambiante en el que las nuevas tecnologías juegan cada día un papel más importante. La manera en que la empresa plantee la adopción de estas nuevas tecnologías dependerá en que se conviertan en una nueva oportunidad de negocio o bien en una seria amenaza.

Las primeras empresas que vieron una oportunidad de negocio en la incorporación de nuevas tecnologías informáticas y de comunicaciones a sus procesos son también las primeras en ser conscientes de que es imprescindible contar con sistemas de protección y de seguridad lógica que aseguren la continuidad del negocio. Por ello, el estándar a utilizar para el desarrollo del diseño del plan de seguridad es el ISO/IEC 27002:2005, el cual reúne las mejores prácticas y está orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo.

1.6 DISEÑO METODOLÓGICO

El desarrollo del siguiente trabajo se basará en un diseño metodológico deductivo, que va de lo general a lo particular. El método deductivo es aquél que toma verdades previamente establecidas como principios generales, para luego aplicarlo a casos individuales y comprobar así su validez. Partiré mi investigación desde lo general, realizando un análisis del estado actual de la red, levantamiento de los activos de información, identificación y estimación de riesgos y amenazas a los que se exponen los activos de información de la empresa basado en una metodología que emplea criterios de confidencialidad, integridad y disponibilidad, además de una búsqueda exhaustiva de vulnerabilidades en cada activo, hasta llegar a lo específico, diseñar el plan de seguridad para mitigar peligros de pérdida, fuga, sustracción de datos, y

reducir las vulnerabilidades dentro de los activos de información para así brindar a la compañía protección de sus datos durante su procesamiento, distribución y almacenamiento.

La herramienta que se emplea para la compilación de todo lo referente a la seguridad en la red de datos de la empresa son las técnicas de observación, registro, recopilación, búsqueda, incluidas en la investigación de campo, las cuales consisten en observar, almacenar, archivar, clasificar, comparar personas, fenómenos, hechos, casos, objetos, acciones, situaciones, etc., con el fin de obtener toda la información necesaria dentro de la organización.

Capítulo 2

2. ANÁLISIS DEL MARCO TEÓRICO

Este capítulo encierra todos los conceptos básicos e importantes que formarán parte de la investigación como un marco de referencia para las demás personas no involucras en el trabajo de tesis. Adicionalmente, permitirá conocer y entender de mejor forma la estructura jerárquica conceptual en la que se basa el desarrollo de la tesis, definiendo y detallando conceptos y características de cada tema.

2.1. CONCEPTOS BÁSICOS

2.1.1. Infraestructura de la red

La infraestructura de una red de datos, es la parte más importante, dado que si nuestra estructura es débil y no lo conocemos, nuestra red de datos no puede tener un nivel alto de confiabilidad, por lo que en esta sección proporcionaremos las mejores prácticas para tener o mejorar una infraestructura de red confiable.

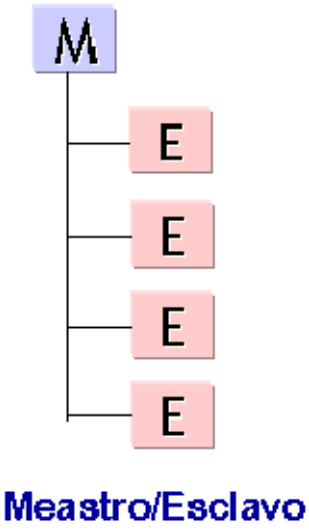
2.1.1.1. Arquitectura

La arquitectura de red es el medio más efectivo para desarrollar e implementar un conjunto de productos que se puedan interconectar. Es el plan con el que se conectan los protocolos y otros programas de software, por ende es necesario que sea útil tanto para los usuarios de la red como para los proveedores de hardware y software.

Las computadoras se comunican por medio de redes. La red más sencilla es una conexión directa entre dos computadoras. Sin embargo, también pueden conectarse a través de grandes redes que permiten a los usuarios intercambiar datos, comunicarse mediante correo electrónico y compartir recursos. Por ello existen tres tipos de arquitecturas básicas que determinan cómo un nodo se comunica con otro dentro de la misma red:

2.1.1.1.1. Maestro/Esclavo

Se refiere a una relación donde un simple nodo ("maestro") inicia y controla una sesión con uno o más dispositivos ("esclavos"). Originalmente diseñado para redes de computadores *mainframe* dónde el mainframe era el computador maestro y otros los otros terminales eran los esclavos. La arquitectura maestro/esclavo no es muy comúnmente usada en redes modernas excepto en casos aislados (por ejemplo, emulación de terminal).



Arquitectura Maestro – Esclavo [4]
Figura 2.1

2.1.1.1.2. Peer-to-peer (p2p)

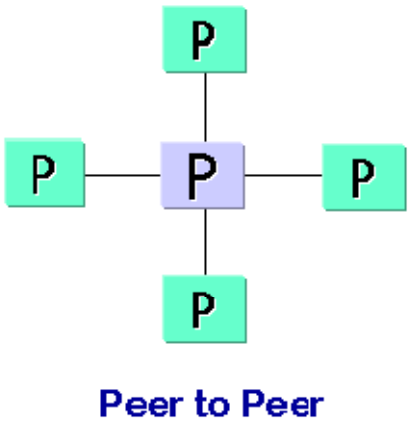
En una red p2p, no hay servidores dedicados, y no existe una jerarquía entre los equipos. Todos los dispositivos conectados son iguales *(peers)*. Cada dispositivo actúa como cliente y servidor, y no hay un administrador responsable de la red completa. El usuario de cada equipo determina los datos de dicho equipo que van a ser compartidos en la red.

Las redes P2P resultan una buena elección para entornos en los cuales:

- Existe como máximo 10 usuarios.
- Los usuarios comparten recursos, tales como archivos e impresoras, pero no existen servidores especializados.

[4] Arquitectura Maestro - Esclavo, Autor Jorge Cortez, www.monografias.com

- La seguridad no es una cuestión fundamental.
- La organización y la red sólo van a experimentar un crecimiento limitado en un futuro cercano.
- Las redes P2P disminuyen su eficacia conforme se incrementa la carga y el número de usuarios, sabiendo además que el control administrativo está ausente.
- Las arquitecturas p2p son típicamente limitadas a ambientes de LAN pequeñas, plataforma única y poco tráfico.



Arquitectura Peer to Peer [5]
Figura 2.2

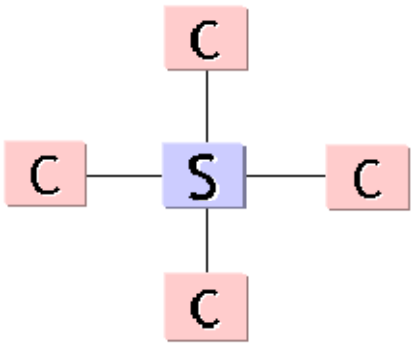
[5] Arquitectura Peer to Peer, Autor Jorge Cortez, www.monografias.com

2.1.1.1.3. Cliente/Servidor

Se refiere a una relación donde servidores dedicados dan soporte a los clientes que están conectados a ellos. Las comunicaciones cliente servidor se encuentran comúnmente en redes grandes, de alto desempeño, multiplataforma donde la seguridad es una prioridad. (Ejemplo, una red bancaria, pública SRI, etc.).

Un servidor dedicado es aquel que funciona sólo como servidor, y no se utiliza como cliente o estación. Los servidores se llaman "dedicados" porque no son clientes a su vez, y porque están optimizados para dar servicio con rapidez a peticiones de clientes en la red, además de garantizar la seguridad de los archivos y directorios. Las redes basadas en servidor se han convertido en el modelo estándar para la definición de redes.

A medida que las redes incrementan su tamaño, por tanto el número de equipos conectados, la distancia física y el tráfico entre ellas crece, generalmente se necesita más de un servidor. La división de las tareas de la red entre varios servidores asegura que cada tarea será realizada de la forma más eficiente posible.



Arquitectura Cliente/Servidor [6]
Figura 2.3

2.1.1.2. Topología de Red

La topología de red, es la forma de tender el cable hacia las diferentes estaciones de trabajo; por muros, suelos y techos del edificio. Determina únicamente la configuración de las conexiones entre nodos, por ende la distancia entre nodos, interconexiones físicas, tasas de transmisión y/o los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.

La topología de una red cuenta con una parte física y lógica, la cual nos permite conocer y entender como los dispositivos de la red se interconectan entre sí utilizando un medio de comunicación.

- **Topología física:** Se refiere al diseño actual del medio de transmisión de la red.
- **Topología lógica:** Se refiere a la trayectoria lógica que da una señal a su paso por los nodos de la red.

[6] Arquitectura Cliente/Servidor, Autor Jorge Cortez, www.monografias.com

Existen varias topologías de red básicas (ducto, estrella, anillo y malla), pero también existen redes híbridas que combinan una o más topologías en una misma red.

Topología Activa: Se denomina topología activa, debido a que cada equipo de trabajo actúa como un repetidor para amplificar y enviarla a la siguiente computadora, por esto ocasiona que una falla de cualquier cable o equipo rompa la conexión y pueda provocar que se caiga toda la red. Están dadas por las siguientes características:

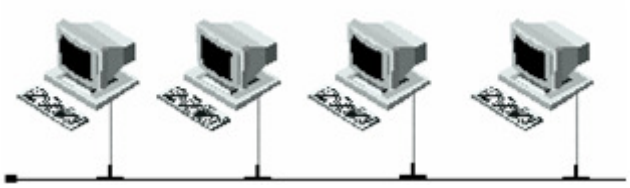
- Se basan en una estructura de árbol, es decir jerárquica.
- Pueden existir aislaciones, cuando existen cambios en la topología.
- Utiliza el RSTP, un protocolo de red para monitorear el estado de todas las trayectorias.

Topología Pasiva: Las computadoras "escuchan" o están en espera. Cuando éstas están listas para transmitir, ellas se aseguran que no haya nadie más transmitiendo, y entonces envían sus paquetes de información. Se basan en la siguiente característica:

- Están basadas en contención (ya que cada computadora debe contender por un tiempo de transmisión).

2.1.1.2.1. Topología de ducto (Bus)

Las redes de ductos son consideradas como topologías pasivas. Las computadoras "escuchan" al ducto. Cuando éstas están listas para transmitir, ellas se aseguran que no haya nadie más transmitiendo en el ducto, y entonces ellas envían sus paquetes de información. Las redes de ducto son fáciles de instalar y de extender. Son muy susceptibles a quebraduras de cable y conectores; además de cortos en el cable que son muy difíciles de encontrar.



Topología de Bus [7]

Figura 2.4

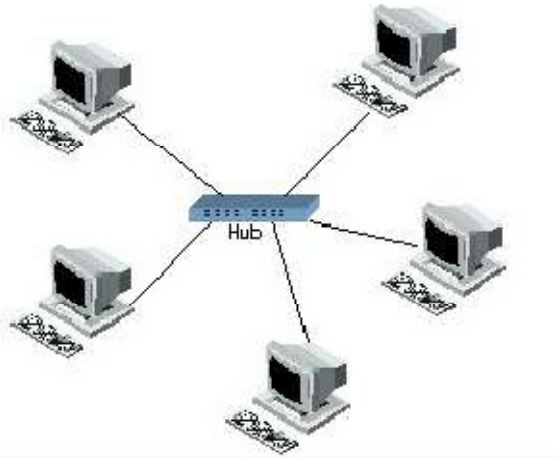
2.1.1.2.2. Topología de estrella (star)

En una topología de estrella, las computadoras en la red se conectan a un dispositivo central conocido como concentrador *(hub)* o a un conmutador de paquetes *(switch)*.

Cada computadora se conecta con su propio cable a un puerto del hub o switch. Este tipo de red sigue siendo pasiva. Debido a que la topología estrella utiliza un cable de conexión para cada computadora, no es muy fácil de expandir, dependerá de cables y número de puertos

[7] Topología de Bus, Autor Helen Valencia S, helen-topologia-de-red.blogspot.com

disponibles en el hub o switch La desventaja de esta topología en la centralización de la comunicación, ya que si el hub falla, toda la red se cae.

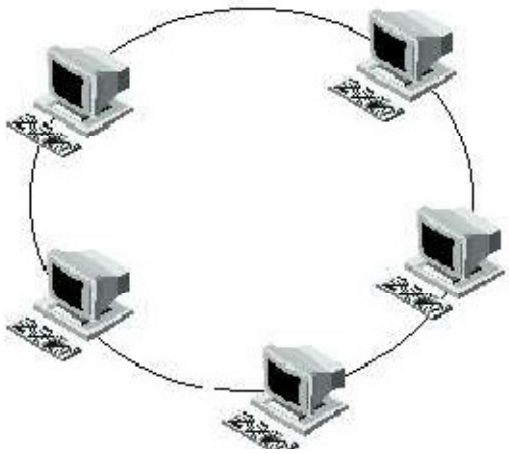


Topología en Estrella [8]
Figura 2.5

2.1.1.2.3. Topología de anillo (ring)

Una topología de anillo conecta los dispositivos de red uno tras otro sobre el cable en un círculo físico. La topología de anillo mueve información sobre el cable en una dirección y es considerada como una topología activa. Las computadoras en la red retransmiten los paquetes que reciben y los envían a la siguiente computadora en la red. El acceso al medio de la red es otorgado a una computadora en particular en la red por un *"token"*.

[8] Topología en Bus, Autor Helen Valencia S., helen-topologia-de-red.blogspot.com

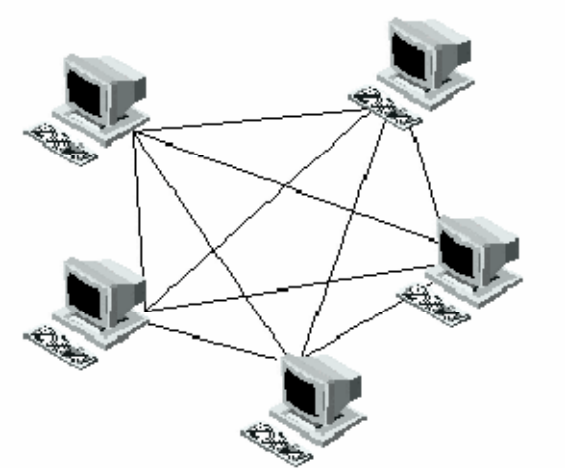


Topología en Anillo [9]
Figura 2.6

2.1.1.2.4. Topología de Malla (mesh)

La topología de malla (mesh) utiliza conexiones redundantes entre los dispositivos de la red, así como una estrategia de tolerancia a fallas. Cada dispositivo en la red está conectado a todos los demás, es decir todos están conectados con todos. Este tipo de tecnología requiere mucho cable (cuando se utiliza el cable como medio, pero puede ser inalámbrico también). Debido a la redundancia, la red puede seguir operando si una conexión se rompe. Las redes de malla, obviamente, son más difíciles y caras para instalar que las otras topologías de red debido al gran número de conexiones requeridas.

[9] Topología en Anillo, Autor Helen Valencia S., helen-topologia-de-red.blogspot.com



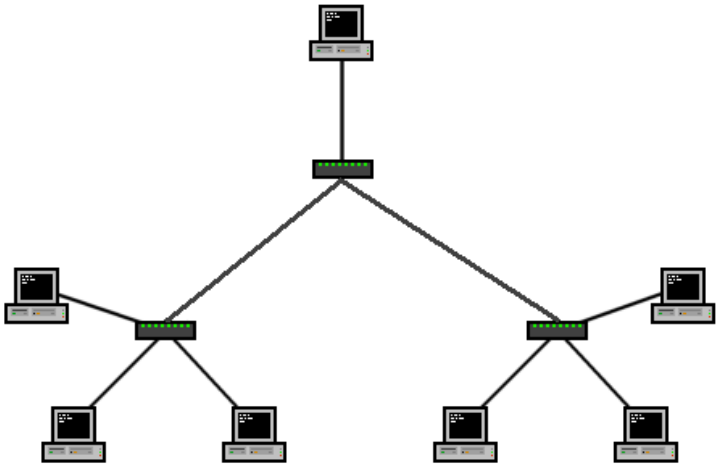
Topología de Malla [10]
Figura 2.7

2.1.1.2.5. Topología en árbol

Topología de red en la que los nodos están colocados en forma de árbol. Posee un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión o broadcast, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

[10] Topología en Malla, Autor Jorge Carrido, redesysegu.blogspot.com



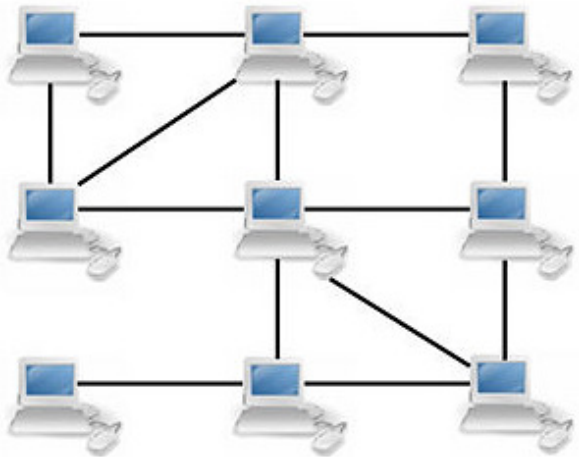
Topología en Árbol [11]
Figura 2.8

2.1.1.2.6. Topología Híbrida

Es una de las más frecuentes y se deriva de la unión de varios tipos de topologías de red, de aquí el nombre de híbridas, es decir estrella-estrella, bus-estrella, etc. Su implementación se debe a la complejidad de la solución de red, o bien al aumento en el número de dispositivos, lo que hace necesario establecer una topología de este tipo.

Las topologías híbridas tienen un costo muy elevado debido a su administración y mantenimiento, ya que cuentan con segmentos de diferentes tipos, lo que obliga a invertir en equipo adicional para lograr la conectividad deseada.

[11] Topología en árbol, Autor José Narváez, teknear.com



Topología Híbrida [12]
Figura 2.9

2.1.1.3. Extensión

Las redes de área local, son redes de computadoras pequeñas, comunes en oficinas, colegios y empresas de espacios reducidos, que generalmente usan la tecnología de broadcast, es decir, aquella en que a un sólo cable se conectan todas las máquinas. Una red puede empezar siendo pequeña para crecer junto con la organización o institución. A continuación se presenta los distintos tipos de redes disponibles según su extensión:

[12]Topologías Híbridas, Autor María Isabel Hinojosa, mariaisabeld09.blogspot.com

2.1.1.3.1. Red de Área Local (LAN)

Una LAN conecta varios dispositivos de red en un área de corta distancia delimitadas únicamente por la distancia de propagación del medio de transmisión, espectro disperso o infrarrojo. Una LAN podría estar delimitada también por el espacio en un edificio, un salón, una oficina, hogar pero a su vez podría haber varias LANs en este mismo espacio. En redes basadas en IP, se puede concebir una LAN como una subred, pero esto no es necesariamente cierto en la práctica. Las LAN comúnmente utilizan las tecnologías Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface) para conectividad, así como otros protocolos tales como Appletalk, Banyan Vines, DECnet, IPX, etc.

2.1.1.3.2. Red de Área Campus (CAN)

Una CAN es una colección de LANs dispersas geográficamente dentro de un campus (universitario, oficinas de gobierno, maquilas o industrias) pertenecientes a una misma entidad en una área delimitada. Una CAN utiliza comúnmente tecnologías tales como FDDI y Gigabit Ethernet para conectividad a través de medios de comunicación tales como fibra óptica y espectro disperso.

2.1.1.3.3. Red de Área Metropolitana (MAN)

Una MAN es una colección de LANs o CANs dispersas en una ciudad. Una MAN utiliza tecnologías tales como ATM, Frame Relay, xDSL *(Digital Subscriber Line)*, WDM

(Wavelenght Division Modulation), ISDN, E1/T1, PPP, etc. para conectividad a través de medios de comunicación tales como cobre, fibra óptica, y microondas.

2.1.1.3.4. Red de Área Extendida (WAN)

Una WAN es una colección de LANs dispersas geográficamente a una distancia considerable una de otra. Las WAN utilizan comúnmente tecnologías ATM *(Asynchronous Transfer Mode),* Frame Relay, X.25, E1/T1, GSM *(Global System for Mobile Communications),* TDMA *(Time Division Multiple Access),* CDMA (*Code Division Multiple Access*), xDSL, PPP *(Point-to-Point Protocol),* etc. para conectividad a través de medios de comunicación tales como fibra óptica, microondas, celular y vía satélite.

2.1.2. Levantamiento de activos de información

Se entiende por activos de información, al conjunto de elementos con valor informático, que contienen datos de diferentes tipos con los que una organización desarrolla su actividad y que son vitales para el avance óptimo y efectivo del negocio de la organización. Es por ello que la seguridad informática tiene como objetivo proteger las principales propiedades de la información, confidencialidad, disponibilidad e integridad.

Definir una guía en la implementación del sistema de administración de la seguridad de la información, se orienta a preservar los siguientes principios de la seguridad informática:

- **Confidencialidad.** Asegurar que únicamente personal autorizado tenga acceso a la información.

- **Integridad.** Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

- **Disponibilidad.** Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno, educativas e investigación. El objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad.

2.1.2.1. Hardware

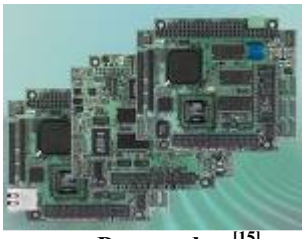
El hardware de computadora provee el fundamento físico básico para el desarrollo de las Tecnologías de Información y Comunicación de la empresa. Un sistema de cómputo moderno está conformado por una serie de dispositivos, que consisten en una unidad central de procesamiento, almacenamiento principal, y almacenamiento secundario.

2.1.2.1.1. Unidad central de procesamiento ó CPU (Central Processing Unit)

Simplemente procesador o microprocesador, es el componente en una computadora digital que interpreta las instrucciones y procesa los datos contenidos en los programas de la computadora. [13]

Gabinete o Case [14]

Figura 2.10



Procesador [15]

Figura 2.11

2.1.2.1.2. Almacenamiento primario

Está directamente conectada a la CPU de la computadora y es fundamental su funcionamiento para que la CPU funcione correctamente. El almacenamiento primario consiste en tres tipos de almacenamiento:

1. **Registros del procesador:** Son internos de la CPU. Contienen información que las unidades aritmético-lógicas necesitan llevar a la instrucción en ejecución. Técnicamente,

[13] Monografía, Autores Roberth Atencio y Yucelis Montilla, http://www.monografias.com/trabajos12/comptcn/comptcn.shtml
[14] Gabinete o Case de PC, Autor Toshiba, descargaok.com
[15] Procesador, Autor INTEL, taringa.net

son los más rápidos de los almacenamientos de la computadora. Proporcionan la manera más rápida para que la unidad central de procesamiento obtenga acceso a los datos.

2. **Memoria caché:** Es un tipo especial de memoria interna usada en muchas CPU para mejorar su eficiencia o rendimiento. Parte de la información de la memoria principal se duplica en la memoria caché. Sin embargo, es más rápida, aunque de mucha menor capacidad que la memoria principal o RAM.

3. **Memoria de acceso aleatorio ó RAM (Random Access Memory):** Es la memoria desde donde el procesador recibe las instrucciones y guarda los resultados. Considera también como el área de trabajo para la mayor parte del software de un computador. Es una memoria volátil porque requiere energía constante para mantener la información almacenada y en caso de falta de energía eléctrica pierde la capacidad de guardar datos e información.

2.1.2.1.3. Almacenamiento Secundario

Conjunto de dispositivos y medios de almacenamiento, que conforman el subsistema de memoria de una computadora, junto a la memoria principal. También llamado periféricos de almacenamiento. La memoria secundaria es un tipo de almacenamiento masivo y permanente es decir *no volátil* debido a que retiene la información almacenada incluso si no recibe corriente eléctrica constantemente, y además posee mayor capacidad de memoria que la memoria principal, aunque esto la vuelve más lenta.

En la actualidad para almacenar información se usan principalmente tres tecnologías; **magnética:** esta tecnología abarca discos duros extraíbles, disquetes, cintas magnéticas; entre otras; **óptica:** incluye dispositivos como CD, DVD, y algunos dispositivos combinan ambas tecnologías, es decir, son dispositivos de almacenamiento híbridos, por ej., discos Zip; y finalmente la **tecnología Flash**: que contiene las Tarjetas de Memorias Flash.

2.1.2.2. Software

Se refiere al equipamiento lógico o soporte lógico de una computadora digital, y comprende el conjunto de los componentes necesarios para hacer posible la realización de tareas específicas.[16]

2.1.2.2.1. Clasificación del software

2.1.2.2.1.1. Software de sistema

Su objetivo es desvincular adecuadamente al usuario de los detalles de la computadora en particular que se use, aislándolo especialmente de procesos referidos a las características internas de: memoria, discos, puertos y dispositivos de comunicaciones, impresoras, pantallas,

[16]Artículo, Autor Kervin Vergara, publicado el 15 de Marzo de 2008, http://www.bloginformatico.com/concepto-y-tipos-de-software.php

teclados, etc. El software de sistema le gestiona al usuario adecuadas interfaces de alto nivel, herramientas y utilidades de apoyo que permiten su mantenimiento.

2.1.2.2.1.2. Software de programación

Es el conjunto de herramientas que permiten al programador desarrollar programas informáticos, usando diferentes alternativas y lenguajes de programación, de una manera práctica.

