INSTITUTO TECNOLOGICO DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS GUADALAJARA
UNIVERSIDAD VIRTUAL

DISEÑO DE UNA ESTRATEGIA PARA IMPLEMENTAR UN SISTEMA DE CONTROL DE ACCESOS PARA LA PROTECCION Y SEGURIDAD DE UNA RED CORPORATIVA

T e s i s

Presentada por

JORGE MANUEL VALENCIA MARTINEZ

Presentada ante la Dirección Académica
de la **Universidad Virtual** del
Instituto Tecnológico y de Estudios Superiores de Monterrey

como requisito para optar al título de

MAESTRO EN ADMINISTRACION DE TECNOLOGIAS DE INFORMACION

Diciembre de 1999
Maestría en Administración de Tecnologías de Información

INSTITUTO TECNOLOGICO DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS GUADALAJARA
UNIVERSIDAD VIRTUAL

DISEÑO DE UNA ESTRATEGIA PARA IMPLEMENTAR UN SISTEMA DE CONTROL DE ACCESOS PARA LA PROTECCION Y SEGURIDAD DE UNA RED CORPORATIVA

T e s i s

Presentada por

JORGE MANUEL VALENCIA MARTINEZ

Presentada ante la Dirección Académica
de la **Universidad Virtual** del
Instituto Tecnológico y de Estudios Superiores de Monterrey

como requisito para optar al titulo de

MAESTRO EN ADMINISTRACION DE TECNOLOGIAS DE INFORMACION

Diciembre de 1999
Maestría en Administración de Tecnologías de Información

Agradecimientos.

A Dios, por haberme permitido cumplir mis objetivos.

A Ale, mi adorable esposa, por su amor y comprensión en todo este tiempo.

A Ana Sofy, mi querida hija, por su ternura y alegría.

A mis padres, por su cariño y apoyo incondicional.

A mi asesor, PhD. Francisco Medina, por su siempre atención y orientación que me permitieron cumplir este objetivo tan importante en mi vida.

A Ignacio Santiago y Jesús Vázquez, por su valiosa participación en mi comité de tesis como sinodales y por su ayuda en el logro de este reto.

RESUMEN

DISEÑO DE UNA ESTRATEGIA PARA IMPLEMENTAR UN SISTEMA DE CONTROL DE ACCESOS PARA LA PROTECCION Y SEGURIDAD DE UNA RED CORPORATIVA.

DICIEMBRE DE 1999

JORGE MANUEL VALENCIA MARTINEZ

INGENIERO EN COMPUTACION.
UNIVERSIDAD AUTONOMA DE GUADALAJARA

MAESTRO EN ADMINISTRACION DE TECNOLOGIAS DE INFORMACION
INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY.

Dirigida por el PhD. Francisco Medina.

En la última década, el número de computadoras en uso ha incrementado exponencialmente. Las computadoras han sido un elemento vital en nuestro entretenimiento y educación, y lo más importante, en como hacemos negocio. Parece obvio que el resultado del crecimiento explosivo en el uso de las computadoras será el crecimiento, más acelerado, del deseo y la necesidad de que esas computadoras se hablen entre sí.

El crecimiento de esta industria se ha dado por dos factores, los cuales tienen diferentes objetivos. El primer factor ha sido la investigación y desarrollo, así como los laboratorios; estos grupos siempre tienen la necesidad de compartir archivos de información, correos electrónicos, etc. a través de las diferentes áreas.

El segundo factor ha sido los intereses de negocio. Hace algún tiempo, sus intereses eran compartir la información dentro de sus instalaciones. En los últimos años, los negocios comenzaron con la necesidad de compartir la información a largas distancias, en áreas lejanas.

Esta es una situación ideal: los negocios, gobiernos e individuos comunicándose entre sí alrededor del mundo, cuando en la realidad esta situación está haciendo cambiar el estatus de algunos pequeños problemas, de baja prioridad a extremadamente importantes. La seguridad es probablemente el más conocido de estos problemas.

Cuando las empresas envían información privada a través de la red, le dan gran importancia a que esta llegue a su destino intacta y sin que halla sido interceptada. Los individuos que envían información personal, desean un medio de comunicación seguro. Finalmente, conectar los sistemas a la red, puede exponer al sistema en sí a ataques y el riesgo de perder la información es alto.

INDICE DE CONTENIDO.

INDICE DE TABLAS.

INDICE DE FIGURAS.

CAPITULO I

INTRODUCCION

En los últimos 25 años, la industria ha hecho una transición de la economía industrial hacia la economía de la información, en las siguientes décadas, la información será la base del bienestar y de la prosperidad.

Existe una confusión entre tecnología de información y competencia /productividad. Las inversiones en tecnologías de información no crean ventajas o productividad por sí solas. No es la tecnología sino el uso de la tecnología la que crea un valor. El valor de la tecnología de información depende de la información y de su rol en las organizaciones (McGee, 1993)

La información es una parte esencial para las organizaciones, los gerentes la utilizan para obtener control y mejorar la toma de decisiones.

La información tiene varios atributos que la hacen valiosa, como la verificabilidad, accesibilidad, claridad, precisión, costo y oportunidad.

Los términos de datos e información, normalmente son usados como sinónimos pero en realidad existe una diferencia. Los datos son desorganizados, no están analizados, no nos indican nada, mientras que la información se refiere a los datos que son significativos y alteran el entendimiento del receptor.

