RESUMEN

La presente tesis ha sido desarrollada pensando en la importancia que tiene la información hoy en día en toda organización. Primeramente se hace una introducción sobre la importancia de un Plan de Seguridad Informática para las organizaciones, se menciona también los Antecedentes, Posicionamiento, Justificación, Objetivos del Proyecto, Alcance y Metodología para el análisis de riesgos y para la seguridad de la información para la empresa Promix Ecuador C.A.

Se ha realizado además un marco teórico sobre la seguridad informática, describiendo las definiciones básicas, los tipos de seguridades, los delitos informáticos más comunes, las políticas de seguridad que una empresa debe tener en cuenta, la seguridad en redes e Internet y por último los puntos más importantes sobre criptografía.

Luego de tener en cuenta las definiciones sobre seguridad informática se realiza un Análisis de la Situación Actual de la empresa tanto en hardware, software, infraestructura física y comunicaciones y así posteriormente se identifican los recursos críticos que tienen la empresa.

Para el Análisis de Riesgos e Impactos, se definen los Niveles de Impacto y luego se clasifican los riesgos según dichos niveles, tanto para hardware, software, infraestructura física y comunicaciones de la empresa.

Posteriormente luego de un Análisis detallado de lo que posee la empresa, se define un Plan de Seguridad tomando en cuenta la Seguridad Física y Lógica, y presentando los controles preventivos, detectivos y correctivos que se deben tomar en cuenta para prevenir, detectar y corregir desastres. Y para concluir, se ha definido las Conclusiones y Recomendaciones que la empresa Promix Ecuador C.A deberá tener en cuenta luego de haber realizado el Análisis de la misma y definido un Plan de Seguridad Informática.

CAPITULO I

1.1 INTRODUCCION

En los últimos años en nuestro medio, la Informática se ha convertido en una de las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, como son los Sistemas de Información.

Todas las organizaciones dependen del procesamiento de datos para la generación de la información vital de la empresa, y esto a su vez está atado a los sistemas computacionales, por esto es imprescindible que dichos sistemas no dejen de funcionar para mantener operativa la organización.

Las amenazas son latentes para las empresas, pudiendo resultar de diferentes fuentes. Pueden ocurrir por desastres naturales, fallas prolongadas de la energía eléctrica, causados por errores humanos, fallas en los equipos, sabotaje de empleados, etc. Estas amenazas resultan ser un problema, y si el daño se prolonga, las pérdidas podrían representar grandes sumas de dinero y por ende poner en inestabilidad a la empresa.

Promix Ecuador C.A. ha creído necesario poner en marcha un Plan de Seguridad Informática que permita llevar a cabo un control sobre la información que maneja la empresa, para garantizar su correcto funcionamiento y evitar pérdidas como consecuencia directa de la ausencia de dicho plan.

La Seguridad en la Informática es de vital importancia para el buen desempeño de los sistemas de información ya que proporciona la protección necesaria para que los sistemas sean confiables y con un buen nivel de seguridad tanto física como lógica. La Seguridad Física se refiere a la protección de hardware y de los soportes de datos, mientras que la Seguridad Lógica se refiere a la protección de la información.

1.2 ANTECEDENTES

"Promix Ecuador C.A." es una compañía multinacional de capital Venezolano que brinda servicios y distribución de productos de consumo masivo a nivel nacional, siendo en un 99% la distribución directa de tarjetas de telefonía celular y pública de la compañía OTECEL EN ECUADOR, actualmente conocida como TELEFONICA. Esta compañía inicia su actividad en el Ecuador, desde Octubre del 2002.

Con el presente estudio se busca establecer políticas de seguridad de la información, autenticación, confidencialidad, integridad y controles de accesos, los cuales permitirán proteger la información, la misma que es el bien más importante de la compañía.

1.3 POSICIONAMIENTO

Para muchas organizaciones, la información y las tecnologías que las soportan representan su medio o recurso más valioso (de hecho, muchas organizaciones reconocen los beneficios potenciales que la tecnología puede aportar).

“Promix Ecuador C.A.” es una compañía que ha crecido con gran rapidez en el Ecuador, siendo su principal negocio la distribución y venta de tarjetas de telefonía celular y de cabina. Como consecuencia de este negocio, el manejo de la información se convierte en un aspecto de suma importancia para la misma.

En la actualidad, la compañía dispone de ciertas medidas de seguridad para salvaguardar los bienes y la información, pero estas no son suficientes ya que no cuenta con una guía capaz de enfrentar el tratamiento a los problemas de vulnerabilidad de la información así como la multitud de amenazas y ataques que se puedan presentar en un momento dado.

1.4 JUSTIFICACION

En vista de que el uso de teléfonos celulares así como el de cabinas de telefonía pública se ha incrementado a nivel nacional, en el Ecuador existen tres compañías que actualmente brindan el servicio antes mencionado, Promix se encuentra calificada con la Compañía OTECEL (Bellsouth), actualmente TELEFONICA.

Entre las principales actividades que demuestran deficiencia en su seguridad están:

- La ausencia de un Plan de Seguridad Informática.
- La ausencia de normativas de confidencialidad de la información para los empleados de la compañía.
- La ausencia de seguridades en los diferentes accesos a los sistemas que maneja la compañía.

Estos y otros aspectos más hacen que la Gerencia General de Promix Ecuador C.A se vea en la necesidad de solicitar que se defina un Plan de Seguridad Informática para que la información que maneja la compañía sea integra, confiable, confidencial, segura y oportuna.

1.5 OBJETIVOS DEL PROYECTO

1.5.1 Objetivo General

Plantear la aplicación de Medidas de Seguridad Informática que permitan garantizar la confidencialidad, integridad, oportunidad y confiabilidad de la Información dentro de la empresa Promix Ecuador C.A.

1.5.2 Objetivos Específicos

- Definir la situación actual de Promix Ecuador C.A. para tener una visión específica en lo referente a equipos informáticos y manejo de la información.
- Realizar el inventario de los recursos humanos, hardware, software, infraestructura física, comunicaciones de la compañía.
- Identificar los recursos críticos de la compañía.
- Realizar el Análisis de Riesgos e Impactos.
- Evaluar los Sistemas de Información que maneja la compañía.

- Evaluar los equipos que maneja la compañía tanto en su utilización como seguridad de los mismos.
- Proponer un plan de seguridad informática para la empresa Promix Ecuador C.A.

1.6 ALCANCE

Los siguientes puntos describen el Alcance del presente proyecto de Tesis:

- Establecimiento de un Marco Teórico de Seguridad Informática donde se describirá los conceptos básicos; Tipos de Seguridades: Seguridad Física y Seguridad Lógica; Delitos Informáticos; Políticas de Seguridad; Protección de la Información; Amenazas contra la Seguridad; Seguridades en Redes e Internet; Criptografía.

- Análisis sobre la Situación Actual de la compañía Promix Ecuador C.A, definiendo los recursos de la compañía y determinando aquellos recursos críticos que actualmente tiene la empresa.

- Análisis de Riesgos e Impactos, tanto en hardware, software, infraestructura física y comunicaciones.

- Definición de un Plan de Seguridad Informática.

1. Evaluación del Hardware:

a) Seguridad Física y Lógica (Controles Preventivos, Controles Detectivos y Controles Correctivos).

2. Evaluación del Software:

a) Descripción de los Sistemas de Aplicación.

b) Seguridad Física y Lógica (Controles Preventivos, Controles Detectivos y Controles Correctivos).

3. Evaluación de la Infraestructura Física:

a) Seguridad Física (Controles Preventivos, Controles Detectivos y Controles Correctivos).

4. Evaluación de las Comunicaciones:

a) Seguridad Física y Lógica (Controles Preventivos, Controles Detectivos y Controles Correctivos).

1.7 METODOLOGIA

Metodología de Análisis de Riesgos:

Desarrollada la identificación de la falta de controles y el establecimiento de un plan de seguridades. En base a cuestionarios, se identifica vulnerabilidades y riesgos, y se evalúa el impacto para más tarde identificar controles que garanticen la seguridad.

Posteriormente mediante un juego de simulación analizamos el efecto de los distintos controles en la disminución de los riesgos analizados, eligiendo de esta forma un Plan de Seguridad que compondrá el informe final de la evaluación.

Metodología de Seguridad:

1. Para la Evaluación de los Sistemas de Aplicación se llevarán a cabo las siguientes actividades:
   - Solicitud de la documentación del análisis y diseño de los sistemas de aplicación.
   - Solicitud de la documentación de los Sistemas de Aplicación (manuales técnicos, de operación de usuario, diseño de archivos y programas).
   - Recopilación y análisis de los procedimientos administrativos de cada sistema (flujo de información, formatos, reportes y consultas).
   - Análisis de claves, redundancia, control, seguridad, confidencialidad y respaldos.
   - Evaluación directa de la información obtenida contra las necesidades y requerimientos del usuario.
   - Análisis y evaluación de la información recopilada.

2. Para la evaluación de los equipos se llevará a cabo las siguientes actividades:
   - Solicitud de los estudios de viabilidad y características de los equipos actuales, proyectos sobre ampliación de equipo, su actualización.
   - Solicitud de contratos de compra y mantenimientos de equipo y sistemas.
   - Solicitud de información acerca de los procesos de obtención, actualización y mantenimiento de respaldos.
   - Solicitud de Contratos de Seguros.

- Visita técnica de comprobación de seguridad física y lógica de las instalaciones.

3. Elaboración y presentación del informe final (conclusiones y recomendaciones)

CAPITULO II

MARCO TEÓRICO DE SEGURIDAD INFORMÁTICA

2.1 DEFINICIONES BÁSICAS

2.1.1 Información

La **Información** es un conjunto de datos, los mismos que sirven para tomar una decisión; es un componente vital para el Control.

Existe información que debe o puede ser pública y aquella que debe ser privada, en esta segunda debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociéndolas siguientes características en la Información:

- Es crítica: es indispensable para garantizar la continuidad operativa.
- Es valiosa: es un activo con valor en si misma.
- Es sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

2.1.2 Sistema Informático

El **Sistema Informático** es el conjunto de recursos técnicos, financieros y humanos, que consiste en el almacenamiento, procesamiento y transmisión de la información de la organización.

Cuando un Sistema Informático se encuentra mal diseñado, este puede convertirse en una herramienta muy perjudicial para toda la empresa ya que como las máquinas obedecen a las órdenes recibidas, y la modelización de la empresa está determinada por las computadoras que materializan los Sistemas de Información, la gestión y la organización de la empresa no puede depender de un Software y Hardware mal diseñados.

2.1.3 Definición de Seguridad Informática

Seguridad Informática es la protección de la información y los activos relacionados con su captación, almacenamiento, transmisión, proceso, distribución y uso.

El objetivo de la seguridad informática es mantener ante todo la integridad, la disponibilidad, la privacidad, el control y la autenticidad de la información que es manejada mediante una computadora; además de reducir la probabilidad del impacto a un nivel mínimo aceptable, a un costo razonable y asegurar la adecuada y pronta recuperación.

2.1.4 Confidencialidad

La confidencialidad es el servicio de seguridad que permite que la información no pueda estar disponible o ser descubierta por o para terceras personas, entidades o procesos que no se encuentran autorizados. La confidencialidad, denominada también privacidad o secreto, se refiere a la capacidad que tiene el sistema para evitar que personas no autorizadas puedan acceder a la información que se encuentra almacenada en él.

Existen algunos mecanismos que se utilizan para salvaguardar la confidencialidad de los datos como por ejemplo:

- Se utilizan técnicas de control de acceso a cualquier sistema.
- El cifrado de la información confidencial o de las comunicaciones.

2.1.5 Integridad

La integridad es un servicio de seguridad, el mismo que garantiza que la información que se encuentran en un sistema no sea modificada y destruida por personas no autorizadas.

Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema. En el ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la *autenticidad.* Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, saber quién los envió y conocer la fecha exacta de cuando fueron enviados y recibidos.

2.1.6 Disponibilidad

Es el grado en que un dato se encuentra en el lugar, momento y forma en que es requerido por el usuario autorizado.

Para que un sistema se lo considere seguro, éste debe mantener la información correctamente almacenada con el hardware y el software funcionando perfectamente y además debe respetar los formatos para su recuperación en forma satisfactoria.

2.1.7 Autenticidad

La autenticidad permite verificar que la información requerida es válida y utilizable en tiempo, forma y distribución, así como el de determinar si un usuario tiene el permiso para acceder a un sistema o red. Normalmente se lo realiza con una contraseña (sólo el usuario legítimo puede conocer).

2.2 TIPOS DE SEGURIDADES

Los tipos de seguridades establecidos son:

- Seguridad Física
- Seguridad Lógica

2.2.1 Seguridad Física

Debemos tomar en cuenta que aunque nuestra empresa sea la más segura desde el punto de vista de ataques externos tales como hackers, virus, etc.; la seguridad de la misma será nula si no se ha previsto como combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras de recuperación.

La seguridad física consiste en la aplicación de procedimientos de control y barreras físicas, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere tanto a los controles, mecanismos de seguridad, y medios de acceso remoto dentro y alrededor del Centro de Cómputo, implementados para proteger el hardware y medios de almacenamiento de datos.

Tener controlado el ambiente y acceso físico permite:

- Disminuir riesgos.
- Trabajar mejor manteniendo la sensación de seguridad.
- Descartar falsas hipótesis si se produjeran incidentes.
- Tener los medios necesarios para luchar contra accidentes.

2.2.1.1 Tipos De Desastres

Dentro de la seguridad física se preveen algunas amenazas como por ejemplo:

- Desastres naturales, incendios accidentales e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

A continuación se analizan los peligros más importantes que se tienen en un centro de procesamiento:

2.2.1.1.1 Incendios

Los incendios son la causa del mal uso de combustibles, fallas en las instalaciones eléctricas y el traslado y almacenamiento de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Para reducir los riesgos de incendio en un centro de cómputo se debe tomar en cuenta los siguientes aspectos:

- El área en la que se encuentran las computadoras deben estar en un local que no sea combustible o inflamable.
- El local no debe situarse encima, debajo o alrededor de áreas que procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Los materiales de las paredes deben ser incombustibles y extenderse desde el suelo al techo.
- Deben construirse un piso falso instalado sobre el piso real, con materiales resistentes al fuego y que sean inconsumibles.
- En el área de proceso debe prohibir el fumar.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles.
- Deben evitarse los materiales plásticos e inflamables.

Para proteger los equipos de cómputo, estos deben ser instalados en áreas en donde el acceso sea estrictamente para el personal autorizado.

2.2.1.1.2 Inundaciones

Las inundaciones son definidas como invasiones de agua causadas por escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o física.

2.2.1.1.3 Instalación Eléctrica

Cuando se trabaja con computadoras, estamos trabajando con electricidad, por lo tanto debemos tener en consideración que este tipo de áreas deben tener una mayor seguridad física. Este tipo de problemática abarca desde el usuario hogareño hasta la gran empresa.

Con el pasar del tiempo, los sistemas se vuelven cada vez más complicados por lo que es necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Algunos de los problemas eléctricos al que se enfrentan los usuarios son las subidas y caídas de tensión, y además el ruido que interfiere en el funcionamiento de los componentes electrónicos.

Otro problema es la instalación de los cables puesto que estos se utilizan para construir las redes locales que van desde el cable telefónico normal hasta el cable coaxial o a la fibra óptica.

Los riesgos más comunes para el cableado son los siguientes:

- Interferencia: Pueden estar generadas por cables de alimentación de maquinaria pesada, así como por equipos de radio o microondas.
- Corte del cable: Cuando por algún motivo, la conexión establecida se rompe impidiendo que el flujo de datos circule por el cable.
- Daños en el cable: Cuando existe un cable dañado, esto afecta la transmisión de los datos ocasionando que las comunicaciones dejen de ser confiables.

2.2.1.1.4 Acciones Hostiles

- **Robo**

Para la empresa, las computadoras son equipos valiosos y al igual que las piezas de stock e incluso el dinero; están expuestas a cualquier acción hostil. Además, es frecuente que las personas que operan las computadoras de la empresa, utilicen las mismas para realizar trabajos privados o trabajos para otras organizaciones, y de esta forma, robar tiempo de máquina. El software, es una propiedad muy fácil de sustraerla y, las cintas y discos son fácilmente copiados sin dejar ningún rastro.

- **Sabotaje**

En los centros de procesamiento de datos, el sabotaje es uno de los peligros más temidos. Físicamente, con una sola pasada de un imán, la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección.