2.1.2.2.1.3. Software de aplicación

Es aquel que permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios.

2.1.2.2.1.4. Comunicación

Es el proceso mediante el cual se transmite información de una entidad a otra. Todas las formas de comunicación requieren un emisor, un mensaje y un receptor. En el proceso comunicativo, la información es incluida por el emisor en un paquete y canalizada hacia el

receptor a través del medio. Una vez recibido, el receptor decodifica el mensaje y proporciona una respuesta.

2.1.2.2.1.4.1. Switch

Es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI *(Open Systems Interconnection)*. Un conmutador interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro. Su empleo es muy común para conectar múltiples redes entre sí para que funcionen como una sola. Un conmutador suele mejorar el rendimiento y seguridad de una red de área local.[17]

2.1.2.2.1.4.2. Hub

Es un equipo de redes que permite conectar entre sí otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos los demás. Para lograrlo, está compuesto por varios puertos a partir de los que se distribuye la información. Así, cuando un paquete de datos ingresa por uno de los puertos, es retransmitido por el resto de los puertos a los otros componentes que integran la red, de forma tal que todas estas terminales puedan compartir archivos, impresoras, etc., y estén comunicadas continuamente.

[17] Manual de Preparación CISM, Autor ISACA, 2005, Pág. 147, Estados Unidos de Norteamérica.

2.1.2.2.1.4.3. Bridge

Son elementos inteligentes, constituidos como nodos de la red, que conectan entre sí dos subredes, transmitiendo de una a otra el tráfico generado no local. Al distinguir los tráficos locales y no locales, estos elementos disminuyen el mínimo total de paquetes circulando por la red por lo que, en general, habrá menos colisiones y resultará más difícil llegar a la congestión de la red. [18]

Se encargan de filtrar el tráfico que pasa de una a otra red según la dirección de destino y una tabla que relaciona las direcciones y la red en que se encuentran las estaciones asignadas. Las redes conectadas a través de bridge aparentan ser una única red, ya que realizan su función transparentemente; es decir, las estaciones no necesitan conocer la existencia de estos dispositivos, ni siquiera si una estación pertenece a uno u otro segmento.

2.1.2.2.1.4.4. Router

Es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). El router interconecta segmentos de red o redes enteras, haciendo pasar paquetes de datos entre estas redes tomando como base la información de la capa de red. Además toma decisiones con respecto a la mejor ruta para el envío de datos a través de una red

[18]Monografía, Autor Ulises Zeus, http://www.monografias.com/trabajos11/inter/inter.shtml

interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados.[19]

2.1.2.2.1.5. Servicios de Red

Los servicios de red están instalados generalmente en uno o más servidores para proporcionar recursos compartidos a cliente computadoras. Los servicios de red se configuran en LANs para asegurar seguridad y la operación de uso fácil. Ayudan a la red para funcionar eficientemente [20]. Servicios de red corporativos del uso de LANs tales como:

- **DNS** *(Domain Name System)*: Para dar nombres a IP y Direcciones MAC. Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado al internet o a una red privada.

- **DHCP** *(Dynamic Host Configuration Protocol)*: Asegurar de que cada estación en la red tenga un IP address válido, es decir facilita la carga administrativa automatizando la asignación del IP de nodos en la red.

- **E-mail** y **archivos de red:** Son también servicios de red. Son usualmente implementados en un ambiente de LAN, debido a que permiten que los usuarios tengan acceso a cualquier impresora conectada con la red, archivos en el servidor u otros nodos conectados a la misma, y a la transferencia de datos dentro de la red.

[19] Manual de Preparación CISM, Autor ISACA, 2005, Pág. 149, Estados Unidos de Norteamérica.
[20] Artículo, Autor José Mancheno U., publicado el 12 de Septiembre del 2009 http://www.worldlingo.com/ma/enwiki/es/Network_service

2.1.2.2.1.6. Personas

La persona es definida como un ser racional y consciente de sí mismo, poseedor de una identidad propia. Jurídicamente se define a la persona como todo ente susceptible de adquirir derechos y contraer obligaciones. Viene del latín: *persōna* y este del griego: *prósōpon* (máscara del actor, personaje).[21]

2.1.2.2.1.6.1. Usuario

Un usuario es la persona que utiliza o trabaja con algún objeto o que es destinataria de algún servicio público, privado, empresarial o profesional. En sentido general, un usuario es un conjunto de permisos y de recursos (o dispositivos) a los cuales se tiene acceso. Es decir, un usuario puede ser tanto una persona como una máquina, un programa, etc.[22]

2.1.2.2.1.6.2. Junta de Accionista y Gerentes

La Junta General de Accionistas es un órgano de administración y fiscalización dentro de la sociedad anónima, donde se toman las decisiones clave para la marcha y funcionamiento de

[21]Glosario, Autor Diccionario de la lengua española, http://www.wordreference.com/definicion/persona
[22]Glosario, Autor Diccionario de la lengua española, http://www.wordreference.com/definicion/usuario

la sociedad. El término gerente denomina a quien está a cargo de la dirección de alguna organización, institución o empresa o parte de ella. El papel del gerente es utilizar tan eficientemente como sea posible los recursos a su disposición a fin de obtener el máximo posible de beneficio de los mismos. En otras palabras, maximizar la utilidad productiva de su organización, sección, etc.

2.1.2.2.1.6.3. Empleados

Persona que desempeña un cargo o trabajo y que a cambio de ello recibe un sueldo. Por regla general, el trabajador que preste algún servicio es un empleado del contratante, por ende este último posee todo el control sobre él, tanto en lo referente a lo que debe hacer como a la manera de hacerlo dentro de la empresa [23].

2.1.2.2.1.7. Procesos

Un proceso se define como un conjunto de tareas, actividades o acciones lógicamente relacionadas entre sí que, a partir de una o varias entradas de información, materiales o de salidas de otros procesos, dan lugar a una o varias salidas también de materiales (productos) o información con un valor añadido. Conjunto de acciones o actividades sistematizadas que se realizan o tienen lugar con un fin.

[23] Artículo, Autor Federico Saviria S., publicado el http://www.irs.gov/publications/p179/ar02.html

2.1.2.2.1.8. Información

La Información es un recurso vital, generado por los sistemas de información. Las organizaciones utilizan también otros recursos como materiales, materias primas, energía y recursos humanos, todos ellos sujetos a cada vez mayores restricciones en su uso y crecimiento, debido a problemas de escasez y, por tanto, de coste [24].

La información es un conjunto organizado de datos, que constituye un mensaje sobre un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su uso racional es la base del conocimiento. Durante los últimos veinte años, los investigadores han desarrollado un creciente campo de investigación sobre el valor de la información y sus características únicas. Algunas de las características únicas de la información incluyen:

- La información es cara de producir, no así de reproducir ya que apenas dispone de costos.

- La información puede ser un bien público, privado, o un bien híbrido.

- Dependiendo del tipo de bien (público, privado o híbrido), el valor de la información puede aumentar o disminuir en función de su disponibilidad.

- El valor de la información es, en gran medida, subjetivo.

[24]Artículo, Autor Jorge Ruíz, http://html.rincondelvago.com/importancia-de-la-informacion-en-la-empresa.html

2.1.1. Amenazas

Son circunstancias o incidentes que tienen la probabilidad de ocasionar daño a un recurso de información al explotar las vulnerabilidades en el sistema. La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad conocida a veces como falencias *(flaws)* o brechas *(breaches)* representa el grado de exposición a las amenazas en un contexto particular.

2.1.1.1. Humanas

La proyección de las posibles amenazas que resultan de la interacción entre el ser humano y la compañía, es un factor decisivo en cuanto a la estabilidad y calidad del negocio e influye directamente sobre el beneficio y la sustentabilidad que brinda a los usuarios o clientes. Ejemplos son: descuido, operación inadecuada, administración ineficiente, sabotaje y otros.

2.1.1.2. Tecnológicas

El análisis de riesgo y vulnerabilidad se basa en la evaluación integral de la empresa. Hoy en día, las compañías necesitan protegerse contra una serie de amenazas cada vez más diversas, rápidas y sofisticadas que provienen tanto del interior como del exterior de la organización. Ejemplos son: malware, phishing, spam, redes sociales y otros.

2.1.2. Vulnerabilidades

Conjunto de fallas e irregularidades dentro de la infraestructura de la empresa o provenientes de los productos suministrados por terceras personas, de forma administrativa y tecnológica. La mayor parte de las instrucciones a los sistemas que se producen en la actualidad, deben a la explotación de vulnerabilidades, por ello es de vital importancia todas aquellas susceptibles de ser aprovechadas por una amenaza, para evitar que está llegue a materializarse.

2.1.2.1. Tecnologías de Información y Comunicación

Las tecnologías de la información y la comunicación (TICs) son un conjunto de técnicas, desarrollos y dispositivos avanzados que integran funcionalidades de almacenamiento, procesamiento y transmisión de datos. En las redes actuales, existen muchos componentes necesarios para que estas funcionen, cuantos más componentes, más probabilidad tenemos que algo falle.[25]

Estos problemas pueden ocurrir en servidores, fallos de discos, fuentes de alimentación, tarjetas de red, routers, switches, componentes de red, acceso a internet, aplicaciones y por debilidad en sus sistemas de seguridad.

[25] Resumen, Autor Enrique Márquez Solís, http://www.gestiopolis.com/administracion-estrategia/terminos-del-derecho-de-internet-y-las-tecnologias-de-la-informacion.htm

2.1.2.2. Personas

En la organización pueden existir errores internos como externos. El personal que trabaja en la empresa puede provocar fallos en los sistemas de la compañía, pérdidas de información debido a falta de formación o de conocimiento. Igualmente si no existe una adecuada administración de RRHH dentro de la organización; ocasionará problemas en la selección, permanencia y despido del personal, convirtiéndose en un riesgo para la empresa y la información que manipula.

En ocasiones, personas ajenas a la empresa pueden querer dañarla por algún motivo, por ende es necesario preparar a la organización para evitar ataques externos a sus TICs. Actualmente en las empresas públicas y privadas se ha experimentado la ingeniería social, que consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. El objetivo principal de esta técnica, es engañar a la gente para que revele contraseñas u otra información que comprometa la seguridad de la empresa u organización a la que pertenece.

2.1.2.3. Procesos

En una falla de proceso, la ejecución arroja un resultado incorrecto, los procesos provocan que el sistema se desvíe de las especificaciones y el proceso puede suspender su progreso. Entre los más comunes errores que causan la falla de los procesos están: los interbloqueos, tiempo expirado, violación de protección, error en la entrada provista por el usuario. [26] Dependiendo del tipo de error que cause que un proceso falle, este proceso puede ser abortado o reiniciado desde un estado anterior. Es necesario establecer y entender la estructura organizacional de los

[26] Monografía, Autor Chevez Cruz Mileydi, http://www.itistmo.edu.mx/Pag%20Informatica/APUNTES_archivos/page0002.htm

procesos dentro de la empresa y verificar que se encuentren alineados con los objetivos del negocio.

2.1.3. Plan de Seguridad

La infraestructura de telecomunicaciones actual se ha encargado de concebir nuevos y novedosos negocios, que han permitido la expansión y generación de mercados antes desconocidos. En esta medida la información que viaja a través de millones de tecnologías de información y comunicación, se ha convertido en uno de los mayores tesoros de las empresas, y en el motor de conocimiento para reconocer las fluctuaciones del entorno en el cual se encuentran. Por tanto, se hace necesario mantener y desarrollar posiciones y acciones claras y seguras frente a la información estratégica y relevante de la compañía.

Como definición un Plan de Seguridad, es la expresión utilizada para denominar al sistema de seguridad diseñado y el cual constituye el documento básico que establece los principios organizativos y funcionales de la actividad de seguridad de información en una entidad y agrupa claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

El vigente mundo empresarial se enfrenta a un entorno cambiante en el que las nuevas tecnologías juegan cada día un papel más importante. La manera en que la empresa plantee la adopción de estas nuevas tecnologías dependerá en que se conviertan en una nueva oportunidad de negocio o bien en una seria amenaza.

Las primeras empresas que vieron una oportunidad de negocio en la incorporación de nuevas tecnologías informáticas y de comunicaciones a sus procesos son también las primeras en ser conscientes de que es imprescindible contar con sistemas de protección y de seguridad lógica que aseguren la continuidad del negocio. Por ello, el estándar a utilizar para el desarrollo del diseño del plan de seguridad es el ISO/IEC 27002:2005, el cual reúne las mejores prácticas y está orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo. Este Estándar contiene un número de categorías de seguridad principales, entre las cuales se tienen once cláusulas:

- Política de seguridad.
- Aspectos organizativos de la seguridad de la información.
- Gestión de activos.
- Seguridad ligada a los recursos humanos.
- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.

- Gestión de incidentes en la seguridad de la información.

- Gestión de la continuidad del negocio.

- Cumplimiento.

Capítulo 3

3. ANÁLISIS DEL ESTADO ACTUAL DE LA RED DE LA EMPRESA

Dentro de este capítulo se abarca el análisis de la red de datos de la empresa, a través de un levantamiento exhaustivo de los activos de información que posee, categorizados en ocho grupos: hardware, software, comunicaciones, servicios de red, información, personas, procesos y red, haciendo hincapié en este último, a detalle en su arquitectura, topología, y extensión.

3.1. Levantamientos de activos de información

Se entiende por activos de información, al conjunto de elementos con valor informático, que contienen datos de diferentes tipos con los que una organización desarrolla su actividad y que son vitales para el avance óptimo y efectivo del negocio de la organización. Es por ello que la seguridad informática tiene como objetivo proteger las principales propiedades de la información: confidencialidad, disponibilidad e integridad.

Una vez analizada la infraestructura de red de la organización e identificados los sistemas informáticos que operan sobre la misma, se detallará los activos de información contenidos en cada uno de ellos, los cuáles son necesarios e importantes para sostener de forma eficiente la actividad normal de la red de datos de la empresa. El levantamiento de los activos de información, describe las características y especificaciones técnicas de cada activo que posea la empresa referente a: hardware, software, comunicaciones, servicios de red, información y red, además se detallará la estructura organizacional de procesos y personas.

A partir de este punto, se describirá el proceso del levantamiento de los activos de información dentro de Neumac S.A., lo cual servirá para un mayor entendimiento y ayudará a la clasificación idónea de cada ítem de activo que forme parte de la red de datos de la compañía. Los activos de información se han agrupado en las siguientes clases:

3.1.1. Hardware

Se especifica todo el hardware del que dispone la empresa para llevar a cabo sus procesos informáticos. En esta tabla se muestran las diferentes categorías de ubicación para los activos de hardware:

No. Activos	Categoría Activo	Propiedad	Tipo
5	$Equipos_1$	Área de Ventas	Hardware
3	$Equipos_2$	Área de Contabilidad y Contaduría	Hardware
2	$Equipos_3$	Área de Diseño y Mecánica	Hardware

4	$Equipos_4$	Área de Gerencia e Importaciones	Hardware
1	$Equipos_2$	Área de Recepción	Hardware
6	Impresoras	Distribuidas en todas las áreas	Hardware
5	Escáneres	Área de Ventas Área de Diseño y Mecánica Área de Gerencia e Importaciones	Hardware

Activos de Hardware
Tabla 3.1

La empresa cuenta con un equipamiento informático un poco obsoleto para el tipo de equipos que existen hoy en día. Los computadores están escasos en memoria RAM. Además existen fallos en dispositivos de entrada y salida como teclados, parlantes, mouses, y lectores de CD/DVD RW. Para mayor detalle de las especificaciones técnicas de los activos de hardware consultar el anexo de hardware, ubicado en la página 173.

3.1.2. Software

En la descripción de software, se muestra todos los programas, de los que está provista la compañía, especialmente aquellos que están destinados a almacenar datos dentro de la empresa. También, se especificará el nivel de protección del software con el que cuenta, para poder analizar posteriormente los riesgos a los que puede estar expuesta. En esta tabla se muestran las diferentes categorías de ubicación para los activos de software:

No. Activos	Nombre Activo	Propiedad	Tipo
4	Software de Prevención	Área de Contabilidad y Contaduría Área de Diseño y Mecánica Área de Gerencia e Importaciones	Software
2	Software de Protección	Área de Contabilidad y Contaduría Área de Gerencia e Importaciones Área de Diseño y Mecánica	Software
4	Software de Corrección	Distribuidas en todas las áreas	Software
4	Software de Diseño	Área de Diseño y Mecánica	Software
5	Software de Entretenimiento	Distribuidas en todas las áreas	Software

Activos de Software
Tabla 3.2

Los equipos de la empresa no están excesivamente cargados de software pero se aprecia un grave problema en la seguridad del mismo. Se dispone de antivirus pero éstos no están correctamente actualizados lo que puede ser un grave problema de seguridad. Adicionalmente, el firewall usado en todos los equipos es el que trae por defecto el Sistema Operativo Windows y aunque no sea un mal software no es el más indicado para un entorno empresarial. Dos de los cuatro tipos de equipos existentes en la compañía, tienen instalada la versión Home

Edition del Sistema Operativo Windows XP; puede ser más útil disponer de la versión Professional debido a sus características para conexiones en red. Y analizando individualmente cada tipo de equipo, encontramos las siguientes observaciones:

Equipo$_1$, cuenta con un Sistema Operativo XP Professional Service Pack 3 y con la versión 4.7 del antivirus Avast. Este antivirus dispone adicionalmente de antispyware y antirootkit y proporciona una seguridad adecuada para el equipo. Actualmente el antivirus de este equipo no se encuentra correctamente actualizado por lo que puede ser una amenaza para la seguridad del dispositivo. El equipo está protegido por el Firewall de Windows. La empresa cuenta con 5 computadoras con estas características en el área de Ventas.

Equipo$_2$, utiliza la protección del sistema McAfee Virus Scan Professional. El cual dispone, además del antivirus, antispyware y anti-hacker. Proporciona una seguridad adecuada al equipo aunque de igual manera que en el caso del equipo 1 el antivirus no se encuentra correctamente actualizado. Este equipo también cuenta con la protección del antispyware AD-Aware SE Professional el cual sí se encuentra correctamente actualizado. El equipo está protegido por el Firewall de Windows. La empresa cuenta con 3 computadoras con las mismas características en el área de Contabilidad y Contaduría.

Equipo$_3$, utiliza como protección el antivirus AVG en su versión 7.5. Este programa está instalado en su versión gratuita y se encuentra correctamente actualizado. También dispone del antispyware de AVG en su versión 7.5 y con la protección del AD-Aware SE Personal. Ambos antispyware se encuentran correctamente actualizados. La empresa cuenta con 2 computadoras con las mismas características en el área de Diseño y Mecánica.

Equipo 4, cuenta con un Sistema Operativo XP Professional Service Pack 3, la protección del antivirus ESET NOD en su versión 4.2.42.3. También cuenta con el antispyware de AVG también en su versión 7.5. Así mismo cuenta con la protección del AD-Aware SE Personal. Ambos antispyware se encuentran correctamente actualizados. La empresa cuenta con 2 computadoras con las mismas características en el área de Gerencia e Importaciones. Para

mayor detalle de las especificaciones técnicas de los activos de software consultar el anexo de software, ubicado en la página 174.

3.1.3. Comunicaciones

A continuación se van a detallar los distintos tipos de comunicaciones de los que dispone la empresa y la red de datos, incluyendo activos como: switches, faxes, teléfonos fijos y móviles, módems, APs, entre otros. Las comunicaciones estables y disponibles en el momento que son requeridas dentro de la compañía son fundamentales para establecer conexiones con clientes, proveedores y sucursales fuera del país. En esta tabla se muestran las diferentes categorías de ubicación para los activos de comunicaciones:

No. Activos	Nombre Activo	Propiedad	Tipo
9	Teléfonos	De toda la empresa	Comunicaciones
2	Faxes	De toda la empresa	Comunicaciones
2	Switches	De toda la empresa	Comunicaciones
1	Access Point	De toda la empresa	Comunicaciones
1	Módem	ISP	Comunicaciones

1	PBX	De toda la empresa	Comunicaciones

Activos de Comunicaciones
Tabla 3.3

Los equipos de comunicaciones, se encuentran en buen estado y funcionamiento, la mayoría son nuevos y cuentan con el respaldo de garantía de las marcas. A excepción de la PBX Panasonic que presenta problemas en la configuración de las líneas, debido a que está diseñada para recibir 10 llamadas automáticamente, pero por causas del software de instalación por defecto del fabricante, solo permite el acceso a cinco llamadas entrantes y el resto son rechazadas. Para mayor detalle de las especificaciones técnicas de los activos de hardware consultar el anexo de comunicaciones, ubicado en la página 178.

3.1.4. Servicios de red

En seguida se van a puntualizar los diferentes tipos de servicios de red de los que dispone la compañía, considerando que generalmente los servicios de red están instalados en uno o más servidores para proporcionar recursos compartidos a clientes-computadoras.

3.1.4.1. DNS

Sus siglas son: *(Domain Name System)*; está a cargo del ISP (Proveedor de Servicios de Internet), el cuál es el encargado de dar nombres a las IP.

3.1.4.2. DHCP

Sus siglas son *(Dynamic Host Configuration Protocol)*; este servicio tiene como finalidad el asegurar de que cada computadora en la red tenga un *IP address* válido, es decir facilita la carga administrativa automatizando la asignación del IP en lo nodos de la red de datos. Igualmente este servicio está a cargo del ISP contratado.

3.1.4.3. Servidor de Correo Electrónico

El servidor por defecto utilizado en la empresa es el Outlook Express, el cuál es usado para mantener un correo interno; además de llevar de forma organizada sus eventos, reuniones con proveedores y clientes. Esta aplicación está instalada en cada una de las computadoras de la red (configuración clientes) y existe una máquina independiente que trabaja como servidor. Para lograr la conexión se definen una serie de protocolos, los mismos que son parte del servidor de mail, cada uno con una finalidad concreta:

- **SMTP** *(Simple Mail Transfer Protocol)*: El servidor lo utiliza para el envío de correo, ya sea desde el servidor de correo a otro, o bien, desde un cliente de correo electrónico al servidor.

- **POP** *(Post Office Protocol)*: El servidor lo emplea para obtener los mensajes guardados en el servidor y pasárselos al usuario.

3.1.4.4. Servidor de archivos

Es un tipo de servidor en una red de computadoras cuya función es permitir el acceso remoto a archivos almacenados en él. El sistema operativo utilizado por el servidor de archivos es *Windows Server 2003*, pertenece a la familia de Windows de la marca Microsoft para servidores que salió al mercado en el año 2003. Está basada en tecnología NT y su versión del núcleo NT es la 5.2.

NEUMAC S.A. almacena dentro del servidor de archivos, las liquidaciones de aduana, facturas de importaciones, y todo documento legal que sea de utilidad a la compañía durante los 3 trimestres del año laboral. Para los clientes del servidor de archivos, la localización de los ficheros compartidos es transparente. Es decir, no hay diferencias perceptibles para los usuarios de la empresa si un documento está almacenado en el servidor de archivos o en el disco de la propia máquina, debido al bajo nivel de seguridad que dispone el mismo.

3.1.4.5. Servidor WEB

El Servidor web se ejecuta continuamente en una computadora de la empresa, manteniéndose a la espera de peticiones por parte de un cliente y responde a estas peticiones adecuadamente, mediante una página web que se exhibirá en el navegador; el link de la compañía es: *www.neumac.com*. El portal web de la empresa corre ó trabaja sobre la plataforma IIS, que

contiene una serie de servicios para los computadores que funcionan con Windows, entre los servicios que ofrece son: FTP, SMTP, y HTTP/HTTPS.

Este servidor WEB utiliza una interfaz de entrada común, la *World Wide Web* que permite a un navegador web solicitar datos de un programa ejecutado en un servidor web. Es un mecanismo de comunicación entre el servidor web y una aplicación externa. La empresa utiliza su página web para realizar ventas nacionales e internacionales, publicar su inventario de productos y servicios, precios, cotizaciones y como ayuda para los clientes ante cualquier duda que tengan acerca de las maquinarias y servicios o de la empresa en general.

3.1.4.6. Servidor Proxy

La empresa utiliza este servidor como un equipo intermediario situado entre los usuarios y la Internet, para registrar el uso del Internet y también para bloquear el acceso a determinadas páginas webs consideradas ofensivas o dañinas para la red y los usuarios. Este mecanismo de seguridad es implementado por la compañía dedicada a dar mantenimiento de las computadoras y por el ISP, dentro del entorno de Intranet.

3.1.4.7. Base de Datos

El sistema de inventarios implementado en la empresa es la base de datos FOX DATE, que ofrece a los usuarios un conjunto de herramientas para crear aplicaciones de bases de datos para escritorio, entornos cliente/servidor, tablet PC o para la Web. Es un sistema Gestor de

Bases de datos o Database Management System (DBMS), y desde la versión 7.0, se convirtió en un sistema administrador de bases de datos relacionales, producido por Microsoft.