La adopción de la administración de sistemas de información (MIS), sistemas de información ejecutivos (EIS), sistemas para soportar la toma de decisiones grupales (GDSS) y la inteligencia artificial (AI), trae resultados estratégicos para las organizaciones como por ejemplo: mejorar la eficiencia operacional, especialmente en la toma de decisiones y control. La eficiencia operacional permite a las compañías reducir sus costos, haciendolos más competitivos. Otros ejemplos serían la presentación de otras opciones estratégicas para los ejecutivos; el rompimiento de barreras entre departamentos y niveles jerárquicos; reducción de niveles jerárquicos, haciendo una organización más plana (Daft,1993).

Por otro lado, (McGee, 1993) menciona el rol de la información en cada una de las tres partes en una estrategia: diseño, ejecución e integración.

- **La información y el diseño de una estrategia:** La información sobre el ambiente competitivo y la organización actual ayuda a los ejecutivos a identificar oportunidades y amenazas para la compañía, que ayudan a crear estrategias más efectivas.

- **La información y la ejecución de una estrategia:** Las tecnologías de información brindan nuevas alternativas para el diseño de procesos en la creación de nuevos productos y servicios, los ejecutivos pueden usar la información para diferenciar estos productos y servicios.

- **La información y la integración:** La información de la retroalimentación es clave en la creación de organizaciones aprendientes, una vez ejecutada la estrategia para alcanzar

sus objetivos hay que reconocer la necesidad de modificar éstos cuando ya no son efectivos.

Cabe mencionar que uno de los problemas más grandes a los que se enfrenta cualquier organización en la era de la información, es el robo precisamente de ésta. Actualmente estamos viviendo en un mundo globalizado en el que cada vez es más necesario la transmisión de información de un lado a otro electrónicamente. Esto se puede lograr a través de líneas telefónicas, enlaces satelitales, de fibra óptica, etc.. Por lo tanto, se hace indispensable que los administradores de las redes de telecomunicaciones implementen políticas de seguridad que mantengan la integridad y confidencialidad de la información.

Objetivo de la Tesis.

Diseñar una estrategia de control de accesos inválidos, desde el exterior, para redes de información corporativas, en base al desarrollo de las políticas de seguridad de la empresa y a las tecnologías existentes.

Alcance.

La aplicación de esta estrategia para probar sus resultados está fuera del alcance de esta tesis.

La seguridad de una red corporativa abarca tanto la parte interna como externa, esta tesis sólo se enfocará a los accesos de la parte externa.

El estudio de campo se hará sólo en una empresa, por lo que se tratará de un caso específico.

Estructura de la tesis.

La tesis cuenta con cuatro capítulos y un anexo los cuales se clasifican de la siguiente manera. El primer capitulo menciona la importancia y tipos de sistemas de información que hay, asi como el papel de estos en el diseño, ejecución e integración de estrategias. El segundo capitulo describe la historia de Internet y la importancia que tiene la seguridad en las redes corporativas. En el tercer capitulo se describe la metodología de la investigación. En el cuarto capitulo se desarrolla la investigación de campo, se describe el análisis del caso y concluye con la explicación de la estrategia. Por ultimo, el anexo refiere a las diferentes organizaciones consultoras de seguridad.

CAPITULO II.

REVISION BIBLIOGRAFICA

2.1.- INTERNET

Historia de Internet

Una red de computadoras es un grupo de ellas enlazadas por diferentes medios (cables, líneas telefónicas, fibra óptica, satélite, etc..) de manera que pueden transferir información entre ellas. Internet es simplemente una red de redes.

Internet comenzó en los años 60 como resultado de la Guerra Fría. Con la finalidad de minimizar la vulnerabilidad de varios sistemas de cómputo del Departamento de Defensa de los Estados Unidos, conectaron cuatro computadoras mainframe en California, Colorado y Utah vía líneas telefónicas y es ahí cuando nace Internet.

En los años 70, la red (llamada ARPAnet y después MILnet) creció y conectó varias instituciones militares y de investigación y fué administrada por *"Advanced Research Projects Agency (ARPA)"*.

En los años 80, la *"National Science Foundation (NSF)"* habilitó una red central de datos de alta capacidad (NSFnet), que fué la infraestructura más importante para la Internet en EUA.

Uno de las más grandes problemas en la transmisión de datos en los últimos años, fué que las redes de computadoras tenían complicaciones al quererse comunicar con otras redes debido a la gran variedad de tipos de sistemas de cómputo que se estaban utilizando y

por que dichos sistemas utilizaban diferentes estándares y protocolos. El problema fué resuelto por ARPA en los 70's con el desarrollo del estándar TCP/IP (Transmission Control Protocol / Internet Protocol). Este estándar permite enviar pequeñas porciones de datos (paquetes) que incluye direcciones a dónde el paquete debe ser enviado en la Internet. El estándar TCP/IP provocó que otras redes, fuera de Internet, crecieran y se interconectaran permitiendo usos comerciales y facilitando el acceso a los individuos vía módems y computadoras personales para conectarse a la Internet.

En 1983, DARPA (Agencia de Proyectos de Investigación Avanzada de la Defensa) requirió que todas las computadoras conectadas a la ARPAnet usaran el protocolo TCP/IP y entonces ARPAnet fue dividida en dos redes, ARPAnet y MILnet. La NSF vió el potencial de la Internet para enlazar todos los centros de investigación científica, fundando entonces la NSFnet. Eventualmente, NSFnet comenzó a proveer el soporte a la red central de la Internet y en 1990, la ARPAnet dejó de dar el soporte.

Hoy día, no hay país o persona dueña de la Internet, es verdaderamente un foro de comunicación abierta.