2.2.1.1.5 Control de Accesos

El control de accesos requiere de la capacidad de identificación, el permitir o negar el acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

Por ejemplo para controlar el acceso a un edificio existe un servicio de vigilancia, este servicio es el encargado de colocar en lugares estratégicos a distintos guardias para cumplir con sus objetivos y controlar el acceso del personal.

Cuando una persona ajena desea ingresar al edificio, se deberá registrar sus datos personales, los motivos de su visita, la hora de ingreso y egreso, y otros aspectos según políticas de la empresa, además se deberá pedir su credencial de identificación.

Para controlar el ingreso y egreso de los vehículos, el personal de vigilancia deberá registrar en cada planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la empresa.

Se puede tener una protección electrónica, como por ejemplo la detección de robo, de intrusión, de asalto y de incendios, estos funcionan con la utilización de sensores conectados a centrales de alarmas.

Estas centrales están conectadas a los elementos de señalización que son los encargados de hacerles saber de una situación de emergencia. Cuando uno de los elementos sensores detectan alguna situación de riesgo, éstos transmiten el aviso a la

central; ésta procesa toda la información que se ha recibido y ordena en respuesta la emisión de señales sonoras alertando de la situación.

2.2.2 Seguridad Lógica

La información es el activo más valioso que posee cada empresa, y por lo tanto deben existir técnicas, más allá de la seguridad física, que aseguren dicha información. Estas técnicas las brinda la Seguridad Lógica.

La Seguridad Lógica se basa en la aplicación de procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a aquellas personas autorizadas para hacerlo.

Los objetivos que se plantean serán:

- Restringir el acceso a los diferentes programas y archivos que posee la empresa.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y los programas correctos en y por el procedimiento correcto.
- Que la información que se transmite sea recibida por el destinatario y no a otro.
- Que la información recibida sea exactamente la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia, para la transmisión de la información.

2.2.2.1 Control de Accesos

El control de accesos tiene un papel muy importante dentro de la Seguridad Lógica para una empresa, ya que se pueden implementar sobre el Sistema Operativo, sobre los sistemas de aplicación, sobre bases de datos, sobre paquetes específicos de seguridad o en cualquier otro utilitario.

Estos controles constituyen ayuda muy importante ya que permite proteger al sistema operativo de la red, así como también al sistema de aplicación y a los demás programas, de la utilización o modificaciones por personal no autorizado; para mantener la integridad de la información que posee la empresa y para resguardar la información confidencial de accesos no autorizados.

La identificación y la autenticación es la base para la mayor parte de los controles de accesos y para el seguimiento de las actividades de los usuarios. Se denomina **Identificación** al momento en que cualquier usuario registrado se identifica al sistema; y **Autenticación** a la verificación que realiza el sistema sobre la identificación de dicho usuario.

Para realizar la autenticación de la identidad del usuario existen cuatro técnicas:

- Algo que solamente el usuario conoce ya sea una clave secreta de acceso o password, una clave criptográfica, etc.
- Algo que el individuo posee por ejemplo una tarjeta magnética.

- Algo que identifica a cada individuo unívocamente: por ejemplo las huellas digitales o la voz.
- Algo que cada persona es capaz de hacer: como por ejemplo los patrones de escritura.

Es conveniente, desde el punto de vista de la eficiencia, que cada usuario sea identificado y autenticado solamente una vez, pudiendo acceder de esta única forma a todas las aplicaciones y los datos a los que su perfil le permita, así como para acceder tanto a sistemas locales como a sistemas en los que deba acceder en manera remota.

Una de las posibles técnicas para implementar una única identificación de usuarios es la utilización de un servidor de autenticaciones en donde los usuarios se identifiquen, y además que posteriormente se encargue de autenticar al usuario sobre los equipos restantes a los que éste pueda acceder. Este servidor no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas geográficas como lógicamente.

2.2.2.2 Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario de cada empresa sobre los recursos y a la información. Esta modalidad puede ser:

- **Lectura:** El usuario solamente puede leer o visualizar la información pero no puede cambiarla o alterarla. Dicha información podrá ser únicamente copiada o impresa.
- **Escritura:** Este tipo de acceso permite agregar datos, modificar o borrar la información.
- **Ejecución:** Este acceso permite al usuario ejecutar programas.

- **Borrado:** El usuario puede eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado como una forma de modificación.

2.2.2.3 Control de Acceso Interno

Se utilizan solo Palabras Claves para que permitan la autenticación del usuario para que de esta manera se puedan proteger todos los datos y aplicaciones. El usuario se ve en la necesidad de utilizar una variedad de palabras claves para poder acceder a diferentes sistemas siendo muy difícil recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida el propósito de esta técnica.

2.2.2.4 Control de Acceso Externo

Se pueden utilizar dispositivos de control de puertos que autorizan el acceso a un puerto determinado y pudieran estar físicamente separados o estar en otro dispositivo de comunicaciones, por ejemplo un módem.

Otro método es el utilizar Firewalls o también conocidos como Puertas de Seguridad ya que permiten bloquear o filtrar el acceso entre dos redes o más, generalmente una privada y una externa por ejemplo el Internet. El Firewall permite que los usuarios internos se conecten a una red externa previniendo al mismo tiempo la incursión de atacantes o virus a los sistemas de la organización.

2.3 DELITOS INFORMÁTICOS

2.3.1 Fraudes Cometidos Mediante El Manejo De Computadoras

- **Manejo De Los Datos De Entrada O Sustracción De Datos**

Es el delito informático más común puesto que es relativamente fácil de cometer y difícil de descubrir.

Este delito no requiere de conocimientos demasiado técnicos en informática y puede ser realizado por cualquier persona que acceda a las funciones de los procesamientos de datos en la fase de adquisición de estos.

- **Manejo De Programas**

Es bastante difícil de descubrir y muy frecuentemente pasa inadvertida debido a que el delincuente debe poseer conocimientos más técnicos en informática. Este delito consiste en manipular los programas que existen en el sistema o en introducir nuevos programas o nuevas tareas.

- **Manejo De Los Datos De Salida**

Se ejecuta fijando un objetivo en el funcionamiento del sistema informático. El ejemplo más común es el cometido hacia los cajeros automáticos mediante la adulteración de instrucciones para la computadora en la fase de adquisición de datos.

2.3.2 Daños o Alteraciones De Programas o Datos Computarizados

2.3.2.1 Sabotaje Informático

Es la acción de borrar, quitar o alterar sin permiso funciones o datos con intención de entorpecer el funcionamiento normal del sistema. Las técnicas que permiten cometer este tipo de sabotajes son:

- **Virus**

Es una serie de instrucciones programáticas que pueden adjuntarse a los programas existentes y propagarse a otros programas informáticos. Un virus puede insertarse en un sistema por medio de una pieza legítima de soporte lógico que ha quedado infectada.

- **Gusanos**

Se realizan de forma análoga al virus con el objetivo de introducirlo en programas legítimos de procesamiento de datos o para adulterar o suprimir los datos, pero se diferencia del virus porque no tiene la facultad de regenerarse.

Los efectos del ataque de un gusano pueden ser tan graves como los del ataque de un virus: por ejemplo, un programa gusano que posteriormente se auto destruirá puede ordenar a un sistema informático de un banco para que transfiera permanentemente dinero a una cuenta ilícita.

- **Bomba Lógica o Cronológica**

Es necesario conocimientos especializados puesto que requiere la programación de la destrucción o adulteración de datos en un momento dado del futuro. A diferencia de los virus y gusanos, las bombas lógicas son difíciles de descubrir antes de que exploten; por eso, de todos los mecanismos informáticos criminales, las bombas lógicas tienen un potencial de daño mucho mayor. Su explosión puede programarse para que ocasione el máximo de daño y para que se ejecute mucho tiempo después de que el delincuente se haya marchado.

- **Hackers o Piratas Informáticos**

El acceso generalmente se produce desde un lugar exterior, ubicado en la red de telecomunicaciones. El delincuente aprovecha la falta de solidez en las medidas de seguridad para tener acceso o bien puede descubrir fallas en las medidas de seguridad vigentes o en el sistema en si. Frecuentemente, los piratas informáticos se infiltran como usuarios legítimos del sistema; esto sucede a menudo en los sistemas en donde los usuarios emplean contraseñas comunes o contraseñas de administración que se encuentran en el mismo sistema.

2.4 POLÍTICAS DE SEGURIDAD

La política de seguridad es la forma en que los distintos niveles de la misma organizan, gestionan, protegen y distribuyen la información tratada a cada nivel.

Dentro de los objetivos principales de una política de seguridad tenemos:

- Informar con el mayor nivel de detalle a los usuarios, empleados y gerentes de las normas que se deben cumplir para resguardar los componentes de los sistemas de la empresa u organización.
- Suministrar las pautas para configurar y controlar los sistemas informáticos y de redes para que estén en correlación con la política de seguridad.

Son los dirigentes junto con los expertos en tecnologías informáticas, quienes definirán los requisitos de seguridad, identificando y dando prioridades a los distintos elementos de las actividades realizadas, y así los procesos de mayor importancia recibirán más protección. Las políticas de seguridad deben ser consideradas como parte de la operatividad habitual y no como un extra añadido.

2.4.1 Tipos de Políticas

Existen principalmente tres tipos de políticas, cada una de las cuales actúa a distinto nivel y aborda distintos aspectos de la seguridad:

- Políticas administrativas
- Políticas de control de accesos
- Políticas de control de flujo

2.4.1.1 Políticas Administrativas

Este tipo de política se encarga de los procedimientos administrativos relacionados con la seguridad, no de los aspectos técnicos y de ejecución de la misma.

Entre los aspectos a ser tratados por este tipo de políticas las más importantes son:

- Análisis y Gestión de Riesgos.
- Política de actuación en caso de desastre.
- Monitoreo y auditoría del sistema y de los empleados.

- Entrenamiento y formación de los usuarios.
- Política de copias de seguridad.

2.4.1.2 Políticas de control de accesos

Éstas establecen bajo que condiciones cada sujeto puede acceder a cada objeto. Se entiende por sujeto a cualquier usuario, programa, computador remoto u otro dispositivo que pueda tener acceso a nuestro sistema. Entenderemos por acceso cualquier acción aplicada sobre los objetos, tal como leer, escribir, modificar o ejecutar. Y finalmente, entenderemos por objeto cualquier fichero, directorio, proceso en memoria, dispositivo de nuestro sistema.

Existen diferentes criterios de clasificación de las políticas de control de accesos:

Compartición frente a menor y mayor privilegio:

- Las políticas de menor privilegio establece que los sujetos sólo pueden acceder a aquellos objetos que necesitan para realizar su trabajo.
- La política de compartición de máximo privilegio es la contraria, ya que en ella todos los sujetos pueden acceder por defecto a todo el sistema.

Granularidad:

Se define la granularidad como el tamaño mínimo de los objetos accesibles, y por tanto susceptibles de ser protegidos. Puede ser una granularidad muy fina (a nivel de

direcciones individuales), o muy gruesas (a nivel de segmento de memoria o de dispositivo).

Abiertas frente a cerradas:

- Las políticas cerradas prohíben por defecto cualquier acceso. Para que un acceso sea posible debe estar necesariamente permitido. Este tipo de políticas son más seguras, ya que permiten examinar cada objeto del sistema y definir si es accesible o no, cómo es accesible y para quién. En este punto se puede aplicar por ejemplo una política de menor privilegio a la hora de definir los accesos. Este tipo de políticas son más costosas, ya que requieren del administrador de la seguridad una comprobación completa de todos los aspectos del sistema y un conocimiento de sus características de seguridad.

- Las políticas abiertas permiten por defecto cualquier acceso. Para que no se pueda acceder a un objeto debe prohibirse explícitamente. Este tipo de políticas son más inseguras, ya que descuidan el análisis de la seguridad de todo el sistema y tan solo se preocupan de determinados objetos. Este tipo de políticas son menos costosas para el administrador de la seguridad.

2.4.1.3 Políticas de control de flujos

Estas políticas tratan sobre la difusión de la información una vez accedida, estableciendo cuales son los canales legítimos para su diseminación. Cuando se habla de canales, no se refiere siempre a canales físicos de transmisión de información, sino a

sistemas de transferencia, a las distintas formas en la que la información puede fluir de un sujeto origen a un sujeto destino.

2.5 SEGURIDAD EN REDES E INTERNET

Se debe entender por una red como un entorno en donde hay más de un computador independiente.

Con la conexión al Internet, el usuario podrá tener acceso a otras computadoras ubicadas en cualquier parte del mundo y así ejecutar sus programas, también podrá tener acceso a un sin fin de aplicaciones que no estarían disponibles sin este recurso.

A la hora de acceder a los recursos, el uso de una red informática aumenta la fiabilidad de los mismos, puesto que su replicación permite seguir disponiendo de recursos alternativos en caso de fallo.

El hecho de compartir los recursos por medio de la red aumenta el número de usuarios implicados y por consiguiente el número de posibles ataques.

Con respecto a la privacidad de la información se hace más difícil mantenerla en cada nodo debido al aumento de posibles usuarios que pueden penetrar en el mismo. Por otro lado al transferirse la información, en muchos casos sin ningún tipo de protección, aumenta el número de puntos en los que puede ser interceptada y desvelada. Sobre la integridad, la transmisión de la información es un claro peligro para su mantenimiento,

los mensajes pudieran ser interceptados, modificados, borrados, o inclusive pudieran insertarse mensajes falsos o espurios.

En relación a la autenticidad, al utilizarse redes informáticas no solo es necesario autentificar a los usuarios, sino también a los nodos.

En el nivel físico, esto se realiza por medio de placas de redes, además de una conexión entre ellas. Se debe fijar una comunicación utilizando el mismo lenguaje entre los diferentes sistemas operativos y placas. Este lenguaje se lo conoce como PROTOCOLO.

Ciertos protocolos están encargados de transportar datos, mientras que otros se encargan de arreglar de forma correcta los datos, y otros de la comunicación entre las computadoras. Así de esta manera podemos definir a **Protocolo** como el conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

2.5.1 Redes TCP/IP

El modelo TCP/IP esta formado por un completo conjunto de protocolos de comunicación, entre los que se destacan dos: TCP (Transmissión Control Protocol) e IP (Internet Protocol). Todos los protocolos utilizados son estándares internacionalmente admitidos y, salvo los de más bajo nivel, son independientes del hardware y del sistema operativo utilizado.

Los distintos protocolos se integran en cuatro capas o niveles fundamentales. Cada capa tiene sus respectivas funciones y ofrecen servicios específicos, y en una transmisión entre dos extremos, los mismos niveles en el emisor y en el receptor tratan con la misma información.

En las redes TCP/IP los cuatro niveles utilizados son:

- **Nivel 1 o nivel de acceso a la red:** Define como transmitir los datagramas IP sobre un soporte físico.
- **Nivel 2 o nivel de Internet:** Define los paquetes básicos de transmisión o datagrama y se encarga entre otros aspectos del encadenamiento de los mismos. En este nivel suele usarse el protocolo IP.
- **Nivel 3 o nivel de transporte:** Proporciona los servicios de transmisión extremo a extremo garantizando una serie de características en la transmisión. En este nivel se utilizan los protocolos TCP.
- **Nivel 4 o nivel de aplicación:** Se encuentran las distintas aplicaciones y procesos que utilizan la red, tales como telnet, ftp o el correo electrónico (SMTP).

2.5.2 Estructura Básica de la Web

World Wide Web (www) es conocida como "telaraña que cubre el mundo". La estructura básica de ésta radica en que el protocolo HTTP (HiperText Transfer Protocol) opera como un transporte genérico que conduce varios tipos de información desde servidor hasta el cliente.

El protocolo HTTP es un protocolo cliente-servidor para sistemas de información distribuidos. Este protocolo es genérico porque actúa como un conducto para mover datos de aplicación, es sin estado porque no mantiene un estado, es decir que cuando se requiere una transferencia a través de HTTP, se crea la conexión luego realiza la transferencia y posteriormente se termina la conexión, es orientado a objetos porque tiene etiquetas que señalan el tipo de datos que se va a transferir por la red.

Cada servidor se relaciona de una forma única con un Localizador Unificado de Recursos (URL), éste a su vez está relacionado con una dirección IP. El tipo de datos más común es HTML (HiperText Markup Language) que es transportado a través de HTTP.

El Internet es la red de computadoras más grande del mundo. Sin embargo la importancia de Internet no radica únicamente en la cantidad de máquinas interconectadas sino en lo servicios que brinda al usuario.