La empresa utiliza esta herramienta para almacenar toda la información referente a clientes, cuentas y maquinarias. En esta tabla se muestran las diferentes categorías de ubicación para los servicios de red:

No. Activos	Nombre Activo	Propiedad	Tipo
1	DNS	Proveedor de Servicios de Internet (ISP)	Servicios de red
1	DHCP	Proveedor de Servicios de Internet (ISP)	Servicios de red
1	Mail	De toda la empresa	Servicios de red
1	Archivos	De toda la empresa	Servicios de red
1	WEB	De toda la empresa	Servicios de red
1	Proxy	De toda la empresa	Servicios de red
1	Base de Datos	Área de Ventas	Servicios de red

Activos de Servicios de Red
Tabla 3.4

Los servicios ofrecidos por el ISP trabajan de forma normal y eficiente, brindando disponibilidad y estabilidad a las actividades normales del negocio. Pero en cuanto a los servicios de correo electrónico, web y de archivos muestran varias vulnerabilidades que podrían acarrear futuros inconvenientes a la empresa; además de que su funcionamiento es lento e inseguro. El sistema de inventarios también tiene falencias en su seguridad, tales como redundancia e inconsistencia de datos, dificultad para tener acceso a los datos, aislamiento de los datos, sobreescritura de archivos, etc.

3.1.5. Información

La información es un recurso vital, producido por los sistemas de información dentro de una organización. Para maximizar su utilidad, un negocio la debe manejar correctamente tal como maneja los demás recursos, por ende los administradores y personal en general dentro de Neumac S.A necesitan comprender que hay costos asociados con el procesamiento, distribución y almacenamiento de toda información. Además que la información que se encuentra alrededor es fundamental para el éxito de un negocio y que su uso estratégico servirá para posicionar la competitividad necesaria y suficiente de la empresa. Para un mejor entendimiento, la información dentro de esta sección ha sido clasificada en dos tipos: pública y privada.

3.1.5.1. Información Pública

Son aquellos archivos, registros o datos que están disponibles para ser difundida al público. Dentro de este grupo se encuentran: fichas técnicas, catálogos, información de ventas, flayers, diseños de planos, etc. Este tipo de información está disponible para todos los miembros de la compañía.

3.1.5.2. Información Privada

Son aquellos datos que son confidenciales. Es inviolable, por ende su lectura, modificación o cualquier tipo de manipulación por parte de personas ajenas a ella, está prohibida. La información considerada como privada dentro de la empresa es: nómina de clientes, nómina de proveedores, ingresos de mercaderías, inventario de importaciones, remisiones, cuentas de clientes, etc.

Inmediatamente se van a señalar los diferentes tipos de información de los que dispone la empresa, considerando que la información puede ser un bien público ó privado. Dependiendo del tipo de bien, el valor de la información puede aumentar o disminuir.

No. Activos	Nombre Activo	Propiedad	Tipo
1	Nómina de Clientes Nómina de Proveedores	Ventas Almacén Secretaria-Recepcionista Contabilidad	Información Privada

1	Ingresos Inventario Confirmaciones de Importaciones Remisiones	Bodeguero	Información Privada
1	Toda la información circulante en la compañía	Gerente General	Información Privada y Pública
1	Fichas técnicas Información de Ventas	Gerente Técnico	Información Pública
1	Cuentas de Clientes	Vendedores Técnicos	Información Privada
1	Fichas técnicas Planos Nómina de Clientes	Jefe de Mantenimiento	Información Pública
1	Catálogos Confirmaciones Pedidos de Importación	Ventas Almacén	Información Pública
1	Planos Confirmación de Clientes	Jefe de Diseño e Ingeniería Mecánica	Información Pública

Activos de la Información
Tabla 3.5

Los activos de información son manejados de forma segura y confidencial hasta cierto punto dentro de la empresa, sin embargo, aun existen datos que son distribuidos y almacenados de forma inequívoca, es decir son colocados sobre escritorios sin protección alguna, conversaciones confidenciales son tratadas en ambientes abiertos, la información expuesta en los servidores y base de datos no se encuentra resguardada, lo que podría evidenciarse en pérdidas de información, sustracción de cuentas, etc.

3.1.6. Personas

La persona es definida como un ser racional y consciente de sí mismo, poseedor de una identidad propia. Dentro del ambiente laboral de la empresa Neumac SA., se distinguen tres grupos de personas: ***usuario***, persona que es destinataria de algún servicio público, privado, empresarial o profesional; ***gerente*** se denomina a quien está a cargo de la dirección de la organización, y finalmente ***empleados*** aquellos que desempeñan un cargo o trabajo y que a cambio de ello recibe un sueldo.

No solo el esfuerzo o la actividad humana quedan comprendidos en este grupo, sino también otros factores que dan diversas modalidades en cuanto la selección y ubicación de los cargos como: conocimientos, experiencias, motivación, intereses vocacionales, aptitudes, actitudes, habilidades, potencialidades, salud, etc.

A continuación se van a indicar los diferentes tipos de activos de personas de los que dispone la compañía, considerando su cargo, función, y jerarquía en la empresa.

No. Activos	Propiedad	Tipo
1	Gerente General	Gerente Usuario
1	Gerente Técnico	Gerente Usuario

1	Jefe de Diseño e Ingeniería Mecánica	Empleado Usuario
1	Jefe de Producción y Taller	Empleado Usuario
5	Soldadores - Ayudante	Empleado Usuario
3	Operadores de Máquinas	Empleado Usuario
3	Mecánicos	Empleado Usuario
1	Jefe de Mantenimiento	Empleado Usuario
1	Ayudante – Jefe Mantenimiento	Empleado Usuario
3	Vendedores Técnicos	Empleado Usuario
1	Jefe de Importaciones	Empleado Usuario
1	Contadora	Empleado Usuario
1	Secretaria Recepcionista	Empleado Usuario

1	Bodeguero	Empleado
1	Mensajero	Empleado
2	Personal de Seguridad	Empleado
2	Vendedores de Almacén	Empleado Usuario

Activos del Personal
Tabla 3.6

La nómina de empleados dentro de Neumac S.A.; consta de 30 personas. Siendo una empresa pequeña en el país, el organigrama general de la organización está bien distribuido, y la asignación de cargos de forma jerárquica y ordenada. Cada empleado conoce su rol y las responsabilidades que este posee, ya es independiente de cada persona ejercer un trabajo eficiente y a conciencia dentro de la compañía.

3.1.7. Procesos

Un proceso se define como un conjunto de tareas, actividades o acciones lógicamente relacionadas entre sí que, a partir de una o varias entradas de información o productos, dan lugar a salidas también de materiales (productos) o información con un valor añadido. Neumac S.A emplea este conjunto de acciones o actividades sistematizadas para controlar el diseño, mantenimiento, importación y ventas de sus equipos y maquinarias hidráulicas. En esta tabla se muestran las diferentes categorías de ubicación para los procesos:

No. Activos	Nombre Activo	Propiedad	Tipo
1	Proceso Administrativo	Gerencia General Gerencia Técnica	Proceso
1	Proceso de Producción	Jefatura de Producción y Taller	Proceso
1	Proceso de Control	Secretaria/Recepcionista Bodeguero Personal de Seguridad Contadora	Proceso
1	Proceso de Diseño	Jefatura de Diseño e Ingeniería Mecánica	Proceso
1	Proceso de Mantenimiento	Jefatura de Mantenimiento	Proceso
1	Proceso de Ventas e Importaciones	Jefatura de Importaciones Ventas Técnicas y de Almacén	Proceso

Activos de Procesos
Tabla 3.7

Los procesos dentro de la empresa están correctamente definidos y ejecutados, no encuentro novedades acerca este grupo de activos. El problema surge al momento que dichos procesos se producen y arrojan datos e información, la misma que no es correctamente procesada, distribuida y almacenada dentro de la organización, no en el nivel necesario para sus actividades cotidianas y empresariales; debido al bajo conocimiento sobre seguridad de la información que poseen.

3.1.8. Red

Activo dentro de la empresa que contiene componentes que conforman la infraestructura de los recursos antes mencionados. Se describe a continuación la topología, arquitectura y extensión implementadas, las cuales son el pilar fundamental para lograr la conexión física entre los nodos y la transferencia de datos a los distintos equipos de la red.

3.1.8.1. Arquitectura

Para un estudio más amplio y detallado de la infraestructura de la red de datos de la empresa, se la ha dividido en dos partes: la *parte física* la cual se refiere a la configuración de distribución y conexión de los nodos de red y la *parte lógica* hace referencia a los protocolos que se utilizan para la comunicación interna y externa.

3.1.8.1.1. Física

La tecnología que soporta la infraestructura de la red LAN de Neumac S.A está basada en el protocolo Ethernet y los dispositivos que implementan esta tecnología son switches de capa 2, los mismos que están encargados de interpretar las direcciones físicas de los computadores de la red, con el fin de facilitar y permitir la conectividad entre estaciones, y entre estas estaciones y la Internet, proporcionando y garantizando de esta manera que se puedan acceder

a las aplicaciones propias relacionadas con la labor de la empresa, como: base de datos, portal web, correo electrónico, acceso a ficheros compartidos, etc.

Los switches utilizados en esta red LAN poseen velocidad de 10Mbps o 100Mbps; es decir pueden combinar la conectividad de un dispositivo hub con la regulación de tráfico de un puente en cada puerto. Además, por ser dispositivos de características inteligentes, conmutan paquetes desde los puertos o interfaces de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total contratado. La red de datos de la empresa está compuesta de la siguiente manera:

EXTRANET: Está formada por un módem ADSL marca FiberHome, para la salida al Internet de banda ancha a través de un ISP. Está constituida por un switch central marca 3COM de 8 puertos al cuál se conectan cuatro servidores. Los servidores con los que cuenta la empresa son, *servidor proxy* que es el encargado de permitir el acceso a Internet de todos los equipos de la organización de forma indirecta a través de él; *servidor de correo*, brinda la opción de mantener un correo interno y además de llevar de forma organizada eventos, reuniones con proveedores y clientes; *servidor web*, se ejecuta continuamente en una computadora de la empresa, manteniéndose a la espera de peticiones por parte de un cliente y responde a estas peticiones, mediante la página web de la compañía; *servidor de archivos*, su función es permitir el acceso remoto a archivos o ficheros almacenados en él o directamente accesibles por este, en el momento que lo desee el usuario.

Adicionalmente, al switch (3COM - 8 puertos) se conecta un Access Point marca D-LINK configurado como enrutador, el cual permite la conexión al Wireless de la empresa. El switch anterior, se enlaza en cascada con otro switch marca 3COM de 16 puertos; del cual depende

la base de datos FOX DATE de la compañía, utilizada para almacenar toda la información referente a clientes, cuentas y maquinarias.

INTRANET ó LAN: Se establece a partir de un rack de 2 switches, sobre el cual se enlazan 6 impresoras láser HP, además de las 12 computadoras de escritorio con las que cuenta la empresa. Dentro de esta red también se encuentra la PBX (Central Privada Automática), encarga de distribuir los procesos de tráfico de llamadas de una oficina, utilizando contestadoras automáticas que interactúan con el llamante mediante el teclado del teléfono; haciendo más rápida la comunicación con el destinatario final.

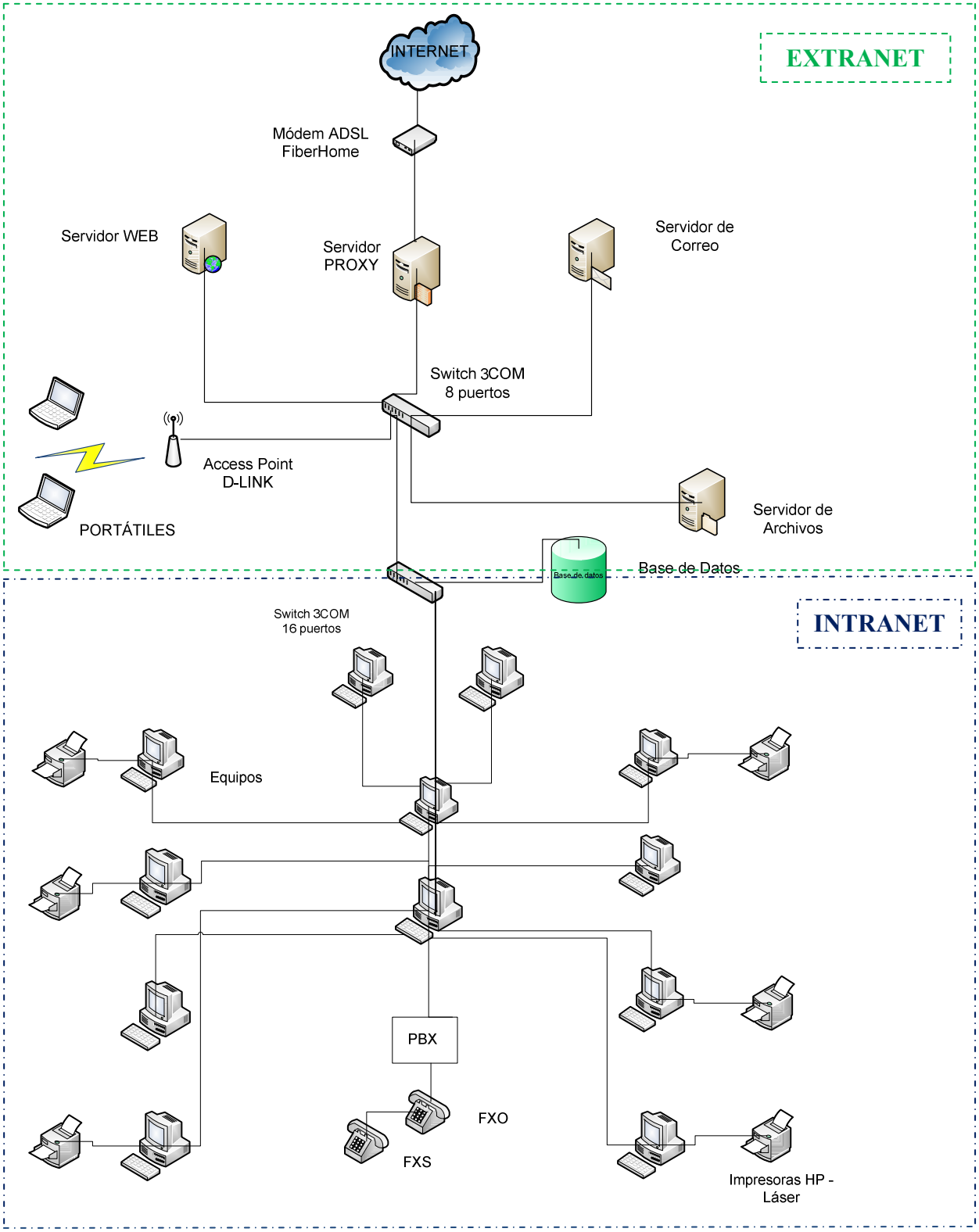


Diagrama de la Red [27]

Figura 3.1

[27] Diagrama de la red de datos, Autor Neumac S.A., fuente Área de Sistemas, año 2010.

3.1.8.1.2. Lógica

La arquitectura es la metodología con que se conectan los protocolos y otros programas de software, siendo beneficiosa su implementación tanto para los usuarios de la red como para los proveedores de hardware y software. En la empresa de estudio (Neumac S.A), la arquitectura de red empleada es un *workgroup*, él cual es un conjunto de 12 computadoras que comparten datos y recursos como: impresoras, scanner y otros dispositivos, pero no requieren de un servidor central. Este mecanismo causa un descontrol en la administración del sistema, además de incurrir en un uso excesivo de la línea LAN; por ello este tipo de implementación es utilizada en un sistema de red sencillo y básico como el que dispone la compañía.

Esta arquitectura de red, trabaja con el protocolo NetBEUI *(Extended User Interface)*, es una versión mejorada de NetBIOS que permite el formato o arreglo de la información en una transmisión de datos. El problema que presenta este protocolo es que no soporta el enrutamiento de mensajes hacia otras redes, solo de forma interna en su red, debido a que su estructura no es jerárquica, sino que tiene una estructura denominada *flat-address space*, es decir, utiliza nombres para ubicar los hosts, en una LAN pequeña, pero, cuando la información requiere ser enviada por una LAN grande o WAN es necesario utilizar direcciones lógicas. Por estas razones, NetBEUI, utiliza otros protocolos de encaminamiento como: IPX/SPX y TCP/IP.

El protocolo IPX (*Internetwork Packet Exchange*); es empleado por NetBEUI, para encaminar paquetes no orientados a conexión dentro de la red LAN de la empresa, esto es,

que no requiere establecer una conexión antes de que los paquetes se envíen a su destino. Y SPX (*Sequenced Packet eXchange*), actúa sobre IPX, y de esta manera asegurar la integridad de los paquetes enviados y de los paquetes de confirmación recibidos entre los nodos individuales de la red de datos de Neumac S.A. Al mismo tiempo regula la velocidad a la que se envían y reciben los paquetes, a manera de reducir el riesgo de corrupción y controlar el tiempo de retardo.

El problema con los protocolos de encaminamiento utilizados por NetBEUI es que ya están en desuso, debido a la aparición de TCP/IP y a su gran acogida en el mercado, la ventaja y utilidad que le brinda a la red de datos de la compañía, es poder utilizar múltiples protocolos de red, para permitir la conectividad con Internet, situación que no se da con los protocolos anteriores.

La solución temporal que se optó en la empresa para resolver estos inconvenientes en su arquitectura de red, es instalar tanto NetBEUI como TCP/IP en cada estación de trabajo y además configurar el workgroup para usar NetBEUI en la comunicación dentro de la LAN *(Intranet)* y TCP/IP para la comunicación hacia afuera de la LAN *(Extranet o WAN).*

3.1.8.2. Topología

Dentro de la empresa la topología utilizada es la conexión en árbol, la cual posee un nodo de enlace troncal, ocupado por dos switches, desde el que se ramifican los demás nodos, para que pasen todos los paquetes, datos e información hacia toda la red. Es importante acotar que si existiera una falla en determinado nodo no implicaría interrupción en las comunicaciones; a pesar de compartir el mismo canal de comunicaciones, debido a la redundancia del nodo, lo

que sí podría suceder es aislamiento en ese nodo debido a una falla puntual en la ruta de conexión del mismo.

La topología en árbol de la red de datos, toma la forma de una combinación de varias topologías en estrella, donde todas sus estaciones están conectadas directamente a un punto central *(switch core)* y todas las comunicaciones entrantes y salientes se realizan necesariamente a través de éste.

Topología en Árbol [28]
Figura 3.2

El arreglo de la figura 3.2 representa la topología empleada en la red de la empresa, consiste en una conexión distribuida en la que un grupo de computadoras proveen de información a otras computadoras, que a su vez se interconectan con otras; compartiendo recursos y aplicaciones a través del nodo central.

[28] Representación topología en árbol, Autor Wikipedia, nuestrowiki.wikispaces.com

3.1.8.3. Extensión

La extensión de red empleada dentro de la compañía es una LAN (*Red de Área Local)*, que se caracteriza por ser *"la interconexión de varias computadoras y periféricos, limitada fisicamente a un edificio para compartir recursos e intercambiar datos y aplicaciones."*[29] El esquema de esta red de área local, permite compartir bases de datos, programas y periféricos como módems, tarjetas RDSI o de memoria, impresoras, faxes, teclados, etc.; facilitando el uso de otros medios de comunicación como servidores de correo, web, y de archivos.

El diseño adecuado de la red LAN de Neumac S.A, proporciona un proceso distribuido en la comunicación entre nodos, es decir, las tareas se pueden distribuir en distintos nodos permitiendo la integración de los procesos e información dentro de la red de datos. Esta funcionalidad de la red de datos brinda a la empresa la posibilidad de centralizar su información, procesos y procedimientos; ayudando así en la administración y gestión de los equipos.

La ventaja de esta red de área local es ofrecer a la empresa una ordenada y flexible gestión de la información y de los recursos, además de no requerir una inversión excesiva en periféricos y compartir el acceso a Internet por medio de una única conexión de banda ancha entre varias computadoras conectados a la red *(conexión ADSL).* Además facilita el almacenamiento y la recuperación de programas y datos utilizados por los empleados y usuarios de la compañía, pero tanto el software como las configuraciones usadas en este tipo de extensión necesitan

[29] Manual de Preparación CISM, Autor ISACA, 2005, Pág. 149, Estados Unidos de Norteamérica.

mantener la seguridad de estos programas y datos. Por desgracia, la mayoría del software LAN brinda un bajo nivel de seguridad, dando mayor importancia a proporcionar capacidad y funcionalidad que seguridad a la información.

Finalmente este análisis de la red de datos a través del levantamiento de los activos de información, permitió obtener un enfoque más a detalle del tipo de red de datos que maneja la empresa, es decir topología, extensión, arquitectura empleada; además del inventario informático de cada ítem de los activos de información restantes que contenga la red de datos de la compañía referente a: hardware, software, comunicaciones, servicios de red, información, personas y procesos. Cada uno de los datos obtenidos dentro de este capítulo, nos servirá como un marco de referencia para encontrar los riesgos y vulnerabilidades a las que está expuesta la red, incluyendo a sus activos de información.

Capítulo 4

4 ANÁLISIS DE RIESGOS DE LA RED DE INFORMACIÓN

Se entiende como análisis de riesgos informáticos, *al proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos la red de datos así como su probabilidad de ocurrencia y el impacto de las mismas* [30], el cual permite determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo y salvaguardar los activos de información de la empresa.

Inicialmente, en este capítulo se ha realizado un inventario consolidado de todos los ítems de activos de información que dispone la empresa, para almacenar las características propias de cada uno dentro de tablas dinámicas, posteriormente se ha estimado el grado de confidencialidad, integridad y disponibilidad de cada grupo de activo de información, aplicando una metodología para el almacenamiento y protección de la información. Y finalmente, se describe la búsqueda de vulnerabilidades que presenta la red de datos de la empresa y cada uno de los activos que la integran, dando énfasis a los que contienen información crítica y relevante para la compañía.

[30] Manual de Preparación CISM, Autor ISACA, 2005, Pág. 78, Estados Unidos de Norteamérica.

4.1 Identificación de Riesgos

Una vez conocidos los recursos que se debe proteger, es momento de identificar las amenazas que los rodean. Una amenaza es la *circunstancia o incidente que tiene la probabilidad de ocasionar daño a un activo de la empresa al explotar las vulnerabilidades en el sistema* [31].

La primera fase contemplada es la búsqueda y análisis de riesgos, es decir identificar el peligro, entendiendo como tal la fuente o situación con capacidad de daño dentro o fuera de la empresa. El siguiente paso va a consistir en estimarse el riesgo, entendiéndose este como una combinación de la posibilidad o probabilidad y de las consecuencias (impacto) que dejaría si se manifestara el peligro.

Por estas razones, se ha realizado una valoración en función del grado de confidencialidad, integridad y disponibilidad que tiene cada ítem en los grupos de activos de información. La metodología empleada es, SU – CADI, perteneciente a la consultora integral en almacenamiento y protección de la información *(SUAPI)*. Dicho método nos permite clasificar los activos de información, almacenar las características de cada activo en un único inventario consolidado, y realizar una estimación cualitativa de los riesgos de los activos de información. Cuando se refiere a clasificar, está metodología define claramente su concepto, *clasificar* significa asignarle valores cualitativos y de riesgo a cada ítem de activo. Por ende este procedimiento basa su teoría de agrupación y clasificación en dos parámetros fundamentales:

[31] Manual de Preparación CISM, Autor ISACA, 2005, Pág. 78, Estados Unidos de Norteamérica.

4.1.1 Inventario Consolidado

Se lo denomina como una base de datos consolidada de todos los ítems de los activos de información donde se almacenan las características propias de cada ítem. Previamente los activos de información fueron agrupados, clasificados (hardware, software, comunicaciones, servicios de red, información, personas, procesos y red) y detalladas sus características técnicas, para posteriormente ubicarlos en una tabla, conocida como *inventario consolidado.*

En las siguientes tablas se observarán los inventarios consolidados de cada grupo de activos de información de Neumac S.A., esta ilustración servirá para un mayor entendimiento a lo explicado anteriormente.

Hardware

Los parámetros escogidos para la agrupación de los activos de hardware estuvieron fundamentados en la *sensibilidad* (asociados con integridad y disponibilidad) de los equipos informáticos disponibles en la empresa, además de considerar el *área de dependencia* (asociado con confidencialidad) al que pertenecen.

Categoría Activo	**Propiedad**	**Tipo**	**Grado**		
			Confidencialidad	***Integridad***	***Disponibilidad***
$Equipos_1$	Área de Ventas	Hardware	Alta	Alta	Alta
$Equipos_2$	Área de Contabilidad y Contaduría	Hardware	Alta	Alta	Alta
$Equipos_3$	Área de Diseño y Mecánica	Hardware	Media	Media	Media

Equipos$_4$	Área de Gerencia e Importaciones	Hardware	Alta	Alta	Alta
Equipos$_2$	Área de Recepción	Hardware	Media	Media	Media
Impresoras	Distribuidas en todas las áreas	Hardware	Baja	Baja	Baja
Escáneres	Área de Ventas Área de Diseño y Mecánica Área de Gerencia e Importaciones	Hardware	Baja	Baja	Baja

Inventario Consolidado de Hardware
Tabla 4.1

Los resultados obtenidos en la agrupación de hardware muestran lo siguiente, son activos **clase A**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado alto para la empresa, son activos de **clase B**, los cuales cuya confidencialidad, integridad y disponibilidad tienen un grado medio, y finalmente son activos de **clase C**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado bajo para la compañía, sujetados a los parámetros de agrupación establecidos previamente dentro de este grupo.

