UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA
DIVISIÓN DE ESTUDIOS DE POSGRADO

DESARROLLO DE UN MODELO PARA LA PLANEACIÓN DE LA SEGURIDAD EN REDES LOCALES

T E S I S

P R E S E N T A D A P O R :

ING. BEATRIZ SÁNCHEZ GÓMEZ

PARA OBTENER EL GRADO DE :

MAESTRA EN INGENIERÍA
(PLANEACIÓN)

DIRIGIDA POR : M.I. RUBÉN TÉLLEZ SÁNCHEZ

México, D.F. 2003

AGRADECIMIENTOS

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México y en especial a la División de Estudios de Posgrado de la Facultad de Ingeniería.

Al M.I Rubén Téllez Sánchez por la asesoría de éste trabajo.

En general a todos los profesores que contribuyeron a mi formación académica.

DEDICATORIAS

DEDICATORIAS

A mi esposo Ricardo
Con todo mi amor, gracias a tu apoyo y esfuerzo siempre salgo adelante en todo lo que me propongo.

A mi hija Lissete
Porque tu compañía en ésta etapa, me alentó a emprender y realizar esta meta, con todo mi amor.

A mi hijo Kevin
Gracias a ti conozco el más hermoso sentimiento que me impulsa a seguir adelante, con todo mi amor.

A mi mamá Juanita
Por el apoyo que me dio para la culminación de esta meta.

A mi hermano Gabriel
Por su apoyo y por estar siempre al pendiente de mi y mis seres queridos.

A mis sobrinos y sobrinas en especial a Gaby
Por su ayuda desinteresada.

Beatriz

ÍNDICE

INTRODUCCIÓN

INTRODUCCIÓN

ANTECEDENTES

El siglo XX ha producido profundos cambios en la tecnología, la economía y la cultura. Este cambio en nuestras vidas ha ocurrido fundamentalmente por la accesibilidad de la información, según avanza el siglo se continúan viendo rápidos avances en las tecnologías de la información. Mucha gente forma parte activa de la comunidad electrónica global, gracias al recien aumento de los servicios interactivos y de Internet. Estos servicios son utilizados para intercambiar correo personal profesional, realizar compras entre otros muchos servicios, hacer reservaciones y conocer otras personas.

Nuestra dependencia de las computadoras se ha ido incrementando en los últimos treinta años. En la década de los sesenta, los sistemas basados en una computadora central se convirtieron en los equipos estándar de muchas compañías. Los años setenta vieron el advenimiento de las pequeñas computadoras que permitieron automatizar los procesos de departamentos y empresas pequeñas.

Actualmente la tecnología informática y de comunicaciones electrónicas representa un elemento estratégico en cualquier empresa que requiere la mejora de los bienes y/o servicios que ofrece al mercado. De hecho los resultados de los análisis de calidad o de reingeniería, en los procesos de negocio basan en un gran porcentaje, su utilización como mecanismos que permiten automatizar tareas, agilizar y eliminar capturas, reducir costos y tiempos etc. Lo que obliga a las empresas a depender cada vez mas de su utilización.

El uso que hoy en día se esta dando a la tecnología informática, origina problemas de seguridad en el acceso y explotación de la información, utilizada a través del equipo de cómputo. Por esta razón, es necesario que las empresas cuenten con los elementos de seguridad necesarios para sus sistemas y equipos de computo, para ello requieren llevar acabo la planeación de la seguridad en su red.

Hoy en día el crecimiento de las grandes corporaciones, empresas de gobierno, secretarías de estado, y en general cualquier entidad pública o privada requiere de la interacción de su personal con equipos computacionales, ya sean estos multiusuarios, monousuarios e inclusive computadoras personales. Que mediante periféricos de comunicación, como *modems* o redes locales, accedan a la información y aplicaciones de diversos tipos que se utilizan para su trabajo diario o para la toma de decisiones.

Sin embargo, a medida de que se automatizan estos ambientes, la Información y los equipos que la contienen corren un riesgo inminente de que estos puedan ser accesados por personas o entidades ajenas a los que la emplean, existiendo vulnerabilidades tales como; inexistencia e insuficiencia de controles, espionaje y venta de información a competidores, mal uso y destrucción de información, sabotaje, etc.

Las computadoras son un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de ésta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.

Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Ante esta situación, en el transcurso del siglo XX, el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y de derecho.

Por poner un ejemplo se puede pensar en que por una u otra razón, el centro de cómputo o las librerías sean destruidos o usados inapropiadamente, ¿cuanto tiempo pasaría para que esta organización estuviese nuevamente en operación? El centro de cómputo puede ser el activo más valioso y al mismo tiempo el más vulnerable.

En la situación actual de criminología, los delitos de cuello blanco han incluido la modalidad de los delitos hechos mediante la computadora o los sistemas de información, de los cuales el 95% de los detectados han sido descubiertos por accidente. La gran mayoría no han sido divulgados para evitar dar ideas a personas mal intencionadas. Es así como la computadora ha modificado las circunstancias tradicionales del crimen; muestra de ello son los fraudes, falsificaciones y venta de información hechos en las computadoras o realizados a través de las computadoras.

Durante mucho tiempo se consideró que los procedimientos de auditoría y seguridad eran responsabilidad de la persona que elabora los sistemas, sin considerar que son también responsabilidad del usuario y del departamento de auditoría interna.

Entre los delitos más conocidos (muchos de ellos no son identificados o divulgados por evitar repercusiones) está el del *Banco Wells Fargo Co.* Por un fraude de $21.3 millones de dólares, en el cual se evidenció que la protección de los archivos es todavía inadecuada, y la publicada el 17 de septiembre de 1987 en la que los Alemanes encontraron los archivos confidenciales de la NASA. Otro de los delitos que se han cometido en los bancos consiste en insertar mensajes fraudulentos y transferir dinero de una cuenta a otra, con la consecuente ganancia de los intereses.

Existe también el caso de un muchacho de 15 años que entró a la computadora de la Universidad de Berkeley en California y destruyó los archivos, y el estudiante de la escuela Dalton en Manhattan que entró a la red canadiense, identificándose como un usuario de alta prioridad y tomó el control de los sistemas de una embotelladora de Canadá.

En México existe el antecedente que la base de datos de todos los registrados en el Instituto Nacional Electoral, fue vendida sin autorización de las autoridades correspondientes. Ejemplos como éstos existen muchos, y la mayoría de ellos no se dan a conocer para no dar ideas a personas que puedan cometer delitos o bien para evitar problemas de publicidad negativa.

En la actualidad, y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar el llamado virus de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización (piratas) y a veces borra toda la información que se tiene en un disco.

Con los acontecimientos mundiales que se presentan en el ámbito global como actos terroristas, terremotos, espías cibernéticos, estados climáticos, etc., Han puesto el tema de seguridad e informática entre las prioridades del sector empresarial en México.

El riesgo de sufrir alguna agresión cibernética; perder información vital para operar o ser víctima de fraude financiero, ha generado que los negocios del país consideren seriamente destinar un presupuesto para la seguridad de sus redes, ya que si los sistemas de protección en países desarrollados como Estados Unidos son vulnerables, México no es la excepción ya que el 95 por ciento de las empresas que cuentan con equipo de computo están indefensas.

Los consorcios de nuestro país apenas destinan uno por ciento de sus presupuestos en seguridad informática[1], La conciencia sobre la vulnerabilidad de las redes, en los sectores financiero, telecomunicaciones y gobierno se está empezando a dar en México pero la inversión es baja. Las grandes empresas empiezan a destinar uno por ciento de sus presupuestos para reforzar su seguridad.

Pero se estima que para el 2004 la inversión en este rubro, por parte de firmas mexicanas, represente entre tres y cinco por ciento de sus presupuestos.

[1] Señaló James Teel, Vicepresidente de soluciones de Business Connectivity de 3 Com, fuente Periodrio El Financiero 13, de septiembre de 2002.

En México no existen estadísticas confiables sobre los daños económicos causados por fallas en seguridad, y que permitan evaluar el nivel de seguridad de las empresas.[2] Los resultados de estudios sobre seguridad de redes internacionales arrojan indicadores y tendencias similares a lo que sucede en México. Según encuesta de seguridad realizada por el FBI de marzo del 2001 a marzo del 2002 delitos computacionales en U.S.A generaron pérdidas financieras por 405 millones de dólares, los resultados afirman que el 49 por ciento de las firmas reportaron incidentes de acceso no autorizado a las redes, por parte de sus empleados. También se ha detectado que los ataques externos están tomando más fuerza que los internos, aunque éstos también continuaran en ascenso y son los que más daños financieros producen.

Reforzar la seguridad no sólo implica invertir en tecnología, sino crear una cultura de seguridad en la organización. Para lograrlo se debe hacer un diagnóstico de la seguridad de la empresa; determinar los requerimientos de seguridad, desarrollar un política de seguridad interna y externa, valuar los activos informáticos, clasificar la información de acuerdo a su importancia y confidencialidad. Diseñar los procesos a ser aplicados. Esto es de suma importancia ya que los ataques a los sistemas pueden ocasionar que las empresas dejen de operar y pierdan más del 50 por ciento de su inversión.

Actualmente el crecimiento de la computación distribuida es uno de los motores que impulsa el desarrollo de la seguridad. Debido a que gracias a ella se permite compartir recursos e información entre los equipos, así como el acceso a una gran variedad de servicios pasando por redes y múltiples plataformas. Lo que origina que así como nos da grandes beneficios, también represente altos riesgos para los dueños de la información contenida en éstos. Debido a que el uso de la red local tiene riesgos y con ellos los problemas de seguridad a los que se enfrenta toda organización que usa la información electrónica.

Lo anterior ha originado que los usuarios de redes tengan la necesidad de llevar a cabo la planeación de la seguridad en las mismas. Que les permita administrar y proteger la información que reside en estos sistemas y el *hardware* que las conforma. De tal manera que sea imposible para las personas y/o sistemas el acceso a ellos, e incluso la restricción dentro del mismo grupo de trabajo o compañía, de ciertas partes de la información y/o aplicaciones computacionales.

[2] Según datos del área de control y administración de riesgos electrónicos de Mancera Ernts& Young. , fuente Periodrio El Financiero 13, de septiembre de 2002.

PROBLEMÁTICA

En el momento que las computadoras se conectan unas con otras, la seguridad en éstas empieza a tener gran importancia. Antes, cuando las computadoras estaban aisladas, el principal responsable de la información y del equipo era solo el personal que utilizaba ese equipo o el que lo operaba diariamente. En este entorno, si había un cambio o daño del equipo o información, se conocía claramente quién estaba operando el equipo y por lo tanto quién era el responsable.