En los años 90, las redes comerciales conectadas a la Internet fueron permitidas para hacer negocio en la misma Internet, y en 1993, la NSF creó la InterNIC, que provee servicios como registro de nombres de dominio, directorios y bases de datos e información sobre los servicios de la Internet. (Forcht, 1996)

El crecimiento de Internet

El crecimiento explosivo de la Internet y la integración de las redes comerciales han propiciado el incremento de los usuarios de Internet. Este crecimiento incluye usuarios que no son parte de una academia o una comunidad de investigación.

Debido a que el uso de Internet se esta haciendo cada vez más común en las áreas de educación, investigación, negocios y recreación, los temas de seguridad, confiabilidad, propietariedad y responsabilidad son cada vez más importantes (Forcht, 1996)

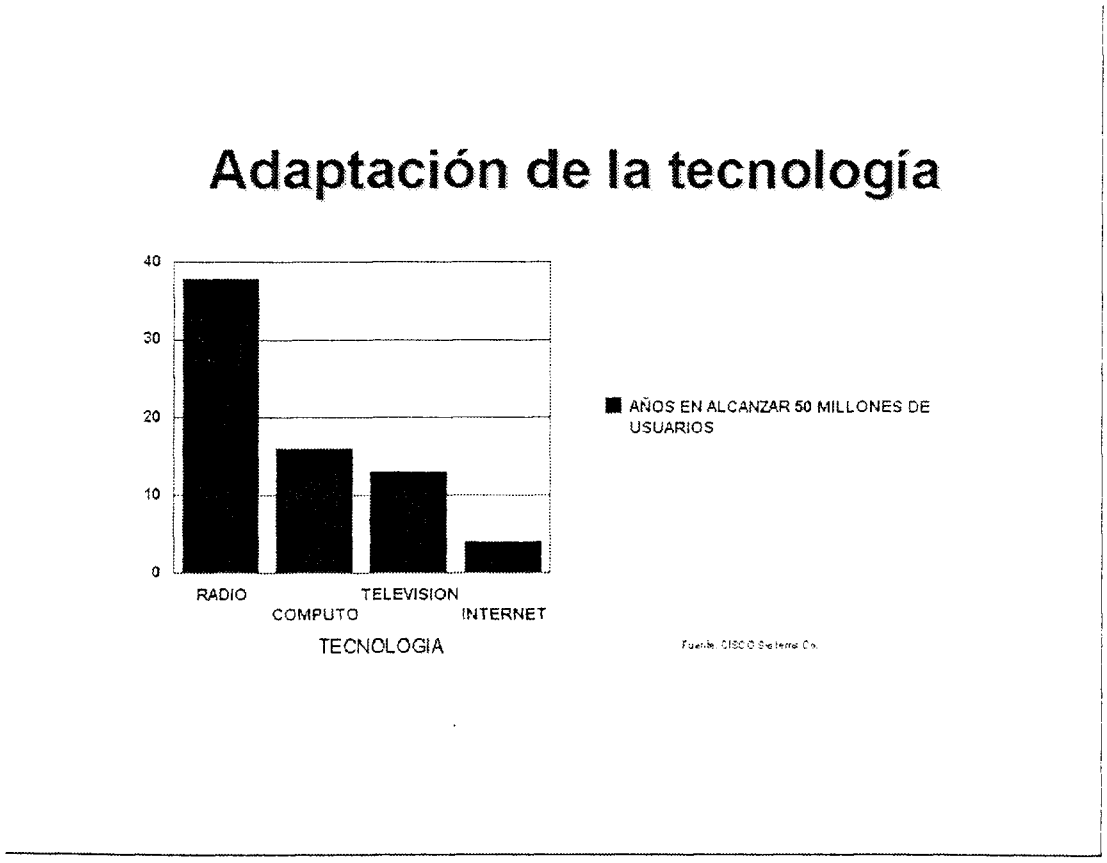

Figura 2.1: Fuente CISCO Systems Co.