Software

Los parámetros seleccionados para la agrupación de los activos de este grupo estuvieron fundamentados en el *nivel de seguridad* (asociado con disponibilidad e integridad) que brindan los diferentes tipos de software que posee la empresa, además de considerar el *área de dependencia* (asociado con confidencialidad) al que pertenecen.

Nombre Activo	Propiedad	Tipo	Grado		
			Confidencialidad	***Integridad***	***Disponibilidad***
Software de Prevención	Área de Contabilidad y Contaduría Área de Diseño y Mecánica Área de Gerencia e Importaciones	Software	Alta	Alta	Alta
Software de Protección	Área de Contabilidad y Contaduría Área de Gerencia e Importaciones Área de Diseño y Mecánica	Software	Alta	Alta	Alta
Software de Corrección	Distribuidas en todas las áreas	Software	Alta	Alta	Alta
Software de Diseño	Área de Diseño y Mecánica	Software	Media	Media	Media
Software de Entretenimiento	Distribuidas en todas las áreas	Software	Baja	Baja	Baja

Inventario Consolidado de Software
Tabla 4.2

Los resultados obtenidos en la agrupación de software muestran lo siguiente, son activos **clase A**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado alto para la empresa, son activos de **clase B**, los cuales cuya confidencialidad, integridad y disponibilidad tienen un grado medio, y finalmente son activos de **clase C**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado bajo en la organización, sujetados a los parámetros de agrupación establecidos previamente dentro de este grupo.

Comunicaciones

Los parámetros elegidos para la agrupación de los activos de comunicaciones estuvieron fundamentados en el *tipo de información* (relacionado con confidencialidad) y la *sensibilidad* (relacionado con integridad y disponibilidad) que manejan los diferentes dispositivos informáticos disponibles en la empresa.

Nombre Activo	**Propiedad**	**Tipo**	**Grado**		
			Confidencialidad	***Integridad***	***Disponibilidad***
Teléfonos	De toda la empresa	Comunicaciones	Media	Alta	Alta
Faxes	De toda la empresa	Comunicaciones	Baja	Baja	Baja
Switches	De toda la empresa	Comunicaciones	Baja	Alta	Alta
Access Point	De toda la empresa	Comunicaciones	Alta	Alta	Alta
Módem	ISP	Comunicaciones	Baja	Alta	Alta
PBX	De toda la empresa	Comunicaciones	Media	Alta	Alta

Inventario Consolidado de Comunicaciones
Tabla 4.3

Los resultados obtenidos en la agrupación de activos de comunicaciones muestran lo siguiente, son activos **clase A**, aquellos cuya confidencialidad, integridad y disponibilidad

tienen un grado alto para la empresa, son activos de **clase C**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado bajo, son activos de **clase D**, aquellos donde la confidencialidad es media, y la integridad y disponibilidad son altas, y finalmente son activos de **clase E**, donde la confidencialidad es baja, y la integridad y disponibilidad son altas en la organización, sujetados a los parámetros de agrupación establecidos previamente dentro de este grupo.

Servicios de red

Los parámetros seleccionados para la agrupación de los servicios de red estuvieron fundamentados en la *calidad del servicio* (asociado con disponibilidad e integridad) y en el *tipo de información* (asociado a la confidencialidad) que almacenan los servidores disponibles en la empresa.

Nombre Activo	**Propiedad**	**Tipo**	**Grado**		
			Confidencialidad	***Integridad***	***Disponibilidad***
DNS	Proveedor de Servicios de Internet (ISP)	Servicios de red	Baja	Alta	Alta
DHCP	Proveedor de Servicios de Internet (ISP)	Servicios de red	Baja	Alta	Alta
Mail	De toda la empresa	Servicios de red	Alta	Alta	Alta
Archivos	De toda la empresa	Servicios de red	Alta	Alta	Alta
WEB	De toda la empresa	Servicios de red	Alta	Alta	Alta

Proxy	De toda la empresa	Servicios de red	Alta	Alta	Alta
Base de Datos	Área de Ventas	Servicios de red	Alta	Alta	Alta

Inventario Consolidado de Servicios de Red
Tabla 4.4

Los resultados obtenidos en la agrupación de servicios de red muestran lo siguiente, son activos **clase A**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado alto para la empresa, y son activos de **clase E**, aquellos donde la confidencialidad es baja, y la integridad y disponibilidad son altas, sujetados a los parámetros de agrupación establecidos previamente dentro de este grupo.

Información

Los parámetros escogidos para la agrupación de la información estuvieron fundamentados en la confidencialidad, integridad y disponibilidad del *contenido de los datos* que se maneja y almacena en cada área de dependencia dentro de la organización.

Nombre Activo	**Propiedad**	**Tipo**	**Grado**		
			Confidencialidad	***Integridad***	***Disponibilidad***
Nómina de Clientes Nómina de Proveedores	Ventas Almacén Secretaria-Recepcionista Contabilidad	Información Privada	Alta	Alta	Alta
Ingresos Inventario Confirmaciones de Importaciones Remisiones	Bodeguero	Información Privada	Alta	Alta	Alta

Toda la información circulante en la compañía	Gerente General	Información Privada y Pública	Media	Media	Media
Fichas técnicas Información de Ventas	Gerente Técnico	Información Pública	Media	Media	Media
Cuentas de Clientes	Vendedores Técnicos	Información Privada	Alta	Alta	Alta
Fichas técnicas Planos	Jefe de Mantenimiento	Información Pública	Baja	Baja	Baja
Catálogos y folletos publicitarios	Ventas Almacén	Información Pública	Baja	Baja	Baja
Pedidos de Importación	Jefe de Importaciones	Información Privada	Media	Media	Media
Planos Confirmación de Clientes	Jefe de Diseño e Ingeniería Mecánica	Información Pública	Media	Media	Media

Inventario Consolidado de la Información
Tabla 4.5

Los resultados obtenidos en la agrupación de información muestran lo siguiente, son activos **clase A**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado alto para la empresa, son activos de **clase B**, los cuales cuya confidencialidad, integridad y disponibilidad tienen un grado medio, y finalmente son activos de **clase C**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado bajo en la organización, sujetados a los parámetros de agrupación establecidos previamente dentro de este grupo.

Personas

Los parámetros seleccionados para la agrupación de los activos de personas estuvieron fundamentados en la *jerarquía del cargo* (asociado con la disponibilidad e integridad) y en el *tipo de información* (asociado a la confidencialidad) que maneja cada empleado dentro de la compañía.

Propiedad	**Tipo**	**Grado**		
		Confidencialidad	***Integridad***	***Disponibilidad***
Gerente General	Gerente Usuario	Alta	Alta	Alta
Gerente Técnico	Gerente Usuario	Alta	Alta	Alta
Jefe de Diseño e Ingeniería Mecánica	Empleado Usuario	Alta	Alta	Alta
Jefe de Producción y Taller	Empleado Usuario	Alta	Alta	Alta
Soldadores	Empleado Usuario	Baja	Baja	Baja
Operadores de Máquinas	Empleado Usuario	Baja	Baja	Baja
Mecánicos	Empleado Usuario	Media	Media	Media

Jefe de Mantenimiento	Empleado Usuario	Alta	Alta	Alta
Ayudante – Jefe Mantenimiento	Empleado Usuario	Baja	Baja	Baja
Vendedores Técnicos	Empleado Usuario	Media	Media	Media
Jefe de Importaciones	Empleado Usuario	Alta	Alta	Alta
Contadora	Empleado Usuario	Alta	Alta	Alta
Secretaria Recepcionista	Empleado Usuario	Media	Media	Media
Bodeguero	Empleado	Media	Media	Media
Mensajero	Empleado	Media	Media	Media
Personal de Seguridad	Empleado	Alta	Alta	Alta
Vendedores de Almacén	Empleado Usuario	Media	Media	Media

Inventario Consolidado del Personal
Tabla 4.6

Los resultados obtenidos en la agrupación del personal muestran lo siguiente, son activos **clase A**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado alto para la

empresa, son activos de **clase B**, los cuales cuya confidencialidad, integridad y disponibilidad tienen un grado medio, y finalmente son activos de **clase C**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado bajo en la organización, sujetados a los parámetros de agrupación establecidos previamente dentro de este grupo.

Procesos

Los parámetros designados para la agrupación de los procesos estuvieron fundamentados en la *disponibilidad, confidencialidad e importancia* de los mismos al momento de ser ejecutados durante las actividades cotidianas de la empresa.

Nombre Activo	**Propiedad**	**Tipo**	**Grado**		
			Confidencialidad	***Integridad***	***Disponibilidad***
Proceso Administrativo	Gerencia General Gerencia Técnica	Proceso	Alta	Alta	Alta
Proceso de Producción	Jefatura de Producción y Taller	Proceso	Alta	Alta	Alta
Proceso de Control	Secretaria/Recepcionista Bodeguero Personal de Seguridad Contadora	Proceso	Media	Media	Media
Proceso de Diseño	Jefatura de Diseño e Ingeniería Mecánica	Proceso	Media	Media	Media

Proceso de Mantenimiento	Jefatura de Mantenimiento	Proceso	Media	Media	Media
Proceso de Ventas e Importaciones	Jefatura de Importaciones Ventas Técnicas y de Almacén	Proceso	Media	Media	Media

Inventario Consolidado de Procesos
Tabla 4.7

Los resultados obtenidos en la agrupación de los procesos muestran lo siguiente, son activos **clase A**, aquellos cuya confidencialidad, integridad y disponibilidad tienen un grado alto para la empresa, son activos de **clase B**, los cuales cuya confidencialidad, integridad y disponibilidad tienen un grado medio en la organización, sujetados a los parámetros de agrupación establecidos previamente dentro de este grupo.

Red

Los parámetros seleccionados para la agrupación del activo de red estuvieron fundamentados en la *confidencialidad, disponibilidad e integridad de la infraestructura* sobre la cual trabajan equipos, sistemas, dispositivos informáticos y los anteriores activos disponibles en la empresa.

Nombre Activo	**Propiedad**	**Tipo**	**Grado**		
			Confidencialidad	***Integridad***	***Disponibilidad***
Arquitectura Física Arquitectura Lógica	De toda la empresa	Arquitectura de Red	Alta	Alta	Alta

Topología en Árbol	De toda la empresa	Topología de Red	Alta	Alta	Alta
Red LAN	De toda la empresa	Extensión de Red	Alta	Alta	Alta

Inventario Consolidado de Red
Tabla 4.8

Los resultados obtenidos en la agrupación de red muestran lo siguiente, son activos de **clase A**, aquellos donde la confidencialidad es baja, y la integridad y disponibilidad son altas, sujetados a los parámetros de agrupación establecidos previamente dentro de este grupo.

4.1.2 Estimación cualitativa de los riesgos de los activos de información en base a criterios de confidencialidad, integridad y disponibilidad

Este parámetro estima el costo cualitativo en función de los ítems de activos asignados a cada grupo. SU-CADI calcula estos costos, considerando que un ítem puede servir a varias entidades, y que la criticidad de ese ítem para cada uno de ellas puede ser diferente, por ende se basa en criterios de confidencialidad, integridad y disponibilidad.

Previamente la información dentro de la empresa fue clasificada en tres tipos, **tipo A**, contiene datos altamente confidenciales para la empresa, donde su privacidad, integridad y disponibilidad son fundamentales para los negocios de la misma, **tipo B,** dispone de datos de confidencialidad media, es decir información cuya privacidad, integridad y disponibilidad son requeridas para el desempeño óptimo de la compañía por ende no pueden ser asequible para

todas las personas, y finalmente el **tipo C,** almacena datos no confidenciales, que pueden ser expuestos al público y donde su privacidad, integridad y disponibilidad es baja. En la siguiente tabla, se muestra más detalle sobre la clasificación de la información en los diferentes tipos:

CLASIFICACIÓN DE LA INFORMACIÓN		
Tipo A	**Tipo B**	**Tipo C**
Balances económicos, estrategias de negocios, mercadeo de productos, remisiones, balances contables, estados financieros, ficheros en base de datos.	Nómina de clientes, nómina de proveedores, ingresos de mercadería, inventario de importaciones, información de ventas, cuentas de clientes y proveedores, planos técnicos, inventarios de pedidos y confirmación de clientes, mensajes de correo electrónico, detalle llamadas telefónicas.	Catálogos de productos y maquinarias, fichas técnicas, folletos publicitarios.

Clasificación de la Información
Tabla 4.9

Adicionalmente a la clasificación de la información, se realizo una estimación del tiempo de recuperación ó RTO, es decir el tiempo de inactividad que pueden permanecer los equipos y servicios que forman parte de la compañía sin recibir un impacto grave, para a partir de esto valorar, si los activos de información son considerados con un grado alto, medio o bajo de confidencialidad, integridad y disponibilidad para la empresa. Estas estimaciones están basadas en datos estadísticos proyectados por empresas especializadas en análisis de riesgo, las cuales buscan determinar la necesidad cíclica de la información, las interdependencias y requerimientos de la organización, a partir de las necesidades de los usuarios y la gerencia.

ESTIMACIÓN DEL TIEMPO ENTRE FALLAS		
Riesgo	**Tiempo de Inactividad**	**Causas de Interrupción**
Bajo	Hasta 12 horas	Como averías leves se consideraría: Falla en equipos, dispositivos, servidores, aparatos de comunicaciones. Fallas en antivirus debido a las actualizaciones. Cortes de energías, fallos de discos, fuentes de alimentación, tarjetas de red, routers, switches.
Medio	Hasta 24 horas	Como averías graves se consideraría: Desperfectos o fallos que no permitan seguir utilizando un equipo o dispositivo. Cortes de energía, daños en empresas prestadoras de servicio como ISP, empresa eléctrica, compañía de teléfono. Fallos en sistemas operativos.
Alto	Mayor a 48 horas	Como averías muy graves se consideraría: Baja total de los firewalls y antivirus de los equipos que impliquen pérdidas de información. Desconfiguración de los dispositivos de comunicación. Denegación total al acceso de ficheros situados en BSD, servidor web, servidor de correo. Daño de periféricos por problemas eléctricos que contengan información confidencial,

		como disco duros, memorias extraíbles, etc.

Tiempo de Recuperación (RTO)
Tabla 4.10

Se considero adicionalmente, la probabilidad de ocurrencia de cada una de las amenazas señaladas más adelante, en base a la gravedad del impacto de la amenaza, el tipo de activo afectado y como está preparada la empresa para sobrellevarlo. Dichos valores enunciados en esta clasificación fueron extraídos de estadísticas proyectadas por empresas especializadas en mediciones de este tipo (Cobit), las cuales buscan reducir las probabilidades de que un agente interno o externo perjudique recursos y activos de una empresa. A continuación se describe la categorización:

Probabilidad: Se define como posibilidad de incidencia de que ocurra un evento cuya magnitud e impacto se evidencie en pérdida o daño a condiciones locales específicas.

- **Alta:** Todas aquellas amenazas cuya frecuencia de afectación en los activos de información es repetitiva; es decir se presentan hasta diez veces en el año aprovechándose de fallas de seguridad claramente descuidadas en la empresa.

- **Media:** Todas aquellas amenazas cuya frecuencia de afectación en los activos de información es regular, es decir se presentan hasta cinco veces en el año aprovechándose de debilidades de seguridad, aparentemente controlados con sistemas.

- **Baja:** Todas aquellas amenazas cuya frecuencia de afectación en los activos de información es fortuita o nula; es decir se presentan hasta dos veces en el año, y rara vez pueden aprovecharse de fallas de seguridad en la empresa.

Otro factor a considerar, son las amenazas, las cuales han sido clasificadas en altas, medias y bajas, según la repercusión o el alcance que tengan sobre la compañía, midiendo el impacto que dejarían si llegaran a materializarse sobre algún activo de información de la empresa.

- **Alta:** Estas amenazas tienen una repercusión muy grave dentro de la empresa en el caso de producirse; son las amenazas que deberán evitarse siempre. El impacto podría medirse en pérdidas económicas para la empresa de un alto valor monetario y a veces con consecuencias irreparables.

Medición del Impacto

Este cálculo permitirá medir las pérdidas causadas por las amenazas de este tipo, a través del factor de exposición, el valor de aquellos activos categorizados como clase A en la sección anterior y la razón anualizada de ocurrencia.

Factor de Exposición (FE): Este parámetro representa el porcentaje de pérdida que una amenaza alta causaría en los activos clase A dentro de la compañía, tomando como referencia un año laboral, es decir 365 días, donde el porcentaje de exposición es total (100%), y una muestra del total, es decir 1 día, obteniendo como resultado un valor constante.

365 días ---------- 100%
1 día ---------- X

X = 0.2739 %

Valor Activos (VA): Es el valor del costo de adquisición estimado del total de los activos clase A que posea la compañía.

VA= $ 1 000.000

Pérdida Única Esperada (SLE): Representa el valor monetario asignado a la pérdida provocada por una amenaza alta en un evento determinado. Para estimar las

pérdidas incurridas durante la acción de una amenaza alta, se multiplica el valor de los activos, en este caso clase A por el porcentaje del factor de exposición.

SLE = VA * FE
SLE = $ 1 000.000 * 0.2739 %
SLE = $ 273900

Razón anualizada de ocurrencia (ARO): Este parámetro representa la frecuencia estimada para la ocurrencia de una amenaza alta expresada anualmente, se toma como referencia dentro de la clasificación de las probabilidades, la probabilidad alta, obteniendo como valor hasta 10 veces de ocurrencia en el año.

ARO= 10

Pérdida Anualizada Esperada (ALE): Dicho parámetro obtiene el valor monetario que expresa la pérdida anual financiera esperada por la organización debido a una amenaza alta, multiplicando la pérdida única esperada por la razón anualizada de ocurrencia.

ALE= SLE * ARO
ALE = $ 273900 * 10
ALE = $ 2 709 000

- **Media:** Las amenazas tienen una repercusión grave dentro de la compañía en el caso de producirse. El impacto podría medirse en pérdidas económicas considerables para la empresa pero que tienen una solución a corto plazo.

Medición del Impacto

Este cálculo permitirá medir la pérdida causada por las amenazas de este tipo, a través del factor de exposición, el valor de aquellos activos categorizados como clase B, D, E en la sección anterior y la razón anualizada de ocurrencia.

Factor de Exposición (FE): Este parámetro representa el porcentaje de pérdida que una amenaza media causaría en los activos clase B, D, E dentro de la compañía, tomando como referencia un año laboral, es decir 365 días, donde el porcentaje de

exposición es total (100%), y una muestra del total, es decir 1 día, obteniendo como resultado un valor constante.

365 días ---------- 100%
1 día ---------- X

X = 0.2739 %

Valor Activos (VA): Es el valor del costo de adquisición estimado del total de los activos clase B, D, E que posea la empresa.

VA= $ 100.000

Pérdida Única Esperada (SLE): Representa el valor monetario asignado a la pérdida provocada por una amenaza media en un evento determinado. Para estimar las pérdidas incurridas durante la acción de una amenaza media, se multiplica el valor de los activos, en este caso clase B, D, E por el porcentaje del factor de exposición.

SLE = VA * FE
SLE = $ 100.000 * 0.2739 %
SLE = $ 27390

Razón anualizada de ocurrencia (ARO): Este parámetro representa la frecuencia estimada para la ocurrencia de una amenaza media expresada anualmente, se toma como referencia dentro de la clasificación de las probabilidades, la probabilidad media, obteniendo como valor hasta 5 veces de ocurrencia en el año.

ARO= 5

Pérdida Anualizada Esperada (ALE): Dicho parámetro obtiene el valor monetario que expresa la pérdida anual financiera esperada por la organización debido a una amenaza media, multiplicando la pérdida única esperada por la razón anualizada de ocurrencia.

ALE= SLE * ARO
ALE = $ 27390 * 5

ALE = $ 130 950

- **Baja:** Las amenazas tienen una repercusión leve dentro de la empresa. Su impacto pérdidas cuantiosas en valor monetario y no afectan prácticamente en ningún grado a la seguridad de la organización.

Medición del Impacto

Este cálculo permitirá medir la pérdida causada por las amenazas de este tipo, a través del factor de exposición, el valor de aquellos activos categorizados como clase C en la sección anterior y la razón anualizada de ocurrencia.

Factor de Exposición (FE): Este parámetro representa el porcentaje de pérdida que una amenaza baja causaría en los activos clase C dentro de la compañía, tomando como referencia un año laboral, es decir 365 días, donde el porcentaje de exposición es total (100%), y una muestra del total, es decir 1 día, obteniendo como resultado un valor constante.

365 días ---------- 100%
1 días ---------- X

X = 0.2739 %

Valor Activos (VA): Es el valor del costo de adquisición estimado del total de los activos clase C que posea la empresa.

VA= $ 10.000

Pérdida Única Esperada (SLE): Representa el valor monetario asignado a la pérdida provocada por una amenaza media en un evento determinado. Para estimar las pérdidas incurridas durante la acción de una amenaza baja, se multiplica el valor de los activos, en este caso clase C por el porcentaje del factor de exposición.

SLE = VA * FE
SLE = $ 10.000 * 0.2739 %
SLE = $ 2739

Razón anualizada de ocurrencia (ARO): Este parámetro representa la frecuencia estimada para la ocurrencia de una amenaza baja expresada anualmente, se toma como referencia dentro de la clasificación de las probabilidades, la probabilidad baja, obteniendo como valor hasta 2 veces de ocurrencia en el año.

ARO= 2

Pérdida Anualizada Esperada (ALE): Dicho parámetro obtiene el valor monetario que expresa la pérdida anual financiera esperada por la organización debido a una amenaza baja, multiplicando la pérdida única esperada por la razón anualizada de ocurrencia.

ALE= SLE * ARO
ALE = $ 2739 * 2
ALE = $ 5478

Los criterios utilizados para la agrupación, ordenamiento y categorización de las amenazas a las que están expuestos los activos de información de la empresa, estuvieron fundamentados en las principales propiedades de la información, definidos de la siguiente manera:

1. **CONFIDENCIALIDAD**

Alta

- Robo de activos de información de la empresa, que repercute en la sustracción de equipamientos, sistemas y documentos que almacenan datos del tipo A para el negocio de la empresa.

  La gravedad de la amenaza puede considerarse como alta debido a que la información sustraída es de máxima utilidad para la empresa, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000. La probabilidad de que se produzca es baja debido a que la

empresa cuenta con medidas físicas de protección necesarias para que los equipos y sistemas informáticos estén resguardados.

- Pérdida no intencionada de activos directamente relacionados con información tipo A, debido a fallos del personal.

  La gravedad de la amenaza puede considerarse como alta debido a que la información no está replicada en ningún otro equipo, ni generalmente, en ningún otro soporte, la pérdida del fichero sería irreparable, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000. La probabilidad de que se produzca es media debido a que, generalmente, dentro de la empresa únicamente se cuenta con una copia de cada fichero almacenado pero el personal es cuidadoso con los equipos y sistemas de la compañía.

- Acceso no autorizado a los activos de información de la empresa que almacenen datos e información de tipo A.

  La gravedad de la amenaza puede considerarse como alta debido a que la información de este tipo requiere una confidencialidad, integridad y confidencialidad esenciales para la empresa, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000. La probabilidad de que se produzca es media debido a que a pesar de que no existe el control y resguardo necesario para este tipo de información, son pocos los equipos informáticos que contienen estos datos, además que siempre están en custodia del Gerente o responsable de las áreas involucradas.

- Falla en las medidas de seguridad de los activos de información dentro de la empresa durante un tiempo superior a 48 horas que afecte directamente a información tipo A.

  La gravedad de la amenaza puede considerarse como alta, porque un fallo grave en las medidas de seguridad de la empresa perjudicará

gravemente el negocio de ésta, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000. La probabilidad de que se produzca es baja, pues las medidas de seguridad física están en correcto funcionamiento, y aunque las medidas de software no tengan un control adecuado sobre su actividad, se podría recurrir al soporte técnico de terceras personas.

Media

- Robo de activos de activos de información de la empresa, que repercute en la sustracción de equipamientos, sistemas y documentos que almacenan datos del tipo B.

  La gravedad de la amenaza puede considerarse como media debido a que la información de este tipo es un importante activo pero no es vital para futuros negocios de la compañía, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950. La probabilidad de que se produzca es baja debido a que la empresa cuenta con medidas físicas de protección necesarias para que los equipos y sistemas informáticos estén resguardados.

- Pérdida no intencionada de activos directamente relacionados con información tipo B, debido a fallos del personal.

  La gravedad de la amenaza puede considerarse como media debido a que puede afectar al retraso de alguna de las operaciones de la empresa si no se puede acceder momentáneamente a la información de este tipo, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950. La probabilidad de que se produzca es media debido a que, generalmente, dentro de la empresa únicamente se cuenta con una copia de cada fichero almacenado pero el personal es cuidadoso con los equipos y sistemas de la compañía.

- Acceso no autorizado a los activos de información de la empresa que almacenen datos e información tipo B.

  La gravedad de la amenaza puede considerarse como media debido a que la información de este tipo es un importante activo para negocios actuales y futuros para la empresa, además para el desarrollo normal de sus actividades, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950. La probabilidad de que se produzca es alta debido a que, generalmente, dentro de la empresa no existe el control y resguardo necesario para este tipo de información, además existen varios equipos y sistemas informáticos que contienen estos datos por ende el nivel de seguridad brindado es bajo.