Debido a que los ambientes de redes de área local por sus características propias tienden a ser más vulnerables que otros, ya que el uso de estos es por varias personas y también se tienen conectados varios equipos. Resulta importante el investigar como se puede llevar acabo la planeación de la seguridad de los mismos; para poder evitar, prevenir y corregir los problemas de seguridad en éstos; Ya que es un problema que actualmente sé está presentando y preocupa a las personas involucradas con el manejo de la información automatizada empleada en su labor diaria, y a los proveedores de productos y servicios de las mismas.

La problemática que se plantea y analiza en la presente tesis es la inseguridad que existe en las redes de área local.

Falta de seguridad en las redes de área local. Que se refleja en la perdida, robo, manipulación de la información y los equipos.

Procedimientos y políticas inadecuados que permitan detectar y evitar riesgos presentes y futuros.

OBJETIVO GENERAL

Identificar los factores que intervienen en el proceso de planeación para proponer un modelo de seguridad en redes de área local

OBJETIVOS ESPECIFICOS

- Validar la metodología para llevar acabo la planeación de la seguridad aplicándola a un caso real.
- Determinar que políticas y procedimientos de seguridad son necesarios para su control y seguimiento.

HIPÓTESIS

- La identificación y análisis de los requerimientos de seguridad en los sistemas distribuidos es la base para la planeación de la seguridad de los mismos.
- La evaluación de factores de riesgo que determina la vulnerabilidad en los sistemas computacionales distribuidos.
- La planeación de la seguridad en los sistemas distribuidos debe llevarse acabo para conocer, prevenir, mejorar y dar confiabilidad a la información que reside en éstos sistemas.

PRESENTACIÓN

En la introducción de esta tesis se establece el contexto general en el que se encuentra en este momento la seguridad de las redes de área local, las antecedentes que han propiciado este problema, el objetivo general y los específicos así como la hipótesis.

En el capítulo uno se describen a detalle las características de las redes de área local y los conceptos generales relacionados con la seguridad que se emplean para el desarrollo de la presente tesis.

En el capítulo dos se establece la problemática con respecto a la seguridad de las redes locales, los puntos vulnerables en la red, para el desarrollo del modelo propuesto para la planeación de la seguridad, y se explica como se realizó el análisis de riesgos.

En el capítulo tres se desarrolla y describe el modelo propuesto a partir del análisis de la seguridad realizado en el capítulo dos, se explica la matriz propuestas para el análisis de riesgos, y la matriz de evaluación de la seguridad de la red. Como se debe llevar acabo la implantación de la seguridad en la red y el desarrollo de estándares de seguridad.

En el capítulo cuatro se explica a detalle las características de la red donde se aplicó el modelo propuesto y los resultados obtenidos de la evaluación de la seguridad, así como la propuesta de solución encontrada.

Por último se presentan las conclusiones y recomendaciones de la tesis.

CAPÍTULO 1

CONTEXTO TECNOLÓGICO EN LAS REDES LOCALES

CONTEXTO TECNOLÓGICO EN LAS REDES LOCALES

1.1 CONCEPTOS GENERALES

En la problemática de seguridad en sistemas distribuidos es importante conocer cual es la causa o causas que originan la perturbación del sistema; Qué consecuencias se pueden tener una vez presentada, para ello es necesario conocer las características del sistema y los conceptos involucrados con el mismo, para poder clasificar e identificar los diferentes niveles de seguridad que se requieren; de tal manera que se pueda prevenir, eliminar o atacar los problemas que se puedan presentar en el sistema. Para tal efecto a continuación se definen los conceptos relacionados con el desarrollo de la presente tesis:

HARDWARE: El *har*(duro) *ware* (materia) son todos los componentes electrónicos físicos de un sistema de cómputo, incluyendo los dispositivos periféricos, tarjetas, monitores, etc.

SOFTWARE: El *sotf*(suave) *ware*(materia) está constituido por las instrucciones que permiten a los componentes físicos de una computadora llevar acabo una operación. En sentido estricto se le llama así a cualquier programa que le indique a una computadora como efectuar una operación.

1.2 SISTEMAS COMPUTACIONALES DISTRIBUIDOS

Este término se ha venido utilizando para denominar indistintamente diferentes clases de sistemas informáticos. En los que la potencia del tratamiento de la información se encuentra repartida en el espacio en la figura 1.1; en donde se representa un esquema general de un sistema distribuido. En él aparecen un conjunto de elementos de tratamiento de la información interconectados, en lo que se ha denominado un mecanismo de comunicación e interconexión.

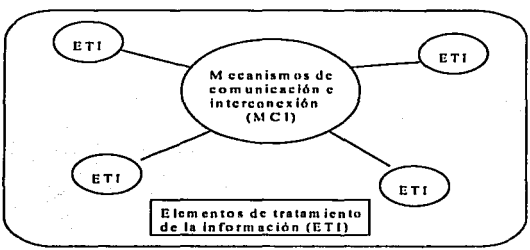

Figura 1.1 Elementos del tratamiento de la información

Se tienen varias soluciones desarrolladas de las cuales existen cuatro tipos de sistemas:

a) Redes de computadoras
b) Redes locales de computadoras
c) Sistemas multicomputadores
d) Sistemas multiprocesadores

En la figura 1.2 se presentan las diferentes soluciones mencionadas anteriormente de acuerdo al área geográfica para la cual se emplean cada una.

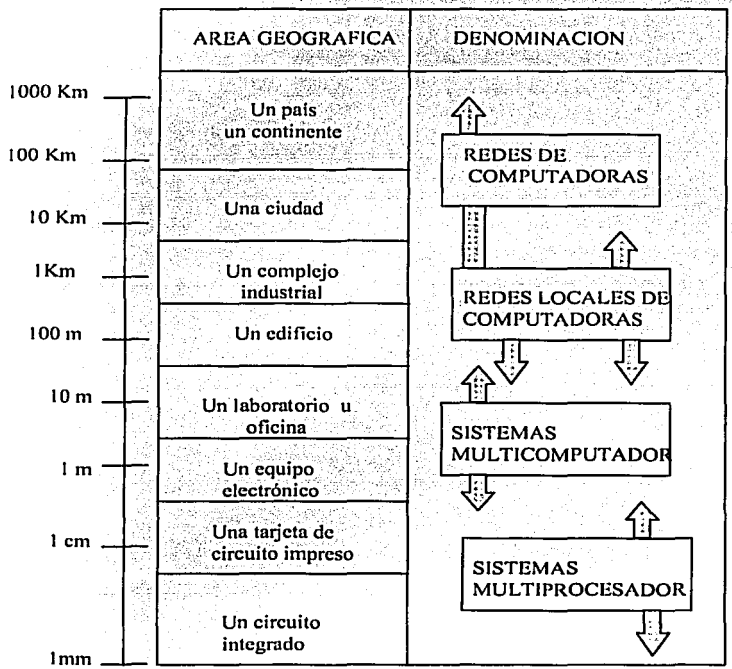

Figura1.2 Tipos de redes

Redes de computadoras: Estas redes tienen el objetivo fundamental de compartir recursos, es decir, permiten a cualquier usuario de cualquier computador accesar y utilizar los recursos, ya sean hardware y software del conjunto de las máquinas que constituyan la red.

Sistemas multicomputadores:

Cuando se descentralizan las funciones en un computador y así aparecen en las máquinas clásicas, unidades especializadas en la manipulación de periféricos.

Sistemas multiprocesadores

Son máquinas potentes para el tratamiento de la información basadas en la cooperación sistemática y ordenada de los elementos de menos potencia, funcionan en paralelo.

1.3 CARACTERÍSTICAS DE REDES LOCALES

De éstos el que nos presta principal atención es el de red local; que es un sistema interconéctado de computadoras, periféricos y líneas de comunicaciones en un sóo lugar;las redes locales son de todos los tamaños y estilos. En las redes locales,las computadoras y los periféricos del sistema se conectan mediante alambres de cobre o fibras de vidrio que los unen. Las redes locales también pueden enlazarse con otras redes a través de diferentes tecnologías de comunicaciones a larga distancia.

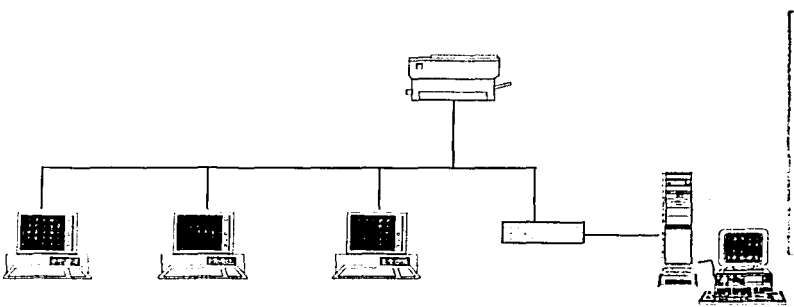

Figura 1.3 Esquema básico de una red local

CARACTERISTICAS:

◊ Medio de comunicación común.
◊ Los usuarios conectados pueden compartir recursos.
◊ Manejan altas velocidades de transmisión.
◊ No regulado (un usuario puede ser el dueño y operarlo).

1.4 CONCEPTOS ASOCIADOS A LA TECNOLOGÍA EN ESTUDIO

COMPONENTES: Una red de área local tiene los componentes básicos siguientes:

HARDWARE

SERVIDOR : Cualquier dispositivo de hardware o rutina de software que provee uno o más servicios predefinidos a una población de entidades usuarias, tales como nodos en una red.

SERVIDOR DE IMPRESORAS: Sistema de computación en red que recibe, maneja y ejecuta los pedidos de impresión de otros dispositivos de red.

ESTACIONES DE TRABAJO: Cualquier equipo conectado a una red, con capacidad propia de proceso tiene recursos propios (procesador, memoria, unidades de disco.)

CABLE: Medio de transmisión que consiste en alambres o fibras ópticas envueltas por una cubierta protectora.

TARJETAS DE INTERFAZ: Adaptador normalmente instalado dentro de la máquina que ofrece capacidades de comunicación de la red desde y hacia la computadora.

NODO: Término genérico que se refiere a una entidad que puede tener acceso a una red. Se usa también el término dispositivo (*device*).

CONCENTRADORES: Caja que concentra (de ahí su nombre) segmentos de cable de una red local para su mejor distribución y administración. No solo es un centro sencillo de concentración de cables si no que también provee las funciones para la construcción de puentes, asignación de ruta y otras funciones administrativas.

ENRUTADOR (*ROUTER*): dispositivo que puede decidir cuál de varios caminos debe seguir el tráfico de la red, basándose en alguna métrica óptima. También se conoce como *gateway*: Servidor de intercomunicaciones (aunque esta definición de *gateway* ya casi no se usa) los enrutadores envían paquetes de una red a otra, basados en la información de la capa de red.

PUENTE (*BRIDGE*): Dispositivo que conecta dos segmentos de una red y pasa paquetes entre ellos.

PERIFERICOS:

MODEM: (modulador- de modulador) Dispositivo que convierte señales digitales a una forma adecuada para transmisión sobre medios de comunicación analógicos viceversa.