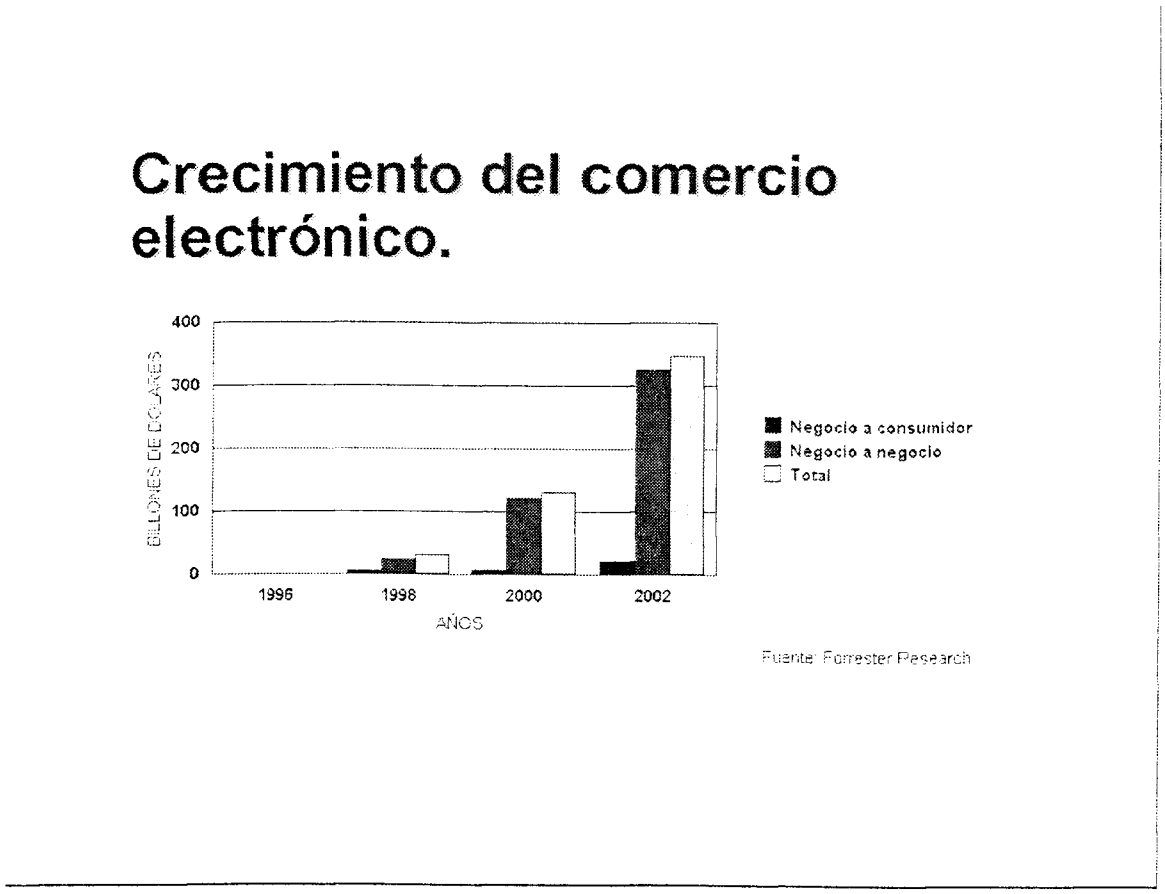

Figura 2.2: Fuente Forrester Research

Uso de Internet.

La información disponible en la Internet es de gran interés para las instituciones educativas, de investigación, negocios, etc..

Por mencionar algunos tipos de información:

Información de historia.

Información de literatura, como por ejemplo:

Colecciones de libros en línea

Revistas en línea

Periódico

Etc.

Información económica, por ejemplo:

Censos

Reportes gubernamentales

Tipos de cambio

Etc.

Información recreativa, por ejemplo:

Deportes.

Lugares turísticos

Música

Intercambio de archivos con otras personas.

Etc..

La Internet se está haciendo una herramienta cada vez más poderosa para los negocios y para las finanzas. Miles de compañías están entrando al *World Wide Web* (WWW), mercadeando todo, desde planes vacacionales, flores, pizzas, música, etc.. Las tiendas en línea cada vez son más comunes, en donde puedes comprar casi cualquier cosa solo tecleando tu número de tarjeta de crédito.

Debido a este crecimiento del comercio en Internet, muchas organizaciones y consumidores están siendo más conscientes de la seguridad de la información que está siendo almacenada y transmitida a través de la Internet. (Forcht, 1996)

Seguridad en Internet.

El reto: debido a que no hay individuo, compañía, agencia de gobierno, región, país o asociación que controle la Internet, nadie tiene la autoridad de dictar políticas o acciones que prometan un uso seguro de Internet. La información está en riesgo como nunca antes. A pesar de que hoy en día la información es una fuerza competitiva de las organizaciones, la naturaleza de la misma está cambiando constantemente. Junto con estos cambios ha surgido la necesidad de proteger y asegurar la información, sin importar de que forma esté.

¿Qué hace a Internet tan vulnerable a los ataques electrónicos ? La Internet es un sistema descentralizado formado por millones de computadoras a nivel mundial. Cada una de estas máquinas cuenta con sus propias claves de acceso y sus procedimientos de seguridad. En la mayoría de los casos, la Internet es tan poderosa hasta en su enlace más débil, y los intrusos que penetran en alguna parte del sistema pueden rápidamente tener acceso a la mayor parte del resto. El " *Computer Emergency Response Team (CERT)*", una organización que monitorea continuamente a la Internet, recientemente anunció un documento describiendo las nuevas formas en que los "crackers" -nombre dado a los usuarios de computadoras malévolos- están explorando huecos en la red global para obtener el control de las computadoras.

Debilidades: los servidores de cómputo en una red ofrecen con frecuencia acceso total a otras computadoras internas especificando su dirección de IP (Internet Protocol). Para penetrar al servidor, los "crackers" se adueñan de la dirección IP de una de estas computadoras internas. Un firewall (dispositivo(s) de seguridad en una red) mal configurado, dejará penetrar al "cracker" dentro del sistema. CERT comenta que las intrusiones están creciendo a un ritmo de 50 % anual y que casi el 97 % de las intrusiones

no son detectadas. Alrededor de 1.2 millones de intrusiones fueron reportadas en 1992. Recientemente los "crackers" están utilizando herramientas que automatizan el proceso necesario para obtener el control total de los sistemas de cómputo. (Forcht, 1996)

2.2.- SEGURIDAD DE COMPUTO.

(Cheswick, 1995) define seguridad como el que nadie haga las cosas que tu no quieres que se hagan con, en, hacia o desde las computadoras o cualquier dispositivo periférico.

Para implementar un mecanismo de seguridad efectivo, Cheswick menciona tres preguntas que deben ser contestadas:

- ¿Qué recursos tratamos de proteger ?
- ¿De quién queremos proteger los sistemas de cómputo ?
- ¿Qué tanta seguridad podemos adquirir ?

(Stallings, 1995) comenta que la investigación y desarrollo de la seguridad de cómputo y de red se enfocan en cinco servicios que abarcan las funciones requeridas de la seguridad de la información:

1. Confidencialidad: Requiere que la información en un sistema de cómputo así como la transmitida sólo pueda ser accesada por las partes autorizadas.
2. Autenticación: Requiere que el origen del mensaje esté correctamente identificado, con la seguridad que la identidad no sea falsa.