Con la utilización de Telnet o e-mail, el servicio presenta una interface ANSI (sin gráficos), solo con caracteres alfanuméricos. Por medio de un programa cliente, la gestión se vuelve más sencilla, visual y agradable, como sucede con la WWW donde se presentan cada página en formato gráfico.

- **Telnet (Telecommunicating Networks)**

Este protocolo fue diseñado y elaborado para brindar un servicio de conexión remota (remote login). Forma parte del conjunto de protocolos TCP/IP y depende básicamente del protocolo TCP para el nivel de transporte.

El protocolo Telnet permite tener acceso a los recursos y ejecutar los programas de un equipo remoto en la red, como si se tratara de un terminal real conectado en forma directa al sistema remoto. Luego de haber realizado la conexión, el usuario puede iniciar la sesión con su clave de acceso.

2.6 CRIPTOGRAFÍA

2.6.1 Definición

La palabra Criptografía proviene del griego kryptos (oculto) y grafía (escritura): Escritura oculta. La Criptografía es pues la ciencia que estudia la escritura secreta, es decir, la forma de escribir ocultando el significado. En la práctica, la Criptografía se ocupa del cifrado y el descifrado de mensajes para evitar que caiga en manos poco confiables. Cifrar información consiste en convertir un mensaje en claro en un mensaje cifrado mediante el uso de una clave.

2.6.2 Criptografía en la Seguridad Informática

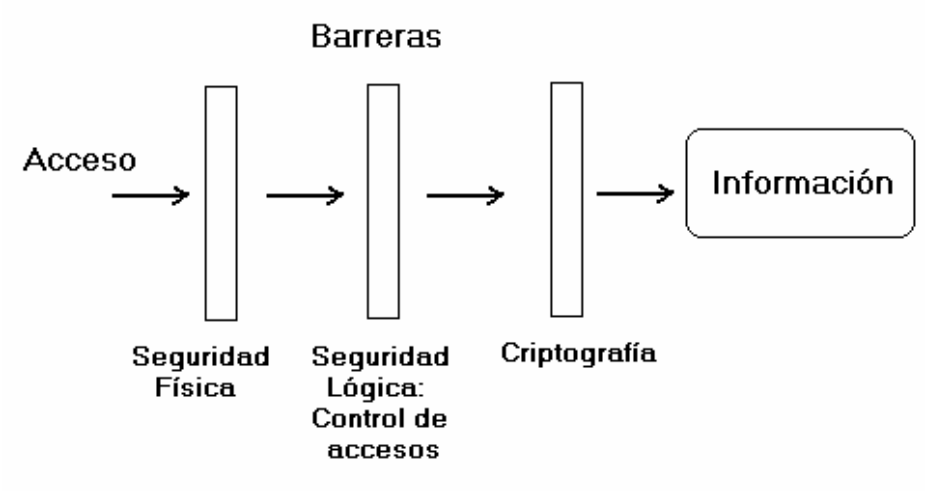


Figura 2.1: (Criptografía en la Seguridad Informática)

La Criptografía puede aplicarse en dos ámbitos de la seguridad informática: en el almacenamiento de información y en la transmisión de la misma, es decir, la Criptografía se utiliza para proteger los datos que se encuentran almacenados en los sistemas basados en computador o que son enviados a través de redes de computadores como lo es el Internet.

Veamos como la Criptografía se relaciona con cada uno de las características de la seguridad informática:

- **Confidencialidad:** El cifrado de la información es un excelente método para preservar la privacidad de la misma. Aunque se acceda a la información, o se intercepte mientras se transfiere, si está cifrada sigue siendo inútil a menos que pueda descifrarse.

- **Integridad Y Precisión:** Algunos sistemas criptográficos incorporan medios para prevenir que se dañe la integridad de la información, esto es, que ésta sea modificada voluntaria o involuntariamente. El sistema permite detectar cualquier pequeño cambio que se haya producido en el mensaje original.

- **Autenticación:** La Criptografía puede usarse también para asegurar la autenticidad de los mensajes. Esto es, asegurar que el mensaje ha sido enviado por quién se identifica como su emisor. Se trata de identificar sin posible error el origen de los mensajes. En relación con la autenticación suelen utilizarse las denominadas firmas digitales. Se trata de añadir algún tipo de información en el mensaje o de utilizar de algún modo las claves para validar en destino el origen del mensaje.

Los dos principales objetivos de la Criptografía son: la *privacia* la misma que consiste en prevenir que alguna persona no autorizada espíe los datos; y la *autenticación* que consiste en evitar que los datos sean modificados por alguien no autorizado.

Los programas encriptadores necesitan de un texto a encriptar y además una clave proporcionada por el usuario de manera que cada texto con diferente clave sea totalmente único e indescifrable. El método de desencriptación o descodificación vendría a funcionar solamente cuando el usuario otorgue la clave correcta, para así volver a tener el documento original.

2.6.3 Sistemas Criptográficos actuales

2.6.3.1 El sistema DES (Data Encryption Standard)

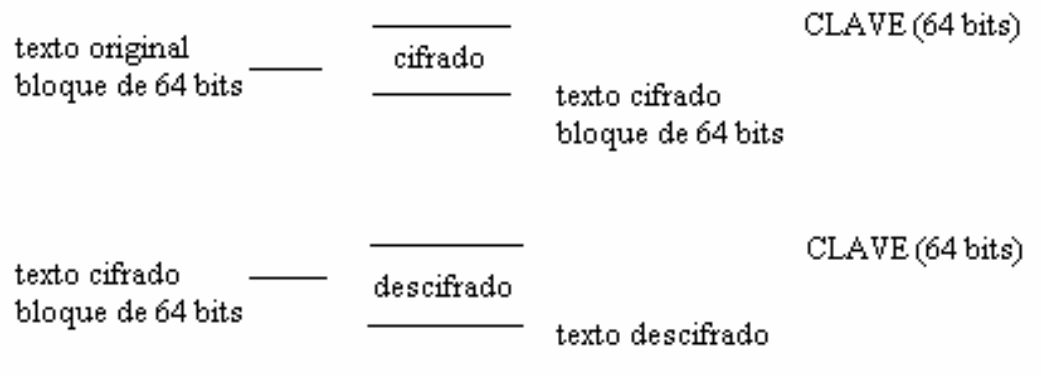
El algoritmo DES es uno de los sistemas de cifrado considerado de alta seguridad, dado que se ha transformado en un estándar reconocido por las agencias americanas y que se trata de un sistema de gran fortaleza. El origen de DES se debe a una petición realizada en 1973 por el NBS (National Bureau of Standards) a distintos fabricantes para someter criptosistemas que pudieran servir como base a un estándar de cifrado de textos reservados no clasificados. IBM disponía de un sistema altamente seguro denominado LUCIFER basado en una clave de 128 bits. Este sistema fue sometido al examen de la NBS y, tras ser analizado por expertos de la NSA (National Security Agency), y ser reducido a 56 bits, fue aceptado y denominado DES.

2.6.3.1.1 Funcionamiento del DES

La seguridad de un sistema criptográfico basado en DES, está determinada por la seguridad de las claves de cifrado y descifrado ya que el algoritmo DES es de conocimiento público.

Los sistemas DES son ideales para la Criptografía de información almacenada en medios magnéticos pero tiene sus limitaciones a nivel de información a ser transmitida por canales de comunicaciones cuando surge la necesidad de autenticar la identidad del emisor del mensaje o se desea simplificar la administración de las claves.

Bajo el control de una clave criptográfica o clave privada el DES cifra un bloque de texto original en un bloque de texto cifrado, ambos de 64 bits, de los cuales 56 son usados directamente por el algoritmo y 8 son utilizados para detección de errores. El descifrado convierte los datos a su forma original si se usa la misma clave.



La clave es generada de tal modo que 56 bits de los 64 son usados por el algoritmo y 8 son usados como bits de paridad impar de cada byte de 8 bits, es decir, existe un número impar de bits 1 en cada byte.

2.6.3.2 Sistemas de Claves Públicas

En este tipo de sistemas se utilizan dos claves: una clave pública y una clave privada. En un grupo de usuarios, cada uno de ellos posee dos claves distintas:

- La clave pública K', es aquella que puede ser conocida por todos los usuarios del sistema.
- La clave privada K, es conocida solo por su propietario.

Aunque estas claves están relacionadas matemáticamente, la fortaleza del sistema esta en manos de la imposibilidad computacional de obtener una a partir de la otra.

Este tipo de sistemas se denominan Asimétricos porque no podemos usar una misma clave para cifrar y descifrar un mensaje. Ambas claves deben ser usadas en el proceso. Si ciframos un mensaje con una de ellas, debemos descifrarlo con la otra. Para que un sistema sea seguro se deben usar las dos claves, el emisor tiene que cifrar el mensaje secreto utilizando la clave pública del receptor.

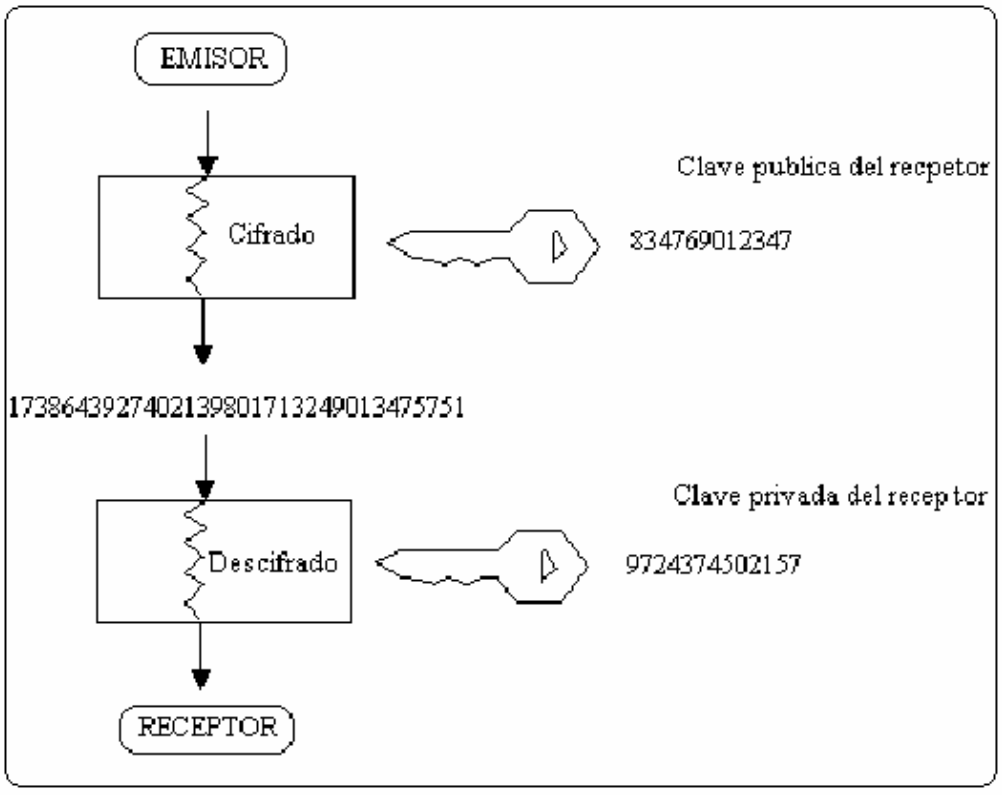


Figura 2.2: (Cifrado por medio de la clave pública del receptor)

Para que un mensaje se lo pueda descifrar se debe utilizar únicamente la clave privada de receptor, con lo que garantiza de esta forma la confidencialidad del mismo. La clave pública del receptor no sirve para descifrar el mensaje, y por tanto tan solo el receptor, puede descifrarlo.

Por otra parte el mensaje no es auténtico, ya que cualquier usuario puede conocer la clave pública del receptor, cualquier usuario puede ser el emisor del mensaje. La recepción de un mensaje cifrado con la clave pública del receptor no identifica unívocamente al emisor, y por tanto no lo autentifica.

Si el emisor quiere garantizar la autenticidad de un mensaje, debe cifrarlo con su clave pública.

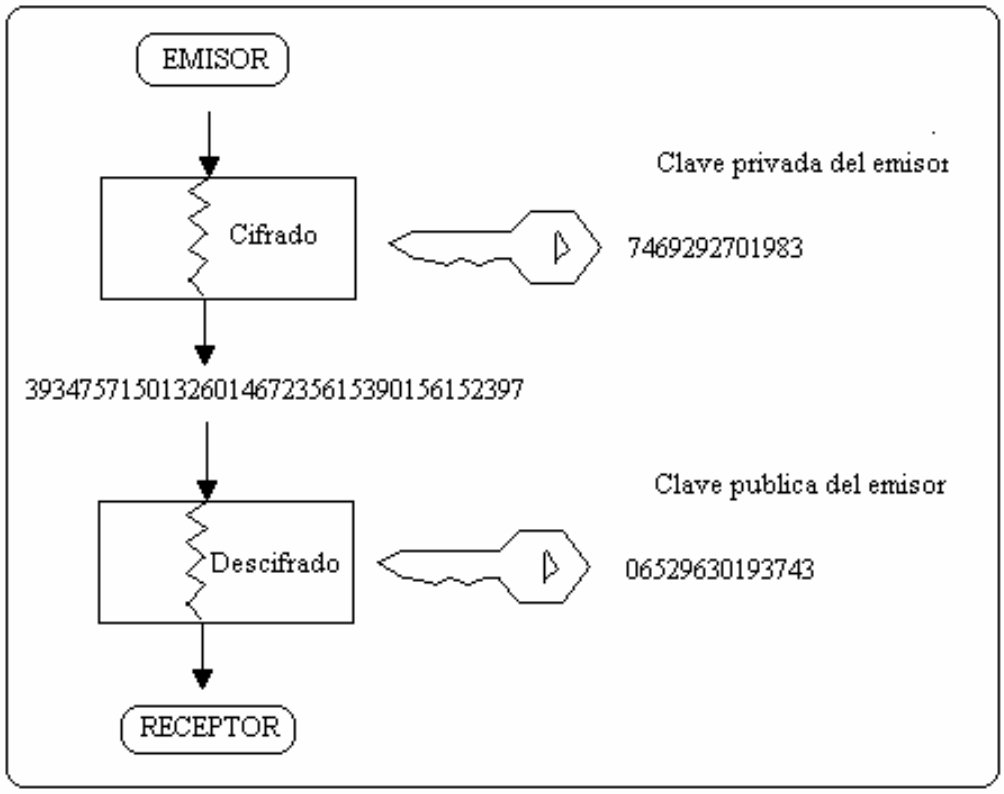


Figura 2.3: (Cifrado por medio de la clave privada del emisor)

El receptor podrá descifrarlo usando la clave pública del emisor. Dado que todo el mundo puede conocer la clave pública del emisor, no se garantiza la confidencialidad del mensaje ya que cualquier persona puede descifrarlo.

Sin embargo, dado que tan solo el emisor conoce su propia clave privada, tan solo él puede ser el origen del mensaje, con lo que se garantiza la autenticidad del mismo. El secreto y la autenticidad en este tipo de sistemas se logran por separado.

2.6.3.3 Firma Digital

Una firma digital es una firma electrónica la misma que se utiliza para:

- Autenticar la identidad del emisor de un mensaje.
- Autenticar el firmante del documento.
- Autenticar el dueño de una tarjeta de crédito.
- Asegurar que el contenido original de un mensaje.
- Asegurar que el documento enviado no ha sido cambiado.

Una firma digital es generada desde un certificado digital empleando una tecnología de llave pública y privada.

Estas llaves son una serie de números asignados al propietario. El firmante ocupa la llave privada para firmar un documento electrónico, y el receptor ocupa la llave pública, que anteriormente mando el firmante, para demostrar que la firma es auténtica.
Los beneficios que tiene una firma digital son:

- Es fácil de transportar.
- No puede ser fácilmente excluida.
- No puede ser reproducida por otra persona.
- Puede ser automáticamente sellada a tiempo.
- Puede ser utilizada con cualquier tipo de mensaje, ya sea codificado o no, de manera que el receptor puede estar completamente seguro de la identidad del emisor del mensaje así como que el mensaje no llegó defectuoso o incompleto.

2.6.3.3.1 Las Funciones Hash.

Las funciones hash o funciones resumen se utilizan en la firma digital, uno de los inconvenientes para el proceso de cifrado ocurre cuando los mensajes que se intercambian llegan a tener un gran tamaño por lo que es conveniente cifrar un resumen del mismo aplicando al mensaje una función hash.