MODULACIÓN: Proceso por el cual se transforman las características de las señales para representar información. Los tipos de modulación incluyen frecuencia modulada (FM) en donde señales de diferentes frecuencias representan los valores de datos diferentes, y amplitud modulada (AM), donde la amplitud de la señal varía para representar los diferentes valores de datos.

DEMODULACIÓN: Proceso de devolver una señal modulada a su forma original, los módems hacen la demodulación tomando una señal analógica y regresándola a su forma original.

SOFTWARE

SISTEMA OPERATIVO DE RED: Es el ambiente operativo por medio del cual una computadora puede trabajar con más de un usuario simultáneamente, por lo que puede tener varias terminales conectadas.

SISTEMA OPERATIVO DE LAS ESTACIONES DE TRABAJO: Es el conjunto organizado de programas que controla todas las operaciones de una computadora, administrando todos los componentes del equipo

APLICACIÓN: Programa de computación diseñado para desempeñar una tarea específica, tal como la contabilidad, el análisis científico, el procesamiento de texto o la autoedición.

OTROS CONCEPTOS IMPORTANTES SON:

VIRUS : programa diseñado para dañar un sistema de cómputo sin el conocimiento ni permiso del usuario. Un virus puede conectarse a otro programa, a la tabla de partición, a la pista de la carga inicial del sistema, en un disco duro, cuando cierto evento ocurre, tal como cuando llega una fecha determinada, o cuando se ejecuta un programa específico, el virus entra en acción.

AUTENTIFICACIÓN: Es el proceso para determinar confiablemente la identidad de un elemento de la red.

CRIPTOGRAFÍA: La palabra criptografía viene de la conjunción de dos palabras griegas: cripto que significa secreto u oculto y grafía o escritura, por lo que al hablar de la criptografía se refiere al arte de la escritura secreta.

El uso de algoritmos de criptografía o encriptación nos permite:

- Mantener la privacidad de la información que se transmite a través de la red.
- Pueden ser usados para detectar modificaciones no autorizadas.

SEGURIDAD: Se define como la cualidad o el estado de estar libre de daño.

SEGURIDAD INFORMÁTICA: Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados a una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del *hardware*, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas.

1.5 SEGURIDAD EN REDES LOCALES

Históricamente la seguridad ha sido vista como un proceso de construcción de barreras alrededor de un sistema. Pero una forma de examinar los controles, dará un entendimiento completo y más realista de los problemas de seguridad en las organizaciones.

Existen dos tipos de seguridad que es importante señalar, la seguriad física y la seguridad lógica:

Seguridad física; Es la protección física que actúa en el momento que se origina cualquier evento que pueda dañar al equipo e información.

Seguridad lógica: Es aquella que controla los accesos a la información exigiendo identificaciones y autemtificación del usuario.

Es importante enfatizar que la planeación de la seguridad en redes de área local, permite al usuario evaluar las alternativas para tomar una decisión de como implementar la seguridad y conocer el grado de confiabilidad que puede tener en su red. Así es como la presente tesis lleva acabo la planeación de la seguridad en redes locales a través del análisis de las causas que originan los problemas y sus relaciones con otras, para establecer los niveles de seguridad que permitan evitar o disminuir el impacto que de presentarse puede tener sobre el funcionamiento normal de la red.

1.6 ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD

Es una técnica estructurada que ayuda a identificar la presencia y efectividad de los controles de seguridad. Generalmente es usado para examinar las reglas en los sistemas existentes y evaluar las especificaciones definidas para la seguridad de nuevos sistemas. Principalmente se usa para validar la seguridad de sistemas altamente comerciales después de que son puestos en producción.

Las amenazas contra la seguridad en los sistemas distribuidos son desafiantes.

La figura 1.4 mustra los tipos básicos de amenazas contra la seguridad de los datos e información de la red.

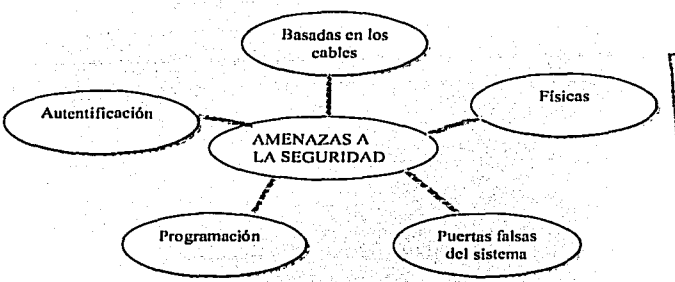

Figura 1.4 Tipos de amenazas a la seguridad de los datos de red

Físicas: Se refiere a cualquier evento que pueda ocasionar un daño físico en la red y con ello la pérdida de información que reside en el equipo. (fuego, agua, temblor, etc.)

Basadas en los cables: La naturaleza del procesamiento distribuido se basa en la comunicación de diversas computadoras a través de un medio. Se deduce que se podría escuchar el tráfico de la sesión y recoger información.

Autentificación: Este término hace referencia al proceso por el que una computadora determina si alguien está autorizado a solicitar o dar ciertos servicios del servidor. Sin la identificación adecuada, no habría seguridad en los sistemas distribuidos.

Programación: Las violaciones contra la seguridad que verdaderamente son significactivas e interesantes provienen del código. Un ejemplo de ello, son los virus que amenazan tanto la integridad como la seguridad de los datos.

Puertas de falsas del sistema: Son introducidas en los sistemas operativos para permitir el acceso al sistema en el caso de que un cliente pierda toda la información con la que realiza sus accesos autorizados, lo cual representa un gran riesgo ya que en muchas ocasiones se puede prestar al mal uso de los mismo por personal no autorizado.

Políticas de seguridad

Toda política de seguridad debe ser holística, es decir debe cubrir todos los aspectos relacionados con la misma, sin omitir ninguno.

La política debe adecuarse a nuestras necesidades y recursos, valorar las posibles contingencias.

Las políticas de seguridad deben abarcar los siguientes niveles:

- Físico
- Humano
- Lógico
- Logístico

Todos son muy importantes y si alguno se omite puede afectar la seguridad del sistema.

Nivel Físico: Se debe restringir el nivel físico inmediato, ya que éste establece la defensa contra agentes nocivos estableciendo medidas para limitar el acceso como normas de contingencia o recuperación. Aquí es importante recordar que quien tiene el acceso físico a la computadora tiene control absoluto de la misma. El grado de seguridad dependerá del tipo de necesidades para cada red; ya sea impedir o controlar el acceso de personal no autorizado hasta evitar el consumo de alimentos en las áreas de cómputo.

Nivel humano: Se pueden considerar varios subniveles; El responsable del sistema, Las personas que accedan al sistema, las personas ajenas al sistema.

Nivel lógico: Incluye las medidas de acceso y políticas de empleo de los recursos protegidos.

Nivel logístico: Considera las interacciones entre los elementos y la coordinación de los mismo, mediante el establecimiento de políticas comunes para coordinar la labor. Lo cual genera el buen funcionamiento del sistema.

HERRAMIENTAS TRADICIONALES DE SEGURIDAD

En la práctica los gerentes de seguridad no examinan la efectividad de los controles muchos tratan los informes de incidentes por monitoreos automáticos o reportes de excepción. Las herramientas mas comúnmente usadas para la seguridad son:

Revisión de la seguridad: Análisis de la vulnerabilidad es un proceso de revisión en el cual el sistema expuesto es identificado y evaluado usando técnicas formales como revisión de la seguridad en la información, esta revisión depende de la experiencia de las habilidades de los evaluadores.

Análisis de riesgo; Es la prueba formal de identificación del tratamiento y vulnerabilidad para determinar el nivel de riesgo por interpretación. El riesgo es expresado desde el punto de vista de un rango relativo de valores. Varias metodologías de análisis de riesgo y herramientas de software son empleadas. Debe notarse que los complejos mecanismos de análisis de riesgos complican el proceso de su identificación.

Auditoria funcional: Es un proceso de revisión que se enfoca en la identificación de existencia de controles específicos, en puntos de un sistema o en las aplicaciones y en la medida de la efectividad de estos controles. Esta revisión es típicamente realizada por auditores, que emplean una metodología estructurada. Herramientas de software son empleadas para la evaluación básica de los niveles de control de los sistemas.

Hackers: Gente que ingresa ilegalmente al sistema.

Firewall: Es una computadora que actúa como conectivo entre una red privada interna y alguna otra se usa como barrera de protección, puede transmitir información desde una red interna a la internet. Examina información entrante.

Filtros: Filtra información enviada a una red. Algunas barreras de protección pueden examinar cada parte de la información enviada a la red.

Contraseñas: Permite a los miembros de un grupo acceder a ciertos recursos de la red.

Software de monitoreo de red: Permite registrar en forma automatizada las bitácoras de actividad de un archivo, respaldo de información.

Unidades de tolerancia a fallas: Métodos de arreglo redundante consisten en varios discos utilizados para almacenar información duplicada.

Striping **(distribución)**: Distribuir equitativamente la información en pequeñas partes en los discos duros, si falla una unidad toda la información se pierde.

Imagen de Espejo: Se duplica la información de un disco a otro, cuando la información de la paridad es almacenada en una *raid*, los datos perdidos pueden ser rápidamente restaurados.

CAPITULO 2

EVALUACIÓN DE LA SEGURIDAD EN REDES LOCALES

EVALUACIÓN LA SEGURIDAD EN REDES LOCALES

2.1 OBJETIVO DE LA SEGURIDAD EN REDES LOCALES.

No existe un solo método para examinar la seguridad que sea apropiado para todos los ambientes. Se deben emplear recursos internos y externos para realizar el análisis. Uno de ellos es que el personal puede identificar y corregir problemas y detectarlos cuando estos ocurren rápidamente para proveer un estado de seguridad, así se pueden reconocer, detectar y reportar abusos en el sistema. Pero este tipo de control considera que existe personal competente. Generalmente el gerente de seguridad, un programador y un auditor deben participar en este procedimiento.

Como actualmente la información reside por lo general en redes, la técnica usada para examinarlas depende en parte del tipo de sistema. Debido al explosivo crecimiento de las estaciones de trabajo y las redes de área local (LAN) se necesita analizar la seguridad de éstas, ya que existe una diversidad de tecnología y diferentes accesos. Por tal motivo para examinar este tipo de redes se debe enfocar el análisis en áreas, que representan gran potencialidad de riesgo o a las más sensibles como lo son: las estaciones de trabajo, el server, los componentes relativos de la comunicación como son puentes, enrutadores módems, etc; así como lo es el sistema operativo y el software en general de la red.

La seguridad basada en esquemas de cliente/servidor, viola los perímetros del sistema de seguridad cuando esta viaja a través de la red:

Básicamente los objetivos de la seguridad en las redes son:

Integridad: Prevenir la modificación no autorizada del contenido de los mensajes.