3. Integridad: Requiere que los sistemas de cómputo y la información transmitida sean modificadas sólo por las partes autorizadas. La modificación incluye, escribir, borrar, crear, etc..
4. No rechazo: Requiere que ni el transmisor ni el receptor sean capaces de negar una transmisión, que efectivamente realizaron.
5. Control de acceso: Requiere que los accesos a las fuentes de información sean controlados por el sistema destino.

(Russell, 1991) menciona tres aspectos distintos de la seguridad de cómputo:

- Discreción (a veces llamado confidencialidad): Asegura que los usuarios sólo accesen a la información que les es permitida
- Precisión (a veces llamado integridad) y Autenticidad: Un sistema de cómputo seguro debe mantener una integridad continua de la información. Significa que el sistema no corromperá la información o permitirá cambios accidentales o maliciosos.
- Disponibilidad: Un sistema de cómputo seguro deberá mantener la información disponible para los usuarios. Significa que el hardware y software del sistema trabaje eficientemente y que el sistema sea capaz de recuperarse rápida y completamente en caso de un desastre.

Dependiendo de los sistemas o el ambiente, un aspecto puede tener más importancia que otros. Cada organización deberá definir el tipo de seguridad que necesita y ésta influenciará en las técnicas y productos necesarios para cumplir con sus requerimientos.

Los elementos básicos de cualquier sistema de cómputo se hacen más importantes cuando se considera el uso de Internet. Los parámetros a considerar son:

- Autenticación: Significa establecer la identidad, usualmente es una combinación de quién eres, algo que sabes y algo que tienes.
- Control de acceso: Controla lo relacionado de qué o quién puede tener acceso a un objeto. El control de acceso debe considerar la autorización, los derechos y los privilegios.
- Integridad: Se refiere a la condición actual de los datos comparados con su estado original.
- Confidencialidad: Se refiere a mantener la información privada y no disponible para los usuarios no autorizados. (Forcht,1998)

2.3.- POLITICAS DE SEGURIDAD

Una política de seguridad es un estatuto formal de las reglas que la gente y dispositivos, que tienen acceso a la tecnología y a la información de una organización, deben cumplir .

Las metas de la política estarán determinadas por los siguientes puntos:

- Servicios ofrecidos contra la seguridad proporcionada.
- La facilidad de uso contra la seguridad.
- El costo de la seguridad contra el riesgo de perderla. (RFC 2196, *Site Security Handbook*)

Una política de seguridad es un conjunto de decisiones que determinan la postura de una organización en cuanto a seguridad. Más precisamente, una política de seguridad determina los límites de un comportamiento aceptable y la respuesta que debe dar en caso de violaciones. Naturalmente las políticas de seguridad difieren de organización a organización. Una universidad tiene diferentes necesidades que una organización que desarrolla productos y que de una institución militar. Pero toda organización debe contar con una. (Cheswick, 1995)

Antes que una organización pueda reforzar la seguridad en su red, la organización debe medir los riesgos y desarrollar una política clara en cuanto al acceso a la información y la protección. La política necesita especificar quién tendrá acceso a qué información, las reglas que un individuo debe seguir con respecto a la información de otros y cómo reaccionará la organización en caso de violación. (Comer, 1995)

Por otro lado, Steven Tellen en su articulo *Intranet Organizations* menciona que las estrategias de seguridad no deben ser basadas en productos o tecnologías actuales o futuras. Necesitan ser basadas en necesidades funcionales y riesgos de la organización. La parte medular del desarrollo de una estrategia de seguridad es determinar qué necesita estar protegido y de quién. Menciona también que la seguridad no es gratis, cada vez que queremos incrementar la seguridad, la compañía paga en términos de incremento en la complejidad de los accesos, incrementos en los tiempos de respuesta y la reducción en comunicaciones. La seguridad es un balance de valor, de riesgo y de lo práctico.

(Comer, 1995) comenta que la política de seguridad debe ser conocida por cada empleado y debe ser capaz de resolver las siguientes preguntas:

- ¿Qué tan importante es la información para la organización ?
- ¿Qué significa derechos reservados y cuál es la política de la organización en cuanto a la copia de dicha información ?
- ¿Qué tanta información a la que tienes acceso puede ser discutida con otros empleados y con gente de fuera ?
- ¿La organización trabaja con información que pertenece a otras organizaciones ? ¿Puedes discutir dicha información con otros ?
- ¿Qué información puedes importar a la compañía ?
- ¿Puedes usar tu computadora personal y un módem en el trabajo para accesar información de un *"bulletin board service (BBS)"?*
- ¿Cuáles son los derechos de propiedad intelectual y cómo afectan a lo que haces en el trabajo ?

¿Por qué son importantes?

(Russell, 1991) en su libro "Computer Security Basics" habla de la seguridad en las computadoras. Con el crecimiento del número de los sistemas de cómputo que han sido atacados, la gente está tomando más seriamente el asunto de la seguridad en las computadoras. Pero, a pesar del crecimiento de este interés, todavía hay usuarios que no entienden lo que es seguridad de cómputo y por qué es tan importante para ellos.

La seguridad de cómputo debe proteger tu máquina en sí y todo lo que se le relaciona -edificio, terminales e impresoras, cableado, discos, etc..- lo más importante es

proteger la información almacenada en ellas. Es por ello que la seguridad de cómputo se le llama como seguridad de la información. A la parte de edificios, accesos y ubicación se le llama seguridad física.

(Telleen, 1998) menciona en su artículo *Intranet Organizations* que la principal preocupación de los ejecutivos y gerentes al implementar una red es la seguridad, pero no tanto en el aspecto técnico sino en el aspecto organizacional y estratégico. Steven divide la seguridad en tres áreas básicas: almacenamiento, acceso y transmisión.