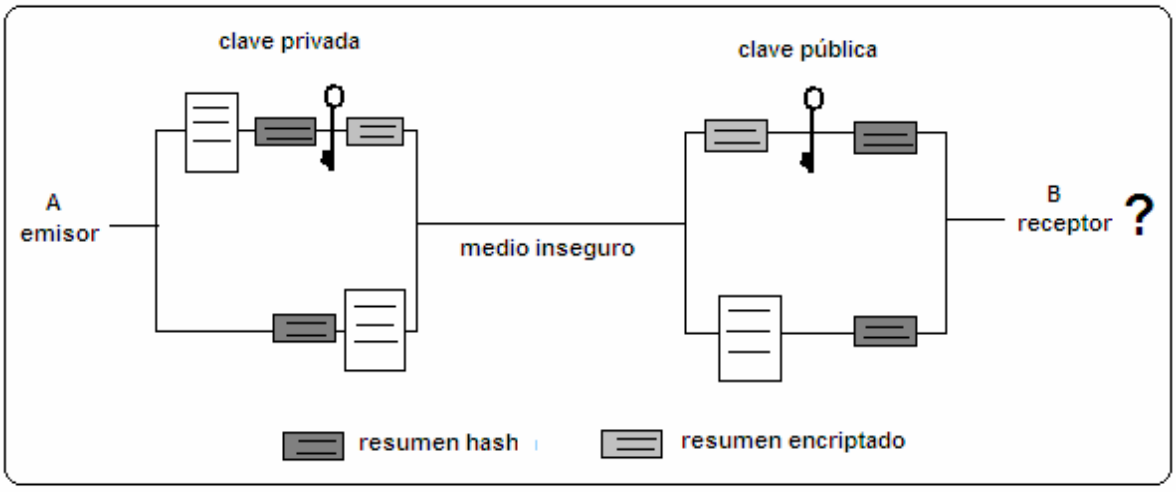


Figura 2.4: (Firma digital con resumen hash)

Su funcionamiento es el siguiente:

1. El emisor aplica al documento una función hash conocida para obtener un resumen hash del mismo.
2. Este resumen lo encripta con su clave privada.
3. Posteriormente es enviado el documento original plano y el resumen hash encriptado, al receptor.
4. El receptor B coloca la función hash al resumen sin encriptar y con la llave pública de A desencripta el resumen encriptado.
5. Si ambos coinciden está seguro de que el documento fue enviado por el emisor A, caso contrario, el documento ha sido interceptado durante el medio de envío y modificado.

El alfabeto a utilizar se expresa en el siguiente catálogo:

Tabla 2.1: (Código ASCII para utilizar en Funciones Hash)

Elemento del Alfabeto	Valor B64	Valor ASCII
0	A	65
1	B	66
2	C	67
3	D	68
4	E	69
5	F	70
6	G	71
7	H	72

Elemento del Alfabeto	Valor B64	Valor ASCII
32	g	103
33	h	104
34	i	105
35	j	106
36	k	107
37	l	108
38	m	109
39	n	110

Elemento del Alfabeto	Valor B64	Valor ASCII
8	I	73
9	J	74
10	K	75
11	L	76
12	M	77
13	N	78
14	O	79
15	P	80
16	Q	81
17	R	82
18	S	83
19	T	84
20	U	85
21	V	86
22	W	87
23	X	88
24	Y	89
25	Z	90
26	a	97
27	b	98
28	c	99
29	d	100
30	e	101
31	f	102

Elemento del Alfabeto	Valor B64	Valor ASCII
40	o	111
41	p	112
42	q	113
43	r	114
44	s	115
45	t	116
46	u	117
47	v	118
48	w	119
49	x	120
50	y	121
51	z	122
52	0	48
53	1	49
54	2	50
55	3	51
56	4	52
57	5	53
58	6	54
59	7	55
60	8	56
61	9	57
62	+	43
63	/	47

Es una clave simétrica estándar internacional. La utilizan, por ejemplo, todos los ordenadores.

E	**n**		**u**	**n**		**r**	**i**	**n**	**c**	**ó**	**n**		**d**	**e**	
69	110	32	117	110	32	114	105	110	99	243	110	32	100	101	32

l	**a**		**M**	**a**	**n**	**c**	**a**		**d**	**e**		**c**	**u**	**y**	
108	97	32	77	97	110	99	104	97	32	100	101	32	99	117	121

o		**n**	**o**	**m**	**b**	**r**	**e**		**n**	**o**		**q**	**u**	**i**	**e**
111	32	110	111	109	98	114	101	32	110	111	32	113	117	105	101

Podemos utilizar los códigos ASCII de un texto para hacer cualquier cálculo.

E	**n**		**u**	**n**		**r**	**i**	**n**	**c**	**ó**	**n**		**d**	**e**	
69	110	32	117	110	32	114	105	110	99	243	110	32	100	101	
		-1312			224			990			-15840			-6868	-22806

	l	**a**		**M**	**a**	**n**	**c**	**h**	**a**		**d**	**e**		**c**	
32	108	97	32	77	97	110	99	104	97	32	100	101	32	99	
		-7372			-4365			1144			6500			6831	2738

u	y	**o**		**n**	**o**	**m**	**b**	**r**	**e**		**n**	**o**		**q**	
117	121	111	32	110	111	109	98	114	101	32	110	111	32	113	
		-444			-8658			1254			7590			8927	8669

-11399

Aquí, cada tres caracteres, con sus códigos ASCII, se opera **(1º-2º)*3º.**

La suma de los resultados es una función HASH que identifica perfectamente el texto.

CAPITULO III

ANÁLISIS DE LA SITUACIÓN ACTUAL

3.1 SITUACIÓN ACTUAL DE LA COMPAÑÍA

La empresa Promix Ecuador C.A se encuentra ubicada al norte de la ciudad de Quito, cuya dirección es Av. Naciones Unidas E6-99 y Japón, en el edificio del Banco Bolivariano, en donde ocupa el piso 4.

La distribución departamental de la organización es la siguiente:

Tabla 3.1: (Clasificación de los departamentos con sus respectivas funciones)

DEPENDENCIA	FUNCION
Gerencia General	▪ Manejo y Dirección de la compañía. ▪ Toma de Decisiones.
Departamento Financiero / Administrativo	▪ Operaciones Financieras y Administrativas. ▪ Manejo de Procesos Contables y recursos económicos de la compañía. ▪ Manejo de Personal. ▪ Solución de problemas del personal.

DEPENDENCIA	FUNCION
Departamento de Sistemas	▪ Soporte al usuario en lo que respecta a informática. ▪ Administración de la red de información. ▪ Solución de problemas de la red.
Departamento de Ventas	▪ Captación de nuevos clientes. ▪ Capacitación a los vendedores de la compañía. ▪ Control de las ventas diarias.

3.1.1 Recursos Humanos

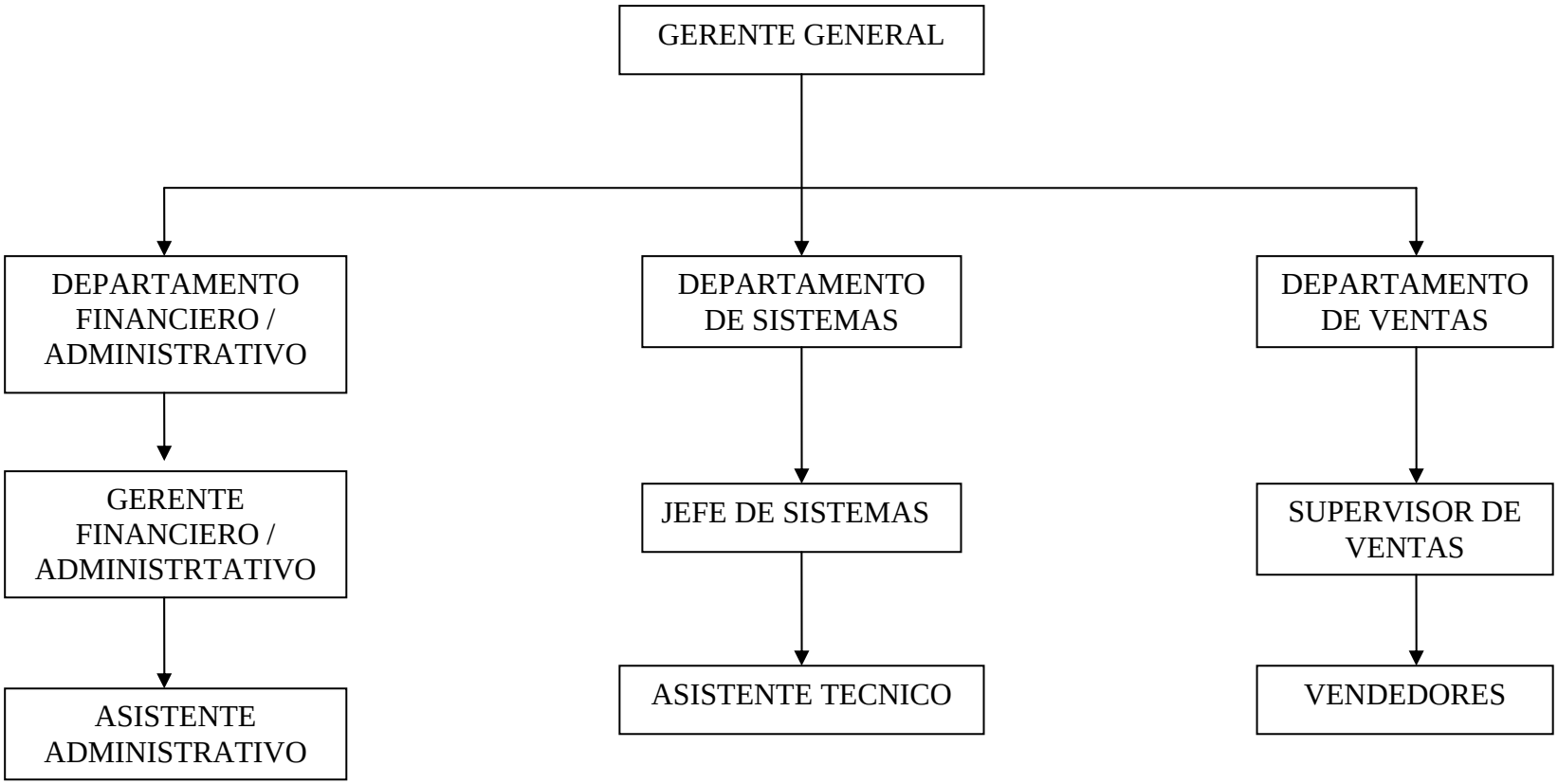


Figura 3.1: (Organigrama Organizacional de Promix Ecuador C.A.)

A continuación se describen los cargos de cada empleado y las funciones que los mismos cumplen dentro la compañía:

- Gerente General

Coordinar el desarrollo de las diferentes operaciones en el país para obtener las metas establecidas por la Compañía.

Dentro de las responsabilidades que debe cumplir están las siguientes:

a) Hacer un seguimiento del desempeño del personal del país.
b) Visitar las diferentes locaciones de clientes para lograr mayor control de las operaciones.
c) Actuar como enlace entre Venezuela y Ecuador (suministrar información)
d) Captar nuevos clientes y negocios.

- Gerente Financiero / Administrativo

Manejo financiero y administrativo de las operaciones de la compañía para cumplir con los requerimientos de la Gerencia General.

Dentro de las responsabilidades que debe cumplir están las siguientes:

a) Reporte de gastos y caja chica.
b) Trámite de Visas, Coordinación de Viajes y demás servicios generales.
c) Preparar la información diaria de la situación bancaria, que incluya saldos, depósitos y egresos.
d) Recepción, almacenamiento, control y facturación de las tarjetas Telpago recibidas para la venta por cuenta de OTECEL, así como de los otros inventarios adquiridos para la comercialización.
e) Situar los gastos en los límites establecidos en el presupuesto de operaciones.

- Asistente Administrativo

Manejo administrativo de las operaciones en el tiempo adecuado y de acuerdo a los requerimientos y prioridades.

Dentro de las responsabilidades que debe cumplir están las siguientes:

a) Reportes de ingresos y facturación.
b) Reportes de clientes nuevos por ruta.
c) Radar semanal de ventas de cada ruta.
d) Actualización de Datos de Clientes.
e) Reportes de Ventas Diarias.
f) Actualización de Datos de Vendedores.

- Asistente Técnico

Lograr que el usuario trabaje con su computadora en forma óptima mediante soporte técnico y asesoramiento sobre funcionamiento de sistema y redes.

Dentro de las responsabilidades que debe cumplir están las siguientes:

a) Instalación de software.
b) Solución de virus, fallas de hardware y software.
c) Configuración de Internet.
d) Solución de problemas de red.
e) Creación y cierre de cuentas de e-mail.
f) Orientación sobre la utilización y funcionamiento de los programas que utiliza la compañía.
g) Soporte a usuario.

- Supervisor de Ventas

Lograr que el trabajo de cada Vendedor sea eficaz y prospero para la compañía.

Dentro de las responsabilidades que debe cumplir están las siguientes:

a) Controlar las ventas diarias de cada Vendedor.

b) Mantener un alto nivel de venta.

c) Visitar a los clientes.

d) Mantener la información de ventas al día.

3.1.2 Hardware

Se detallan los equipos de computación, así como los equipos de impresión existentes en la compañía. (Ver ANEXO A – Inventario de Equipos de Computación). Cabe indicar que la mayoría de los equipos de computación son Clones. Además cuenta con un Servidor de Aplicaciones y Datos y otro Servidor de Correo Electrónico. (Ver ANEXO C – Características de los Servidores).

Tabla 3.2: (Descripción de Equipos de Computación de Promix Ecuador C.A)

EQUIPOS DE COMPUTACIÓN	CANTIDAD
Monitor SAMSUNG SyncMaster 551v	10
CPU Genius Pentium 4 Intel	10
Toshiba Satellite A40 SP151	4

Tabla 3.3: (Descripción de Equipos de Impresión de Promix Ecuador C.A)

EQUIPOS DE IMPRESIÓN	CANTIDAD
Hewlett Packard LaserJet 1200 Series	4
Epson LX-300+	1

3.1.3 Software Base y de Aplicación

Promix Ecuador C.A cuenta con un sistema de licenciamiento a nivel mundial para el software base de cada computador, además dispone de licencias individuales para algunos programas.

A continuación, se detalla el tipo de licenciamiento que dispone la compañía:

Tabla 3.4: (Tipos de Licenciamiento de Software que dispone Promix C.A)

TIPO DE LICENCIAMIENTO	DESCRIPCION
GLOBAL	Licencia mundial adquirida por la compañía a la empresa que desarrolla el software.
INDIVIDUAL	El licenciamiento se lo hace de acuerdo a la requisición del software. La licencia debe ser adquirida previa la instalación.
LIBRE	No se requiere licencia para la instalación del software.

Los sistemas base que dispone la compañía Promix Ecuador C.A son los siguientes:

Tabla 3.5: (Software Base que poseen los computadores de Promix C.A)

SOFTWARE	TIPO DE SOFTWARE	LICENCIAMIENTO
Microsoft Windows 2000	Sistema Operativo en la compañía.	Global
Microsoft Windows XP	Sistema Operativo en la compañía.	Global
Microsoft Windows 2003 Server	Sistema Operativo de Servidores de la Compañía.	Global
Microsoft Office XP Professional	Suite para procesamiento de texto, hoja electrónica y presentaciones.	Global
Adobe Reader 5.0	Sistema de lectura de archivos PDF.	Libre
WinZip 8.0	Herramienta de Compresión y descompresión de información.	Libre
Internet Explorer 6.0	Navegador de Internet propio de Microsoft.	Libre
Norton Antivirus 2003	Sistema de Detección de Virus Informáticos.	Global

Los sistemas de aplicación que dispone la compañía Promix Ecuador C.A son los siguientes:

Tabla 3.6: (Software de Aplicación que posee Promix C.A)

SOFTWARE	TIPO DE SOFTWARE	LICENCIAMIENTO
SAINT	Sistema de Administración de Inventarios.	Individual
TELPAGO	Herramienta Access para el manejo de Información.	Individual
SYS2	Sistema de Contabilidad.	Individual

3.1.4 Infraestructura física

Tabla 3.7: (Infraestructura Física de Promix Ecuador C.A)

COMPONENTE	SITUACION ACTUAL
Infraestructura Arquitectónica de Promix Ecuador C.A.	▪ Promix Ecuador C.A se encuentra ubicada en la Av. Naciones Unidas E6-99 y Japón, en el edificio del Banco Bolivariano. ▪ El piso que ocupa la compañía es arrendado y el edificio es de hormigón con grandes ventanales, además dispone de persianas de plástico en todas las ventanas. ▪ El cuarto de servidores no dispone de ventanales y sus paredes son de madera.