Privacidad: Prevenir que la información no sea revelada a entidades no autorizadas.

Autentificación: Proceso de establecer pruebas de identidad.

El objetivo de la seguridad en las redes locales es precisamente proteger todos los componentes que la conforman de ahí que se definan en la figura 1.5, los siguientes dominios de seguridad. (1) Procesos; hardware, protección de circuitos, registros, privilegios. Software, protección de archivos, control de acceso, identificadores de usuarios. (2) Dispositivos de almacenamiento; al momento de realizar las copias fallas de hardware y software. (3) Comunicaciones, cruce de líneas, acceso técnico de intrusos, (4) Terminales remotas; acceso de intrusos,

copia de información (5) Usuarios; autorización, autentificación, depuración. y (6) Personal de sistemas; Supervisión de acceso a sistemas, archivos, características de protección.

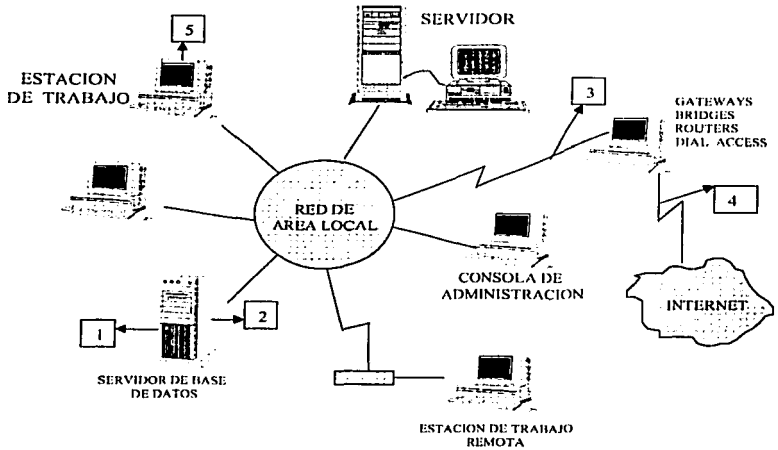

Figura 1.5 Dominios de seguridad para la red local

Las estaciones de trabajo pueden determinar la seguridad de la red entera, una sola estación de trabajo puede funcionar en varios modos de operación, como un solo procesador, un componente de una red o una terminal remota. Cada uno de estos modos de operación presenta diferentes requerimientos de seguridad.

Las caracteristicas de seguridad de los componentes de comunicación debe ser relativa al control y acceso a esta en dos direcciones:

La seguridad propia de los componentes de comunicaciónes.
Protección de los componentes mismos.

2.2 SEGURIDAD DE LA INFORMACIÓN QUE RESIDE EN LA RED.

Una de las consideraciones más importantes en el desarrollo y operación activa de un sistema de información administrativo es la seguridad. Con forme más está en línea un sistema, un mayor número de gente tiene acceso al sistema.

Un sistema de información tiene muchos puntos vulnerables y gran riesgo de pasar por alto las amenazas de seguridad al sistema de información y del centro de cómputo. Estas amenazas se presentan de muchas formas. Delitos cometidos por especialistas, desastres naturales, vandalismo y descuidos entre otros.

Seguridad de un centro de cómputo: Este puede tener varios puntos vulnerables; el hardware, el software, las bases de datos, las comunicaciones de datos y el personal.

Hardware: Si falla el hardware, falla el sistema. La amenaza de falla puede minimizarse si se tiene seguridad en el acceso de personal no autorizado y si se observan medidas para mantener en operación todo el hardware.

Software: Se necesita el control riguroso sobre el desarrollo del software y la documentación de un sistema de información para minimizar la oportunidad de cometer un delito mediante computadoras. Los procedimientos de control de operaciones que se integran al diseño vigilaran en forma constante la exactitud de procesamiento.

En las bases de datos está contenida materia prima para la información. En algunos casos, las bases de datos son el líquido vital de una compañía por lo que deben protegerse.

Comunicación de datos: La mera existencia de capacidades de comunicación de datos en donde los datos se transmiten mediante el enlace de una computadora con otra supone una amenaza a la seguridad.

Personal: Se debe poner una atención especial sobre las personas que tienen acceso a los sistemas de información computarizados y a los datos confidenciales ya que pueden tener errores u omisiones con la información que accedan.

Seguridad en los sistemas de información: Esta se puede clasificar en física y lógica; La seguridad física se refiere al hardware, las localidades, los discos magnéticos y otros materiles que podrían ser robados, destruídos o accesar a información confidencial.

La seguridad lógica se integra al software permitiendo que sólo el personal autorizado tenga acceso y utilice el sistema. Este tipo de seguridad para sistemas

en línea se logra fundamentalmente a través de contraseñas y códigos de autorización.

2.3 DESCRIPCION A DETALLE DEL PROBLEMA

La problemática que se desea analizar es: Las inadeacudas medidas de seguridad en las redes de area local, que originan que se presenten en general los siguientes problemas;

- Fraude vía sesión.
- Acceso a la red vía módem por intrusos expertos.
- Daño y destrucción a información por virus de computadora
- Uso de información valiosa del cliente por personas que la emplean para beneficio propio.
- Estaciones de trabajo olvidadas por el administrador del sistema.
- Datos sensitivos no destruidos.
- Uso de claves de acceso visibles.
- Aplicaciones críticas en equipos poco protegidos.
- Pérdida, robo, manipulación de la información.

Otro aspecto que puede propiciar el que se generen los problemas antes mencionados es el de tener procedimientos y políticas inadecuados que permitan detectar y evitar riesgos presentes y futuros.

Debido a que las causas que originan los riesgos existentes en las redes son diversas, y que sí estas no son detectadas o prevenidas en su momento pueden originar nuevos problemas, con consecuencias mayores, por tal motivo resulta importante el conocer cómo se pueden prevenir o evitar éstos problemas, los cuales pretenden plantear a detalle y analizar para encontrar sus causas y con ello proponer soluciones a los mismos.

2.4 CONOCIMIENTO DEL SISTEMA

Con el conocimiento de las características del sistema y de la problemática se puede construir el mapa conceptual del sistema figura1.6, en donde se especifican los componentes que la constituyen y las relaciones entre estos.

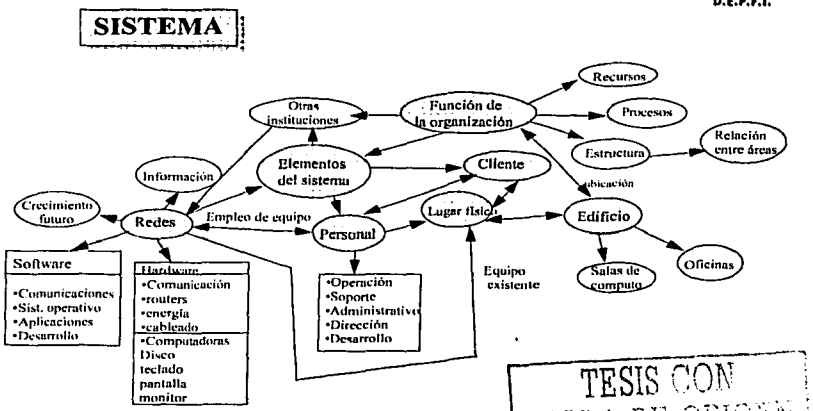

Figura 1.6 Mapa conceptual del sistema

A partir del mapa conceptual se puede observar que las redes son empleadas por personal de diferentes áreas. Y que por su función la ubicación del equipo, el acceso a la red puede encontrarse en diferentes lugares físicos, y utilizar la red de diferentes maneras; ya sea para comunicarse con otra, para acceder a aplicaciones que le permitan al personal realizar sus tareas diarias, o acceder software que utilizan para desarrollar nuevas aplicaciones, o simplemente para explotar la información que se encuentra almacenada en la misma, y que muchas de las operaciones que se efectúen en la red dependen de la función que lleve acabo la organización de su estructura, sus procesos y la relación que esta tenga con otras instituciones o áreas.

Como ya se explicó anteriormente la red local es un sistema formado por dispositivos de procesamiento de información interconectados por un medio común de comunicaciones.

Entonces se pueden enunciar los aspectos más relevantes del sistema como:

- Él poder compartir recursos trae mayores posibilidades desde el punto de vista de las aplicaciones y también disminuye los costos por usuario conectado.

- Es posible interconectar equipo de diferente tecnología, proveedor y aplicación que se encuentre en diferentes lugares físicos.

El procesamiento distribuido permite tener unidades redundantes, no depender de un único elemento central, poder procesar en el lugar donde se originan los datos y se toman las decisiones, es decir, desde cualquier punto de la red poder acceder a la información requerida.

Se tiene comunicación entre terminales, acceso a bases de datos y documentación útil, el soporte de correo electrónico, etc.

Velocidades mayores, transmisión simultánea de información de distinta naturaleza.

Distribución física del Hardware. Las LANS permiten optimar la disposición de los equipos, mejorando la interrelación entre el hombre y la máquina, los requerimientos ambientales, reduciendo costos de instalación, mejorando estéticamente los lugares de trabajo.

Simplicidad y flexibilidad de modificaciones y cambios en configuración y empleados, las altas y bajas de los elementos de la red no afectaran al resto de los usuarios, ni implican cambios en el software de control.

2.5 PLANEACIÓN DE LA SEGURIDAD

Metodología de la planeación racional

La metodología de planeación racional es la empleada para obtener el modelo a desarrollar, en la presente tesis, la cual propone la formulación del problema, ya mencionado anteriormente, continuando con la formalización y calibración del modelo. Para ello se analiza el estado actual de cada una de las partes del sistema que en este caso es la red local. Ya se menciono anteriormente, como está constituida, a partir de ésto se empezó a obtener una visión de la situación presente, para de ahí, pasar a las etapas subsecuentes: obtención de datos, generación de alternativas, evaluación y selección, por último la implantación y control.

Para llevar acabo el **análisis de riesgo** se propone una matriz donde se identifican las diferentes partes que constituyen la red y el riesgo que pueden presentar cada una, dando una propuesta de solución para su prevención una vez terminada esta matriz a través del análisis de causa efecto de cada aspecto. A las personas involucradas con el uso, mantenimiento, administración de las redes se les proporcionara la matriz para ser contestada por la persona responsable de cada aspecto en el caso de estudio para posteriormente evaluar los principales riesgos e identificar el estatus de la seguridad: Cuales son las causas que originan los problemas y sus consecuencias así como las posibles soluciones para el mismo, y el tiempo aproximado para establecer las medidas de seguridad y procedimientos para su control.

2.6 ANÁLISIS DE RIESGOS

Una vez establecidas las características del sistema y la identificación de los elementos del mismo, así como la función que desempeñan cada uno de ellos. Se llevo acabo una encuesta con el personal involucrado con el uso y administración de la red. A fin de conocer mas a detalle la problemática que se tiene en cada una de las partes de la red, las causas que los originan y sus posibles efectos. Para ello se llevo acabo un análisis de causa - efecto, y se obtuvo una lista donde se clasifican e identifican los diferentes niveles de calamidades y su impacto sobre el sistema.