Las decisiones que hagas o no hagas con relación a la seguridad, como administrador, determinarán qué tan segura o insegura es tu red, qué tanta funcionalidad ofrece y qué tan fácil es de usar. De cualquier manera, no podrás tomar buenas decisiones de seguridad sin antes determinar cuáles son tus objetivos. Hasta que definas dichos objetivos de seguridad, no podrás hacer uso efectivo de las diferentes herramientas de seguridad por que simplemente no sabrás que revisar y que restricciones imponer. (RFC2196, Site Security Handbook)

(Karanjit, 1997) menciona que es importante tener una política de seguridad de red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de su compañía. Vale la pena implementar una política de seguridad si los recursos y la información que su organización tiene en sus redes merecen protegerse. La mayoría de las organizaciones tienen en sus redes información delicada y secretos importantes; esto debe de protegerse del vandalismo, del mismo modo que otros bienes valiosos como la propiedad corporativa y los edificios de oficina.

La mayoría de los diseñadores de redes por lo general empiezan a implementar soluciones de "firewalls" antes de que se haya identificado un problema en particular de seguridad de red. Quizá una de las razones de esto es que idear una política de seguridad de red efectiva significa plantear preguntas difíciles acerca de los tipos de servicios de interredes y recursos cuyo acceso se permitirá a los usuarios, y cuales tendrán que restringirse debido a los riesgos de seguridad.

Si actualmente usted tiene acceso irrestricto a la red, puede ser difícil aplicar una política que limite ese acceso. También debe tomar en cuenta que la política de seguridad que se debe usar es tal, que no disminuirá la capacidad de la organización. Una política de red que impide que los usuarios cumplan efectivamente con sus tareas, puede traer consecuencias indeseables: los usuarios de la red quizá encuentren la forma de eludir la política de seguridad, lo que la vuelve inefectiva.

Una política de seguridad en redes efectiva es algo que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar.

¿Qué políticas existen?

(Karanjit, 1997) en su libro Firewalls y la seguridad en Internet indica que al elaborar las políticas que reflejan la seguridad en una red pueden adoptarse dos posturas principales. Estas declaraciones fundamentales constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas.

a) Lo que no se permite expresamente está prohibido, es el primer enfoque de seguridad. Esto significa que su organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.

b) La línea de pensamiento alternativa es: Lo que no se prohibe expresamente está permitido. Esto significa que, a menos que usted indique expresamente que cierto servicio no está disponible, todos los demás si lo estarán.

El desarrollo de una política de seguridad.

Definir una política de seguridad de red significa elaborar procedimientos y planes para salvaguardar los recursos de red contra pérdida y daño. Uno de los enfoque posibles para elaborar dicha política es examinar lo siguiente:

- ¿Qué recursos esta usted tratando de proteger ?
- ¿De quienes necesita proteger los recursos ?
- ¿Qué tan posibles son las amenazas ?
- ¿Qué tan importante es el recurso ?
- ¿Qué medida puede implementar para proteger sus bienes de forma económica y oportuna ?
- Examine periódicamente su política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red.

Forcht comenta que cuando se está diseñando una política de seguridad, se debe alcanzar un balance entre la gente y la tecnología para que el plan sea funcional.

Cuando se está adoptando una nueva política relacionada con tecnologías de cómputo, la psicología humana debe tomar lugar considerando los siguientes puntos:

- Introducir políticas de seguridad a largo plazo, no apresuradas ni a la carrera.
- Proveer casos de estudio o ejemplos reales de requerimientos de seguridad.
- Enfatizar las mejoras más que la reducción de fallas.
- Tomar en cuenta los comentarios de los empleados que son críticos en un crimen computacional o que soportan una política de seguridad establecida.
- Identificar a los altos ejecutivos que están más a favor de la política de seguridad.
- Describir claramente las debilidades de seguridad, pero inmediatamente exponer una medida efectiva y alcanzable de seguridad.
- Balancear los pro's y contra's de la política de seguridad.
- Asignar a ciertos empleados para que tomen la responsabilidad de la seguridad de la información dentro de su grupo. Rotar el puesto periódicamente.
- Desarrollar políticas de seguridad y procedimientos claros. Hacerlo fácil de actuar de acuerdo a la política y ser claro en las sanciones si no se cumplen.
- Reforzar estándares de seguridad para incrementar la participación de los empleados.
- Poner atención a todo el personal durante el programa.
- Mejorar la seguridad un poco a la vez, trabajar de los pequeños a los más grandes procedimientos.

La RFC 2196 menciona que el propósito principal de una política de seguridad es informar a los usuarios de sus obligaciones para proteger la tecnología y los activos de información. Otro propósito es proveer una base con la cual se configurará y auditará a los sistemas de cómputo y redes para el cumplimiento de la política.

También comenta que los involucrados en la formación de la política de seguridad deberían ser:

- El administrador de seguridad del sitio.
- Personal de tecnologías de información.
- Administradores de diferentes áreas de la organización.
- El grupo de respuesta ante incidentes de seguridad.
- Representantes de los grupos afectados por la política de seguridad.
- La gerencia responsable.
- El departamento legal

Por otro lado indica algunas características que hacen que una política de seguridad sea buena:

- Debe ser implementada a través de procedimientos de administración de sistemas, publicando las guías de un uso aceptable, u otro método apropiado.
- Debe ser reforzada con herramientas de seguridad y con sanciones.
- Debe definir claramente las áreas de responsabilidad de los usuarios, administradores y la gerencia.