- Falla en las medidas de seguridad de los activos de información dentro de la empresa durante un tiempo máximo de 24 horas y que afecte directamente a información tipo B.

  La gravedad de la amenaza puede considerarse como media pues aunque el tiempo de fallo de la seguridad no sea extenso, compromete seriamente a la empresa y sus operaciones, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950. La probabilidad de que se produzca es media pues como se ha comentado las medidas de seguridad física están en correcto funcionamiento, pero las medidas software no tienen un control adecuado sobre su actividad.

Baja

- Robo de activos de la empresa en el cual son sustraídos documentos que almacenan datos del tipo C para el negocio de la empresa.

  La gravedad de esta amenaza puede considerarse como baja puesto a la importancia de la información perdida, su impacto se contabiliza en pérdidas económicas alrededor de $ 5478. La probabilidad de que se

produzca es media debido a que está expuesta al público y por ende puede ser sustraída.

- Pérdida de activos que contienen información tipo C, debido a fallos del personal.

  La gravedad de esta amenaza puede considerarse como baja puesto a la importancia de la información almacenada en esos ficheros pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478. La probabilidad de que ocurra es media, debido a que los empleados no brindan un nivel alto de protección a este tipo de datos, sin embargo existen pocos equipos y sistemas informáticos que almacenen este tipo de datos.

- Acceso no autorizado a los activos de información de la empresa que almacenen datos e información tipo C.

  La gravedad de la amenaza puede considerarse como baja debido a que los datos contenidos no son confidenciales para la empresa, por ende su exposición al público es normal, aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478. La probabilidad de que se produzca es alta debido a que, generalmente, dentro de la empresa no existe control y resguardo necesario para este tipo de información.

- Falla de seguridad de los activos de información dentro de la empresa durante un periodo inferior a 12 horas, que afecte directamente a información tipo C.

  La gravedad de esta amenaza puede considerarse como baja puesto que aunque el fallo de elementos de seguridad es peligroso, estos no afectan a información crítica pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478. La probabilidad de que ocurra es alta ya que pequeños errores o fallos temporales suelen ser frecuente.

2. INTEGRIDAD

Alta

- Se daría por desastres naturales, cuyo impacto en el edificio donde se encuentra la empresa, provocará un daño estructural en el edificio, y por ende daños severos en los activos de información de la empresa.

  La gravedad de la amenaza sería muy alta porque los daños estructurales generados serían numerosos, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000, pero la probabilidad de que se produzca es media pues la empresa está muy bien protegida contra ese tipo de amenazas, posee infraestructura antisísmica.

- Si un gran incendio afectara a todo el edificio donde está ubicada la empresa, dejando inutilizadas completamente todas las instalaciones de la compañía así como destruido todo el equipamiento informático y la información vital del tipo A que se encuentre en cualquier tipo de soporte.

  La gravedad de la amenaza sería alta porque podría producir la paralización total de la actividad de la empresa por un periodo de tiempo muy largo si no se dispone de una copia de Backup convenientemente actualizada y que no se localizara en las instalaciones que han sido afectadas por el fuego, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000; aunque la probabilidad de que se llegue a materializar es baja debido a que si se produce un incendio de estas características debido a un descuido o de una forma intencionada la empresa cuenta con extinguidores y

dispositivos para ayudar a controlar el fuego y evitar que no se produzcan daños graves en el edificio.

- Si un intruso realiza un análisis a la red de datos de la empresa a través del escaneo de puertos y del tráfico de la red para explorar servicios y sistemas operativos vulnerables.

  La gravedad de la amenaza sería alta porque si el intruso cumple su objetivo y descubre puntos débiles dentro de la red, fácilmente podría ocasionar pérdidas de información, capturas de contraseñas, entre otros graves problemas, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000, y la probabilidad de que se llegue a materializar es media debido a que la infraestructura de la red es propensa a estos ataques consecuencia de su bajo nivel de seguridad.

- Ataques de fuerza bruta a la red de datos con el fin de conseguir contraseñas o información tipo A de usuarios administrados o con privilegios altos dentro de la red.

  La gravedad de la amenaza sería alta porque se capturarían claves de administrador, se podrían modificar accesos, ACLs, además de información tipo A, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000 y la probabilidad de que se llegue a materializar es alta debido a que las contraseñas usadas dentro de la red no son robustas por ende fácilmente pueden ser descifradas.

- Se daría por ataques de enmascaramiento o spoofing a la red, donde el intruso trataría de obtener acceso a datos tipo A o recursos de la misma suplantando la identidad de usuarios autenticados.

  La gravedad de la amenaza sería alta porque si el intruso llegaría a autenticarse como usuario legítimo y con altos privilegios en la red de datos podría robar, modificar o eliminar información tipo A, su

impacto se contabiliza en pérdidas económicas de $ 2 709 000 y la probabilidad de que se llegue a materializar es media debido a que la infraestructura de la red es propensa a estos ataques consecuencia de su bajo nivel de seguridad.

- Acceso no autorizado mediante la Internet a servicios basados en Web, como correo electrónico, configuración del portal web, para explorar las vulnerabilidades existentes.

  La gravedad de la amenaza sería alta porque se obtendría acceso a servicios privados de la empresa y se podrían alterar configuraciones, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de seguridad de los servidores existentes en la compañía.

- Si la red de datos sufre ataques de bombardeo y spamming de correo electrónico, generando que colapse el servidor de mails durante un tiempo mayor a 48 horas.

  La gravedad de la amenaza sería alta porque si colapsa el servidor de mails existiría retardo en las comunicaciones con el extranjero, proveedores, clientes, y afectaría al negocio debido al extenso tiempo de inactividad, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de seguridad del servidor de correo electrónico.

- Si la red de datos sufre ataques de denegación de servicio (DoS) ocasionado pérdida de la conectividad o sobrecarga de los recursos computacionales de los sistemas de la misma durante un tiempo mayor a 48 horas.

La gravedad de la amenaza sería alta porque implica un grave problema para las actividades normales de la compañía, además no permite que la red de abasto a la cantidad de usuarios existentes, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de seguridad que presenta la infraestructura de red.

- Si la red de datos es víctima de ataques por medio de Botnets, permitiendo que sea contralada remotamente y manipulada información tipo A para que cada equipo y sistema disponible se convierta en "zombie" durante un tiempo mayor a 48 horas.

  La gravedad de la amenaza sería alta porque un ataque de estos generaría consumo excesivo de los recursos de las máquinas y del ancho de banda, además que la integridad de la información tipo A estaría en peligro, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de resguardo que brindan los sistemas de seguridad informática en la empresa.

Media

- Se daría por desastres naturales también, y el impacto lo recibiría directamente al suministrador de servicios de la empresa, como suministrador de energía eléctrica, ISP, compañía de seguros, etc.; afectando las actividades cotidianas de la compañía.

  La gravedad de esta amenaza puede considerarse como media porque puede afectar el funcionamiento normal de la empresa así como al funcionamiento de los equipos informáticos de ésta si los problemas de las empresas suministradoras son graves y los cortes del servicio se prolongan demasiado, su impacto se contabiliza en pérdidas

económicas alrededor de $ 130 950 y la probabilidad de que ocurra es media pues es frecuente que puedan producirse cortes intermitentes de luz durante una tormenta o sismo.

- Incendio en una parte localizada del edificio que aunque no afecte directamente el equipamiento informático puede dificultar las labores normales de trabajo dentro de la empresa.

  La gravedad de la amenaza puede considerarse como media porque al producirse un incendio se generaría retrasos en ciertas áreas de la compañía, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se produzca es baja aunque en este caso los equipos de extinción tendrían mucho más fácil la labor de extinguir rápidamente el fuego.

- Si un intruso realiza un análisis del tráfico de la red de datos de la empresa empleando un *sniffer* para capturar claves o información tipo B.

  La gravedad de la amenaza sería media porque podría ocasionar pérdidas de información tipo B ó capturas de contraseñas, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se llegue a materializar es alta debido a que la infraestructura de la red posee un bajo nivel de seguridad sobre todo en dispositivos de comunicaciones.

- Ataques de fuerza bruta a la red de datos con el fin de conseguir contraseñas o información tipo B de usuarios con privilegios restringidos dentro de la red.

  La gravedad de la amenaza sería media porque se capturarían claves de usuarios con privilegios restringidos, además de información tipo B, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950

y la probabilidad de que se llegue a materializar es alta debido a que las contraseñas usadas dentro de la red no son robustas por ende fácilmente pueden ser descifradas.

- Se daría por ataques de enmascaramiento o spoofing a la red, donde el intruso trataría de obtener acceso a datos tipo B o recursos de la misma suplantando la identidad de usuarios autenticados.

  La gravedad de la amenaza sería media porque si el intruso llegaría a autenticarse podría robar, modificar o eliminar información tipo B, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se llegue a materializar es media debido a que la infraestructura de la red es propensa a estos ataques consecuencia de su bajo nivel de seguridad.

- Acceso no autorizado mediante la Internet a servicios como correo electrónico, configuración del portal web, para acceder a información tipo B.

  La gravedad de la amenaza sería media porque se obtendría acceso a servicios privados de la empresa, además se manipularía información tipo B, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de seguridad de los servidores existentes en la compañía.

- Si la red de datos sufre ataques de bombardeo y spamming de correo electrónico, generando que colapse el servidor de mails durante un tiempo máximo de 24 horas.

  La gravedad de la amenaza sería media porque si colapsa el servidor de mails existiría retardo en las comunicaciones pero se puede acceder a los servidores alternos (S. Web) para mantener actualizado el vínculo

con proveedores y clientes, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de seguridad del servidor de correo electrónico.

- Si la red de datos sufre ataques de denegación de servicio (DoS) ocasionado pérdida de la conectividad o sobrecarga de los recursos computacionales de los sistemas de la misma durante un tiempo máximo de 24 horas.

  La gravedad de la amenaza sería media porque no permitiría que la red de abasto a la cantidad de usuarios existentes durante el tiempo de inactividad del servicio, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se materialice es media debido al bajo nivel de seguridad que presenta la infraestructura de red.

- Si la red de datos es víctima de ataques por medio de Botnets, permitiendo que sea contralada remotamente y manipulada información tipo B para que cada equipo y sistema disponible se convierta en "zombie" durante un tiempo máximo de 24 horas.

  La gravedad de la amenaza sería media porque el tiempo de control sobre la red no es extenso aunque la integridad de información tipo B estaría en peligro, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de resguardo que brindan los sistemas de seguridad informática en la empresa.

Baja

- Se daría en el caso de cortes de electricidad de corta duración por problemas en la instalación eléctrica del edificio debidos a una tormenta o por problemas de las líneas de la empresa suministradora.

  La gravedad de esta amenaza puede considerarse como baja porque no contar con energía eléctrica por un tiempo escaso no paralizaría completamente a la empresa, pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478 y la probabilidad de que ocurra es alta pues es frecuente que puedan producirse cortes intermitentes de luz durante una tormenta o sismo.

- Incendio en una oficina de computadoras dentro de la empresa y que afecte directamente a equipos o periféricos en concretos.

  La gravedad de esta amenaza puede considerarse como baja porque las pérdidas materiales serían leves, pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478. La probabilidad de que ocurra es alta, pues es relativamente fácil que se produzca un cortocircuito que provoque un fuego aunque como es centralizado sería de fácil y rápida extinción.

- Si un intruso realiza un análisis del tráfico de la red de datos de la empresa empleando un *sniffer* para capturar claves o información tipo C.

  La gravedad de la amenaza sería baja porque podría ocasionar pérdidas de información tipo C, pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478 y la probabilidad de que se llegue a materializar es alta debido a que la infraestructura de la red posee un bajo nivel de seguridad sobre todo en dispositivos de comunicaciones.

- Ataques de fuerza bruta esporádicos a la red de datos con el fin de conseguir contraseñas o información tipo C de usuarios normales y de pocos privilegios dentro de la red.

  La gravedad de la amenaza sería baja porque se capturarían claves de usuarios con pocos privilegios, además de información tipo C, pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478, y la probabilidad de que se llegue a materializar es alta debido a que las contraseñas usadas dentro de la red no son robustas por ende fácilmente pueden ser descifradas.

- Se daría por ataques de enmascaramiento o spoofing a la red, donde el intruso trataría de obtener acceso a datos tipo C o recursos de la misma suplantando la identidad de usuarios autenticados.

  La gravedad de la amenaza sería baja porque si el intruso llegaría a autenticarse podría manipular información tipo C, pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478 y la probabilidad de que se llegue a materializar es media debido a que la infraestructura de la red es propensa a estos ataques consecuencia de su bajo nivel de seguridad.

- Acceso no autorizado mediante la Internet a servicios como correo electrónico, configuración del portal web, para acceder a información tipo C.

  La gravedad de la amenaza sería baja porque se obtendría se manipularía información tipo C, pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de seguridad de los servidores existentes en la compañía.

- Si la red de datos sufre ataques de bombardeo y spamming de correo electrónico, generando que colapse el servidor de mails durante un tiempo máximo de 12 horas.

  La gravedad de la amenaza sería baja porque si colapsa el servidor de mails existiría retardo en las comunicaciones pero se puede acceder al correo personal de cada empleado para tramitar o gestionar cualquier actividad importante durante el corto período de inactividad, pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de seguridad del servidor de correo electrónico.

- Si la red de datos sufre ataques de denegación de servicio (DoS) ocasionado pérdida de la conectividad o sobrecarga de los recursos computacionales de los sistemas de la misma durante un tiempo máximo de 12 horas.

  La gravedad de la amenaza sería baja porque aunque se suspendería el servicio y por ende no habría abasto a la cantidad de usuarios existente, el tiempo de inactividad es corto, pero aún así su impacto se contabiliza en pérdidas económicas alrededor de $ 5478 y la probabilidad de que se materialice es media debido al bajo nivel de seguridad que presenta la infraestructura de red.

- Si la red de datos es víctima de ataques por medio de Botnets, permitiendo que sea contralada remotamente y manipulada información tipo C para que cada equipo y sistema disponible se convierta en "zombie" durante un tiempo máximo de 12 horas.

  La gravedad de la amenaza sería baja porque el tiempo de control sobre la red no es extenso, se volverían lentos los sistemas y equipos de la empresa por el consumo excesivo de recursos, y se compromete la integridad de información tipo C, su impacto se contabiliza en

pérdidas económicas alrededor de $ 5478 y la probabilidad de que se llegue a materializar es media debido al bajo nivel de resguardo que brindan los sistemas de seguridad informática en la empresa.

3. DISPONIBILIDAD

Alta

- Corte eléctrico que se prolongue varios días. Afectará gravemente al desarrollo normal de las actividades de la empresa durante un largo periodo de tiempo, mayor a 48 horas de trabajo.

  La gravedad de la amenaza sería alta porque interrumpiría las operaciones y actividades cotidianas de la empresa, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000 aunque la probabilidad de que se llegue a materializar es baja, debido a que entran en funcionamiento sistemas de energía alternos como UPS.

- Falla en los Sistemas Operativos de todos los equipos informáticos de la empresa durante un tiempo superior a 48 horas.

  La gravedad de la amenaza puede considerarse como alta porque perjudicará gravemente el negocio de la empresa debido, sobre todo, a que pueden producirse importantes agujeros de seguridad, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000 aunque la probabilidad de que se produzca es baja, pues los Sistemas Operativos están correcto funcionamiento, además se podría recurrir a soporte técnico de terceras personas.

- Falla en los sistemas de comunicación informática durante un tiempo superior a 48 horas.

La gravedad de la amenaza puede considerarse como alta porque un fallo en las comunicaciones informáticas afectará especialmente a la empresa si se produce en épocas del año determinadas, en las que por ejemplo debido al fallo en las comunicaciones se imposibilite el acceso de los clientes al portal web, envío de e-mails, etc., desde la organización, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000. La probabilidad de que se produzca es media, debido a que la compañía depende de empresas externas proveedoras del servicio de comunicaciones.

- Pérdida temporal superior a 48 horas del acceso a ficheros con información tipo A para la empresa.

  La gravedad de la amenaza puede considerarse como alta porque la denegación al acceso de la información afectará a la empresa en la realización de sus actividades, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000. La probabilidad de que se produzca es media, porque si existe Backup de algunos ficheros pero no de todos, y por lo general las copias de seguridad son respaldadas cada tres meses, dejando este intervalo de tiempo desprotegido.

- Falla indefinida en todos de los servidores de la empresa mayor a 48 horas.

  La gravedad de la amenaza puede considerarse como alta porque denegaría el acceso a los clientes al portal web, las importaciones y exportaciones se retrasarían e interrumpiría las actividades operativas de la organización, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000 y la probabilidad de que se produzca es media, debido al mal estado de funcionamiento de los equipos informáticos y de la baja seguridad de los mismos, sin embargo se podría recurrir en soporte técnico a terceras personas.

- Falla indefinida en todas las estaciones de trabajo de que dispone la empresa mayor a 48 horas.

  La gravedad de la amenaza puede considerarse como alta porque perjudicaría gravemente el negocio de la empresa, su impacto se contabiliza en pérdidas económicas alrededor de $ 2 709 000 aunque la probabilidad de que se produzca es media, debido al mal estado de funcionamiento de los equipos informáticos sin embargo se podría disponer de soporte técnico de terceras personas.

Media

- Corte eléctrico de menor duración y que afectará al desarrollo de las actividades de la empresa por un tiempo no superior a 24 horas.

  La gravedad de la amenaza puede considerarse como media porque altera de forma leve las actividades y operaciones de la compañía, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se produzca es baja debido a que la empresa cuenta con sistemas de alimentación interrumpida, que abastecerían con energía eléctrica durante ese tiempo.

- Falla en el Sistema Operativo de algunos de los equipos informáticos durante un tiempo máximo de 24 horas.

  La gravedad de la amenaza puede considerarse como media, pues si falla un equipo en el que se encuentra información tipo B y no existen copias de los ficheros podría ocasionar pérdidas y retrasos en las actividades, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950. La probabilidad de que se produzca es baja pues los Sistemas Operativos están correctamente actualizados, además se podría recurrir a soporte técnico de terceras personas.

- Falla en los sistemas de comunicación informática durante un tiempo no superior a 24 horas.

  La gravedad de la amenaza puede considerarse como media porque un fallo en las comunicaciones informáticas no afectará especialmente a la empresa, salvo que el fallo se produzca en épocas del año determinadas donde más ventas realiza la empresa (Junio - Septiembre) y evite el acceso y distribución de información tipo B, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950. La probabilidad de que se produzca es media, debido a que la compañía depende de empresas externas proveedoras del servicio de comunicaciones.

- Pérdida temporal no superior a 24 horas del acceso a ficheros de tipo B.

  La gravedad de la amenaza puede considerarse como media porque la denegación al acceso de la información afectará a la empresa en la realización de sus actividades, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950. La probabilidad de que se produzca es media, porque si existe Backup de algunos ficheros pero no de todos, y por lo general las copias de seguridad son respaldadas cada tres meses, dejando este intervalo de tiempo desprotegido.

- Falla temporal de un período máximo de 24 horas de trabajo en uno de los servidores de la empresa.

  La gravedad de la amenaza puede considerarse como media porque impediría el acceso a aplicaciones, ficheros e información necesaria en la empresa, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se produzca es media, debido al mal estado de funcionamiento de los equipos informáticos, a la baja

seguridad de los mismos o por la dependencia existen a empresas proveedores de servicios.

- Falla temporal de un período máximo de 24 horas en uno de las estaciones de trabajo que dispone la compañía.

La gravedad de la amenaza puede considerarse como media porque retrasaría las actividades normales de la empresa a pesar de que el tiempo de interrupción es corto, su impacto se contabiliza en pérdidas económicas alrededor de $ 130 950 y la probabilidad de que se produzca es media, debido al mal estado de funcionamiento de los equipos informáticos, sin embargo se podría disponer de soporte técnico de terceras personas.

Baja

- Corte eléctrico de poca duración y que afectará al desarrollo de las actividades de la empresa por 12 horas o menos.

La gravedad de esta amenaza puede considerarse como baja porque la inactividad del servicio eléctrico no es extenso, su impacto se contabiliza en pérdidas económicas alrededor de $ 5478 y la probabilidad de que ocurra es media pues es relativamente fácil que se produzca un pequeño corte en el suministro eléctrico debido, por ejemplo a una sobrecarga en la red del suministrador, pero rápidamente entrarían en funcionamiento los UPS que dispone la compañía.

- Falla en el Sistema Operativo de un equipo que contenga información tipo C durante un periodo inferior a 12 horas.

La gravedad de esta amenaza puede considerarse como baja puesto que si el equipo contiene información tipo C, y el periodo del fallo es inferior a 12 horas, su impacto se contabiliza en pérdidas económicas

alrededor de $ 5478. La probabilidad de que ocurra es baja, pues los Sistemas Operativos están correctamente actualizados y se podría recurrir a soporte técnico de terceras personas.

- Falla en los sistemas de comunicación durante un periodo inferior a 12 horas.

  La gravedad de esta amenaza puede considerarse como baja puesto que cortes de baja duración en las comunicaciones no afectan en ninguna forma a los procesos realizados en la empresa, su impacto se contabiliza en pérdidas económicas alrededor de $ 5478. La probabilidad de que ocurra es media pues debido a problemas de la empresa suministradora es frecuente sufrir cortes leves de servicio a lo largo de un día.

- Falla menor de un período máximo de 12 horas en alguno de los servidores de la empresa.

  La gravedad de la amenaza puede considerarse como baja porque el tiempo de inactividad es corto, su impacto se contabiliza en pérdidas económicas alrededor de $ 5478 y la probabilidad de que se produzca es media, debido al mal estado de funcionamiento de los equipos informáticos o por fallas de procesamiento en los sistemas.

- Pérdida temporal no superior a 12 horas del acceso a ficheros de tipo B.

  La gravedad de la amenaza puede considerarse como baja porque la denegación al acceso de este tipo de información, su impacto se contabiliza en pérdidas económicas alrededor de $ 5478. La probabilidad de que se produzca es media, porque si existe Backup de algunos ficheros pero no de todos, y por lo general las copias de seguridad son respaldadas cada tres meses, dejando este intervalo de tiempo desprotegido.

- Falla de dispositivos de entrada y salida que formen parte alguna estación de trabajo de que dispone la empresa.

  La gravedad de esta amenaza puede considerarse como baja porque este incidente no afectaría gravemente a la empresa, su impacto se contabiliza en pérdidas económicas alrededor de $ 5478 y la probabilidad de que ocurra es alta, debido a que algunos de estos dispositivos poseen problemas de averías y están en estado obsoleto.

Después del análisis de riesgos efectuado a los activos de la red de datos de la empresa, se puede concluir que el factor de exposición de dichos recursos es alto, debido al bajo nivel de seguridad que disponen, además el cálculo del impacto de las amenazas estimo pérdidas considerables e importantes en los activos de información si no se logra mitigar el riesgo dentro de límites y costos aceptables para la empresa.

4.2 Vulnerabilidades

En el apartado anterior se han enumerado las posibles amenazas que podrían afectar a la empresa describiendo el virtual impacto que tendría dentro de la compañía en el caso de producirse y la probabilidad de que dicho evento se materialice, además se realizo un registro de aquellas amenazas que ya han dañado activos de información de la organización y el impacto que dejaron en la misma. En esta sección se van a identificar las vulnerabilidades que tiene la empresa y que pueden ser aprovechadas por alguna amenaza para producir algún tipo de daño.

Para evaluar las distintas vulnerabilidades, se van a seguir las mismas categorías de activos de información usadas para la identificación de riesgos, es decir hardware, software, comunicaciones, servicios de red, información, personas, procesos y red. La mayor parte de las intrusiones a los sistemas que se producen hoy en día se deben a la explotación de vulnerabilidades, por ello es de vital importancia poder identificar todas aquellas vulnerabilidades susceptibles de ser aprovechadas por una amenaza, para evitar que ésta llegue a materializarse. La vulnerabilidades pueden deberse a fallos de seguridad de la propia empresa o fallos de seguridad en los productos suministrados por terceras empresas.

4.2.1 Vulnerabilidades relacionadas con el Hardware

Dentro de la empresa, los problemas con el hardware afectan directamente a los procesos informáticos de la organización lo que puede provocar graves problemas en el transcurso normal de los negocios de la misma. Se pueden identificar las siguientes vulnerabilidades:

- *Falta de políticas de Backup.*
- *Falta de dispositivos SAI que garanticen el suministro eléctrico.*
- *Equipos informáticos obsoletos.*
- *Averías en periféricos de entrada y salida.*
- *Escases en memoria RAM, lo que obliga al personal a almacenar información importante en dispositivos que pueden ser fácilmente sustraídos (CD, DVD, memorias USB).*

4.2.2 Vulnerabilidades relacionadas con el Software

Los fallos y errores de software son muy perjudiciales, y son éstos los que más fácilmente pueden llegar a producirse si no se tiene cuidado con su correcto mantenimiento. Las vulnerabilidades del software son las más sensibles de ser aprovechadas por amenazas para infligir algún tipo de daño dentro de esta empresa. Se pueden identificar las siguientes vulnerabilidades:

- *Mala actualización de los sistemas como antivirus, firewalls y demás software de seguridad, que pueden provocar la infección de virus.*
- *Se dispone de software elaborado para la empresa por personal externo a ésta (sistema de inventarios), pero que no responde adecuadamente del mantenimiento del mismo.*
- *Se emplean versiones de sistemas operativos que no cuentan con las características necesarias para un óptimo funcionamiento de la red.*
- *No existen políticas para la adquisición y mantenimiento del software dentro de la empresa.*

- Existe violación a las licencias de uso de software al utilizar números excesivos o sin derechos de autor de copias de software.