COMPONENTE	SITUACION ACTUAL
Instalaciones Eléctricas	▪ Todas las tomas eléctricas del edificio cumplen con las normas de seguridad. ▪ El edificio dispone de una planta de electricidad suministrada con combustible, la cual está en capacidad de entregar energía a todo el edificio durante un lapso de 4 horas. ▪ Existen UPS's POWERCOM de 500VA individuales por cada equipo de computación, los mismos que funcionan sin problema.
Detectores de Humo y Alarmas	▪ Promix Ecuador C.A cuenta con un completo sistema de detección de humo y alarmas troncalizado vía telefónica en monitoreo, cuya empresa proveedora es PREVISTRONIC. ▪ Promix cuenta con 8 detectores de humo y 6 sensores de alarma.
Extintores de Incendio	▪ El cuarto de servidores dispone de un extintor de incendios. ▪ Además, disponen de 4 extintores de incendios adicionales, localizados en áreas estratégicas.
Cableado Estructurado	▪ La compañía cuenta con una red de cableado estructurado categoría 5 certificado.
Acceso Físico a las instalaciones	▪ El edificio cuenta con guardianía privada, la misma que controla el acceso al edificio las 24 horas por lo que existe un control riguroso de las personas que ingresan al mismo.

COMPONENTE	SITUACION ACTUAL
Acceso Físico al Cuarto de Servidores y Seguridad	▪ El cuarto dispone de una cerradura electrónica con clave, la misma que es conocida solo por el personal de Sistemas. ▪ Posee cajas fuertes donde salvaguardan la información
Salidas de emergencia	▪ El edificio cuenta con escaleras externas de emergencia.
Central Telefónica	▪ La Central Telefónica KX-TA308 de marca PANASONIC se encuentra ubicada en el cuarto de Servidores la misma que se encuentra conectada a un UPS el cual proporciona 30 minutos de energía.

3.1.5 Comunicaciones

Promix Ecuador C.A dispone de comunicaciones LAN (Red de Área Local) con un sistema de cableado estructurado categoría 5 certificado, con dos puntos de red por usuario, con velocidades de transmisión de hasta 100 Megabits por segundo.

La compañía posee un switch D-Link DES-1024R+ de 24 puertos 10/100Mbps y 1 slot para Fibra FX Module, cada toma cumple con las norma de categoría 5 UTP certificado, 1 Router D-Link DI-704P de 4 puertos para brindar Internet a todos los usuarios. (Ver ANEXO B – Características del Switch y Router).

La salida a Internet se lo hace a través de un MODEM ADSL marca HUAWEI SmartAX MT800 Series que se encuentra conectado al Router, además la compañía cuenta con un Central Telefónica Panasonic KX-TA 308 con 3 líneas y 8 extensiones la misma

que actualmente brinda acceso a 30 empleados en Quito, además, la Central Telefónica puede conectar una variedad de equipos de comunicación, teléfonos inalámbricos, contestadoras telefónicas, fax y cualquier otro equipo que trabaje con líneas de teléfonos convencionales.

3.2 DEFINICIÓN DE RECURSOS CRÍTICOS

Tomando en cuenta los ámbitos físicos y lógicos, se determinará la vulnerabilidad de los sistemas que son parte de las funciones de la compañía además de las posibles amenazas tanto presentes como futuras que afecten al recurso humano, hardware, software y comunicaciones que posee actualmente la compañía.

Tabla 3.8: (Recursos Asociados al Nivel de Riesgo)

TIPO DE RECURSO	RIESGO
Indispensable	El funcionamiento no puede estar fuera de servicio por su gran importancia.
Necesario	Su funcionamiento no representa mayor importancia ya que puede ser sustituido por mecanismos.
Opcional	Su funcionamiento puede ser adicional ya que puede o no estar en servicio por lo que cuya labor no es trascendental.

3.2.1 Recursos Humanos

El personal tanto del Departamento Financiero / Administrativo, Departamento de Sistemas y Departamento de Ventas cuentan con un Jefe directo el mismo que esta sobre un cierto número de personas que componen cada departamento; este a su vez reporta al Gerente General la evaluación de las actividades desarrolladas por el personal del departamento.

Cabe mencionar que dentro de cada departamento de la compañía, sí existe la Segregación de Funciones, pues cada persona está encargada de cumplir una función específica, pero no se lo cumple a cabalidad.

3.2.2 Hardware

Se identifican los riesgos correspondientes al equipo de hardware, en este caso se ha tomando en cuenta únicamente los equipos que intervienen en las funciones de mayor importancia para la compañía.

A continuación se especifica el hardware considerado crítico en cada departamento de Promix Ecuador C.A:

Tabla 3.9: (Abreviatura de los equipos de computación)

EQUIPO	ABREVIATURA
Computadores	C
Laptops	L
Servidores	S
Impresoras	I

Tabla 3.10: (Definición del hardware considerados como críticos)

DEPARTAMENTO	TIPO DE RECURSO	C	L	S	I
Gerencial	Indispensable	1	1	0	1
Financiero / Administrativo	Indispensable	3	1	0	2
Sistemas	Indispensable	2	1	2	1
Ventas	Indispensable	4	1	0	1

3.2.3 Software Base y de Aplicación

La compañía tiene un estricto manejo del software puesto que el uso de licencias de cada aplicación está regulado de acuerdo a las necesidades de cada usuario, de ésta regulación se encarga el Departamento de Sistemas:

Dentro del software base que posee licenciamiento global se encuentran los siguientes:

- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows 2003 Server
- Microsoft Office XP Professional
- Norton Antivirus 2003

Además, existe un sistema de licenciamiento individual donde encontramos los siguientes paquetes de software:

- SAINT
- TELPAGO
- SYS2

El departamento de Sistemas es el que tiene el control de instalación de cada uno de los paquetes, y en caso de que el usuario desee instalar algún software por su cuenta, deberá cumplir ciertas normas que se han establecido en la compañía.

A continuación se especifica el software considerado crítico en cada departamento de Promix Ecuador C.A.:

Tabla 3.11: (Abreviatura del Software Instalado)

SOFTWARE	ABREVIATURA
Microsoft Windows 2000	W2000
Microsoft Windows XP	WXP
Microsoft Windows 2003 Server	W2003S
SAINT	SAINT
TELPAGO	TLP
SYS2	SYS2

Tabla 3.12: (Definición del Software Instalado considerado crítico)

DEPARTAMENTO	TIPO DE RECURSO	W2000	WXP	W2003S	SAINT	TLP	SYS2
Gerencial	Indispensable	1	1	0	0	0	0
Financiero / Administrativo	Indispensable	3	1	0	1	1	1
Sistemas	Indispensable	2	1	2	0	0	0
Ventas	Indispensable	4	1	0	1	2	0

3.2.4 Comunicaciones

Los equipos de comunicación considerados críticos en cada departamento de Promix Ecuador C.A. son los siguientes:

Tabla 3.13: (Abreviatura de los Equipos de Comunicación)

EQUIPO DE COMUNICACION	ABREVIATURA
Router D-Link	ROUTER
Switch D-Link	SWITCH
Modem Huawei	MODEM
Central Telefónica	CT

Tabla 3.14: (Definición de los Equipos de Comunicación)

DEPARTAMENTO	TIPO DE RECURSO	ROUTER	SWITCH	MODEM	CT
Gerencial	Opcional	0	0	0	0
Financiero / Administrativo	Opcional	0	0	0	0
Sistemas	Indispensable	1	1	1	1
Ventas	Opcional	0	0	0	0

CAPITULO IV

ANÁLISIS DE RIESGOS E IMPACTOS

4.1 RIESGOS E IMPACTOS

Existen varias definiciones de Riesgo:

- "Es la probabilidad de ocurrencia de un evento no deseado, con un impacto significativo en la planificación." [1]

- "Es la posibilidad de sufrir daño o pérdida, o la exposición a ésta." [1]

Es fundamental realizar el análisis detenido de los recursos críticos de una organización. Dentro de este análisis se enmarca la determinación de los riesgos y el impacto que sobre estos pueden darse de producirse un desastre.

Los principales riesgos que se ha considerado para nuestro estudio dentro de Promix Ecuador C.A. son lo siguientes:

[1] www.ingenieria.cl/escuelas/industrial/archivos/umayor_admproy_Julio2002_capitulo_5.pdf

Desastres Naturales:	▪ Terremotos. ▪ Incendios.
Fallas Eléctricas:	▪ Apagones. ▪ Variaciones de Voltaje.
Acciones Hostiles:	▪ Infiltraciones físicas. ▪ Hackers y Crackers.
Daños a la Información:	▪ Fallas en Equipos Informáticos. ▪ Desconfiguraciones.
Fallas en las Comunicaciones:	▪ Fallas en Equipos de Comunicación.

Tabla 4.1: (Definición de Niveles de Impacto)

NIVEL	IMPACTO	DESCRIPCION
1	Catastrófico	Las pérdidas de la empresa son extremadamente altas, las consecuencias afectan de manera total a la organización.
2	Crítico	Existen pérdidas considerables, las consecuencias afectan parcialmente a la organización de forma grave.
3	Marginal	Existen pérdidas de menos grado, las consecuencias afectan de manera superficial a la organización.
4	Despreciable	No existen pérdidas, las consecuencias no afectan al funcionamiento de la organización.

Tabla 4.2: (Clasificación de los Riesgos según su Nivel de Impacto)

RIESGOS	NIVEL DE IMPACTO			
	1	2	3	4
Desastres Naturales	✓			
Fallas Eléctricas		✓		
Acciones Hostiles		✓		
Daños a la Información		✓		
Fallas en las Comunicaciones		✓		

Según el Nivel de impacto existen 4 homologaciones que se deben tener en cuenta para saber el tiempo de recuperación del hardware, software, infraestructura física, y comunicaciones:

Tabla 4.3: (Tiempo de recuperación según el nivel de impacto)

NIVEL DE IMPACTO	TIEMPO DE RECUPERACION
Catastrófico	No es recuperable
Crítico	24 - 48 horas
Marginal	2 - 4 horas
Despreciable	Ninguno

4.1.1 Hardware

Tabla 4.4: (Definición de riesgos potenciales con respecto al Hardware)

DEPARTAMENTO	EQUIPO	TIPO DE RECURSO	DESCRIPCION DE RIESGO	TIEMPO RECUPERACION	RECURSOS RESPALDO	NIVEL DE IMPACTO
Gerencial	1 Computador	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	24-48 horas	Equipo del Departamento Financiero / Administrativo, Sistemas o Ventas.	Crítico
	1 Laptop	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	24-48 horas	Equipo del Departamento Financiero / Administrativo, Sistemas o Ventas.	Crítico

DEPARTAMENTO	EQUIPO	TIPO DE RECURSO	DESCRIPCION DE RIESGO	TIEMPO RECUPERACION	RECURSOS RESPALDO	NIVEL DE IMPACTO
	1 Impresora	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	2-4 horas	No requerido.	Marginal
Financiero / Administrativo	3 Computadores	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	24-48 horas	Equipo del mismo departamento Financiero.	Crítico
	1 Laptop	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	24-48 horas	Equipo del mismo departamento Financiero.	Crítico
	2 Impresoras	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	2-4 horas	No requerido	Marginal

DEPARTAMENTO	EQUIPO	TIPO DE RECURSO	DESCRIPCION DE RIESGO	TIEMPO RECUPERACION	RECURSOS RESPALDO	NIVEL DE IMPACTO
Sistemas	2 Computadores	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	24-48 horas	Equipo del mismo departamento de sistemas.	Crítico
	1 Laptop	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	24-48 horas	Equipo del mismo departamento de sistemas.	Crítico
	2 Servidores	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	24-48 horas No es recuperable	Un servidor es backup del otro y viceversa.	Crítico Catastrófico

DEPARTAMENTO	EQUIPO	TIPO DE RECURSO	DESCRIPCION DE RIESGO	TIEMPO RECUPERACION	RECURSOS RESPALDO	NIVEL DE IMPACTO
	1 Impresora	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	2-4 horas	No requerido.	Marginal
Ventas	4 Computadores	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	24-48 horas	Equipo del departamento Gerencial, Financiero, Sistemas.	Crítico
	1 Laptop	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	24-48 horas	Equipo del departamento Gerencial, Financiero, Sistemas.	Crítico

DEPARTAMENTO	EQUIPO	TIPO DE RECURSO	DESCRIPCION DE RIESGO	TIEMPO RECUPERACION	RECURSOS RESPALDO	NIVEL DE IMPACTO
	1 Impresora	Indispensable	• Fallas Eléctricas. • Fallas en el equipo. • Robo.	2-4 horas	No requerido	Marginal

4.1.2 Software Base y de Aplicación

Tabla 4.5: (Definición de riesgos potenciales con respecto al Software)

DEPARTAMENTO	SOFTWARE	TIPO DE RECURSO	DESCRIPCIÓN DEL RIESGO	TIEMPO DE RECUPERACIÓN	NIVEL DE IMPACTO
Gerencial	Microsoft Windows 2000 Microsoft Windows XP	Indispensable Indispensable	• Errores de Ejecución y/o Sistema. • Insuficiencia de Memoria. • Error de conectividad con la red.	24-48 horas 24-48 horas	Crítico Crítico
Financiero / Administrativo	Microsoft Windows 2000 Microsoft Windows XP SAINT TELPAGO SYS2	Indispensable Indispensable Indispensable Indispensable Indispensable	• Errores de Ejecución y/o Sistema. • Insuficiencia de Memoria. • Error de conexión con la Base de Datos de SYS2. • Error de conexión con la Base de Datos de SAINT.	24-48 horas 24-48 horas 24-48 horas 24-48 horas 24-48 horas	Crítico Crítico Crítico Crítico Crítico

DEPARTAMENTO	SOFTWARE	TIPO DE RECURSO	DESCRIPCIÓN DEL RIESGO	TIEMPO DE RECUPERACIÓN	NIVEL DE IMPACTO
			• Error de conexión con la Base de Datos de TELPAGO. • Error de conectividad con la red.		
Sistemas	Microsoft Windows 2000 Microsoft Windows XP Microsoft Windows 2003 Server	Indispensable Indispensable Indispensable	• Errores de Ejecución y/o Sistema. • Insuficiencia de Memoria. • Error de conectividad con la red.	24-48 horas 24-48 horas 24-48 horas	Crítico Crítico Crítico
Ventas	Microsoft Windows 2000 Microsoft Windows XP TELPAGO	Indispensable Indispensable Indispensable	• Errores de Ejecución y/o Sistema. • Insuficiencia de Memoria. • Error de conexión con la Base de Datos de TELPAGO. • Error de conectividad con la red.	24-48 horas 24-48 horas 24-48 horas	Crítico Crítico Crítico

4.1.3 Infraestructura Física

Tabla 4.6: (Definición de riesgos potenciales con respecto a la Infraestructura Física)

COMPONENTE	DESCRIPCION DE RIESGO	TIEMPO DE RECUPERACION	NIVEL DE IMPACTO
Infraestructura Arquitectónica de Promix Ecuador C.A.	▪ El cuarto de servidores se encuentra cerrado por paredes de madera.	No es recuperable	Catastrófico
Instalaciones Eléctricas	▪ No se cuenta con una red centralizada de UPS. ▪ No se cuenta con un plan emergente de seguridad en caso de fallas eléctricas. ▪ Muy pocos equipos cuentan con protección contra variaciones de voltaje. ▪ Los servidores cuentan con UPS's que abastecen tan solo con 20 minutos de energía	24-48 horas 24-48 horas 24-48 horas 24-48 horas	Crítico Crítico Crítico Crítico

COMPONENTE	DESCRIPCION DE RIESGO	TIEMPO DE RECUPERACION	NIVEL DE IMPACTO
Detectores de Humo y Alarmas	▪ Pese a que existe un moderno sistema de detección de humo y sistema de alarmas, en algunas ocasiones el sistema ha fallado producto de quema en fusibles producidos por apagones.	24-48 horas	Crítico
Extintores de Incendio	▪ No todo el personal se encuentra capacitado para el uso de los extintores. ▪ Algunos de los extintores se encuentran con su fecha de expiración cumplida.	2-4 horas 24-48 horas	Marginal Crítico
Cableado Estructurado	▪ No existe documentación donde se detalle la ubicación de los puntos de red y el cableado.	24-48 horas	Crítico