Para el análisis de los riesgos detectados se empleo la técnica de Análisis de Problemas Potenciales (PPA) ya que este método esta diseñado de acuerdo a los principios sistemáticos del análisis de problemas. Primero un problema potencial es definido desde el punto de vista de una desviación entre que puede ser y que debe ser. Así la precisa naturaleza del problema potencial es determinada, seguida por una valoración del grado de riesgo del problema, su(s) causa(s), las posibilidades de ocurrencia, prevención o reducción de efectos, y planes de contingencia.

Para llegar al análisis de los problemas se siguieron los siguientes pasos:

Definir los objetivos: Que necesita ocurrir para que una solución pueda ser implementada.

Generar una matriz con los problemas potenciales por tipo (a partir del listado obtenido de los riesgos), cualquier cosa que ocurra que afecte el funcionamiento normal del sistema y sus posibles consecuencias.

Identificación de la naturaleza especifica de cada problema, para buscar las posibles causas y sus efectos.

Determinar el riesgo asociado a cada problema de acuerdo al grado de impacto que tiene sobre el sistema su presencia, para determinar en que categoría esta, a través de una evaluación de cada problema. Ya que los problemas que envuelven alto riesgo deben ser prioritarios con respecto a los problemas que tienen riesgo moderado y otros que pueden ser ignorados por no tener gran impacto sobre el sistema de presentarse.

Para determinar la naturaleza del problema es necesario de acuerdo con el modelo propuesto analizar y categorizar los diferentes riesgos, y darle una importancia de acuerdo al impacto que de presentarse tienen sobre el sistema.

El mejor camino para prevenir un problema potencial es tomar la acción para remover completamente la posible causa o al menos reducir su grado de ocurrencia.

Si generalmente pasa que algunas acciones preventivas son insuficientes en el significado de reducir o eliminar una causa. En tal situación el gerente debe desarrollar planes de contingencia que especifiquen exactamente que acciones pueden ser tomadas si el problema ocurre. Los planes de contingencia deben ser empleados para sustituir las acciones preventivas ya que prevenir acciones usualmente es menos costoso a la implementación de planes de contingencia y siempre deben ser usados al menos que sea un plan que produzca resultados más eficientes

Por último, se deben establecer normas y estándares para monitorear y controlar las medidas de seguridad ya implementadas. Para ello, se deben establecer revisiones periódicas sobre el buen funcionamiento de las mismas y el apego a éstas para que en los casos que sea necesario la modificación o actualización de alguna de ellas se lleve acabo con el tiempo requerido.

De acuerdo con este modelo se obtuvieron las siguientes tablas donde se categorizan y clasifican los diferentes tipos de riesgos, sus respectivas causas y proponer el procedimiento o solución que debe se implementado para prevenir o eliminar el riesgo.

CAPÍTULO 3

MODELO PARA LA EVALUACIÓN Y PLANEACIÓN DE LA SEGURIDAD EN REDES LOCALES

MODELO PARA LA EVALUACIÓN Y PLANEACIÓN DE LA SEGURIDAD EN REDES LOCALES

3.1 DESARROLLO Y DESCRIPCIÓN DEL MODELO

Para el desarrollo del modelo propuesto se analiza el sistema distribuido a detalle, todos los elementos involucrados en el mismo y las características de cada uno, la relación entre estos y la función que cada uno desempeña.

Una vez identificados los problemas que pueden ocurrir en cada uno de los elementos que conforman la red local, se lleva acabo el análisis **causa -efecto**, para identificar con cada problema qué causa o efecto tiene sobre el sistema, así es como surge la matriz de evaluación de la seguridad con sus correspondientes especificaciones.

Para la implementación de la seguridad se lleva acabo un análisis de los resultados obtenidos al aplicar la matriz de evaluación de la seguridad y se crea un comité de seguridad el cual se encargará de dar seguimiento a las acciones que se requieren llevar acabo para dar solución a cada uno de los problemas detectados. Crear los estándares de seguridad necesarios para el control y seguimiento de la seguridad de la red.

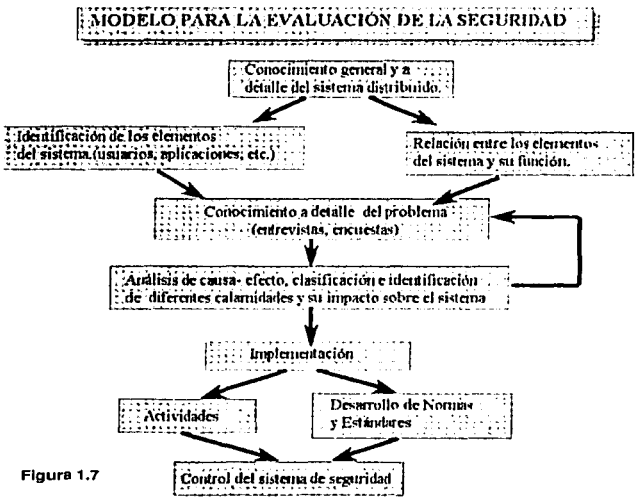

Figura 1.7

La figura 1.7 nos describe el modelo propuesto para la planeación de la seguridad en la red local. Primeramente se debe conocer a detalle cada una de las partes del sistema distribuido, para identificar los elementos que constituyen el sistema y la relación que existe entre ellos; así como la función que desempeñan cada uno de ellos dentro del sistema para que éste trabaje de manera adecuada. Una vez analizado lo anterior, como se específico en el capítulo dos de esta tesis, se procede a detectar a detalle los problemas que se pueden presentar de seguridad en la red, por medio del análisis causa-efecto se obtiene la matriz de la tabla 1.1, donde se enuncian los diferentes riesgos y su impacto sobre el sistema descrito en la misma.

Con la información obtenida de la matriz de análisis de riesgos (tabla 1.1), se propone la matriz de la tabla 1.2 para evaluar la seguridad del sistema que se desea analizar, ésta matriz debe ser aplicada a la red donde se llevará acabo su planeación partiendo de los resultados obtenidos con la matriz de evaluación (tabla 1.2). Una vez lo anterior se llevará acabo la planeación para la implementación de la seguridad del sistema, desarrollando la serie de actividades requeridas para tal fin. Dentro de las mismas actividades se debe considerar el desarrollo de las normas y estándares necesarios para llevar el control futuro del sistema una vez implantados.

3.2 MATRIZ DE ELEMENTOS DE ANÁLISIS DE RIESGO

La tabla 1.1 está compuesta por una columna de riesgo donde se especifican los diferentes tipos de riesgo que se pueden presentar en los elementos del sistema, la causa tanto física o lógica que lo origina y en la última columna se propone un procedimiento o solución a desarrollar o implantar para eliminar y controlar el riesgo.

Tabla 1.1 Matriz de elementos de análisis de riesgo

RIESGO	CAUSA FISICA (No existe)	CAUSA LOGICA (No existe)	PROCEDIMEINTO O SOLUCION
Acceso no autorizado a los archivos de red	Seguridad en el servidor	Control de acceso lógico, ni Encripción	Autorización de procesos. Administración de passwords
Actividades sobre archivos sin autorización	Establecimiento de propiedad de archivos o derechos de cada usuario sobre los archivos	Registros de actividades de cada usuario, ni firma de acceso al sistema	Administración y control de usuarios en red. Autentificación para transacciones sensitivas.
Distribución de información no autorizada	Protección de equipo.	Contraseñas de usuario de acuerdo a la información que utiliza, asignación de derechos sobre archivos y aplicaciones.	Administración y control de usuarios en red. Procedimientos para distribución de información.
Uso no apropiado de privilegios	Seguridad sobre las facilidades de red	Registro de actividades de cada usuario, ni firma de acceso al sistema	Monitoreo de actividades , passwords, asignación de privilegios de usuarios.
Perdida de la información que reside en el servidor	Respaldo de la información, disco espejo.		Establecer procedimientos y políticas para el respaldo de la información
Acceso a información importante que reside en la red	Encripción de la información	Análisis del tráfico de la red	Instalar Software de encripción en la red. Determinar información importante
Uso inapropiado de los recursos de la red	Control de acceso a los componentes importantes de la red	Establecer privilegios para el acceso a los recursos de red	Establecer un plan para controlar el acceso a los recursos de red.
Uso no autorizado del modem, línea telefónica y terminal	Dispositivos de protección del host, entre terminal - modem - teléfono. Dispositivos de autentificación de mensajes y datos	Contraseñas para el uso de módems.	Dispositivos de encripción y autentificación para acceso. Limitar el número de personas con privilegios especiales.
Situaciones de emergencia que pongan en peligro la red como inundaciones, temblores etc.	Establecer lugares fuera de sitio donde se pueda continuar con la operación normal de la red.	Contraseñas de acceso para el personal autorizado a utilizar la red.	Establecer personal responsable para casos de emergencia, planes de contingencia
Pérdida o manipulación de la información que reside en la red	Registros de empleados autorizados para acceder la información	Software de control del uso de la red, monitorio, acceso, encripción.	Clasificación de la información Implementación de estándares. Respaldos de información.

RIESGO	CAUSA FISICA (No existe)	CAUSA LOGICA (No existe)	PROCEDIMEINTO O SOLUCION
Persona que sin autorización permanentemente extrae, borra y destruye información del equipo.		Pérdida, destrucción de la información.	Uso de contraseñas, respaldo de información.
Persona que tiene acceso a información no autorizada para su puesto o área de trabajo.	Uso inadecuado de la información, manipulación de la misma		Restricción de acceso a la información. Administración de usuarios y cuentas.
Uso inadecuado del software que reside en la red	Sin autorización se utiliza el software de la empresa para beneficios personales		Políticas y estándares para el uso de software, control de acceso al mismo. Bitácoras de acceso.
Acceso a los sistemas de comunicación cuando hay conexión fuera de red		cuando se transmite información por los medios de comunicación al exterior de la red se puede acceder a la misma	Encriptación de los datos que viajan fuera de la red. Segmentación de red y control de rutes. Seguridad dial up.
Daño físico del procesador central de la red	Fallas del equipo que controla los recursos de la red.		Mantenimiento preventivo al equipo, monitoreo del mismo, equipo paralelo que pueda entrar en operación en caso de fallas
Daños, pérdida de los recursos de la red.	Ubicación inadecuada del equipo de red control de acceso al mismo.		Control de acceso a los recursos de la red, estándares para la ubicación de recursos. Contratación de seguros.
Daño del software e información que reside en la red por virus		Información contaminada por virus.	Respaldo de información fuera de sitio, software antivirus. reporte de incidentes.
Mala configuración de los recursos de la red.	Pérdida de tiempo por no poder acceder a los recursos de red.	Software que reside en la red no cuenta con licencias ni la configuración adecuada.	Licencias de software, control de versiones, apego a administración y configuración de software.