Los componentes de una buena política de seguridad son:

- Guías de compra de tecnología de cómputo que especifiquen los requerimientos de seguridad. Esta debe sustituir las políticas y guías de compra actuales.
- Definir las expectativas de privacidad como el monitoreo de correo electrónico, claves de acceso y entrada a los archivos de los usuarios.

- Definir los derechos de acceso y privilegios especificando las guías de uso aceptable para los usuarios y la gerencia. Esta debe proveer guías para las conexiones externas, comunicación de datos, dispositivos de red, y la implementación de nuevo software en los sistemas. También debe especificar el método de notificación de mensajes.
- Definir las reglas de claves de acceso y establecer las guías de autenticación de localidades remotas así como el uso de dispositivos de autenticación.
- Definir las expectativas de disponibilidad.
- Describir el control de los mantenimientos internos y externos a los sistemas de tecnologías de información y a la red, así como el personal que los realice.
- Definir qué tipos de violaciones deberán ser reportados y a quién.

Para que una política de seguridad sea viable en un largo tiempo, requiere de mucha flexibilidad. La política de seguridad debe ser independiente de algún hardware o software específico. Los mecanismos para actualizar la política de seguridad deben ser claramente definidos. Esto incluye el proceso, el personal involucrado y la gente que deberá firmar los cambios. (RFC 2196)

Un aspecto importante de la política de seguridad de red es asegurar que todos conozcan su propia responsabilidad para mantener la seguridad. Es difícil que una política de seguridad se anticipe a todas las amenazas posibles. Sin embargo, las políticas si pueden asegurar que para cada tipo de problema haya alguien que lo pueda manejar de manera responsable. (Karanjit, 1997)

Según Tellen, los pasos para desarrollar una política de seguridad son:

- **Hacer un documento por escrito y que conste de dos partes: fijar las metas y asignar responsabilidades.**

Los objetivos deben dar una idea de dónde estamos, haciendo balance entre el valor contra el costo; los requerimientos del negocio contra el riesgo; sistema abierto contra protegido y qué es lo más adecuado para la empresa. Identificar si la política es: lo que no está explícitamente denegado, está permitido o lo que no está explícitamente permitido, está denegado.

En la sección de responsabilidades se deberá especificar cómo se administrará la seguridad, quién es responsable de mantener y monitorear la estrategia de seguridad y la política y quién revisará la estrategia y la política.

- **Crear un proceso escrito que describa cómo la responsabilidad de la seguridad será delegada, implementada y reforzada.**

Esta incluye una sección gerencial y una sección del empleado.

La sección gerencial contiene una descripción de responsabilidades de cada nivel gerencial y organizacional, los objetivos de seguridad y el cómo serán monitoreados. Se debe proveer estándares que ayuden a la gerencia tomar decisiones consistentes con las políticas y objetivos corporativos.

En la sección del empleado se necesita describir claramente las responsabilidades, expectativas y sanciones requeridas para una implementación de seguridad efectiva.

- **Definir un programa de auditorías para monitorear y administrar la política.**

  La política de seguridad debe ser auditada por auditores internos y externos.

- **Desarrollar una tabla de privilegios.**

  Es recomendable clasificar a los usuarios y hacer las decisiones en base a sus clases en lugar que por individuo. (Telleen, 1998)

¿Dónde se aplican las políticas ?

Una organización puede tener muchos sitios y cada uno contar con sus propias redes. Si la organización es grande, es muy probable que los sitios tengan diferente administración de red, con metas y objetivos diferentes. Si estos sitios no están conectados a través de una red interna, cada uno de ellos puede tener sus propias políticas de red. Sin embargo, si los sitios están conectados mediante una red interna, la política de red debe abarcar todos los objetivos de los sitios interconectados.

En general, un sitio es cualquier parte de la organización que posee computadoras y recursos relacionados con redes. La política de seguridad debe tomar en cuenta la protección de esos recursos. Debido a que el sitio está conectado a otras redes, la política de seguridad del sitio debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas. Este es un punto importante ya que es posible idear una política de seguridad que salvaguarde sus intereses pero sea dañina para los otros. (Karanjit, 1997)

Beneficios.

Durante el desarrollo de una política de seguridad, es importante recordar continuamente que una reducción al riesgo de seguridad trae como consecuencia un costo y que este costo puede ser mayor que el riesgo. El punto es que hay que ser realistas con el proceso de seguridad, no queremos que los competidores accesen fácilmente nuestra información, pero tampoco pagar el costo de tener una información super segura, que de alguna manera u otra el competidor obtendrá dicha información. (Telleen, 1998)

El costo de proteger las redes de una amenaza debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad. (Karanjit. 1997)

2.4.- FIREWALLS

La RFC 2196 menciona que el Firewall es una de las medidas de seguridad más comunes en Internet. Proveen un cierto nivel de protección y son, en general, una manera de implementar la política de seguridad a nivel de red.

Un Firewall actúa como un "gateway" a través del cual pasa todo el tráfico de la red. Los Firewalls ayudan a poner limitaciones en la cantidad y tipo de comunicación entre una red segura y otra red (por ejemplo: Internet u otra parte de la red).

(Cheswick, 1995) define el Firewall como un conjunto de componentes localizado entre dos redes, que en conjunto tienen las siguientes propiedades:

- Todo el tráfico de afuera hacia adentro, o viceversa, debe pasar a través del firewall.

- Solo el tráfico autorizado, definido en la política de seguridad, estará permitido a pasar.
- El Firewall en sí, es inmune a la penetración.