COMPONENTE	DESCRIPCION DE RIESGO	TIEMPO DE RECUPERACION	NIVEL DE IMPACTO
Acceso Físico a las Instalaciones	▪ Pese a que existe guardianía las 24 horas del día, en la mayoría de los casos no se exige la identificación de las personas que ingresan al edificio.	24-48 horas	Crítico
Acceso Físico al Cuarto de Servidores y Seguridad	▪ El cuarto dispone de una cerradura electrónica con clave, la misma que conoce gente que no debería. ▪ El cuarto de servidores no posee un sistema de enfriamiento. ▪ El cuarto de servidores se encuentra separado de las demás oficinas únicamente por una pared de madera.	24-48 horas 24-48 horas 24-48 horas	Crítico Crítico Crítico
Central Telefónica	▪ No se dispone de un manual actualizado del manejo de la Central Telefónica.	2-4 horas	Marginal

4.1.4 Comunicaciones

Tabla 4.7: (Definición de riesgos potenciales con respecto a la Comunicación)

EQUIPO	TIPO DE RECURSO	DESCRIPCION DE RIESGO	TIEMPO DE RECUPERACION	NIVEL DE IMPACTO
1 SWITCH D-LINK	Indispensable	• Fallas Eléctricas. • Daños de Hardware. • Desconfiguración del equipo.	24-48 horas	Crítico
1 ROUTER D-LINK	Indispensable	• Fallas Eléctricas. • Daños de Hardware. • Desconfiguración del equipo.	24-48 horas	Crítico
1 MODEM HUAWEI	Indispensable	• Fallas Eléctricas. • Daños de Hardware.	24-48 horas	Crítico

EQUIPO	TIPO DE RECURSO	DESCRIPCION DE RIESGO	TIEMPO DE RECUPERACION	NIVEL DE IMPACTO
1 CENTRAL TELEFONICA PANASONIC	Indispensable	• Fallas Eléctricas. • Daños en los fusibles. • Desprogramación interna de la central. • Desconfiguración del Hardware de la central. • Desconfiguración del software de la central.	24-48 horas	Crítico

CAPITULO V

PLAN DE SEGURIDAD

5.1 HARDWARE

Luego de haber realizado la investigación correspondiente acerca del recurso informático que posee la empresa Promix Ecuador C.A, en lo que se refiere a los equipos que la empresa posee, se ha llegado a determinar lo siguiente:

- 1 Servidor de Correo Electrónico.
- 1 Servidor de Aplicaciones y de Datos.
- 14 Estaciones de Trabajo:
  - ✓ 10 Desktops
  - ✓ 4 Portátiles
- 5 Impresoras:
  - ✓ 4 Láser
  - ✓ 1 Matricial
- 1 Escáner formato A4
- 13 UPS

Existe un inventario detallado y actualizado sobre dichos equipos, sus características, capacidades, y distribución. (Ver ANEXO A – Inventario de Equipos de Computación).

5.1.1 Seguridad Física

5.1.1.1 Controles Preventivos

- Contratar el mantenimiento preventivo y correctivo para todos los equipos.
- Aplicar cuando sea necesario, el contrato de garantía respectivo a todos y cada uno de los equipos.
- Todos los equipos de hardware contarán con un seguro, el cual será proporcionado por la misma empresa aseguradora de los bienes materiales y vehículos con quien Promix Ecuador C.A tiene el contrato.
- Todos los equipos contarán con etiquetas con vallas de seguridad. Estas serán colocadas en un lugar discreto de los mismos para evitar su visualización a simple vista.
- El equipo detector de estas etiquetas será colocado en la salida, junto a la recepción. De esta forma la guardianía del edificio estará en capacidad de bloquear inmediatamente el posible robo una vez que suene la alarma.

5.1.1.2 Controles Detectivos

- Problemas con los Servidores: Cuando el servidor deja de funcionar correctamente por problemas en los dispositivos o por falla de la fuente de alimentación.

  Solución:

  - ✓ Notificar al Jefe de Sistemas del problema ocurrido.
  - ✓ Determinar si el daño es en algún dispositivo del Servidor o en la fuente de alimentación.

- ✓ Realizar el seguimiento de la resolución del problema a la empresa contratada para mantenimiento.

- Daño en los discos duros de las estaciones: Cuando no reconoce el disco duro, o no se puede acceder al mismo.

  Solución:

  - ✓ Notificar al Departamento de Sistemas lo ocurrido y cual es la estación que tiene el problema.
  - ✓ Revisar el equipo y comprobar si el daño del disco duro es lógico o físico.
  - ✓ Si el daño es físico y requiere el cambio del disco, se debe llamar a la empresa proveedora.
  - ✓ Realizar el seguimiento del cambio de disco duro.
  - ✓ Utilizar un equipo de respaldo para la información.

- Error en la memoria RAM de las estaciones: Cuando se cuelga el computador desplegando una pantalla azul con error de memoria al ejecutar alguna aplicación o al iniciar Windows.

  Solución:

  - ✓ Notificar al Departamento de Sistemas lo ocurrido y cual es la estación que tiene el problema.
  - ✓ Llamar a la empresa proveedora para que den solución al problema.
  - ✓ Realizar el seguimiento del cambio de memoria a la empresa proveedora.
  - ✓ Utilizar un equipo de respaldo para la información.

- Daño en las tarjetas controladoras de las Estaciones: Cuando los mensajes de error no indican problemas en los archivos de sistema o en los controladores de las tarjetas.

  Solución:

  - ✓ Notificar al Departamento de Sistemas lo ocurrido y cual es la estación que tiene el problema.
  - ✓ Llamar a la empresa proveedora para que den solución al problema.
  - ✓ Realizar el seguimiento del cambio de la tarjeta controladora a la empresa proveedora.
  - ✓ Utilizar un equipo de respaldo para la información.

- Pérdida o daños graves de las laptops: Cuando el cambio de la laptop es irremediable.

  Solución:

  - ✓ Notificar al Departamento de Sistemas lo ocurrido.
  - ✓ Comprobar la pérdida o daño de la laptop.
  - ✓ Justificar el cambio de la laptop.
  - ✓ Llamar a la empresa proveedora para que den solución al problema.
  - ✓ Realizar el seguimiento del cambio de la tarjeta controladora a la empresa proveedora.

5.1.1.3 Controles Correctivos

- Problemas con los Servidores: Cuando el servidor deja de funcionar correctamente por problemas en los dispositivos o por falla de la fuente de alimentación.

  Solución:

- ✓ En caso de que el daño sea en algún dispositivo del Servidor o en la fuente de alimentación., referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a al empresa contratada para el mantenimiento preventivo correctivo para que repare la falla del Servidor.
- ✓ Verificar el correcto funcionamiento de los dispositivos del Servidor.
- ✓ Activar el equipo nuevamente para que trabaje.

- Daño en los discos duros de las estaciones: Cuando no reconoce el disco duro, o no se puede acceder al mismo.

  Solución:

  - ✓ Ubicar el disco que presenta los problemas.
  - ✓ Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a al empresa proveedora para reemplazar el disco duro de la estación.
  - ✓ Restaurar la imagen estándar correspondiente al modelo del computador.
  - ✓ Instalar el software de aplicación específico del usuario que no conste en la imagen.
  - ✓ Verificar el correcto funcionamiento del disco duro.

- Error en la memoria RAM de las estaciones: Cuando se cuelga el computador desplegando una pantalla azul con error de memoria al ejecutar alguna aplicación o al iniciar Windows.

  Solución:

  - ✓ Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a al empresa proveedora para reemplazar las memorias por otras con características iguales o similares.

- ✓ Verificar el correcto funcionamiento de la memoria de la estación.

- Pérdida o daños graves de las laptops: Cuando el cambio de la laptop es irremediable.

  Solución:

  - ✓ Certificar la aprobación para el cambio de la laptop.
  - ✓ Referirse a la garantía si se encuentra dentro del periodo del mismo, caso contrario, contactar a al empresa proveedora para reemplazar la laptop por una de similares características.
  - ✓ Restaurar la imagen estándar correspondiente al modelo de la laptop.
  - ✓ Instalar el software de aplicación específico del usuario.
  - ✓ Verificar el correcto funcionamiento de la máquina.

5.1.2 Seguridad Lógica

- Todos los equipos de la empresa, tanto estaciones de trabajo así como los servidores tienen una clave de acceso para que el usuario ingrese.
- Existen definidos dos niveles de usuario dentro de la red:
  - ✓ Nivel Administrativo: Es restringido únicamente para el personal de Sistemas a cargo.
  - ✓ Nivel de Usuarios: Pertenecen todos los demás usuarios de la red.
- El acceso a los recursos compartidos existentes como son impresoras y archivos, se encuentran controlados mediante definición y asignación de usuarios mediante claves de acceso.

5.1.2.1 Controles Preventivos

- Establecer un cronograma de validez de los diferentes tipos de claves de acceso, permitiendo de esta manera la planificación y el control de los cambios y de sus respectivas actualizaciones.

5.1.2.2 Controles Detectivos

- Verificar de forma manual o automatizada, el cumplimiento de los cambios y de las actualizaciones de las claves de acceso a los diferentes recursos informáticos de la empresa.

5.1.2.3 Controles Correctivos

- Realizar un procedimiento que permita cambiar y actualizar todas las claves de acceso que no han sido actualizadas ya sea por el usuario, por el personal de Sistemas o por alguna herramienta administrativa automatizada.

5.2 SOFTWARE

5.2.1 Descripción de los Sistemas de Aplicación

SAINT

Este sistema fue desarrollado en PASCAL y fue adquirido a la empresa TELCEL en la ciudad de Caracas-Venezuela, con la cual se mantiene un contrato de renovación anual y capacitación y asesoría mensual.

Además existe documentación de guía para el usuario, la misma que se encuentra debidamente actualizada. Existe un Manual para el Administrador del SAINT, en el cual se brinda la información necesaria para configurar, instalar, actualizar el aplicativo, así como información sobre la estructura de archivos que maneja, recuperación de información y obtención de respaldos de archivos importantes.

Existe una Guía de Instalación en el cual se especifican los requerimientos del sistema tanto en Hardware como en Software.

En este sistema se lleva el control de entrada y salida de la mercadería además, cumple con las necesidades de PROMIX sobre lo que es Administración el cual se lo utiliza para control de inventarios dando los siguientes reportes:

- Facturación
- Control de Inventarios (por seriales)
- Traslados de Bodegas
- Traslados de Mercaderías
- Ingresos Bodega
- Egresos Bodega

El sistema SAINT tiene Claves de Acceso Usuario para digitación de información y además Claves Administrativas para configuración del sistema y perfiles de acceso, pero no existen políticas claramente definidas para el cambio periódico de clave de acceso ni para la actualización o redefinición de perfil de usuario. Este sistema maneja de forma centralizada el almacenamiento de los datos del sistema.

Se plantean políticas de respaldos para la información del sistema, las cuales son puestas en práctica directamente por el Departamento Financiero. Los respaldos se realizan quincenalmente. A pesar de que el proceso de respaldos de la información se lo lleva a cabo caca quince días, no se ha planteado de manera formal procedimientos debidamente documentados que soporten su obtención, almacenamiento o actualización, así como la designación de responsables de dicho proceso por lo que es necesario establecer dichos procedimientos además el de establecer políticas para llevar a cabo la actualización del perfil y clave de acceso.

TELPAGO

Este sistema fue desarrollado en ACCESS y fue implementado por la empresa TELCEL en la ciudad de Caracas-Venezuela, con la cual se mantiene un contrato para capacitación y asesoría mensualmente. La renovación del contrato se lo realiza anualmente.

El sistema TELPAGO es un sistema de Administración el cual en PROMIX lo utilizan para el control de clientes y ventas, el mismo que da los siguientes reportes:

- Visitas Efectivas a clientes
- Visitas no efectivas a clientes
- Reporte de visitas a rutas
- Ventas por ruta
- Ventas por vendedor
- Ventas por Cliente
- Ventas por Factura
- Ventas por Producto
- Ventas por Mercado
- Ventas Generales

Existe un Manual de usuario de este sistema, el cual cuenta con la información necesaria para la configuración y manejo de cada una de sus funciones, este manual posee una descripción bastante explicativa, apoyada gráficamente, sobre todas las opciones disponibles.

Este sistema posee una Base de Datos única (ACCESS) en la cual se almacena toda la información.

Este sistema no maneja claves de acceso, lo que hace extremadamente riesgoso que cualquier persona ingrese al sistema y modifique o dañe los datos que se procesan en él, por lo que es conveniente establecer políticas mediante las cuales se pueda mantener un control de los usuarios que ingresan al mismo.

Para los respaldos se debe desarrollar procedimientos debidamente documentados, para la obtención y actualización de la información.

SYS2

Este sistema fue desarrollado en DATAFLEX y fue adquirido a la Corporación de Servicios Integrados con la cual se mantiene un contrato anual para capacitación y asesoría. Este es un sistema Contable el mismo que permite realizar las siguientes actividades:

- Plan de Cuentas
- Libros Diarios
- Libros Mayores
- Auxiliares
- Consulta de Cuentas Contables
- Reporte de Clientes
- Balance de Comprobación
- Estado Financieros
- Facturación
- Roles de Pago
- Hojas de Costos
- Clientes
- Proveedores
- Retenciones en la Fuente
- Planilla de IESS

Existe un Manual de usuario en el cual se brinda toda la información que se necesita para instalar, configurar y actualizar dicho sistema. Este sistema tiene un único perfil y clave de acceso el mismo que es conocido por el Jefe Financiero de PROMIX y por la persona encargada de realizar las actualizaciones y configuraciones del mismo.

Los respaldos de la información se realizan diariamente, pero al igual que los otros dos sistemas, no existe formalmente procedimientos debidamente documentados que soporten

su obtención, almacenamiento o actualización, así como la designación de responsables de dicho proceso.

5.2.2 Seguridad Física

5.2.2.1 Controles Preventivos

- Establecer una normativa administrativa para la obtención de respaldos de cada usuario. Para esto se definirán sentencias de tal manera que cada usuario, cumpla y controle la obtención de sus respaldos desde su computador hacia el servidor de Datos.
- El respaldo de la información de los servidores de correo y de datos, deberá ser obtenido cada 2 días en horario de 12 de la noche a 7 de la mañana, el cual será configurado automáticamente por el Administrador de la Red.
- Los respaldos deberán ser ubicados en un casillero de seguridad en una institución bancaria, siguiendo el procedimiento que a continuación se detalla:
  - ✓ Obtener los respaldos a las cintas respectivas.
  - ✓ Una vez terminado el proceso de respaldo, guardar las cintas en una caja de seguridad con clave.
  - ✓ Entregar la caja al mensajero de la compañía para que este lleve la misma a la institución bancaria contratada.
  - ✓ Entregar dicha caja a la institución bancaria y recibir el certificado de recepción de la misma.
  - ✓ Cumplir con este procedimiento cada 2 días, excepto Sábados y Domingos.
  - ✓ El Departamento de Sistemas debe disponer de autoridad técnica para exigir el cumplimiento de estas normas.

- ✓ Una normativa administrativa dispondrá que ningún empleado deberá hacer uso de sus espacios de disco en el servidor de respaldos para grabar información que no sea de uso exclusivo para el trabajo, tales como archivos de música, juegos, videos y gráficos.

- Se dispondrá de un disco duro externo adicional con capacidad de 160 Gigabytes, almacenado en el armario del Cuarto de Servidores, el mismo que será usado como backup en caso de daño en el Servidor de Datos.
- Se debe implementar una plataforma más robusta de protección de red y de costo razonable, que no solo sea antivirus sino también una solución que incluya detección y bloqueo de SPYWARE, ADWARE, MALWARE, TROYANOS y otro tipo de información indeseable en la red, bloqueo de puertos por infecciones conocidas y desconocidas, que brinde una consola de administración centralizada desde donde se pueda desplegar actualizaciones a todos los clientes de la red, hacer análisis de parches de seguridad mínimos requeridos y que permita también implementar políticas rigurosas para el control y operación del antivirus en los hosts.
- Para mantener la autenticidad y privacía en los datos e información que se encuentran almacenados en los sistemas basados en computador o que son enviados a través de redes de computadores, se debe utilizar Sistemas Criptográficos como por ejemplo el Sistema DES que se encuentra descrito en el literal 2.6.3.1 del Capitulo II del presente trabajo. Para más información: http://www.htmlweb.net/seguridad/cripto/cripto_7.html

5.2.2.2 Controles Detectivos

- Falta de Espacio en el Servidor de Datos
  - ✓ Notificar el problema ocurrido al Jefe de Sistemas.