4.2.3 Vulnerabilidades relacionadas con la red

La infraestructura de la red de datos de la empresa es uno de los elementos más vulnerables a ser explotados por una amenaza, si no se cuida correctamente su mantenimiento y protección. Se pueden identificar las siguientes vulnerabilidades:

- Bajo nivel de seguridad a la hora de realizar accesos inalámbricos a la red interna de la empresa.
- Falencias en el protocolo de red usado NetBEUI, debido a que no tiene encaminamiento, sólo puede usarse para comunicar nodos en el mismo segmento de red.
- Falencias en protocolos de encaminamiento IPX/SPX porque actualmente ya están en desuso, la mayoría de las redes de datos trabajan sobre TCP/IP.
- Baja tolerancia a fallos de la topología de red, debido a que una avería en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto.
- Existe sobrecarga en el nodo central (switch de core), debido a la cantidad de tráfico que debe soportar y conforme se agreguen más nodos aumentará por lo que un fallo en el nodo central puede dejar inoperante a toda la red.

4.2.4 Vulnerabilidades relacionadas con las comunicaciones

Las comunicaciones estables y disponibles en el momento que son requeridas dentro de la compañía son fundamentales, pero si no se maneja de forma segura, ordenada y eficiente

puede convertirse en un verdadero problema para la empresa. Se pueden identificar las siguientes vulnerabilidades:

- Dependencia exclusiva de un único proveedor de comunicaciones como ISP de la conexión ADSL e inalámbrica.
- La PBX presenta problemas en la configuración de las líneas, lo que ocasiona pérdidas y rechazos en las llamadas entrantes y salientes.
- No existen claves robustas para los usuarios en el acceso inalámbrico al Internet.
- El módem es propiedad de la empresa proveedora del servicio del Internet, si falla el servicio por ende el dispositivo estará fuera de funcionamiento.
- El Access Point no tiene implementada seguridad en su configuración, ni trabaja con encriptación en el envío y recepción de datos.
-Los faxes obsoletos.

4.2.5 Vulnerabilidades relacionadas con los servicios de red

Dentro de la red de datos, se encuentran funcionando cuatro diferentes tipos de servidores y la base de datos, los cuales brindan a la empresa diferentes funcionalidades pero también acarrean vulnerabilidades que fácilmente pueden ser aprovechadas por un hacker y desatar una invasión a los recursos e información que la misma posea. Se pueden identificar las siguientes vulnerabilidades:

- *El servidor de correo electrónico, permitir la visualización de contenido activo, especialmente el uso de ActiveX en los mensajes, que es particularmente peligroso, ya que se puede ejecutar automáticamente algún spyware o adware.*
- *La base de datos, cuenta con un software propenso a desconfiguración, y esto puede ocasionar una pérdida masiva de datos.*
- *No existe un adecuado mantenimiento de la base de datos.*
- *No tiene actualizado los parches de seguridad para el servidor Web.*

- *Servidor proxy, permitir la ejecución remota de código, esto deja vulnerable al servidor debido a que un atacante podría instalar programas; ver, cambiar o eliminar las restricciones; o crear nuevas ACLs.*
- *No cuenta con una lista actualizada en las restricciones dentro de las ACLs.*
- *Los servidores de DNS y DHCP están a cargo del ISP, y por ende si existe un fallo en el proveedor, el servicio estará fuera de funcionamiento hasta que el daño sea reparado.*

4.2.6 Vulnerabilidades relacionadas con la información

La información es el activo más importante con que cuenta la empresa y por lo tanto en donde se debe poner más atención para evitar que tenga vulnerabilidades. Para el correcto mantenimiento de la información generada por la empresa es recomendable que ésta sea replicada en diferentes formatos y en diferentes lugares de donde se ha generado para salvaguardarla. Se pueden identificar las siguientes vulnerabilidades:

- *No existen políticas de Backup de la información.*
- *No existe una ubicación centralizada de almacenamiento de la información; ésta se encuentra repartida en los diferentes equipos de la empresa.*
- *No existen políticas ni medios de cifrado de la información crítica.*
- *No existen planes de contingencia para casos de pérdidas de información.*
- *No existe una política de copias de seguridad por lo que una pérdida de datos serían irreparable.*

4.2.7 Vulnerabilidades relacionadas con el personal

El personal de la empresa es una de las vulnerabilidades más importantes que puede tener una organización debido a que es un punto de fuga de información o un foco de ataques a la

organización. Proteger los activos de la empresa ante terceros o pérdidas accidentales, es de vital importancia para no sufrir pérdidas graves de activos. Se pueden identificar las siguientes vulnerabilidades:

-No existe una política de contraseñas para el acceso a los equipos.
- Falta de conciencia por parte de los responsables de la empresa de que es necesaria una buena política de seguridad informática.
- Escases de educación y preparación a los empleados sobre la importancia de la imagen de la empresa, si por alguna razón la imagen de una empresa resulta dañada por comportamiento del personal, puede conllevar pérdidas millonarias para ella.
- Uso indebido de redes sociales durante las horas laborables, donde es expuesta información de la empresa y del usuario como tal.
- No existen políticas sobre el procesamiento, distribución y almacenamiento de la información dentro del personal de la empresa, por lo que fácilmente podrían ser víctimas de la Ingeniería Social. Para conocer más detalle sobre esta técnica de intrusión dirigirse al anexo Ingeniería Social, situado en la página 179.

4.2.8 Vulnerabilidades relacionadas con los Procesos

En una falla de proceso, la ejecución arroja un resultado incorrecto, los procesos provocan que el sistema se desvíe de las especificaciones y el proceso puede suspender su progreso, esto puede incurrir en que la compañía no pueda realizar efectivamente sus actividades vitales para la continuidad del negocio. Se pueden identificar las siguientes vulnerabilidades:

- El personal que trabaja en la empresa puede provocar fallos en los sistemas de la empresa o pérdidas de información debido a falta de formación, falta de conocimiento, mala intencionalidad.
- Los sistemas y dispositivos que no estén actualizados correctamente pueden causar los siguientes errores en los procesos como: interbloqueos en el sistema, tiempo expirado en

respuestas de servidores, violación de protección a los sistemas de seguridad, error en la entrada provista por el usuario en una aplicación.
- Los procesos al ejecutarse arrojan datos e información, la misma que no es correctamente procesada, distribuida y almacenada dentro de la organización, no en el nivel necesario para sus actividades cotidianas y empresariales.
- No cuentan con políticas para la continuidad del negocio en el caso de que alguno de los procesos falle o sea interrumpido.

5.1 Valoración de las vulnerabilidades

En este apartado se van a valorar las diferentes vulnerabilidades encontradas en la empresa, para posteriormente clasificarlas según el nombre de la vulnerabilidad, el tipo de activo de información que afecta y la valoración que tiene en la escala asignada. Para categorizar las vulnerabilidades se usara el siguiente criterio de valoración:

- **Alta:** La vulnerabilidad es grave debido a que es muy probable que sea aprovechada por una amenaza para infligir daño a la organización y provocar una pérdida de activos irreparables, además de fallas en los procesos y actividades normales de la compañía, si nos es reparada o atendida inmediatamente, es decir máximo 1 mes.

- **Media:** La vulnerabilidad es leve debido a que tiene medianas probabilidades de ser aprovechada por una amenaza, pero de suceder puede ocasionar daños y pérdidas a la empresa, por ende debe ser atendida en un tiempo prudencialmente corto, es decir máximo 3 meses.

- **Baja:** Existe una vulnerabilidad pero las posibilidades que alguna amenaza llegue a materializarse en esa vulnerabilidad son escasas y los daños producidos serían

depreciables, pero por mantener un nivel de seguridad óptimo en la empresa, deben ser atendidas en un plazo máximo a 6 meses.

VULNERABILIDAD	ACTIVOS A LOS QUE AFECTA	VALORACIÓN
Falta de políticas de Backup.	Información de la empresa.	Alta
Falta de dispositivos SAI que garanticen el suministro eléctrico.	Hardware, Software, Comunicaciones, Servicios de red.	Media
Equipos informáticos obsoletos.	Hardware	Media
Escases en memoria RAM, lo que obliga al personal a almacenar información importante en dispositivos que pueden ser fácilmente sustraídos (CD, DVD, memorias USB).	Hardware, Información.	Media
Averías en periféricos de entrada y salida.	Hardware	Baja
Carencia de actualizaciones de los software de seguridad como antivirus, firewalls y de prevención, detección y corrección.	Software, Servicios de red.	Alta
Existen versiones de sistemas operativos que no cuentan con las características necesarias para un óptimo funcionamiento de la red.	Software, Red.	Media
No existen políticas para la adquisición y mantenimiento del software dentro de la empresa.	Software	Media
Bajo nivel de seguridad a la hora de realizar accesos inalámbricos a la red interna de	Comunicaciones, Red	Alta

la empresa.		
Bajo rendimiento por parte de la arquitectura lógica implementada por la compañía.	Red	Alta
Debilidades en el protocolo de red usado NetBEUI.	Red	Alta
Debilidades en protocolos de encaminamiento IPX/SPX.	Red	Alta
Baja tolerancia a fallos de la topología de red.	Red	Alta
Dependencia exclusiva de un único proveedor de comunicaciones.	Comunicaciones	Baja
PBX presenta problemas en la configuración de las líneas.	Comunicaciones	Media
AP no tiene implementada seguridad en configuración.	Comunicaciones	Alta
Faxes obsoletos.	Hardware	Baja
No existe un adecuado mantenimiento de la base de datos.	Software, Servicios de Red	Alta
Falta de parches de seguridad para el servidor Web.	Software, Servicios de Red	Alta
No existe una lista actualizada para las ACLs.	Servicios de Red	Media
No existe una ubicación centralizada de almacenamiento de la información.	Información, Procesos	Media
No existe una política de copias de seguridad.	Información	Alta
No existe una política de contraseñas para el acceso a los equipos.	Comunicaciones	Alta
No existe una política de restricción de acceso a los datos.	Información	Alta
Escases de educación y		

preparación a los empleados sobre la importancia de la imagen de la empresa.	Personal, Procesos	Baja
Uso indebido de redes sociales durante las horas laborables.	Personal	Baja
No existen políticas sobre el procesamiento, distribución y almacenamiento de la información dentro del personal de la empresa.	Personal, Procesos	Alta
No cuentan con políticas para la continuidad del negocio en el caso de que alguno de los procesos falle o sea interrumpido.	Procesos	Alta
Fallos en procesos por falta de formación, conocimiento, mala intencionalidad.	Personal, Procesos	Baja

Valoración de Vulnerabilidades
Tabla 4.11

La valoración de las vulnerabilidades encontradas dentro de los activos de información de la compañía, permitirán en el siguiente capítulo, diseñar un plan global para toda la organización, el cual estará dividido en tres etapas de seguridad para cada nivel de exposición de la vulnerabilidad dentro de la escala asignada, estableciendo tiempos de ejecución respectivamente.

Al concluir este capítulo, los datos obtenidos a partir de la identificación y estimación de riesgos a los grupos de activos de información, el agrupamiento y clasificación de cada ítem de activo dentro un inventario consolidado, y la búsqueda e identificación de vulnerabilidades tecnológicas y humanas que presentan las diferentes categorías de activos, nos brindan una idea concreta de las fortalezas y debilidades que tiene esta red de datos, y de los puntos que deben ser protegidos para elevar el nivel de seguridad de la información dentro de la organización.

Por último, antes de pasar al capítulo del Diseño del Plan de Seguridad, es importante ser consciente del potencial de las amenazas internas y externas a las que está expuesta la empresa, debido a su vínculo empresarial con ventas, importación y exportación de maquinaria agrícola e industrial en el mercado. Dicho perfil, la vuelve vulnerable a peligros que surgen de la interacción entre el ser humano y la compañía, factor decisivo en cuanto a la estabilidad y calidad del negocio e influyente directamente sobre el beneficio y la sustentabilidad que brinda a los usuarios o clientes.

Capítulo 5

5. Diseño del Plan de Seguridad

Hasta este punto se ha realizado un completo análisis de la situación de la empresa en lo que se refiere a la seguridad de la información. A continuación se van a detallar las posibles soluciones que debe implantar la empresa para conseguir establecer un nivel de seguridad aceptable y de esta manera evitar pérdidas y daños de activos de información.

A la hora de realizar el análisis de la empresa, se han detectado ciertas vulnerabilidades graves como por ejemplo que no exista respaldo de la información, que no existan políticas de acceso a la información o la más importante, que los responsables de la empresa no tengan conciencia de la importancia de dotar a su empresa de unas adecuadas medidas de seguridad para proteger la información de la misma. Para conseguir reducir el riesgo de la empresa se van a detallar ocho dominios o áreas de gestión de seguridad basadas en la norma ISO/IEC 27002:2005, que contienen medidas que se deberán emplear para conseguir seguridad en la información y elementos informáticos de la compañía.

5.2 PLAN DE SEGURIDAD GLOBAL

Este plan de seguridad plantea medidas orientadas a mejorar los actuales niveles de seguridad, la misma que considera empleados, procesos y sistemas involucrados directamente con la compañía. Cuenta con el aval de los altos directivos y la junta de accionistas de la misma, brindando su respaldo y apoyo constante a cada una de las políticas, controles y medidas preventivas y correctivas que aquí se han establecido. Adicionalmente este plan global se ha desglosado en tres etapas, los cuales dictaran políticas y controles particulares para resolver y atender las vulnerabilidades de cada grupo, en función de las falencias y debilidades de seguridad encontradas.

5.2.1 Definición del Plan de Seguridad de la Información

La empresa conceptualiza al Plan de Seguridad de la Información como el manejo seguro de los datos e información del negocio para salvaguardar las principales propiedades de la información: confidencialidad, integridad y disponibilidad en su procesamiento, distribución y almacenamiento.

5.2.2 Objetivos

El Plan de Seguridad de la Información dentro de la compañía tiene los siguientes fines:

- Protección de la información y de los sistemas de información.
- Control del acceso, uso, divulgación, interrupción o destrucción no autorizada de la información.
- Estructurar e implementar políticas y normas de seguridad.
- Educar al personal de la empresa sobre el manejo de la información.
- Resguardar la integridad de la información almacenada en sus sistemas de cómputo.

- Ofrece una continua disponibilidad de los sistemas y equipos de información.
- Cumplimiento a las leyes, regulaciones y normas aplicables.

5.2.3 Alcance General

El Plan de Seguridad de la Información se limita en brindar protección a todos los activos de información que formen parte de la empresa, tales como: hardware, software, comunicaciones, servicios de red, información, red, personas y procesos, implicados en las actividades cotidianas del negocio.

La norma ISO/IEC 27002:2005, está conformada por once áreas de seguridad, de las cuales, se han escogido ocho dominios previamente, por ser los que cubren todas las vulnerabilidades encontradas en la empresa y por estar alineados a los objetivos del negocio. A continuación se señala y describe brevemente cada dominio a utilizar dentro de la estructura del plan de seguridad diseñado para la Neumac S.A. El dominio de políticas, permite armar reglas y procedimientos que los empleados, procesos y sistemas deben cumplir, debido a que la empresa no cuenta con esto. El dominio de Gestión de activos fue escogido debido a que cada grupo de activo de información debe conocer cuál es su función dentro de la empresa y quien/quienes son los responsables de los mismos, actualmente la empresa no cuenta con una estructura para el manejo de sus activos.

Posteriormente, el dominio de Seguridad ligada a los recursos humanos, se seleccionó como mecanismo para reforzar el nivel de capacitación y conocimiento del personal de la compañía sobre el manejo seguro de los datos. El dominio de Gestión de Operaciones y Comunicaciones, plantea eliminar las vulnerabilidades que presenta la red de datos y los dispositivos de red. Conjuntamente esta, el dominio de Control de Acceso, el cual fortalece

vulnerabilidades relacionadas con accesos no autorizados a la información y sistemas de la empresa. El dominio de Adquisición, desarrollo y mantenimiento de los sistemas de información, busca minimizar riesgos por vulnerabilidades relacionadas con la adquisición de los equipos informático, el continuo mantenimiento y actualización del software de seguridad y corporativo. El dominio de Gestión de Incidentes de Seguridad, estructura medidas para salvaguardar la información de la empresa, en el caso de producirse un suceso perjudicial en contra de los activos de información. Y finalmente el dominio de Gestión de la Continuidad del negocio, estructura un conjunto de medidas dirigida a mantener la disponibilidad de procesos críticos ante desastres relacionados con la seguridad de la empresa y su infraestructura. Dichos dominios permiten aplicar controles, políticas y medidas para proteger los activos de información de la compañía, además de regularizar el organigrama de empleados y la estructura de procesos en el interior de la empresa, permitiendo mayor protección al momento de procesar, distribuir y almacenar los datos.

Los tres dominios restantes que no fueron incluidos dentro de la estructura del Plan de Seguridad, tales como: Aspectos Organizativos de la Seguridad de Información, Seguridad física y ambiental y Cumplimiento, se debe a que no están dentro del alcance o cobertura de la tesis, es decir no fueron planteados como objetivos, debido a que ya están implícitos en otras áreas de seguridad escogidas dentro de la misma norma de seguridad o porque no se encontró vulnerabilidades asociadas con los mismos, es decir Aspectos Organizativos de la Seguridad de Información está implícita dentro de las políticas generales estructuraras para toda la empresa, ahí se plantean reglas y procedimientos para comprometer a los directivos y propietarios del negocio a invertir en seguridad y apoyar cada uno de los controles y medidas aplicadas *(Dominio Políticas)*. En la Seguridad física y ambiental no se encontraron vulnerabilidades que pongan en riesgo la seguridad de la red que posee la empresa, debido a que tiene implantada una seguridad física alta dentro de sus instalaciones. Y finalmente, el área de cumplimiento está implícita dentro de las políticas y procedimientos estructurados para mantener un apego a las leyes y reglamentos que rigen a nuestra jurisdicción *(Dominio de Adquisición, mantenimiento y desarrollo de sistemas de información)*.

A continuación se detallará por completo el Plan de Seguridad, describiendo y explicando cada dominio a implementar. El primer dominio a estructurar son las políticas de seguridad, las cuales han sido planteadas de forma general para todos los empleados, sistemas y procesos de la compañía, describen estatutos que se deben cumplir para salvaguardar la seguridad de los datos e información, durante su procesamiento, distribución y almacenamiento.

5.2.4 Políticas del Plan de Seguridad para la organización en general

A continuación se detallan las políticas de seguridad estructuradas para proteger los activos de información de la empresa Neumac S.A; donde se describe la forma adecuada del uso de los recursos de información, las responsabilidades y derechos tanto de los usuarios como administradores.

Recursos Humanos

- *Todos los empleados de la organización deberán firmar acuerdos de confidencialidad sobre el uso y manejo de la información al momento de su contratación.*
- *La información propiedad de cada una de las áreas dentro del organigrama de la empresa, es responsabilidad absoluta del gerente respectivo y de los empleados a su cargo.*
- *Todos los empleados deberán acceder a los equipos y sistemas de información utilizando algún programa que permita una comunicación cifrada.*
- *Todos los empleados de la organización, deberán cumplir con los horarios de entrada y salidas previamente establecidos, se prohíbe el ingreso de los mismos en horas no autorizadas.*
- *Todos los empleados de la organización, deberán hacer uso de los activos de información en horas de trabajo, se prohíbe su manipulación en horas no laborables.*

- *Los miembros de la junta de accionistas en conjunto con el gerente general, deben gestionar el riesgo en los activos de información y asignar los recursos financieros para mitigar cualquier tipo de amenaza que atente contra ellos.*
- *Todos los empleados de la organización deben conocer y aceptar los roles y responsabilidades anexadas a su cargo.*
- *La responsabilidad de la gestión de la seguridad de información dentro de la empresa, está a cargo del Gerente General, el cual se compromete a estructurar y hacer cumplir cada uno de los dominios de seguridad implementados, asumiendo su compromiso a través de un contrato legal.*
- *Se deberán firmar acuerdos de cooperación con autoridades relevantes como, Policías, Bomberos, Cruz Roja, en caso de presentarse un incidente de seguridad dentro de las instalaciones de la compañía.*

Sistemas y dispositivos de información

- *Todos los sistemas de información deben ser utilizados por los responsables de su uso, se prohíbe su manipulación por terceras personas ajenas a la empresa.*
- *Todos los sistemas de información deben ser actualizados periódicamente según lo exija el fabricante.*
- *Los sistemas de información que almacenen datos del tipo A, B y C deben ser respaldados semanalmente en un sitio remoto las instalaciones de la empresa.*
- *Todos los sistemas de información deben poseer instalaciones eléctricas seguras, estar alejados de sitios húmedos y contar con ventilación.*
- *Todos los sistemas de información deben ser revisados semanalmente, para evitar averías y desperfectos en su funcionamiento.*
- *Todos los dispositivos de información deben ser configurados con una seguridad alta, permitiendo respaldo y cifrado a los datos manejados.*
- *Todos los dispositivos de información deben ser compatibles entre ellos, para brindar un alto desempeño de funcionamiento en la red de datos.*

- *Todos los sistemas y dispositivos de información deben cumplir estrictamente su función específica, se prohíbe su uso y manipulación para actividades ajenas a la empresa.*

Procesos

- *Todos los procesos administrativos, de producción, control, diseño, mantenimiento y ventas e importaciones, deben ser llevados y ejecutados estrictamente por el personal autorizado.*
- *En todos los procesos administrativos, de producción, control, diseño, mantenimiento y ventas e importaciones, se deben evitar los fallos por falta de conocimiento o mala intencionalidad por parte del personal encargado.*
- *Todos los procesos administrativos, de producción, control, diseño, mantenimiento y ventas e importaciones, se debe seguir el orden jerárquico establecido en el organigrama de la empresa.*
- *Todos los procesos administrativos, de producción, control, diseño, mantenimiento y ventas e importaciones, deben mantener la seguridad de la información obtenida durante la ejecución de los mismos.*

A continuación se detallan las tres etapas en que ha sido divido el plan de seguridad para la red de datos de la empresa Neumac S.A., describiendo y especificando que dominios de seguridad de la norma ISO/IEC 27002:2005, serán implementados en cada etapa y cuáles serán los mecanismos de seguridad a ser desarrollados, para lograr un nivel de seguridad de información aceptable en la organización.

5.3 PLAN DE SEGURIDAD A CORTO PLAZO

Esta etapa del plan de seguridad está diseñada para resolver aquellas vulnerabilidades tipificadas como altas. Dichas debilidades dentro de la empresa deben ser atendidas en un

plazo máximo a un mes, debido a las falencias de seguridad que exteriorizan y a los activos de información que afectan. Se han escogido tres dominios de seguridad para ser desarrollados dentro de esta sección, debido que las vulnerabilidades altas presentadas en la red de datos, serán cubiertas y contrarrestadas con estos, dichos dominios son: *Gestión de Comunicaciones y Operaciones*, se reforzará la seguridad en la red, sus comunicaciones y dispositivos de red, para contrarrestar las vulnerabilidades encontradas; *Control de Acceso*, fortalecerá las seguridad al administrar los privilegios en el control y manipulación de los sistemas, equipos informáticos y de información; y finalmente *Gestión de Incidentes de Seguridad,* que plantea medidas preventivas y correctivas para responder ante incidencia de alguna amenaza en contra de algún activo de información.

5.3.1 Gestión de Comunicaciones y Operaciones

Este dominio tiene como objetivo asegurar la operación correcta y segura de los medios de procesamiento de la información en el interior y exterior de la organización.

- *Establecer políticas de seguridad de acceso a la red.*
- *Instalación de dispositivos de red de acceso gestionable.*
- *Establecer configuraciones de seguridad para la red inalámbrica.*
- *Disponer de un correcto servicio de mantenimiento.*
- *Restauración de copias de Backup.*
- *Prohibición del uso de periféricos extraíbles como memorias USB, CDs., DVDs.*

5.3.1.1 Dispositivos de red

Switches

Se cambiarán los switches de capa2, por switches de capa3 los cuales brindan mayor fiabilidad en las conexiones y el envío y recepción de información, son equipos inteligentes los cuales

mediante programación ofrecen diversas configuraciones que permiten elevar el nivel de seguridad a la red y sus nodos. Además tienen la ventaja del rendimiento "wire speed".

Tipos de Switches de Capa 3

Existen dos tipos de switches capa 3:

• *Packet-by-packet*
• *Cut-trough*

Enrutamiento Paquete por Paquete ***(Packet by packet routing)***

Los switches de este tipo, trabajan igual que un router, pero solo pueden realizar las funciones de un router estándar, enrutando todos los paquetes hacia su destino. Trabajan con los protocolos estándar de los routers, pudiendo así interoperar con los otros switches y los routers de la red. Entre sus funciones de seguridad están las siguientes:

- Procesamiento de rutas: esto incluye construcción y mantenimiento de la tabla de enrutamiento.
- Envío de paquetes: una vez que el camino es determinado, los paquetes son enviados a su dirección destino. El TTL (Time-To-Live) es decrementado, las direcciones MAC son resueltas y el checksum IP es calculado.
- Servicios especiales: traslación de paquetes, autenticación, filtros, etc.