Tabla 1.1 Matriz de elementos de análisis de riesgo

3.3 MATRIZ DE EVALUACIÓN DE LA SEGURIDAD

De acuerdo con la tabla 1.2 anterior se analizaron y clasificaron los principales riesgos, sus causas y la propuesta de solución generando la siguiente propuesta de diagnostico de seguridad, que permita detectar los riesgos para llevar acabo la planeación de la seguridad de la red.

Tabla 1.2 Matriz de evaluación de la seguridad

Elemento de seguridad	Diagnóstico	Del riesgo	Mecanismo o tipo de control de seguridad sugerido
	Existe	No existe	
Estándares y políticas de seguridad			**Son lineamientos que permiten controlar y supervisar la seguridad de la red.**
Estándares y políticas desarrolladas para el uso y operación de la red			Desarrollo de políticas y estandadares para cada elemento de la red. Capacitación, concientización y motivación.
Responsable y propietario de la información que reside en la red.			Establecer documentos que respalden la propiedad o tulización de la información de la red.
Administrador de la seguridad en la red			Existan procedimientos y personal asignado para la seguridad de la red
Bitácoras de control de entrada y salidas			Bitácoras automatizadas o no del acceso a los recursos de la red.
Auditorias permanentes sobre el uso de red			Establecer revisiones anuales sobre los aspectos de seguridad a controlar.
Administración de acceso de usuarios a la red			Personal encargado de la administración de usuarios de red
Equipo asegurado			Contratos para asegurar el equipo de red
Seguridad en las redes de comunicación			proteger los dispositivos de comunicación de acceso físico , encripción de datos que viajan en los mismos.
Autentificación de usuarios de red			Políticas y Bitácoras para asignación y cambios de passwords.
Segmentación de red y control de rutas			Diagramación de la red y ubicación de los recursos.
Seguridad dial up			Encripción de datos sensitivos por harware y bitácoras en los equipos de comunicación.
Protección de sistemas de comunicación			Estándares y políticas para protección de sistemas de comunicación
Identificación y autentificación de usuarios			Políticas para el acceso de usuarios a la red.
Verifiar autentificación cliente y servidor			Monitoreo diario a través del software de red del accceso a las computadoras y servidor.
Administración de usuarios y passwords			Desarrollo de políticas para el uso y asignación de passwords

Elemento de seguridad	Diagnóstico	Del riesgo	Mecanismo o tipo de control de seguridad sugerido
	Existe	No existe	
Planes de contingencia			Contar con planes de contingencia documentados y actualizados.
Detección de accesos no autorizados			Contar con un software de detección de intrusos en la red.
Protección de passwords			Proteger las claves de usuarios y responsabilizar de su uso a los usuarios
Administración de sistemas			Mantener un inventario de los sistemas desarrollados o comprados y su documentación.
Monitoreo de eventos			Mantener un registro de los eventos inadecuados del suso de los recursos de la red.
Monitoreo de sistemas y aplicaciones.			Mantener un registro al diario de los accesos a los sistemas y aplicaciones.
Protección de software			Acciones y políticas para proteger el software.
Monitoreo y verificación del uso del software estandar de la empresa.			Verificar periódicamenre que el software instalado sea el estandar de la empresa.
Aseguramiento de software original			Políticas y procedmientos para el uso empleo y manejo de software.
Software antivirus			Actulizar las versiones de antivirus y mantenerlas habilitadas para cualquier problema.
Respaldos y procedmientos de emergencia			Desarrollar políticas para el uso de respaldos en caso de emergencia.
Reporte de incidentes de software.			Mantener una bitácora sobre incidentes de software.
Control de licencias de software			Actualizar el inventario de software con sus licencias respectivas
Control de versiones			Actualizar una bitácora con la actulización de versiones de software
Copias de protección			Tener respaldos del software se emplea en la empresa
Protección de información, datos, sistemas y aplicaciones			Garantizar la integridad de los datos, información y aplicaciones que residen en la red.
Responsabilidades de desarrolladores, usuarios de sistemas			Establecer la responsabilidad que cada usuario de la red tiene sobre el software y aplicacionos que utiliza en su labor diaria.
Estándares de seguridad			Elaborar estándares de seguriadad para la protección de información, datos, sistemas y aplicaciones.
Procedimientos de control			Revisar y tener actualizados los controles para el uso y utilización de información en la red
Documentación de sistemas			Tener en un lugar seguro las licencias y documentación de sistemas y aplicaciones.
Planes de contingencia y pruebas			Desarrollar y documentar planes de contingencia

Elemento de seguridad	Diagnóstico	Del riesgo	Mecanismo o tipo de control de seguridad
	Existe	No existe	sugerido
Resplado fuera de sitio			Realizar respaldos fuera de sitio diariamente de la información estratégica de la empresa.
Equipos y servicios de recuperación en contingencia			Contar con equipos y servicios bioen especificados para una contingencia.
Tolerancia a fallas			Tener equipo de toleración a fallas en los lugares donde sea importante la operación continua del mismo.
Protección de copias			Realizar copias de protección del software y apliaciones que se utilice para la operación diaria de la empresa.
Prevención de emergencias			Difundir y simular planes de contingencia para emergencias.
Sistemas de seguridad en la red y equipo			Proteger el equipo que se encuentra instalado en la red.
Controles de acceso lógico para limitar el acceso a servidores			Deben de existir restricciones de acceso llógico para el uso de servidores.
Restrincción de acceso a áreas sensitivas			Las áreas más vulnerables de la red deben estar restringidas.
Limitar el acceso físico para computadoras y servidores.			El acceso a los servidores y computadoras debe estar limitado para el uso de personal autorizado.
Existen barreras físicas apropiadas para el equipo de cómputo.			El equipo de cómputo debe estar restringido al uso del personal para el que fue asignado.
Procedimientos de control para puntos de acceso crítico.			Deben existir procedimientos para el uso y acceso a equipo crítico de la red.
El equipo se encuentra protegido contra daño, acceso y uso no autorizado.			Se debe tener la protección y los registros de daño o uso no autorizado del equipo
Los servidores y equipo especial cuentan con seguridad adicional (cuartos cerrados y gabinetes)			Todo el equipo que garantice la continuidad del servicio de red debe contar con medidas de seguridad adecuadas.
Existen servidores de respaldo en caso de falla del servidor principal.			Existir equipos que garanticen la continuidad del servicio en caso de fallas del servidor.
Administración y control de recursos			Tener actulizados y contar con una bitácora sobre los recursos de la red y su utilización.
Estándares de red			Mantener actualizados los estándares de la red.
Protección de equipo de cómputo.			Proteger los equipos de cualquier siniestro o falla que pudiera afectar su funcionamiento normal.

3.4 IMPLANTACIÓN DE LA SEGURIDAD

Una vez detectado el tipo de problema de seguridad que tienen la red, a través de la matriz propuesta para este análisis se debe crear un comité con las áreas o personas involucradas en estos aspectos para:

- Definir la asignación de responsabilidades
- Elaborar un plan para llevar acabo la implementación que incluya las fechas y los recursos asignados a cada tarea
- Participar en la determinación de las políticas de seguridad.
- Hacer el seguimiento de los logros e incluir la aplicación en detalle de las medidas correctivas
- Revisar y comprobar en forma periódica la suficiencia de la seguridad en la red a través de la implementación de controles.

La existencia de este comité esta relacionada con el hecho de que en muchos casos la seguridad deficiente, se debe a la falta de compromiso por parte de todos los que están relacionados con el uso de la información software y hardware de red.

La única forma de asegurar el compromiso es por medio de la participación de todos los afectados para la implementación de las medidas de seguridad, su diseño y aplicación.

Dentro de éste contexto, el uso de un comité es muy aproplado.

Las acciones a realizar por este comité deben considerar los siguientes aspectos:

1. - Formulación de un plan de acción, para llevar acabo la planeación de la implementación de la seguridad en la red.

2. - Garantizar la seguridad efectiva en computación dentro de la red.

3- Diseñar y aplicar los planes efectivos.

4.- Verificar los niveles de efectividad de la seguridad por medio de la revisión y control continuo de las medidas realizadas.

5. - Si es necesario y no existe, generar el procedimiento, norma o estándar para prevenir y monitorear las medidas de seguridad implementadas.

3.5 ESTÁNDARES Y POLÍTICAS DE SEGURIDAD

Es importante en la etapa de implantación de la seguridad al sistema, el incorporar políticas y estándares de seguridad como una parte integral de la actividad de planeación computacional a largo plazo. Los puntos claves a considerar son:

1. - El impacto de la seguridad en computación sobre la estrategia del equipo y los programas existentes en la red.

2. - Las consideraciones de la seguridad de las terminales respecto a:

- Los controles de la aplicación
- Los requisitos físicos y la ubicación.
- La estrategia de las redes, la seguridad y el respaldo.

3. - Los estándares de control de la aplicación, en especial los de reinicio y de respaldo.

4. - Los estándares de los datos y del diseño de archivos.

5. - La función de las auditorías interna y externa y los requisitos durante las fases de diseño, aplicación y operación de la red.

Los aspectos de seguridad deben ser considerados de manera rutinaria en todos los elementos del sistema.

Estándares de seguridad para redes locales

Los estándares deben ser una guía necesaria para que los empleados actuen de tal forma que puedan proteger la información del negocio. Que al final los estándares puedan ser publicados de diferentes formas.

Los estándares deben definir las medidas de protección generales requeridas para todas las circunstancias. Los estándares de seguridad de redes deben ser elementos de protección que sigan los siguientes cuatro niveles.

1. - Niveles en el área de la red, usando un manejo central de la red que pueda facilitar la encripción central de la red, las llaves de protección para la transmisión de datos para autenticación de usuarios en los nodos de la red y que pueda monitorear la actividad de la red.

2. - A nivel computadora central debe proveer la seguridad de paquetes de software que usan los usuarios para identificar accesos.

3. - A nivel LAN usar software que facilite la comunicación entre servidores.

4. - En el ámbito de estaciones de trabajo, el software debe correr en computadoras personales o en estaciones inteligentes.

CAPÍTULO 4

APLICACIÓN DEL MODELO

APLICACIÓN DEL MODELO

4.1 CARACTERÍSTICAS DE LA RED

La red que se analizó es de una empresa de giro financiero. La cual tiene 30 estaciones de trabajo y por lo tanto el número de personas que la utilizan es el mismo, todas las estaciones de trabajo están ubicadas en dos pisos de un mismo edificio, existen cuatro áreas importantes que constantemente hacen uso de la red; la contable, la de atención al cliente, administrativa, y de recursos humanos.

Cuenta con dos servidores uno donde reside la información que maneja a diario la empresa y el otro que está como respaldo. Tiene conectadas cinco impresoras dos de ellas remotas.