- ✓ Preparar el disco duro de backup.
- ✓ Insertar el disco duro en uno de los slots que se encuentren disponibles del servidor de Datos, sin necesidad de apagar el Servidor; el servidor lo detectará automáticamente.
- ✓ Verificar el aumento de espacio en el Servidor de Datos.

- Incumplimiento de la obtención de los respaldos.
  - ✓ Notificar el incumplimiento al Jefe de Sistemas.
  - ✓ Establecer la sanción pertinente.
  - ✓ Realizar inmediatamente la obtención de los respaldos.

5.2.2.3 Controles Correctivos

- La información almacenada en las cintas deberá extraerse hacia el servidor de donde provenga la misma. Las cintas deberán de ser extraídas de la bóveda del Banco previa disposición administrativa por parte del Departamento de Sistemas.
- En caso de pérdida total de la información en los servidores, los respaldos más actualizados serán copiados inmediatamente en los discos duros de los servidores.
- En caso de que la pérdida de la información sea parcial, se reemplazará los archivos dañados o perdidos en forma manual, es decir, se buscarán los mismos en las cintas de acuerdo a un previo a un análisis sobre los daños, el mismo que lo realizará el Departamento de Sistemas.

5.2.3 Seguridad Lógica

5.2.3.1 Controles Preventivos

- Especificar en todo contrato de desarrollo, implementación o adquisición de software, cláusulas pertinentes a la documentación del sistema, especificando cual será la documentación a entregar y el contenido exacto de la misma.
- Designar personal de la empresa responsable de recibir, revisar, evaluar, archivar y actualizar toda la documentación recibida de los sistemas.
- Llevar un registro de todos los usuarios de cada uno de los sistemas o recursos informáticos de la empresa y generar un calendario de actualización de claves de acceso basados en las políticas planteadas por la empresa.
- Definir procedimientos con sus respectivos procesos y actividades para el cumplimiento de funciones.
- Desarrollar un cronograma de obtención, actualización, reemplazo y almacenamiento de respaldos, especificando fechas, contenido, lugar de almacenamiento y persona responsable de su obtención.

5.2.3.2 Controles Detectivos

- Dar seguimiento a la elaboración de la documentación sobre procedimientos mediante la elaboración de informes sobre procesos y actividades que no se encuentran dentro del manual de procedimientos.

- Elaborar un informe en el que se detalle los cambios y actualizaciones de claves de acceso de los diferentes recursos / sistemas de la empresa en cada una de las fechas del cronograma establecido.
- Llevar a cabo verificaciones periódicas sobre el cumplimiento del cronograma de respaldos establecido, con el fin de detectar anomalías o incumplimientos.

5.2.3.3 Controles Correctivos

- Establecer mecanismos mediante los cuales se pueda adjuntar cláusulas a los contratos vigentes en los que no se especifique claramente la elaboración y entrega de documentación de los sistemas.
- Crear manuales de procedimientos de cambio emergente de claves de acceso por parte del personal a cargo de administrar los recursos / sistemas de la empresa.
- Llevar a cabo un cambio emergente de claves de acceso por parte del personal a cargo de administrar los sistemas de la empresa.
- Mantener un histórico de respaldos de tal forma que se pueda recurrir a respaldos anteriores de hasta un mes atrás a la fecha requerida.

5.3 INFRAESTRUCTURA FÍSICA

- Todos los equipos se encuentran conectados en red al servidor principal mediante el dominio PROMIX. Existe definido un solo grupo de trabajo llamado Promix.
- Físicamente la red se encuentra distribuida por toda el área de trabajo de la empresa.

- El cableado de la red ha sido tendido usando cable UTP Categoría 5 y conectores RJ45 la misma que ha sido implementada de acuerdo a las normativas que el cableado estructurado exige.
- Las tomas eléctricas del edificio cumplen con las normas de seguridad y se encuentran debidamente instaladas con conexión a tierra, identificadas y conectadas, tanto a una fuente principal como a una fuente alterna de energía (planta eléctrica).
- El edificio dispone de una planta de electricidad suministrada con combustible, la cual está en capacidad de entregar energía a todo el edificio durante un lapso de 4 horas.
- Existen UPS's de marca POWERCOM de 500VA individuales por cada equipo de computación, los mismos que funcionan sin problema y funcionan como fuente de energía de reserva.

5.3.1 Seguridad Física

5.3.1.1 Controles Preventivos

- Llevar un Libro de Registro de Ingreso en el cual se tenga constancia de todas las personas que ingresan a la empresa.
- Implementar un mecanismo de control de acceso adicional para las áreas restringidas de la empresa como por ejemplo la utilización de tarjetas de acceso.
- Establecer planes de acción para enfrentar cualquier desastre que pueda afectar las instalaciones de la empresa.

- Promix Ecuador C.A cuenta con un completo sistema de detección de humo y alarmas troncalizado vía telefónica en monitoreo, cuya empresa proveedora es PREVISTRONIC. Promix cuenta con 8 detectores de humo y 6 sensores de alarma.
- Se debe cambiar las paredes de madera que actualmente tiene el cuarto de servidores por paredes de cemento para evitar el fácil ingreso de personas mal intencionadas.
- La compañía dispone de 4 extintores de incendios adicionales, localizados en áreas estratégicas y de fácil acceso.
- El edificio cuenta con guardianía privada, la misma que controla el acceso al edificio las 24 horas por lo que existe un control riguroso de las personas que ingresan al mismo.
- El cuarto de servidores dispone de una cerradura electrónica con clave, la misma que es conocida solo por el personal de Sistemas. Además, posee cajas fuertes donde salvaguardan la información.
- El edificio cuenta con escaleras externas de emergencia.

5.3.1.2 Controles Detectivos

- Realizar una auditoría periódica del Registro de Ingresos de las personas a las instalaciones de la empresa.
- Verificar que los mecanismos de control de acceso se cumplan correctamente, según las reglas establecidas por la empresa.
- Verificar con la empresa PREVISTRONIC, que los detectores de humo y los sensores de alarma funcionen correctamente.
- Comprobar que los extintores de incendios no estén con su fecha de expiración caducada.

5.3.1.3 Controles Correctivos

- Sancionar a la persona encargada de llevar el Libro de Registro de Ingreso en caso de que no este cumpliendo con lo dispuesto por la empresa para lograr tener un control de las personas que ingresan a las instalaciones.
- Cambiar los detectores de humo y los sensores de alarma no estén funcionando adecuadamente.
- Cambiar los extintores de incendios que estén con su fecha de expiración caducada.

5.4 COMUNICACIONES

Los equipos de comunicación con que cuenta actualmente la empresa son:

- ✓ 1 Switch
- ✓ 1 Router
- ✓ 1 Modem ADSL
- ✓ 1 Central Telefónica

- La compañía posee un switch D-Link DES-1024R+ de 24 puertos 10/100Mbps y 1 slot para Fibra FX Module, cada toma cumple con las norma de categoría 5 UTP certificado,
- Además posee un Router D-Link DI-704P de 4 puertos para brindar Internet a todos los usuarios.
- El acceso a Internet se lo hace mediante un MODEM ADSL conectado a un Router, el proveedor de Internet es Andinanet.

- Existe una Central Telefónica la misma que cuenta con 3 líneas y 8 extensiones para mantener un contacto continuo con los clientes y proveedores**.**

5.4.1 Seguridad Física

5.4.1.1 Controles Preventivos

- Todos los equipos de comunicación deberán estar conectados a un UPS.
- La protección adecuada del cuarto de servidores incidirá principalmente a la Central Telefónica, al Switch, al Router y demás equipos de comunicación con que cuenta Promix C.A.
- Establecer un Mantenimiento Preventivo-Correctivo con los proveedores de los equipos de comunicación.
- Se debe implementar un ***Firewall*** para:
  - ✓ Protección entre el computador del usuario y el Internet.
  - ✓ Bloquear aquellas entradas que no se encuentran autorizadas a su computadora además de restringir el tráfico externo.
  - ✓ Evitar que intrusos puedan acceder a información confidencial.
  - ✓ Configurar los accesos que se hagan desde Internet hacia la red local.
- Para tener un control total de Administración de redes, se debe adquirir un sistema que permita:
  - ✓ Administración de puntos de red.
  - ✓ Personalización de niveles de usuarios.
  - ✓ Asignación de servicios por redes.
  - ✓ Control total del ancho de banda.

- ✓ Filtrado de contenidos por categorías.
- ✓ Monitorización e informes de acceso a servicios.
- ✓ Estadísticas y reportes del uso de la red.

5.4.1.2 Controles Detectivos

- En caso de que se detecte fallas en los equipos de comunicaciones, se deberá revisar el daño y determinar si se necesita la presencia de la empresa proveedora.
- Cuando se encuentre una desactivación en la comunicación a Internet, se deberá revisar y determinar si el problema es en el Router, en el MODEM o el problema se encuentra en Adinanet.

5.4.1.3 Controles Correctivos

- Referirse a la garantía de los equipos de comunicación si se encuentra dentro del periodo del mismo.
- Verificar el correcto funcionamiento de los equipos de comunicación.
- Si se encuentra problemas en el Router o en el Modem y por este motivo la empresa no puede tener acceso al Internet, se lo deberá resolver lo más pronto posible junto con los proveedores de los mismos.
- Si la falla de conexión a Internet no es por mal funcionamiento ni del Router ni del Modem, se deberá contactar a la empresa proveedora de Internet (Andinanet) para que resuelva el problema.
- Verificar que posteriormente exista conexión a Internet.

5.4.2 Seguridad Lógica

5.4.2.1 Controles Preventivos

- Se deberá disponer de todos los Manuales de Configuración de los equipos de comunicación, dichos Manuales deberán ser facilitados por los proveedores de los mismos.
- Establecer un Mantenimiento Preventivo-Correctivo con los proveedores de los equipos de comunicación.

5.4.2.2 Controles Detectivos

- En caso de que exista un problema de configuración de los equipos de comunicación, se deberá notificar al Departamento de Sistemas y determinar si es necesaria la presencia de las empresas proveedora de los mismos.

5.4.2.3 Controles Correctivos

- En caso de que el Departamento de Sistemas determine que el problema de configuración de los equipos de comunicación es serio, se deberá notificar de inmediato a las empresas proveedoras de los mismos.
- Verificar el correcto funcionamiento de los equipos de comunicación.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Dentro de la situación actual de la empresa se detecta un gran número de medidas de seguridad que necesitan ser implementadas de inmediato, para evitar pérdidas de la información que maneja Promix, por lo cual es importante que la empresa cuente con un Plan de Seguridad.
- El hardware con que cuenta la empresa actualmente se encuentra en óptimas condiciones puesto que Promix es una empresa nueva en el Ecuador. Adicionalmente la empresa cuenta con licenciamiento de todo el software que utiliza.
- Los empleados no cumplen con las políticas de respaldo de la información lo que hace muy riesgoso que dicha información se pierda y no puedan recuperarla.
- La empresa no cuenta con sistemas de seguridad que protejan la información como por ejemplo las denominadas pistas de auditoria, que permiten seguir y conocer la actividad de aquellos que por ejemplo desean acceder a la red de la empresa sin ser una persona autorizada; cualquier intento de hacerlo queda registrado en dichas pistas. Estas pistas sirven también para presentar reportes históricos sobre las actividades que los usuarios realizan dentro de los sistemas en operación, siendo de mucha utilidad al momento de responder una consulta o queja.
- Un punto crítico dentro de los sistemas en operación es que, el sistema TELPAGO no cuenta con claves de acceso, por lo que cualquier usuario puede manipular la información que contiene dicho sistema. Además, cabe mencionar que los empleados

dejan sus contraseñas escritas en cualquier lugar, lo que permite que cualquier persona la obtenga e ingrese a los sistemas y dañe información valiosa para la compañía.

6.2 RECOMENDACIONES

- Para que el presente Plan de Seguridad que se ha propuesto sea efectivo, se deberán cumplir todos y cada unos de los puntos que se han planteado en los controles Preventivos tanto para hardware, software, infraestructura física y comunicaciones, para esto debe existir apoyo de las autoridades para la implementación de dicho Plan.
- Ya que el Departamento de Sistemas es un departamento nuevo dentro de la empresa, se debe especificar claramente los roles y funciones que deben tener, tanto el Jefe de Sistemas como su Asistente, como por ejemplo el de realizar un cronograma para el respaldo de la información, realizar la instalación y configuración del software, dar soporte al usuario, entre otros; para evitar que los mismos usuarios arreglen cualquier problema que tengan con respecto al hardware y al software que manejan.
- El cambio de claves de accesos a los sistemas se deberá realizar periódicamente para evitar que cualquier usuario mal intencionado ingrese y dañe la información.
- Las personas que ingresan al cuarto de servidores deberán ser únicamente aquellas que pertenecen al Departamento de Sistemas (Jefe de Sistemas y Asistente).
- La implementación de un firewall sería el modo más conveniente para que exista protección entre el computador de cada usuario y el Internet, y así evitar el acceso de intrusos externos a la red y a la información.

BIBLIOGRAFIA

- De La Fuente, Reynaldo, Aportes a la Seguridad y Privacidad en Informática y Comunicación de Datos, Segunda Edición Actualizada.

- Seguridad Informática
  http://www.upiicsa.ipn.mx/maestrias/Seguridad%20Informatica/CAPITULO1/cap1.html : Seguridad Informática

- Seguridad Informática
  http://www.monografias.com/trabajos16/seguridad-informatica/seguridad-informatica.shtml : Seguridad Informática

- Auditoría de Sistema y políticas de Seguridad Informática
  http://www.monografias.com/trabajos12/fichagr/fichagr.shtml

- Firewalls y Seguridad en Internet
  http://www.monografias.com/trabajos3/firewalls/firewalls.shtml

- Escuela Politécnica del Ejército (2003), Tesis de Grado “Auditoría Informática de la Agencia Internacional “Ecuador Cargo System” ”

- Productos D-Link
  http://www.dlinkla.com

ANEXO A

INVENTARIO DE EQUIPOS DE COMPUTACIÓN

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
1	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Gerencia
	1	Mouse	Genius PS2 Nestscroll	
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 256Mb Memoria RAM	
			- 80G Disco Duro	
			- Tarjeta de Red D-Link DFE-530TX	
			- Floppy 3.5 HD	
			- CD-RW + DVD	
	1	Impresora	Hewlett Packard LaserJet 1200 Series	
	1	Laptop	Toshiba Satellite A40 SP151	

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
			- Procesador Mobile Intel Pentium 4 a 2.80Ghz	
			- 256MB en Memoria	
			- Disco Duro de 40GB	
			- DVD-ROM + CD-RW 24x	
			- Pantalla TFT de 15 Pulg	
			- Modem 56K	
			- Red 10/100Mbps	
			- Red Inalámbrica 802.11g	
2	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Financiero / Administrativo
	1	Mouse	Genius PS2 Nestscroll	
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 256Mb Memoria RAM	
			- 80G Disco Duro	
			- Tarjeta de Red D-Link DFE-530TX	

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
			- Floppy 3.5 HD	
			- CD-RW 52X	
	1	Impresora	Hewlett Packard LaserJet 1200 Series	
	1	Impresora	Matricial Epson LX-300+	
	1	Laptop	Toshiba Satellite A40 SP151	
			- Procesador Mobile Intel Pentium 4 a 2.80Ghz	
			- 256MB en Memoria	
			- Disco Duro de 40GB	
			- DVD-ROM + CD-RW 24x	
			- Pantalla TFT de 15 Pulg	
			- Modem 56K	
			- Red 10/100Mbps	
			- Red Inalámbrica 802.11g	
3	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Financiero / Administrativo
	1	Mouse	Genius PS2 Nestscroll	
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 256Mb Memoria RAM	
			- 40G Disco Duro	
			- Tarjeta de Red D-Link DFE-530TX	
			- Floppy 3.5 HD	
			- CD-ROM 52X	
4	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Financiero / Administrativo
	1	Mouse	Genius PS2 Nestscroll	
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 256Mb Memoria RAM	
			- 40G Disco Duro	
			- Tarjeta de Red D-Link DFE-530TX	
			- Floppy 3.5 HD	

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
			- CD-ROM 52X	
5	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Sistemas
	1	Mouse	Genius PS2 Nestscroll	
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 512Mb Memoria RAM	
			- 80G Disco Duro	
			- Tarjeta de Red D-Link DFE-530TX	
			- Floppy 3.5 HD	
			- CD-RW 52X	
	1	Impresora	Hewlett Packard LaserJet 1200 Series	
	1	Laptop	Toshiba Satellite A40 SP151	
			- Procesador Mobile Intel Pentium 4 a 2.80Ghz	
			- 256MB en Memoria	
			- Disco Duro de 40GB	
			- DVD-ROM + CD-RW 24x	