Enrutamiento basado en flujo de datos ***(Flow-based routing)***

Los switches de este tipo, utilizan una implementación basada en el enrutamiento rápido de los paquetes *("cut & throw"),* procesando solamente la cabecera y enrutando al destino, este tipo de enrutamiento basado en flujo de datos presenta un inconveniente, es propenso a colisiones, lo que se manifiesta como un serio problema para la fiabilidad y seguridad de la información, debido a que puede haber pérdida y bloqueo de paquetes.

De estos dos tipos, se implementará los switches tipo Packet by packet routing, por poseer mayor rendimiento, debido a que realiza el enrutamiento de todos los paquetes, además dispone de niveles de control y seguridad con los que un enrutador normalmente cuenta, como mecanismos de seguridad para prevenir que un usuario indeseado se conecte a la red, incluso a nivel físico. Pueden filtrar información no deseada incluso de los usuarios que tienen permitido el acceso a la red a través de ACLs, para prevenir ataques a servidores, bases de datos, o proteger aplicaciones con ciertos niveles de seguridad. También cuentan con mecanismos de protección para evitar que un usuario no deseado pueda infiltrarse a la configuración del switch.

Firewalls

Se van a implementar dos tipos de firewalls dentro de la red de datos de la empresa, con el fin de lograr aumentar el nivel de seguridad en las entradas de la Extranet e Intranet, y así evitar intrusiones y accesos nos autorizados.

Perimetral

Implementar un firewall perimetral a la salida al internet, permite evitar intrusiones no deseadas, mejorar las ACLs del servidor proxy a través del bloqueo de IPs y puertos, limitar el tráfico en cada nodo según la necesidad que requiera cada uno, registrar todas las conexiones de entrada y salida realizadas en la extranet.

Subred Oculta

Este tipo de firewall permite asegurar la red interna (intranet) de la empresa, a través de la limitación del tráfico, monitoriza el envío y recepción de datos, brindando una defensa profunda además proporciona un mayor grado de conectividad a los nodos de red.

Tipo de Firewall

Firewall de ISA Server 2006 Enterprise Edition perimetral y de subred oculta

Es una solución de firewall concebida para trabajar dentro de dos escenarios, como FW perimetral, para proteger la infraestructura de la empresa frente al tráfico de red no seguro originado en Internet y como FW de subred oculta, para controlar el tráfico de la red local, y a su vez vigilar el tráfico de entrada y salida para Internet. Esta configuración proporciona una defensa fiable frente a cualquier ataque. Al aislar el host de una red independiente, limita el daño que puede sufrir la red interna. Antes de implementar un corta fuegos se debe buscar cumplir las siguientes consideraciones operativas: incluir una administración de seguridad de red, protección de la red, la detección de intrusiones y la reacción, así como la implementación de requisitos operativos estandarizados.

Capacidades

Los firewalls de estas características poseen las siguientes aplicaciones a la red:

- Permite la implementación de Zonas Desmilitarizadas (DMZ), para servidores Web, servidores FTP y servidores de correo.
- Filtros de paquetes.
- Servidores Proxy.
- Servicios de Conversión de direcciones de red (NAT).
- Software de registro y supervisión de incidentes.
- Medición del throughput que fluye a través de los dispositivos de red.

Routers

De frontera

Este tipo de router sirve para conectar la red corporativa de la empresa a Internet, de manera que actuará como gateway de la red de datos, recogiendo todos aquellos paquetes de datos destinados a máquinas externas.

Access Point

Para mejorar la seguridad de los Access Point en la red inalámbrica de la compañía, se deben realizar configuraciones dentro de los dispositivos tales como:

1. Cambiar la contraseña del administrador
2. Desactivar broadcast SSID
3. Filtrar direcciones MAC
4. Actualizar el firmware constantemente.
5. Activar cifrado WPA, AES.

Protocolos de red

IP

Se cambia el protocolo de red NetBEUI, cuyas vulnerabilidades fueron descritas en el capítulo anterior, por el protocolo IP, el cual es un protocolo orientado a conexión, donde se garantiza la entrega de los paquetes a través de un ACK (acuse de recibo). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes, estas configuraciones se realizan automáticamente entre los dos dispositivos.

Protocolos de enrutamiento

Los protocolos de enrutamiento, usados anteriormente IPX/SPX, mostraban vulnerabilidades en el proceso de encaminamiento, debido a que sólo podían usarse para comunicar nodos en el mismo segmento de red y no estructuraban de forma correcta las tablas de ruteo, provocando pérdidas de paquetes, además actualmente ya están en desuso. Por este motivo se propone utilizar el siguiente protocolo de ruteo:

IP

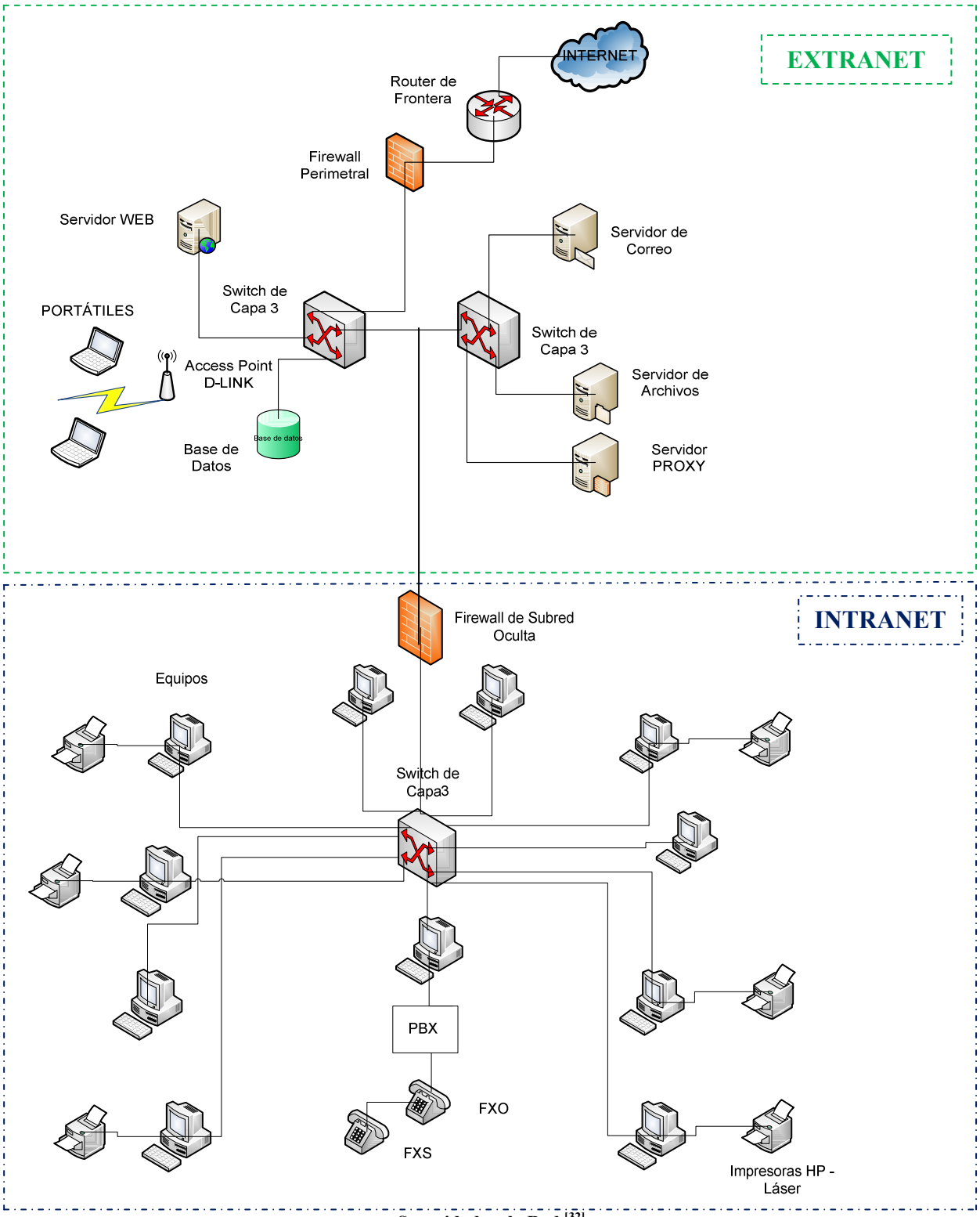
El enrutamiento es la función principal de IP. Los datagramas IP se intercambian y procesan en cada host mediante IP dentro de la red de datos. A su vez IP, utiliza para el enrutamiento de los paquetes, protocolos adicionales para diseñar las tablas de enrutamiento, de los cuales se propone utilizar los siguientes basados en las características de seguridad que brindan:

IGRP

Este protocolo es utilizado por los equipos de red, para intercambiar información acerca de redes basadas en IP. Mejoraría el nivel de seguridad en la red de la empresa, porque utiliza una métrica para determinar la mejor ruta basándose en el ancho de banda, el retardo, la confiabilidad y la carga del enlace. Además ayudaría a administrar mejor la conectividad y el ancho de banda. IGRP, es un protocolo con clase, lo que significa que no pueden manipularse las máscaras de red, brindando mayor fiabilidad a las conexiones.

EGP

Es el protocolo por default utilizado por los routers de frontera. Permite intercambiar información de enrutamiento entre routers de diferentes redes. Adicionalmente este protocolo soporta mensajes de actualización, información sobre la accesibilidad de los routers vecinos, entre otras. Mejoraría la seguridad en las conexiones externas y en el acceso a la Internet.



Seguridad en la Red [32]

Figura 5.1

[32] Gráfico representativo con seguridad implementada en la red, Autor Raisa Gruezo, fuente Tesis titulada Plan de Seguridad para la red de datos de la empresa Neumac S.A., año 2010.

5.3.2 Control de Acceso

Este dominio sostiene que todo acceso no autorizado debe ser evitado y se deben minimizar al máximo las probabilidades de que eso suceda.

- *Establecer una política de contraseñas.*
- *Establecer políticas de ejecución de código.*
- *Establecer políticas de acceso al personal.*
- *Establecer políticas de control de acceso vía firewalls.*
- *Establecer un registro de usuarios y contraseñas.*

Políticas de contraseñas

1. Las contraseñas para el acceso a los sistemas y equipos informáticos deben contar con la siguiente estructura, longitud máxima de 9 caracteres, mínima de 5; contener dígitos numéricos y alfanuméricos, y se prohíbe espacios.
2. Las contraseñas no deben contener o mostrar información personal, como fecha de nacimiento o nombres y apellidos.
3. Las contraseñas de acceso son de uso exclusivo del titular de la misma, se prohíbe el uso de terceros.

Políticas de ejecución de código

1. Se prohíbe la ejecución de programas que intenten descifrar las contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas.
2. Solo se permite ejecutar código relacionado con las actividades cotidianas de la empresa o que esté involucrado con el software corporativo.
3. Todo el código o software que se debe ejecutar en la empresa, debe ser previamente revisado para evitar infecciones con código malicioso.

Políticas de acceso al personal

1. El usuario es la única persona autorizada para leer su propio correo, a menos que él mismo autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad de cómputo.
2. Solo los gerentes de cada área tienen acceso a información tipo A y tipo B.
3. Todos los empleados de la empresa tienen acceso a la información tipo C.

Políticas de control de acceso vía firewall

1. Todas las máquinas de la intranet que deseen acceder al Internet, deberán utilizar el firewall de subred oculta.
2. Todos los servidores de red de la extranet, que deseen acceder al Internet, deberán utilizar el firewall perimetral.
3. Bloqueo de IPs a todas las máquinas y servidores de red que no tengan un acceso autorizado.
4. El firewall perimetral se encarga de llevar un registro del tráfico de entrada y salida a la extranet.
5. El firewall de subred oculta se encarga de llevar un registro del tráfico de entrada y salida a la intranet.

5.3.3 Gestión de incidente en seguridad de información

Este dominio trabaja con reportes de los eventos y debilidades de la seguridad de la información, asegurando una comunicación tal que permita que se realice una acción correctiva oportuna, llevando la información a través de los canales gerenciales apropiados lo más rápidamente posible. Es decir si se elaboran medidas en función de los reportes de eventos de seguridad suscitados en la empresa.

Medidas Preventivas

- Realización periódica de copias de Backup de información tipo A y B localizadas en servidores de red de la empresa, para garantizar la disponibilidad de los datos ante cualquier contratiempo.
- Instalación de un servidor centralizado de copias de seguridad en el cual se almacenen periódicamente copias de los datos actualizados.
- Validación de claves de acceso del personal para disponer de equipos, sistemas, servidores e información de la organización.
- Disponer de copias de respaldo almacenadas en servidores exteriores a la empresa para prevenir posibles fallos de activos de información.
- Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.
- Realizar periódicamente, las actualizaciones oportunas para mantener al día los distintos programas y Sistemas Operativos.
- Disponer de Software de calidad y debidamente revisado.
- Un seguimiento continuo de las actualizaciones de las versiones del sistema de inventarios.
- Disponibilidad de copias de seguridad de los ficheros más importantes en diferentes soportes.
- Actualizar continuamente el software de seguridad de la empresa, es decir el de prevención, detección y corrección.
- Supervisión del tiempo de devaluación de los equipos y sistemas informáticos.
- Supervisión y precaución con los dispositivos extraíbles los cuales pueden ocasionar pérdida de información o infección de virus.
- Conseguir una adecuada concienciación del personal de la empresa sobre lo importante que es mantener un cierto nivel de seguridad en los procesos que se realizan dentro de la empresa.
- Realización de cursos de capacitación sobre la importancia de la seguridad de los datos para el personal de la empresa.
- Prohibir el uso de redes sociales dentro de las horas laborables dentro la empresa.

- Educar continuamente al personal mediante charlas, folletos, conferencias sobre el procesamiento, distribución y almacenamiento de la información, para evitar peligros ligados como la Ingeniería Social.
- Revisar constantemente los dispositivos de entrada y salida.
- No depender únicamente de un solo proveedor de las comunicaciones dentro de la empresa.

Medidas Correctivas

- Blindaje de servidores de red disponibles en la empresa para realizar actividades y operaciones cotidianas.
- Bloqueo de puertos y aplicaciones que puedan ser blancos de intrusiones o infección de virus.
- Instalación de Sistemas Operativos Linux o Centos en los servidores de la compañía; debido a que Windows presenta muchas vulnerabilidades.
- Implementar un firewall perimetral en la salida al Internet para evitar ataques externos a la red, y uno se subred oculta a la entrada de la red interna (intranet).
- Implementar un sistema tolerante a fallos de nodos de red, que permita a la empresa seguir a delante en sus actividades así exista un aislamiento en un nodo.
- Restauración de copias de Backup en el caso de haberse producido una pérdida de datos.
- Firmar acuerdos de niveles de servicios en donde los desarrolladores del sistema de inventarios (base de datos) se comprometan al mantenimiento y supervisión del servicio.
- Actualizar los parches de seguridad del servidor WEB.
- Los empleados deben seguir a cabalidad las políticas implementadas para copias de seguridad, acceso a los datos y para la manipulación de la información (procesamiento, distribución y almacenamiento) dentro de la empresa.
- Los equipos y sistemas informáticos deben ser cambiados para evitar que se vuelvan obsoletos y descontinuados.
- Aumentar memoria RAM a los equipos informáticos de la empresa.

- Los directivos y empleados deben acatar las políticas y normas de seguridad para la adquisición y mantenimiento del software dentro de la empresa.
- Actualizar listas de acceso (ACL) debido a que el personal posee mucha libertad en el Internet y esto es peligroso.
- Bloquear páginas de juegos, y de redes sociales.
- Cambiar los periféricos de entrada y salida de los equipos informáticos.
- Dictar cursos de capacitación y charlas para educar y preparar a los empleados sobre la importancia de la imagen de la empresa.
- Concienciar al personal de la empresa sobre el uso indebido de redes sociales durante las horas laborables.
- Capacitar e instruir a cada empleado sobre los roles y funciones que cumple en la empresa, y así evitar fallos en procesos por falta de formación, conocimiento, mala intencionalidad, además se debe motivar al personal.

5.4 PLAN DE SEGURIDAD A MEDIANO PLAZO

Esta etapa del plan de seguridad está delineada para aquellas vulnerabilidades tipificadas como medias. Dichas debilidades dentro de la empresa deben ser atendidas en un plazo máximo a tres meses, debido a las debilidades de seguridad que exponen y a los activos de información que afectan. Se han escogido dos dominios de seguridad para ser desarrollados dentro de esta sección, debido que las vulnerabilidades medias presentadas en la red de datos, han sido cubiertas y contrarrestadas con estos, dichos dominios son *Gestión de Activos*, reforzará las distribución y asignación del uso de cada activo de información y su responsabilidad dentro de la compañía, *Seguridad ligada a recursos humanos,* fortalecerá e inculcará a los empleados sobre sus responsabilidades y roles a través de la capacitación continua.

5.4.1 Gestión de Activos

Este dominio permite asignar responsabilidades por cada uno de los activos de la organización, del inventario actualizado de todos los activos que se tiene la empresa, y a quien/quienes les pertenecen y el uso específico que deben tener.

Hardware

- *La categoría equipos 1 dentro de los activos de Hardware son responsabilidad del Área de Ventas dentro de la organización, y su uso es exclusivo para realizar ventas, información de ventas, folletos y cualquier tipo de publicidad para la empresa.*
- *La categoría equipos 2 dentro de los activos de Hardware son responsabilidad de las Áreas de Contabilidad y Contaduría, y Recepción dentro de la organización, y su uso se remite a almacenar balances contables, cuentas de clientes y proveedores, organizar eventos, citas, reuniones, llamadas, nóminas del personal, etc.*
- *La categoría equipos 3 dentro de los activos de Hardware son responsabilidad del Área de Diseño y Mecánica dentro de la organización, y su uso es exclusivo para almacenar bocetos de maquinarias, piezas, fichas técnicas y planos.*
- *La categoría equipos 4 dentro de los activos de Hardware son responsabilidad del Área de Gerencia e Importaciones dentro de la organización, y su uso se remite a almacenar remisiones, pedidos, nómina de proveedores, perfiles de productos.*
- *Los escáneres son responsabilidad de las Áreas de Gerencia e Importaciones, Ventas y Diseño y Mecánica dentro de la organización y su uso se remite para información exclusiva de la compañía.*
- *Las impresoras son responsabilidad de todos los empleados de la empresa, independientemente a que área en específico pertenezcan, su uso es exclusivo para información de la organización.*

Software

- *El software de prevención dentro de los activos de Software es responsabilidad de las Áreas de Contabilidad y Contaduría, Diseño y Mecánica, Gerencia e Importaciones y su uso es exclusivo para programas o aplicaciones propias o relacionadas a la empresa.*
- *El software de protección dentro de los activos de Software es responsabilidad de las Áreas de Contabilidad y Contaduría, Diseño y Mecánica, Gerencia e Importaciones y su uso es exclusivo para programas o aplicaciones propias de estas áreas o relacionadas a la empresa.*
- *El software de corrección dentro de los activos de Software es responsabilidad de todas las áreas de la empresa y su uso es exclusivo para programas o aplicaciones propias de estas áreas o relacionadas a la empresa.*
- *El software de diseño dentro de los activos de Software es responsabilidad del Área de Diseño y Mecánica, y su uso es exclusivo para diseñar bocetos de maquinarias, piezas, fichas técnicas y planos.*
- *El software de entretenimiento dentro de los activos de Software es responsabilidad de todas las áreas de la empresa, y su uso es para distracción de los empleados en horarios de descanso.*

Comunicaciones

- *Los dispositivos como teléfonos, switches, faxes, Access Point, son responsabilidad de todas las áreas de la empresa, y su uso es exclusivo para la red de la empresa y para las comunicaciones internas y externas de la misma.*
- *El dispositivo módem es responsabilidad del Proveedor de Servicio de Internet, y su uso es exclusivo para las comunicaciones de la compañía.*
- *La PBX es responsabilidad de todas las áreas de la empresa.*

Servicios de Red

- *Los servicios de DNS y DHCP son responsabilidad del Proveedor de Servicio de Internet, y su uso remite a la asignación de direcciones IP y nombres de dominio.*
- *El servicio de Correo Electrónico es responsabilidad de todas las áreas de la organización, y su uso se remite a la distribución del correo interno en la empresa.*
- *El servidor de archivos es responsabilidad de las Áreas de Contabilidad y Contaduría, Ventas y Gerencia e Importaciones, y su uso es exclusivo para almacenar liquidaciones de aduana, facturas de importaciones, y todo documento legal que sea de utilidad a la compañía durante los 3 trimestres del año laboral.*
- *El servidor WEB es responsabilidad de las Áreas de Ventas y Gerencia e Importaciones, y su uso se remite para realizar ventas nacionales e internacionales, publicar su inventario de productos y servicios, precios, cotizaciones y como ayuda para los clientes ante cualquier duda que tengan acerca de las maquinarias y servicios o de la empresa en general.*
- *El servidor PROXY es responsabilidad de la empresa encargada del mantenimiento de las máquinas, es tercializada por la organización, su uso es exclusivo para bloquear el acceso a determinadas páginas webs consideradas ofensivas o dañinas para la red y los usuarios.*
- *El servidor de archivos (Base de Datos) es responsabilidad de las Áreas de Ventas, Contabilidad y Contaduría, y Gerencia e Importaciones, su uso se remite a almacenar toda la información referente a clientes, cuentas y maquinarias.*

Información

- *La información tipo A es responsabilidad de las áreas de Contabilidad y Contaduría, y Gerencia, y su uso es exclusivo para la toma de decisiones y llevar el registro contable de la empresa.*

- *La información tipo B es responsabilidad de las Áreas de Ventas, Diseño y Mecánica, Importaciones, Recepción, y su uso es exclusivo para el manejo de clientes, cuentas, de reuniones y eventos, además de bocetos de maquinarias y productos.*
- *La información tipo C es responsabilidad de las Áreas de Ventas y Diseño y Mecánica, y su uso es exclusivo para el marketing y publicidad de la empresa.*

Procesos

- *Los procesos administrativos son responsabilidad de Gerencia General y Gerencia Técnica, y su uso es exclusivo de esta dependencia.*
- *Los procesos de producción son responsabilidad de la Jefatura de Producción y Taller, y su uso se remite a la manufactura de la maquinaria.*
- *Los procesos de control son responsabilidad de la Secretaria/Recepcionista, Bodeguero, Contadora, Personal de Seguridad, y su uso se remite a la supervisión de los productos entrantes y salientes, además de la seguridad de la empresa.*
- *Los procesos de diseño son responsabilidad de la Jefatura de Diseño e Ingeniería Mecánica, y su uso se remite al diseño y gestión de la maquinaria.*
- *Los procesos de mantenimiento son responsabilidad de la Jefatura de Mantenimiento, y su uso se remite al cuidado y manutención de los equipos y maquinarias agrícolas e industriales.*
- *El diseño y mantenimiento de la arquitectura, topología y extensión de la red de datos son responsabilidad del administrador de la red, y su uso se remite a la gestión de la misma, sin desviarse de los objetivos y fines de la empresa.*

5.4.2 Seguridad ligada a recursos humanos

En cualquier organización el personal es un punto crítico pues un empleado descontento puede provocar graves daños desde dentro de la organización. El objetivo de este dominio, es asegurar que los empleados entiendan sus responsabilidades, y sean idóneos para los roles para

los cuales son considerados, reduciendo el riesgo de robo, fraude y mal uso de los medios. Por ende, es necesario definir claramente los roles y responsabilidades de cada empleado.

- *La junta de Accionistas son los encargados de proveer económicamente a la compañía, y su responsabilidad es apoyar y respaldar las actividades internas relacionadas con el negocio.*
- *El Gerente General, es el encargado de dirigir a la compañía y a sus subordinados, y su responsabilidad radica en tomar decisiones dentro de la empresa, pensando en su desarrollo económico y publicitario.*
- *El Gerente Técnico, es el encargado de liderar a las áreas de Diseño y Mecánica, y su responsabilidad es tomar decisiones relacionadas con los procesos de producción, mantenimiento y control dentro de la empresa.*
- *El Jefe de Diseño e Ingeniería Mecánica, es el encargado de administrar a los mecánicos y su responsabilidad remite a gestionar actividades relacionadas con el diseño y manufactura de las maquinarias.*
- *El jefe de Producción y Taller, es el encargado de liderar a los soldadores y operadores, y su responsabilidad es gestionar los procesos de producción dentro de la empresa.*
- *El jefe de mantenimiento, es el encargado de liderar a los ayudantes y operadores, y su responsabilidad remite a gestionar los procesos de mantenimiento y control dentro de la empresa.*
- *El Jefe de Importaciones, es el encargado de negociar con proveedores y clientes, y su responsabilidad es gestionar los procesos de de ventas e importaciones.*
- *Los Vendedores técnicos, son los encargados de las ventas de diseños, planos o bocetos de maquinarias, y su responsabilidad es cumplir con las metas trazadas por la empresa.*
- *La Contadora, es la encargada de almacenar, y legalizar los trámites tributarios de la empresa, además de rendir cuenta de los balances contables y su responsabilidad es mantener al día a la empresa en pagos, aranceles, y demás procesos contables.*

- *Los Vendedores de almacén, son los encargados de realizar las ventas por catálogos, folletos de lao productos que ofrece la empresa, y su responsabilidad es cumplir con las metas trazadas por la compañía.*
- *La Secretaria/Recepcionista, es la encargada de organizar, registrar eventos, reuniones, citas con clientes y proveedores, atender llamadas, redactar cartas, memorándums, y su responsabilidad es mantener al día al personal con las novedades de la empresa.*
- *El bodeguero, es el encargado de recibir y enviar los pedidos de maquinarias, y su responsabilidad es asegurar la correcta recepción y emisión de los productos.*
- *El Personal de Seguridad, es el encargado de brindar resguardo a las instalaciones de la empresa, y su responsabilidad es evitar pérdidas de activos o dinero de la organización.*
- *El Mensajero, es el encargado de realizar trámites cortos al personal de la empresa, y su responsabilidad es mantener la confidencialidad y discreción necesaria.*
- *Los Mecánicos, son los encargados de probar las maquinarias antes de ser puestas a la venta, y su responsabilidad radica en realizar las pruebas de control y mantenimiento a los productos.*
- *Los Operadores de máquinas, son los encargados de manejar las máquinas para muestras o exhibiciones, y su responsabilidad es ser cuidadosos con su manipulación.*
- *Los soldadores son los encargados de reparar averías en las maquinarias, y su responsabilidad radica en mantenerlas en condiciones óptimas.*

5.5 PLAN DE SEGURIDAD A LARGO PLAZO

Esta etapa del plan de seguridad está diseñada para aquellas vulnerabilidades tipificadas como bajas. Dichas debilidades dentro de la empresa deben ser atendidas en un plazo máximo a seis meses, debido a su nivel de exposición y que su afectación o perjuicio es controlable con medidas de seguridad sobre los activos de información.