El sistema operativo de la red es Windos NT el cual ofrece seguridad por medio de cuentas y contraseñas, contiene protección para directorios, archivos, y periféricos, establece derechos sobre determinadas operaciones de los usuarios, permite administrar los usuarios que accedan la red. Todos los usuarios tienen acceso a internet y correo electrónico.

El área de sistemas de esta empresa se encarga de administrar el buen funcionamiento y uso de la red, mantener y soportar el software y hardware que está instalado en la red, así como dar asesoría a los usuarios.

Para la operación diaria de las compañías se requiere el uso de la red de manera ininterrumpida ya que ellos acceden y actualizan a diario la información que se encuentra en la red, por el grado de importancia de esta información se requiere realizar el respaldo diario de la misma.

4.2 APLICACIÓN DEL MODELO

Para llevar acabo el análisis de la seguridad la red se proporcionó la matriz de riesgo propuesta al responsable del área de sistemas de la empresa para revisar cada uno de los aspectos a considerar y resolver dudas.

El responsable de la red debe revisar las respuestas de la matriz y si es necesario involucrar el personal dueño o responsable del software o aplicaciones que residen en la red o utilizan el equipo de cómputo en su labor diaria, para estar seguro que la matriz es contestada adecuadamente. Además, se recomienda que los resultados obtenidos sean analizados por personal externo al área de sistemas para tratar de que las respuestas sean completamente imparciales y realmente reflejen el estado general del sistema en estudio.

Cuando se tenga contestada la matriz se debe analizar a detalle la problemática existente en la empresa en cuanto a seguridad. De acuerdo con los resultados obtenidos llevar acabo la planeación para la implementación de la seguridad a corto, mediano y largo plazo, de acuerdo a la prioridad de cada uno de los problemas detectados, estableciendo fechas compromiso y personal involucrado para cada una de las acciones a realizar.

Es importante establecer un comité de seguridad que se encargue de dar seguimiento a las acciones que cada una de las áreas llevará acabo con el fin de que se tenga un control de los avances, con respecto a cada problema detectado y se concluyan en la fecha estipulada. También éste comité permitirá clasificar y asignar el grado de importancia a cada problema, para evitar el mayor número de riesgos o establecer las medidas compensatorias con respecto a los daños o problemas que se llegaran a presentar antes de la implantación de las medidas preventivas correspondientes.

4.3 MATRIZ DE EVALUACIÓN DE LA SEGURIDAD

La matriz propuesta cuenta con tres columnas principales donde se especifica el elemento de seguridad a ser revisado en la red, si este ya fue implementado en él diagnostico de riesgo se debe contestar que ya existe, de lo contrario la respuesta es que no existe. En la tercera columna se explica que tipo de mecanismo o control debe ser desarrollado, o considerado para prevenir o eliminar el riesgo detectado, en esta columna se debe poner atención en la explicación sobre lo que se tiene que realizar para llevar acabo el control de la seguridad, y es sobre lo que deberá trabajar el comité de seguridad para dar solución a ese problema y llevasr acabo la planeación a corto, mediano y largo plazo para la implantación de la seguridad en la red.

Tabla 1.3 Matriz de evaluación de la seguridad

Elemento de seguridad	Diagnóstico	Del riesgo	Mecanismo o tipo de control de seguridad sugerido
	Existe	No existe	
Estándares y políticas de seguridad			**Son lineamientos que permiten controlar y supervisar la seguridad de la red.**
Estándares y políticas desarrolladas para el uso y operación de la red		X	Desarrollo de políticas y estandadares para cada elemento de la red. Capacitación, concientización y motivación.
Responsable y propietario de la información que reside en la red.		X	Establecer documentos que respalden la propiedad o tulización de la información de la red.
Administrador de la seguridad en la red	X		Existan procedimientos y personal asignado para la seguridad de la red
Bitácoras de control de entrada y salidas	X		Bitácoras automatizadas o no del acceso a los recursos de la red.
Auditorias permanentes sobre el uso de red		X	Establecer revisiones anuales sobre los aspectos de seguridad a controlar.
Administración de acceso de usuarios a la red	X		Personal encargado de la administración de usuarios de red
Equipo asegurado	X		Contratos para asegurar el equipo de red
Seguridad en las redes de comunicación			proteger los dispositivos de comunicación de acceso físico , encripción de datos que viajan en los mismos.
Autentificación de usuarios de red		X	Politicas y Bitácoras para asignación y cambios de passwords.
Segmentación de red y control de rutas	X		diagramación de la red y ubicación de los recursos.
Seguridad dial up	X		Encripción de datos sensitivos por harware y bitácoras en los equipos de comunicación.
Protección de sistemas de comunicación	X		Estándares y políticas para protección de sistemas de comunicación
Identificación y autentificación de usuarios			Políticas para el acceso de usuarios a la red.
Verificar autentificación cliente y servidor	X		Monitoreo diario a través del software de red del acceso a las computadoras y servidor.
Administración de usuarios y passwords		X	Desarrollo de políticas para el uso y asignación de passwords
Planes de contingencia	X		Contar con planes de contingencia documentados y actualizados.
Detección de accesos no autorizados		X	Contar con un software de detección de intrusos en la red.
Protección de passwords		X	Proteger las claves de usuarios y responsabilizar de su uso a los usuarios
Administración de sistemas		X	Mantener un inventario de los sistemas desarrollados o comprados y su documentación.

Elemento de seguridad	Diagnóstico	Del riesgo	Mecanismo o tipo de control de seguridad sugerido
	Existe	No existe	
Monitoreo de eventos	X		Mantener un registro de los eventos inadecuados del suso de los recursos de la red.
Monitoreo de sistemas y aplicaciones.		X	Mantener un registro al diario de los accesos a los sistemas y aplicaciones.
Protección de software			Acciones y políticas para proteger el software.
Monitoreo y verificación del uso del software estandar de la empresa.		X	Verificar periódicamenre que el software instalado sea el estandar de la empresa.
Aseguramiento de software original		X	Políticas y procedmientos para el uso empleo y manejo de soltware.
Software antivirus	X		Actulizar las versiones de antivirus y mantenerlas habilitadas para cualquier problema.
Respaldos y procedmientos de emergencia	X		Desarrollar políticas para el uso de respaldos en caso de emergencia.
Reporte de incidentes de software.		X	Mantener una bitácora sobre incidentes de software.
Control de licencias de software		X	Actualizar el inventario de software con sus licencias respectivas
Control de versiones		X	Actualizar una bitácora con la actulización de versiones de software
Copias de protección		X	Tener respaldos del software se emplea en la empresa
Protección de información, datos , sistemas y aplicaciones			Garantizar la integridad de los datos, información y aplicaciones que residen en la red.
Responsabilidades de desarrolladores, usuarios de sistemas		X	Establecer la responsabilidad que cada usuario de la red tiene sobre el software y aplicaciones que utiliza en su labor diaria.
Estándares de seguridad		X	Elaborar estándares de seguriadad para la protección de información, datos, sistemas y aplicaciones.
Procedimientos de control		X	Revisar y tener actualizados los controles para el uso y utilización de información en la red
Documentación de sistemas		X	Tener en un lugar seguro las licencias y documentación de sistemas y aplicaciones.
Planes de contingencia y pruebas		X	Desarrollar y documentar planes de contingencia
Respaldo fuera de sitio	X		Realizar respaldos fuera de sitio diariamente de la información estratégica de la empresa.
Equipos y servicios de recuperación en contingencia		X	Contar con equipos y servicios bioen especificados para una contingencia.
Tolerancia a fallas	X		Tener equipo de toleración a fallas en los lugares donde sea importante la operación continua del mismo.

Elemento de seguridad	Diagnóstico	Del riesgo	Mecanismo o tipo de control de seguridad sugerido
	Existe	No existe	
Protección de copias		X	Realizar copias de protección del software y apliaciones que se utilice para la operación diaria de la empresa.
Prevención de emergencias		X	Difundir y simular planes de contingencia para emergencias.
Sistemas de seguridad en la red y equipo			Proteger el equipo que se encuentra instalado en la red.
Controles de acceso lógico para limitar el acceso a servidores	X		Deben de existir restricciones de acceso llógico para el uso de servidores.
Restrincción de acceso a áreas sensitivas		X	Las áreas más vulnerables de la red deben estar restringidas.
Limitar el acceso físico para computadoras y servidores.		X	El acceso a los servidores y computadoras debe estar limitado para el uso de personal autorizado.
Existen barreras físicas apropiadas para el equipo de cómputo.		X	El equipo de cómputo debe estar restringido al uso del personal para el que fue asignado.
Procedimientos de control para puntos de acceso crítico.		X	Deben existir procedimientos para el uso y acceso a equipo crítico de la red.
El equipo se encuentra protegido contra daño, acceso y uso no autorizado.		X	Se debe tener la protección y los registros de daño o uso no autorizado del equipo
Los servidores y equipo especial cuentan con seguridad adicional (cuartos cerrados y gabinetes)		X	Todo el equipo que garantice la continuidad del servicio de red debe contar con medidas de seguridad adecuadas.
Existen servidores de respaldo en caso de falla del servidor principal.		X	Existir equipos que garanticen la continuidad del servicio en caso de fallas del servidor.
Administración y control de recursos	X		Tener actulizados y contar con una bitácora sobre los recursos de la red y su utilización.
Estándares de red		X	Mantener actualizados los estándares de la red.
Protección de equipo de cómputo.		X	Proteger los equipos de cualquier siniestro o falla que pudiera afectar su funcionamiento normal.

4.4 RESULTADOS DE LA APLICACIÓN DEL MODELO

Como se puede analizar a partir de los resultados de la matriz de evaluación de la seguridad (tabla 1.3), se obtuvieron los siguientes riesgos o vulnerabilidades en la red:

No existe seguridad física en los dispositivos conectados al servidor ni en los que se encuentran de forma remota. (impresoras, equipo de comunicaciones, etc)

No existe un área restringida para acceso al servidor por lo tanto este no tiene seguridad física

Existen muy pocas políticas y estándares de seguridad para:

La asignación de passwords .

Reportes de incidentes de *software.*

Control de licencias de software, versiones y copias de protección.

Responsabilidades de desarrolladores, usuarios de sistemas.

Responsables y propietario de la información de la red.

Protección a datos de diagnóstico de la red.

Obligar al uso de productos estándares de *hardware* y *software.*

Monitoreo de apego a políticas.

Uso de licencias corporativas.

Uso de servidores separados dependiendo de su función.

Plan de recuperación en caso de que los mecanismos de autentificación fallen.

Procedimientos para control de versiones de *software.*

Efectuar periódicamente autoevaluaciones de seguridad informática.

Registros de discrepancias sobre políticas

Desarrollo de estándares de seguridad para apoyo a activos informáticos

4.5 PROPUESTA DE SOLUCIÓN

Todos estos riesgos fueron detectados al aplicar la matriz en esta empresa, y se entrego el resultado al área de sistemas, así como a la dirección para establecer un comité de seguridad y el plan de acción a realizar para el desarrollo de los estándares, y políticas de seguridad que fue el principal problema encontrado.