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
			- Pantalla TFT de 15 Pulg	
			- Modem 56K	
			- Red 10/100Mbps	
			- Red Inalámbrica 802.11g	
6	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Sistemas
	1	Mouse	Genius PS2 Nestscroll	
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 256Mb Memoria RAM	
			- 40G Disco Duro	
			- Tarjeta de Red D-Link DFE-530TX	
			- Floppy 3.5 HD	
			- CD-ROM 52X	
7	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Ventas
	1	Mouse	Genius PS2 Nestscroll	

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 256Mb Memoria RAM	
			- 80G Disco Duro	
			- Tarjeta de Red D-Link DFE-530TX	
			- Floppy 3.5 HD	
			- CD-RW 52X	
	1	Impresora	Hewlett Packard LaserJet 1200 Series	
	1	Laptop	Toshiba Satellite A40 SP151	
			- Procesador Mobile Intel Pentium 4 a 2.80Ghz	
			- 256MB en Memoria	
			- Disco Duro de 40GB	
			- DVD-ROM + CD-RW 24x	
			- Pantalla TFT de 15 Pulg	
			- Modem 56K	
			- Red 10/100Mbps	

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
			- Red Inalámbrica 802.11g	
8	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Ventas
	1	Mouse	Genius PS2 Nestscroll	
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 256Mb Memoria RAM	
			- 40G Disco Duro	
			- Tarjeta de Red D-Link DFE-530TX	
			- Floppy 3.5 HD	
			- CD-ROM 52X	
9	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Ventas
	1	Mouse	Genius PS2 Nestscroll	
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 256Mb Memoria RAM	
			- 40G Disco Duro	
			- Tarjeta de Red D-Link DFE-530TX	
			- Floppy 3.5 HD	
			- CD-ROM 52X	
10	1	Monitor	SAMSUNG SyncMaster 551v de 15”	Ventas
	1	Mouse	Genius PS2 Nestscroll	
	1	Teclado	Genius PS/2 KB-06X	
	2	Parlantes	Genius SP-Q06	
	1	UPS	Powercom 500VA	
	1	CPU	Clon:	
			- Pentium 4	
			- Procesador Intel 2.8G	
			- Bus 533Mhz	
			- 1 Mb Caché	
			- 256Mb Memoria RAM	
			- 40G Disco Duro	

No.	CANT.	EQUIPO	DESCRIPCIÓN	DEPARTAMENTO
			- Tarjeta de Red D-Link DFE-530TX	
			- Floppy 3.5 HD	
			- CD-ROM 52X	

ANEXO B

CARACTERÍSTICAS DEL SWITCH Y ROUTER

SWITCH D-LINK DES-1024R+ DE 24 PUERTOS 10/100MBPS Y 1 SLOT PARA FIBRA FX MODULE

General:

Este switch es adaptable a la estructura rack-mount y a través de sus 24 puertas 10/100Mbps permite la conexión a estaciones de trabajo o servidores. También permite que otros Hubs puedan conectarse a este dispositivo.

Todas las puertas del switch detectan automáticamente el sentido de velocidad en la red de manera de poder trabajar con otros dispositivos a las velocidades 10Mbps o 100Mbps, de acuerdo a la velocidad de transferencia que disponga cada nodo respectivo.

De igual modo, todas las puertas auto-negocian la velocidad de transferencia en modo Full/Half-Duplex.

Control de Flujo IEEE 802.3x:

Esta característica permite a los servidores existentes conectarse directamente a este switch para facilitar una transferencia de datos más rápida y segura. En modalidad Full-Duplex, a 200Mbps, este switch provee altas velocidades a los servidores con una cuota mínima de datos perdidos en la transferencia.

Modulo Opcional de Fibra Óptica:

El Switch DES-1024R+ dispone de un slot para instalar un módulo opcional de 2 puertas de fibra y de este modo poder conectarse a 2 equipos o hacer cascada con otro switch a una distancia máxima de 2 km. utilizando Fibra Óptica.

ROUTER D-LINK DI-704P DE 4 PUERTOS

General

El Internet Server DI-704P en sus dos versiones de HW-A1 y HW-B1, está especialmente diseñado para proteger a los computadores de hackers. Es una manera fácil y segura de compartir la alta velocidad de conexión a Internet a través de módems xDSL o CableMódem y además esta equipado de una puerta bidireccional LPT para conectar directamente una impresora

4 Puertas Switching 10/100Mbps:

El Internet Server y Gateway DI-704P trabaja con las normas de IEEE, y es compatible con las actuales tecnologías de red existentes. Usando la auto-negociación NWay para operar en 10Mbps o 100Mbps, las cuatro puertas 10/100 usan tecnología switching Ethernet reforzando la velocidad y productividad de la LAN en forma importante. Cada puerta también soporta la norma IEEE 802.3x que especifica Control de Flujo de datos en modo Full-Duplex.

Compartiendo una Cuenta ISP:

El Internet Server y Gateway DI-704P permite conectar simultáneamente a Internet hasta 253 computadoras, a través de una única cuenta con el ISP. El Internet Server y Gateway DI-704P trabaja con el protocolo Dynamic Host Configuration Protocol (DHCP) proporcionando asignación dinámica de direcciones IP. Siendo muy flexible, esta solución trabajará con cualquier dispositivo Ethernet, equipos y sistemas operativos que operen sobre TCP/IP.

ANEXO C

CARACTERÍSTICAS DE LOS SERVIDORES

SERVIDOR DE APLICACIONES Y DE DATOS

Características de Hardware:

- Intel Server Chassis SC5250E
- Mainboard Intel Server Board SE7501HG2
- Procesador Intel Xeon 3.0EGhz / 1Mb EN Caché / Bus 800mhz Active (x2)
- Memoria Ram DDR Valueram For Pc333 Ecc 1Gb X 2
- Disco Duro SCSI 36.6Gb (x2) (Raid 1)
- Raid SCRZCSR
- Floppy Alps 3.5 1.44Mb
- Cd-Rw LG 52x

Características de Software:

- Sistema Operativo: Windows 2003 Server

  Configurado como:

  - ✓ Servidor de archivos
  - ✓ Controlador de Dominio

Funciones:

- Controla las cuentas de acceso de los usuarios a la red.
- Controla Políticas de uso de Software y Hardware a dichos usuarios.
- Aloja a los Sistemas de Aplicación (SAINT, TELPAGO, SYS2).

SERVIDOR DE CORREO ELECTRONICO

Características de Hardware:

- Intel Server Chassis SC5200 (2U)
- Mainboard Intel Server Board SE7501WV2
- Procesador Intel Xeon 2.8EGhz / 1Mb EN Caché / Bus 800mhz Pasive
- Memoria Ram DDR Valueram For Pc266 Ecc 512Mb X 2
- Disco Duro 120Gb SATA
- Cd-Rom Slim

Características de Software:

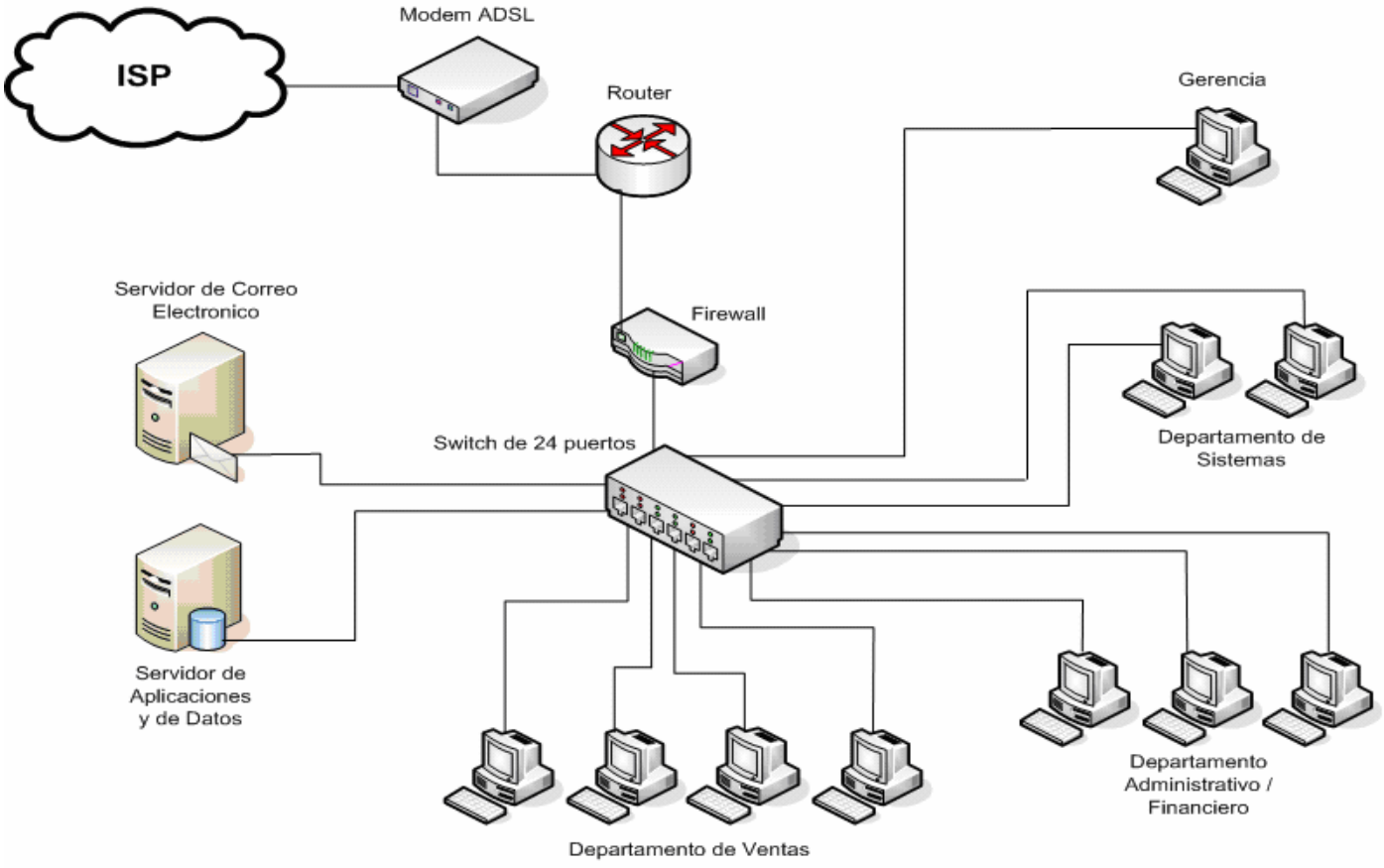
- Sistema Operativo: Windows 2003 Server
- Exchange Server

Funciones:

- Controla las cuentas de Correo Electrónico de los usuarios.
- Implementa el protocolo de conexión (POP3) entre el servidor SMTP y los clientes de correo.

ANEXO D

DIAGRAMA DE RED DE ACUERDO AL PLAN DE SEGURIDAD



LISTA DE ACRONIMOS Y TERMINOS

- **ADWARE:** Variante “comercial” del spyware. Se trata de un pequeño trozo de código que tiene como finalidad recolectar datos a efectos de marketing.
- **ADSL:** Asymmetric Digital Subscriber Line. Línea digital asimétrica de usuario.
- **ANSI:** American National Standards Institute. Instituto Americano de Normalización.
- **ANTIVIRUS / PROGRAMAS ANTIVIRUS:** Son todos aquellos programas que permiten analizar la memoria, las unidades de disco y otros elementos de un ordenador, en busca de virus.
- **ASCII:** American Standard Code for Information Interchange. Código estándar estadounidense para el intercambio de información.
- **BIT:** Binary digit. Es la unidad más pequeña de la información digital con la que trabajan los ordenadores (sistemas informáticos).
- **BYTE:** Es una unidad que mide la cantidad de información, tamaño y capacidad de almacenamiento. Un Byte, equivale a 8 Bits.
- **E-MAIL:** Electronic Mail. Envío de mensajes electrónicos a otros usuarios de la red con dirección electrónica.
- **FIREWALL:** Cortafuegos. Dispositivo que se interpone entre dos redes para controlar sus comunicaciones y ofrecer seguridad.
- **FIRMA DIGITAL:** Código que se adjunta a un mensaje y que garantiza que éste proviene de una determinada persona, la firmante, y que no ha sido alterado.
- **FTP:** File Transfer Protocol. Protocolo de transferencia de archivos.
- **FUNCIONES HASH:** Funciones Resumen. Se utilizan en la firma digital.

- **HACKER:** Denominación dada al usuario especializado en penetrar bases de datos de sistemas informáticos confidenciales con el fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático.
- **HARDWARE:** Término que hace referencia a cada uno de los elementos físicos de un sistema informático (pantalla, teclado, ratón, memoria, discos duros, microprocesador, etc).
- **HOST:** Ordenador que realiza funciones de Servidor, permitiendo que su información sea accedida por otros computadores.
- **HTML:** HiperText Markup Language. Lenguaje de marcas de hipertexto. Códigos de presentación de páginas web.
- **HTTP:** HiperText Transfer Protocol. Protocolo de transferencia de hipertexto. Sistema de reconocimiento de direcciones de páginas web.
- **ISP:** Internet Service Provider. Es un proveedor de acceso a Internet que además ofrece una serie de servicios relacionados con Internet (Proveedor de Servicios Internet).
- **LAN:** Local Area Network. Red de Área Local.
- **MALWARE:** MALicious softWARE. Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos.
- **MODEM:** MOdulador DEModulador. Dispositivo que permite el envío o recepción de datos digitales por vía analógica.
- **NBS:** National Bureau of Standards.
- **NSA:** National Security Agency. Agencia de Seguridad Nacional.
- **POP3:** Post Office Protocol 3. Protocolo de Servicio Postal 3. Entablar la conversación entre el servidor de correo y el ordenador personal del usuario.

- **PROTOCOLO:** Reglas que rigen la comunicación entre diferentes computadores. Para efectos comparativos podemos decir que nuestro lenguaje es un protocolo de comunicación entre personas.
- **RAM:** Random Access Memory. Memoria de acceso aleatorio. Su contenido puede variar de forma dinámica.
- **ROUTER:** Enrutador o encaminador. Nodo en una red TCP/IP encargado de conectar con otras redes, efectuando funciones de encaminamiento, filtrado, etc.
- **SAINT:** Sistema en donde se lleva el control de entrada y salida de la mercadería utilizado por la empresa PROMIX ECUADOR C.A.
- **SISTEMA DES:** Data Encryption Standard. Algoritmo de Encriptación desarrollado por IBM que utiliza bloques de datos de 64 bits y una clave de 56 bits.
- **SLOT:** Ranura de expansión. Mediante los slots añadimos más funcionalidad a los equipos.
- **SMTP:** Simple Mail Transfer Protocol. Comunicación de mensajes de correo entre servidores.
- **SOFTWARE:** Son los ficheros, programas, aplicaciones y sistemas operativos que nos permiten trabajar con el ordenador o sistema informático. Se trata de los elementos que hacen funcionar al hardware.
- **SPYWARE:** Software espía ya que registra, sin que el usuario se de cuenta, la actividad de una persona mientras utiliza el programa, o mientras navega en la red.
- **SWITCH:** Conmutador de circuitos, paquetes o células.
- **SYS2:** Sistema Contable que utiliza la empresa PROMIX ECUADOR C.A.
- **TCP/IP:** Transmission Control Protocol / Internet Protocol. Protocolo de Control de la Transmisión/Protocolo de Internet.

- **TELNET:** Telecommunicating Networks. Acceder a un servidor remoto y trabajar con él en modo Terminal.
- **TELPAGO:** Sistema de Administración que se lo utiliza para el control de clientes y ventas de la empresa PROMIX ECUADOR C.A.
- **TROYANO:** Programa que se infiltra en un ordenador de forma sigilosa y es capaz de registrar su actividad, e incluso las teclas que se escriben en el teclado. Usado generalmente como medio para revelar contraseñas del usuario.
- **UPS:** Uninterrupted Power Supply. Sistema de Alimentación Ininterrumpida.
- **URL:** Uniform Resource Locator. Localizador unificado de recursos - dirección de sitio o página web.
- **UTP:** Unshielded Twisted Pair. Cable trenzado sin blindaje.
- **WWW:** World Wide Web. Red de dimensión mundial. Sistema de información basado en páginas que contienen hipertexto y gráficos.