Se han escogido dos dominios de seguridad para ser desarrollados dentro de esta sección, debido que las vulnerabilidades bajas presentadas en la red de datos, han sido cubiertas y contrarrestadas con estos, dichos dominios son: *Adquisición, desarrollo y mantenimiento de sistemas de información,* buscará estructurar normas y procedimientos que se deberán seguir al momento de comprar y mantener equipos y sistemas, *Gestión de Continuidad del Negocio*, reforzará las medidas preventivas y correctivas que se deben emplear al momento que exista un fallo en las actividades cotidianas y normales del negocio .

5.5.1 Adquisición, desarrollo y mantenimiento de sistemas de información

Este dominio contempla aspectos de seguridad requeridos al momento de adquirir equipos y sistemas, o al desarrollarlos. No solamente se debe considerar la calidad y el precio, sino que la seguridad que ofrecen.

- *Establecer políticas para la adquisición de sistemas de información.*
- *Establecer políticas para el mantenimiento de sistemas de información.*

Políticas de adquisición de sistemas de información

1. Adquirir licencias extendidas de todo el software empleado en la empresa, para a través de esto utilizar las garantías.
2. Asegurarse de la correcta instalación de los sistemas de información de los que dispone la empresa.
3. Instalación en la totalidad de equipos de la empresa, de sistemas de información y software de seguridad que salvaguarde la integridad, disponibilidad y confidencialidad de los equipos.
4. Los equipos informáticos deben ser reemplazados cada 3 años, para evitar que queden obsoletos y descontinuados.

Políticas para el mantenimiento de sistemas de información

1. Actualizar periódicamente las listas de control de acceso del servidor proxy.
2. Realizar periódicamente, o cuando sea requerido por la empresa encarga del mantenimiento de los sistemas de información, las actualizaciones oportunas para mantener al día los distintos programas y sistemas operativos.
3. Descargar los parches de seguridad para cada uno de los servidores de la empresa.
4. Descargar semanalmente las actualizaciones del servidor de correo.
5. Blindar el servidor Web, y actualizar la página de presentación de la compañía.
6. Firmar contratos de acuerdos de niveles de servicio con los proveedores de servicios externos.
7. Asegurarse que las actualizaciones y mantenimiento de la base de datos sean con periodicidad de cada 6 meses.
8. La PBX de la empresa debe ser reconfigurada periódicamente, y debe ser inmediatamente reemplazada si el volumen de usuarios supera su capacidad.

5.5.2 Gestión de Continuidad del Negocio

Este dominio mide las consecuencias de los desastres, fallas en la seguridad, pérdida del servicio y la indisponibilidad del mismo. Es la actividad que se lleva a cabo en una organización para procurar que todos los procesos de negocio críticos estarán disponibles para los clientes, proveedores, y otras entidades que deben acceder a ellos. Por ende, se deben desarrollar e implementar una serie de medidas preventivas y correctivas, buscando minimizar la probabilidad de ocurrencia por ende el efecto o impacto.

Procesos Administrativos

- Realizar continuamente una gestión de proyectos para organizar y administrar los recursos de la empresa.
- Disponer de recursos económicos constantes para mantener un nivel de seguridad aceptable.
- Disponer de un porcentaje de capital determinado para enfrentar adversidades o incidentes.
- Exigir y actualizar anualmente las firmas de acuerdos de niveles de servicios.

Proceso de Producción

- Supervisión constante de la maquinaria y equipos utilizados para la producción.
- Actualización y respaldo continuo de la lista de clientes y proveedores.
- Implementar dispositivos redundantes (SAI, UPS) para que la empresa los utilice en el momento que el servicio de energía eléctrica se suspenda por fallos externos, y afecte a este tipo de procesos.

Procesos de Mantenimiento

- Contratar un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.
- Contratar dos líneas exteriores con suministradores de internet para garantizar siempre una conexión mínima a la red.
- Realizar periódicamente copias de seguridad de los sistemas informáticos y de información.
- Firmar acuerdos de niveles de servicios, con las empresas prestadoras del servicio, para que se comprometan al mantenimiento y supervisión del mismo, en tiempos de recuperación establecidos previamente.
- Contratar otras proveedores alternos para el servicio de comunicaciones (ISP, telefónica) para sirvan de respaldo en el caso que la empresa principal falle.
- Contratación de personal *helpdesk* para que brinde asesoría a los empleados.

Procesos de Control

- Realizar un registro del control de cambios de cada uno de los grupos de activos de información de la empresa.
- Revisión periódica de la instalación eléctrica.
- Instalación de dispositivos automáticos de extinción de incendios.
- Distribución de extintores a lo largo de toda la dependencia de la empresa, en especial cerca de elementos informáticos críticos.

Procesos de Diseño

- Realizar un respaldo periódico de las fichas y planos técnicos.
- Actualizar constantemente el software y las herramientas de diseño.

Al terminar es último capítulo del proyecto, y diseñado y estructurado el plan de seguridad para toda la red de la empresa en base a las vulnerabilidades encontradas, podemos deducir que la seguridad es un proceso continuo, no se pueden establecer medidas, controles y políticas de seguridad extremas y drásticas para mantener la integridad de los datos y procesos de la empresa y luego, olvidar que es necesario realizar un seguimiento continuo de las mismas. Por ello es importante y necesario que cada sección de este documento se ha tomado a conciencia por parte de los dueños y administradores de la empresa como por el personal, ya que al ser ejecutado e implementado este plan de seguridad ayudará y elevará el nivel de seguridad de la información durante su procesamiento, distribución y almacenamiento, aumentando la rentabilidad y confianza en la empresa, mejorando su imagen y logrando éxitos y desarrollo en sus actividades mercantiles.

6. Conclusiones

1. Se pudo diagnosticar exitosamente el estado de funcionamiento actual de la red de información de la empresa, donde se obtuvo como resultado el escenario real de trabajo de la red de datos.

2. Se ha realizado el levantamiento de activos de información, donde se ordenó y agrupó cada ítem de activos, para conocer a cabalidad que es lo que se va a proteger dentro de la organización.

3. Se logró realizar un análisis exhaustivo de riesgos en la empresa, para identificar y estimar los riesgos en los activos de información, en base a criterios de confidencialidad, integridad y disponibilidad.

4. Se logró establecer amenazas humanas y tecnológicas a las que se expone la información de la empresa, durante su procesamiento, distribución y almacenamiento.

5. A través del análisis de riesgos, se pudo identificar vulnerabilidades en los activos de información de la organización, y a su vez categorizarlas en altas, medias y bajas.

6. Se aplicaron exitosamente, los ocho dominios de seguridad de la norma ISO/IEC 27002:2005, los cuales permitieron contrarrestar en su totalidad las vulnerabilidades encontradas en los activos de información.

7. El diseño del Plan de Seguridad estuvo desglosado en tres etapas de seguridad, en el cual cada etapa o sección cubre una categorización de las vulnerabilidades respectivamente.

8. Se pudieron plantear políticas, normas y procedimientos de seguridad que se encuentren alineados al negocio, y que además brinden protección a todos los activos de información de la empresa.

9. En general, se han cumplido exitosamente cada uno de los objetivos planteados al inicio del proyecto, sin perder el alcance y magnitud del mismo, obteniendo los resultados deseados durante la investigación.

10. A lo largo de la realización del proyecto se ha evidenciado en numerosas ocasiones que los responsables de la empresa no son conscientes de lo importante que es la seguridad informática para su proceso de negocio y lo vulnerable que es la empresa a posibles pérdidas de información.

11. A pesar de ser una pequeña empresa requiere una gran atención en lo referente a la seguridad de su información. Neumac S.A. es una empresa con una única sede a nivel nacional y con poco personal, pero aun así requiere un gran esfuerzo, control y supervisión de todos los procesos informáticos que se producen para asegurar que no tengan lugar a pérdidas de información.

7. Recomendaciones

- Mantener correctamente actualizado todo el software de la empresa, antivirus, firewalls, sistemas operativos, sistemas de inventarios, etc.

- Realizar, al menos una vez a la semana, copias de respaldo de todos los datos generados durante el periodo desde la última copia de seguridad.

- Realizar auditorías periódicas, recomendablemente sobre los activos de información, y del nivel de seguridad en que se encuentra la empresa.

- Se recomienda la contratación de personal adecuado para el mantenimiento de los sistemas y los procedimientos de seguridad.

- El personal de la empresa debe seguir las recomendaciones dadas en este documento *(plan de seguridad)*, debido a que si se siguen todas las pautas, la empresa podrá ponerse al día en la seguridad de sus sistemas y alcanzará un nivel de protección aceptable.

8. Anexos

8.1. Activos de Hardware

Equipo 1

Procesador: Intel(R) Pentium(R) 4 CPU 3.00GHz, 2998MHz.

Placa base: ASUSTeK Computer Inc.

Memoria RAM: 512-MB PC2-5300 DDR2 SDRAM (667-MHz) Non-ECC – single channel.

Disco duro: Maxtor 6V160E0 de 149 GB.

Unidades DVD: BENQ DVDDD DW1640.

Tarjetas de red: Intel PRO/1000 MT Network Connection.

Monitor: LG Flatron L1717S.

Equipo 2

Procesador: Intel(R) Pentium(R) 4 CPU 1.80GHz, 1793MHz.

Placa base: Quntumn Designs Limited.

Memoria RAM: 256 MB.

Disco duro: ST360020A de 55,9 GB.

Unidades DVD: LG DVD-ROM DRD8160B.

Tarjetas de red: NIC Fast Ethernet PCI Familia RTL8139 de Realtek.

Monitor: LG Studioworks 700S.

Equipo 3

Procesador: Intel Pentium 4 516* Processor (2.93-GHz, 533-MHz).

Placa Base: HP COMPAQ dx2200.

Memoria RAM: 1 GB PC2-5300 DDR2 SDRAM (667-MHz)

Disco Duro: 40 GB Serial ATA 1.5-Gb/s

Unidades de DVD: CD-ROM drive, CD-RW drive, CD-RW/DVD Combo drive, DVD+R, DVD +/-RW LightScribe drive.

Tarjetas de red: Integrated Realtek 8100C Fast Ethernet Network Connection Agere 56K PCI Modem

Monitor: COMPAQ Presario LCD

Equipo 4

Procesador: Intel(R) Pentium(R) M Processor 1.73GHz, 1728MHz.

Placa Base: HTW00 de Toshiba.

Memoria RAM: 1022MB.

Disco duro: TOSHIBA MK6034GSX de 55.9GB.

Unidades DVD: Pioneer DVD-RW DVR-K165.

Tarjetas de red: Realtek RTL8139/810x Family Fast Ethernet NIC.
Intel(R) PRO/Wireless 2915ABG Network Connection.
Bluetooth Personal Area Network from Toshiba**.**

Impresoras

HP Deskjet 5657

HP Laserjet 1160

Escáner

HP G2710

CANON Lide 25

8.2.Activos de software

Equipo 1

El equipo 1 cuenta con el siguiente Software instalado:

- Sistema Operativo Windows XP Home Edition con Service pack 2

- Acrobat Reader 7.0
- Adobe Photoshop Album Startes Edition 3.0
- Avast! Antivirus
- Barra Yahoo
- Google Toolbar para Internet Explorer
- Java SE Runtime Enviroment 6
- Macromedia Flash Player 8
- Macromedia Shockwave player
- Microsoft .NET Framework 1.1
- Microsoft Office Professional Edition 2003
- Mozilla Firefox
- Nero 6 ultra Edition
- Omni Mouse driver 4.0
- Power DVD
- Software de conexiones de red Intel(R) PRO v9.2.4.9
- Windows Installer 3.1
- Windows media 11
- Base de Datos FoxDate

Equipo 2

El equipo 2 cuenta con el siguiente Software instalado:

- Sistema Operativo Windows XP Professional con Service pack 2
- AD-Aware SE Professional
- Acrobat Reader 5.0
- Adobe Flash player Activex
- Google Toolbar para Internet Explorer
- HP Laserjet 116/1320 series
- HP print Screen utility
- J2SE Runtime Enviroment 5.0
- Java 6

- Nero Burning Room
- McAfee Security center
- McAfee VirusScan Professional
- Microsoft Office 2000 Premium
- Power DVD
- Quick Time
- Windows media 11

Equipo 3

El equipo 3 cuenta con el siguiente Software instalado:

- Sistema Operativo Windows XP Home Edition Service pack 2
- AD-Aware SE Personal
- Adobe Photoshop CS
- Acrobat Reader 8.1
- Autocad 2006
- Autocad 2007
- AVG antivirus 7.5
- AVG antispyware 7.5
- Compresor WinRar
- Compresor WinZip
- Canon Utilities PhotoStich 3.1
- Divx Player
- Google Earth
- Ccleaner V2.09.600
- WinDVD 4
- iTunes
- J2SE Runtime Environment 5.0
- Macromedia Studio MX
- Microsoft Office 2003 Professional
- Microsoft Office 2007 Enterprise

- Mozilla Firefox
- Nero 7
- Panel de control ATI
- PDF Creator
- Quick time
- Skype

Equipo 4

El equipo 4 cuenta con el siguiente Software instalado:

- Sistema Operativo Windows XP Professional Service pack 3
- AD-Aware SE Personal
- Ad-Aware Email Scanner for Outlook
- Adobe Reader 7.0 Español
- Ccleaner
- Compresor WinRAR
- ESET NOD32 Antivirus 4.2.42.3
- Google Chrome
- Java ™ 6 Update 16
- LimeWire 5.3.6
- Malwarebytes Anti-Malware
- Nero OEM
- Skype 3.8
- Google Earth
- Spybot – Search & Destroy
- Trojan Remover 6.8.1
- Microsoft Office 2007 Enterprise
- Mozilla Firefox
- PDF Creator

8.3.Activos de comunicaciones

Equipo 1

Dispone de dos tarjetas de red:

- Intel PRO/1000 MT Network Connection.
- Linksys Wireless-B USB Network Adapter v2.8.

Equipo 2

Dispone de una única tarjeta de red:

- NIC Fast Ethernet PCI Familia RTL8139 de Realtek.
- NGenius 2.4 GHz b/g Wireless PCI Adapter.

Equipo 3

Dispone de tres tarjetas de red:

- Realtek RTL8139/810x Family Fast Ethernet NIC.
- Intel(R) PRO/Wireless 2915ABG Network Connection.

Equipo 4

Dispone de tres tarjetas de red:

- Realtek RTL8139/810x Family Fast Ethernet NIC.
- Intel(R) PRO/Wireless 2915ABG Network Connection.
- Bluetooth Personal Area Network from Toshiba.

Teléfonos

- Panasonic 2.4 GHz Digital Gigarance
- LG 2.4
- Siemens 2.4

Access Point

- AP, D –LINK; 2,4 GHz. 10 dBi; 400 mW Polarización Dua; Power over Ethernet.

Módem

- Conexión, módem ADSL FiberHome, de 1 MB contratada con Tv Cable.

Faxes

- Fax Panasonic Con Altavoz & CallerId Modelo Kx-fp205.
- Fax Panasonic Kx-fg2451 2.4 GHz Identificador.

Switches

- Switch 3COM de 8 puertos.
- Switch 3COM de 16 puertos.

Central Privada Automática

- PBX Panasonic accesible para 10 líneas telefónicas.

8.4.Anexo de ingeniería social

Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

El principio que sustenta a la ingeniería social es que en cualquier sistema "los usuarios son el eslabón débil". Esta técnica también se aplica al acto de manipulación cara a cara para obtener acceso a los sistemas computacionales. La principal defensa contra la ingeniería social es educar y entrenar a los usuarios en el uso de políticas de seguridad y asegurarse de que estas sean seguidas.

Técnicas de Ataque

Directas y Físicas

Es un conjunto de prácticas o métodos para intentar persuadir a un individuo y así completar un objetivo o tarea. El atacante utiliza a los sistemas y dispositivos propios de la empresa para persuadir a los empleados a brindar datos o información sensible y confidencial de la cual el ingeniero social pueda sacar provecho. Una de las herramientas esenciales usadas para la ingeniería social es una buena recolección de los hábitos de los individuos. Las formas más comunes que se emplean dentro de este grupo de técnicas directas o físicas están:

Teléfono

- Personificación Falsa y Persuasión.
- Tretas Engañosas: Amenazas, Confusiones Falsas.
- Falsos reportes de problemas.
- Personificación falsa en llamadas a HelpDesks.
- Completación de Datos Personales.
- Robo de Contraseñas o Claves de Acceso.
- Consulta de buzones de voz.
- Uso fraudulento de líneas telefónicas.
- Uso de Sistemas Internacionales de Voz sobre IP.

Sitio de Trabajo

- Acceso físico no autorizado
- *"Shoulder Surfing",* que significa ver por encima del hombro, ó leer al revés.
- Robar, fotografiar o copiar documentos sensibles.
- Pasearse por los pasillos buscando oficinas abiertas y aprovechar la ausencia de los empleados para husmear.
- Acceso no autorizado al cuarto de PBX y/o servidores.
- Conseguir acceso a los sistemas.
- Instalar analizadores de protocolo escondidos, como sniffers.
- Remover o robar pequeños equipos con o sin datos.

La Basura

"Dumpster Diving", que significa husmear o buscar en la basura información confidencial y relevante propia o sobre la compañía como:

- Listados Telefónicos.

- Organigramas.
- Memorandos Internos.
- Manuales de Políticas de la compañía.
- Agendas en Papel de Ejecutivos con Eventos y Vacaciones.
- Manuales de Sistemas.
- Impresiones de Datos Sensibles y Confidenciales.
- *"Logins"* ó contraseñas.
- Listados de Programas (código fuente).
- Papel Membretado y Formatos Varios.
- Hardware Obsoleto.

Fuera de la Oficina

- Fuga de información en almuerzos de negocios.
- Sesiones con terceros sobre determinados temas relacionados a la empresa, se convierten en confesiones de contraseñas, direcciones de correo electrónico, target de nuevos productos, etc.

Seductivas y/o Inadvertidas

Las técnicas de persuasión seductiva y/o inadvertida consisten en la manipulación de la mente humana por otro individuo, sin que el sujeto manipulado esté consciente de qué causó su cambio de opinión. La persuasión radica en la utilización deliberada de la comunicación para cambiar, formar o reforzar las actitudes de las personas, siendo estas últimas representaciones mentales que resumen lo que opinamos de las cosas, personas, grupos, acciones o ideas.

Autoridad

El atacante procurar estar con la gente de TI o con un alto ejecutivo en la empresa o institución, mostrando seguridad e importancia hacia ellos. Para ello puede usar un tono de voz:

- Intimidante
- Amenazante
- Urgente

Carisma

- Se usan modales amistosos, agradables.
- Se conversa sobre intereses comunes.
- Puede usar la adulación para ganar información del contexto sobre una persona, grupo o producto.

Reciprocidad

- Se ofrece o promete ayuda, información u objetos que no necesariamente han sido requeridos.
- Esto construye confianza, y muestra a la victima una sensación de autenticidad y confiabilidad.

Consistencia

Se usa el contacto repetido durante un cierto período de tiempo para establecer familiaridad con la "identidad" del atacante y probar su confiabilidad.

Validación Social

- Acecha el comportamiento normal de tratar de satisfacer un requerimiento.
- Se puede tomar ventaja de esta tendencia al actuar como un compañero de trabajo necesitando información, contraseñas o documentos para su trabajo.
- La victima usualmente es una persona con cierto potencial de ser segregada dentro de su grupo, o que necesita “ser tomada en cuenta”.

9. Glosario de términos

1.6.1 Red de Información

Está conformada por un conjunto de dispositivos físicos y de programas, mediante el cual podemos comunicar computadoras para compartir recursos e información.

1.6.2 Dispositivos de Red

Una red de información está conectada tanto por hardware como por software. El hardware incluye tanto las tarjetas de interfaz de red como los cables que las unen, mientras que el software contiene los controladores, los cuales son programas que se utilizan para gestionar los dispositivos y el sistema operativo de la red. A continuación se listan los componentes:

- Servidor.
- Estaciones de trabajo.
- Placas de interfaz de red (NIC).
- Recursos periféricos y compartidos.

1.6.3 Intranet

Red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales. El término intranet se utiliza en oposición a internet, una red entre organizaciones,

haciendo referencia por contra a una red comprendida en el ámbito de una organización.

1.6.4 Extranet

Red privada virtual que utiliza protocolos de Internet, protocolos de comunicación y probablemente infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización. Se puede decir que una extranet es parte de la intranet de una organización que se extiende a usuarios fuera de ella.

1.6.5 WAN

Una red de área amplia o WAN (Wide Area Network), está orientada a la interconexión de redes o equipos terminales que se encuentran ubicados a grandes distancias entre sí. Para ello cuentan con una infraestructura basada en poderosos nodos de conmutación que llevan a cabo la interconexión de dichos elementos, por los que además fluyen un volumen apreciable de información de manera continua.

1.6.6 Activo

Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

1.6.7 Amenaza

Cualquier circunstancia susceptible de lograr que la información sufra una pérdida de confidencialidad, integridad y disponibilidad.

1.6.8 Vulnerabilidad

Debilidades en el Sistema o en las medidas de seguridad implementadas que permitiría actuar a una amenaza contra un activo.

1.6.9 Riesgo

Probabilidad de que la amenaza actúe sobre el activo. Se utiliza para cuantificar el daño (probable) que puede causar la amenaza.

1.6.10 Políticas de Seguridad

Son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

10. Nomenclatura de Términos

2.1. **RDSI** = Red Digital de Servicios Integrados.

2.2. **NetBEUI** = NetBIOS Extended User Interface.

2.3. **NetBIOS** = Network Basic Input/Output System.

2.4. **ISO** = International Organization for Standardization.

2.5. **IEC** = International Electrotechnical Commission.

2.6. **ISP** = Internet Service Provider.

2.7. **P2P** = Peer-to-Peer.

2.8. **SMTP** = Simple Mail Transfer Protocol.

2.9. **HTML** = Hyper Text Markup Language.

2.10. **IP** = Internet Protocol.

2.11. **ICMP** = Internet Control Message Protocol.

2.12. **UDP** = User Datagram Protocol.

2.13. **TCP** = Transmission Control Protocol.

2.14. **PBX** = Private Branch Exchange.

11. Bibliografía

Autor Carlos A. Biscione, Año 2009, Resumen Ingeniería Social para no creyentes, IngenieraSocial_CarlosBiscione.pdf, Estados Unidos de Norteamérica.

Autor Carmen D´Souza, Año 2007, Monografía Redes, http://www.monografias.com/trabajos11/reco/reco.shtml, Argentina.

Autor Dr. Pere Marqués Graells, Año 2000, Monografía Las TIC y sus aportaciones a la sociedad, http://www.pangea.org/peremarques/tic.htm, México.

Autor ISACA, Año 2005, Manual de Revisión CISM 2005, Estados Unidos de Norteamérica.

Autor Kevin D. Mitnick & William L. Simon, Año 2006, Libro The art of deception, Estados Unidos de Norteamérica.

Autor Manuel Peralta, Año 2009, Monografía Sistema de Información, http://www.monografias.com/trabajos7/sisinf/sisinf.shtml, Argentina.

Autor Nicolás H. Kosciuk, Año 2006, Resumen Sistemas de Información Gerencial Laudon y Laudon, http://www.scribd.com/doc/20366672/Sistemas-de-informacion-Gerencial-Laudon-y-Laudon.

Autores Organización ISO y el Comité IEC, Año 2006, Documento - Estándar Internacional ISO/IEC 27002:2005, Estados Unidos de Norteamérica.

Autores Organización ISO y el Comité IEC, Año 2007, Documento - Estándar Internacional ISO/IEC 27002:2005, Estados Unidos de Norteamérica.

Autores, SUAPI, Año 2008, Metodología SU – CADI, Argentina.