Las acciones que se llevaron acabo para la planeación a corto plazo fueron:

- El área de sistemas se encargo de establecer la seguridad física para los dispositivos de la red que lo requerían y de restringir el acceso a los mismos. Así como de elaborar políticas para su acceso esto fue prioritario en la planeación para la implementación de la seguridad. Ya que las condiciones en las que se encontraba eran altamente riesgosas por la información que maneja la empresa y debido a que es una red pequeña no representaba mucho problema el encontrar un área adecuada para tal fin.

- Así mismo se oriento al comité de seguridad ya formado sobre las políticas que tenían mayor prioridad y el cómo empezarlas a desarrollar e implementar, para posteriormente difundirlas con el personal de la empresa.

- Registro y actualización de las licencias corporativas.

- Desarrollo de planes de recuperación.

- Procedimientos para el control de versiones de software.

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1	**- Planeación a corto plazo para la seguridad de la red de la empresa**	**25 días**	**lun 03/06/02**	**vie 05/07/02**		
2	**- Seguridad física para los dispositivos de red**	**21 días**	**lun 03/06/02**	**lun 01/07/02**		**2 personas de sistemas**
3	Implementación de fuentes de alimentación duales	5 días	lun 03/06/02	vie 07/06/02		
4	Establecimiento de control de acceso físico	10 días	lun 10/06/02	vie 21/06/02	3	
5	**- Elaboración de políticas de acceso físico**	**11 días**	**lun 17/06/02**	**lun 01/07/02**		**Gerente de sistemas**
6	Desarrollo de políticas para acceso al equipo	4 días	lun 17/06/02	jue 20/06/02		
7	Desarrollo de políticas para casos de contingencia	3 días	vie 21/06/02	mar 25/06/02	6	
8	Desarrollo de políticas para uso del equipo	3 días	mié 26/06/02	vie 28/06/02	7	
9	Autorización e implantación de políticas	1 día	lun 01/07/02	lun 01/07/02	8	Comité de seguridad
10	Desarrollo de planes de recuperación	4 días	mar 02/07/02	vie 05/07/02	2	Gerente de sistemas
11	Registro y actualización de licencias corporativas	5 días	lun 03/06/02	vie 07/06/02		Gerente de sistemas
12	Elaboración de procedimientos para control de licencias de software	5 días	lun 03/06/02	vie 07/06/02		Gerente de sistemas

Las actividades para la planeación a mediano plazo fueron:

- Desarrollo de estándares y políticas para la asignación de passwords, reportes de incidentes de software, control de licencias, versiones y copias de protección.
- Asignación de responsabilidades a desarrolladores y usuarios de sistemas sobre el software y equipo de red.
- Protección y utilización de software para el monitoreo de la red.
- Procedimientos para el registro de eventos que afectan la seguridad del sistema
- Procedimientos para la evaluación de la seguridad.

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1	**- Planeación a mediano plazo para la seguridad de la red de la empresa**	**63 días**	**lun 03/06/02**	**mié 28/08/02**		
2	**- Desarrollo de estándares y políticas**	**45 días**	**lun 03/06/02**	**vie 02/08/02**		
3	Para asignación de passwords	5 días	lun 03/06/02	vie 07/06/02		Comité de seguridad
4	Reporte de insidentes de software	5 días	lun 10/06/02	vie 14/06/02	3	Comité de seguridad
5	Control de licencias de software y versiones	10 días	lun 17/06/02	vie 28/06/02	4	Gerente de sistemas
6	Control de copias de protección	5 días	lun 01/07/02	vie 05/07/02	5	Gerente de sistemas
7	Asignación de responsabilidades a usuarios sobre software	10 días	lun 08/07/02	vie 19/07/02	6	Comité de seguridad
8	Asignación de responsabilidades a usuarios sobre equipo de red	10 días	lun 22/07/02	vie 02/08/02	7	Comité de seguridad
9	Autorización e implantación de políticas	3 días	vie 09/08/02	mar 13/08/02	2	Comité de seguridad
10	**- Instalación y utilización de software de monitoreo de red**	**8 días**	**lun 05/08/02**	**mié 14/08/02**	2	
11	Evaluación de software a comprar	3 días	lun 05/08/02	mié 07/08/02		Gerente de sistemas
12	Pruebas del software	3 días	jue 08/08/02	lun 12/08/02	11	Personal de sistemas
13	Instalación software	2 días	mar 13/08/02	mié 14/08/02	12	Personal de sistemas
14	Procedimientos para el registro de eventos sujetados en la red	5 días	jue 15/08/02	mié 21/08/02	10	Gerente de sistemas
15	Procedimientos para la evaluación de la seguridad de la red	5 días	jue 22/08/02	mié 28/08/02	14	Gerente de sistemas

Dentro de la planeación a largo plazo se considero:

- Monitoreo cada mes sobre el apego a políticas y estándares de seguridad desarrodas e implantadas en las areas de la empresa.
- Llevar acabo cada seis meses la auditoria informática de la empresa.
- Revisión cada seies meses de la seguridad de la red, utilizando la matriz propuesta, esto permitirá validar la vulnerabilidad del sistema una vez implantada su seguridad.

Debido a que esta empresa no contaba con la mayoría de las políticas que requería la mayor parte de la planeación para la implementación de la seguridad fue enfocada al desarrollo e implementación de las mismas.

Para el desarrollo de las políticas y estándares se requiere involucrar a todas las áreas de la empresa. Por esta razón aunque se contaba con personal adecuado no se pudo avanzar rápidamente. Debido a que el personal de cada área destina la mayor parte de su tiempo a cumplir las funciones propias de su área y por lo mismo esto se considero como un trabajo extra. Lo cual implico que el desarrollo de las policías y su implementación fuera lento, pero al final lo importante es que por fin la empresa contó con un esquema de seguridad adecuado y completo.

Se apoyo en el desarrollo de actividades para la implementación de las políticas.

Por ultimo se dieron recomendaciones sobre el monitoreo del apego a las políticas y su actualización.

La auditoria informática y el monitoreo continuo para el cumplimiento de estándares, así como la actualización de estos.

Una vez realizadas todas las acciones mencionadas en la planeación, los insidentes en aspectos de seguridad se vieron reflejados con las medidas implantadas, ya que antes no había forma de registrarlos, estos son escasos pero se tienen las políticas para llevar acabo acciones concretas cuando se presentan.

La empresa tiene un nivel de seguridad que le permitirá si en algun momento se llegara a presentar un riesgo impotante, conservar su información y seguir operando esto representa para la empresa el activo más importante e invaluable por lo que el beneficio es considerable con respecto a los costo que implico la implantación de la seguridad.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Una vez aplicado el modelo se observa que es una herramienta que permite evaluar los factores de riesgo en redes locales en forma rápida y precisa.

Apartir del análisis de seguridad de los sistemas distribuidos se pueden detectar los requerimientos de seguridad del mismo.

La planeación de la seguridad se puede llevar acabo a partir de los resultados obtenidos con el modelo propuesto, ya que al tener una visión precisa de los problemasen la red, se puede empezar a formar el comité de seguridad si es que no existe o si ya se tiene, se llevan acabo las acciones específicas a realizar para cubrir los problemas y se establecen fechas, así como personal responsable de cada actividad.

La planeación de la seguridad en los sistemas distribudos permite conocer las actividades a realizar y el tiempo en el cual estará protegido el sistema, como consecuencia se obtine la confiabilidad de la información que reside en él.

Los dueños de las redes conocen las características de seguridad de la misma y empiezan a preocuparse por corregir aquellos problemas encontrados. Así como se familiarizan mas con los aspectos de seguridad que implica el tener una red instalada para sus operaciones diarias. Esto genera mayor confiabilidad en lo que se tiene instalado, por otro lado tienen mayor control de todos sus recursos e información.

Para la red analizada uno de los principales problemas que se presentaron en el desarrollo e implementación de estándares y políticas de seguridad, fue el compromiso de las personas involucradas para el desarrollo de las mismas, ya que como acción extra al trabajo que realizan a diario tenían que dedicar cierto tiempo al desarrollo de las mismas y ésto genera molestia. En este caso se debe capacitar al personal sobre la importancia de las mismas y los beneficios que obtendrá la empresa y cada una de las áreas.

RECOMENDACIONES

Se recomienda insistir con el comité involucrado en el desarrollo de las políticas y Estándares, en la importancia de la seguridad de la red para que se sientan comprometidos a dar solución a los problemas de seguridad.

Asignar personal dedicado para el desarrollo e implementación de las soluciones de seguridad cuando sea posible por parte de la empresa debido a la importancia y riesgo que el de no llevar acabo la solución al problema implica para la empresa.

Cumplir con las fechas y actividades acordadas en la planeación para la implementación de la seguridad debido al impacto que esta puede tener si se llegara a presentar un problema cuando aún no se han implementado todas las medidas de seguridad.

Evaluar la importancia de cada problema encontrado para establecer prioridades de solución a cada uno, para cubrir los riesgos que pueden tener mayor impacto sobre el buen funcionamiento de la red y las operaciones que se realizan a diario en la misma, amanera de cubrir en forma oportuna los más importantes.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Computer Networks and open Systems
Cassel,Lilian N.
Sudbury, Massachusetts, Jones and Bartlet, 2000.

Disaster Recovey Planning: Networks, Telecomunications and Data comunications.
Bates,1994.

Hackerd secretos y soluciones para la seguridad de redes
Stuart Mcclure
Joel Scambray
George Kurtz
McGraw Hill,2002.

La seguridad de una red con Netware 5
Jose Luis Raya
Cristina Raya
Edit. Alfaomega, Octubre 2000.

Network Security
Charlie Kaufman
Radia Perlman
Mike Speciner
Prentice Hall, 1995.

Network security Esssentials
Stallings, William
Pretince hall,2000.

Piratas Ciberneticos
Jesus de Marcelo Rodao
Alfa Omega,2001.

Project Management
Harold Kerner, PHD
Wilwy.2001.

Redes de computadoras, una guía prática
Michael J. Palmer
Thomson Learning. 2001.

Seguridad e integradad de datos
Tom Stears,Marc Farly, Jeffrey Hsu.
Mc.Graw Hill, 1998.

Servidores Seguros
http://www.htmlweb.net/seguridad/ssl/ssl_II.html
Criptografía, España,2002.
http://www.htmlweb.net/seguridad/seguridad.html
LucianoMoreno.2002.

Técnicas para Análisis de Sistemas
Sánchez G. Gabriel. 1990.

Un sistema de metodologías de planeación
Fuentes Zenón Arturo. 1995.

Virus informáticos
David Harley
Robert Slade
Urs.E. Gattiker
McGraw-hill,2002.