Para (Forcht, 1998), el principal objetivo de un Firewall es proteger una red de otra. En la mayoría de los casos, la red protegida es responsabilidad de una persona o grupo de personas, y la red de la cual nos estamos protegiendo es una red externa en la cual no podemos confiar y desde la cual pueden originarse ataques de seguridad. Proteger la red involucra rechazar a los usuarios no autorizados y prevenir el acceso a la información confidencial de los usuarios no autorizados. Al mismo tiempo, los usuarios autorizados deberían de tener un acceso transparente a los dispositivos de la red.

(Chapman, 1995) menciona que el propósito de los Firewalls de Internet es prevenir los peligros de la Internet en una red interna. Este restringe los accesos a través de un punto bien controlado, previene los ataques de seguridad y restringe la salida a través del mismo punto.

Un Firewall de Internet, normalmente es instalado en el punto en el que tu red segura se conecta a Internet.

Todo el tráfico hacia o desde la Internet pasa a través del Firewall, por que este asegura que el tráfico es aceptable, donde aceptable significa que lo que estemos haciendo -correo electrónico, transferencias de archivos, o cualquier interacción entre sistemas específicos- cumple con la política de seguridad del sitio.

Componentes de un Firewall.

La RFC 2196 comenta que los Firewalls no siempre son una sola máquina, normalmente son una combinación de ruteadores, segmentos de red y hosts.

(Chapman, 1995) menciona que la implementación física de un Firewall varía de sitio a sitio, normalmente está compuesto por ruteadores, hosts, redes y algún software específico. Hay varias maneras de configurar los equipos, esta configuración dependerá de la política de seguridad del sitio, del presupuesto y de las operaciones en general.

(Forcht, 1998) comenta que los Firewalls se componen de:

- Filtros: Los filtros bloquean la transmisión de ciertas clases de tráfico en la red.
- Gateways: Un gateway es una máquina o conjunto de máquinas que proveen servicios para compensar los efectos de los filtros. La red en dónde se encuentra el gateway es llamada zona delimitada (DMZ).
- Gateways internos: Es un gateway localizado en la zona delimitada

Características del Firewall.

(Chapman, 1995) describe lo que los Firewalls pueden hacer:

- Un Firewall es un punto para tomar decisiones de seguridad. Debido a que todo el tráfico pasa a través de este punto, nos permite concentrar las mediciones de seguridad en un sólo punto. De esta manera, las decisiones de seguridad son más eficientes.

- Un Firewall permite reforzar la política de seguridad. Muchos de los servicios que la gente quiere de la Internet, son inseguros. El Firewall es el policía de tráfico para estos servicios. Refuerza la política de seguridad, permitiendo solo los servicios aprobados.
- Un Firewall puede llevar un historial de la actividad en Internet. Debido a que todo el tráfico pasa por él, este es un buen lugar para recolectar información del uso o mal uso de la red y de los sistemas.
- Un Firewall limita tu exposición. Con la existencia de un Firewall limitas los daños de un problema de seguridad en una red, del resto de la red.

También menciona lo que los Firewall no pueden hacer:

- Un Firewall no te puede proteger de los usuarios maliciosos internos. Un Firewall puede evitar que un usuario envíe cierta información por la red, pero el mismo usuario puede copiar la información a un disco, cassette o papel y sacarla fuera del edificio. De igual manera pueden dañar el hardware, el software, modificar programas sin permiso, etc.. Para ello se requiere otras medidas de seguridad y educación al usuario.
- Un Firewall no te puede proteger de conexiones que no pasan a través de él. El Firewall puede controlar el tráfico que pasa a través de el, pero nada puede hacer con el tráfico que no pasa a través de él.
- Un Firewall no te puede proteger de nuevas formas de atacar. Periódicamente, la gente encuentra nuevas formas de ataque, si usan un modo de ataque que nunca antes haya ocurrido es probable que el Firewall no lo detecte. No puedes instalar tu Firewall y esperar que te proteja para siempre.
- Los Firewalls no te protegen contra los virus.

(Garfinkel, 1997) comenta que los Firewalls son parte de la estrategia de seguridad de la organización, desafortunadamente muchas organizaciones basan su estrategia de seguridad solo en el Firewall. Hay muchas organizaciones que tienen problemas de seguridad en su red interna y tratan de resolverlo simplemente instalando un Firewall para bloquear los accesos externos.

(Avolio, 1998) menciona que los Firewalls no son suficientes. Que se requiere de un análisis de riesgos y del negocio, que normalmente se establecen en la política de seguridad, así como en los mecanismos y métodos para implementarla. Pero hacer esto no es suficiente, comenta que los retos, la vulnerabilidad y las necesidades del negocio cambian constantemente. Todo esto debe ser reevaluado periódicamente.

Los métodos de seguridad, como los Firewalls de Internet, son muy populares, pero el problema es que muchas organizaciones creen que con el Firewall de Internet es suficiente para asegurar su red.

2.5.- ORGANIZACIONES CONSULTORAS EN SEGURIDAD.

Alguna organizaciones han formado grupos de especialistas en seguridad que manejan los problemas de seguridad de las computadoras. Estos equipos recaban información acerca de las posibles lagunas de seguridad en el sistema y la difunden y la reportan a las personas adecuadas. Dichos equipos pueden ayudar a rastrear intrusos y proporcionan ayuda y lineamientos para recuperarse de una violación de seguridad. Algunos de estos equipos se encuentran en el anexo.

CAPITULO III.

METODOLOGIA DE LA INVESTIGACION.

Después de estudiar lo que diferentes autores comentan sobre la seguridad en las redes corporativas, era necesario analizar a fondo la estructura de la empresa de estudio, los diferentes departamentos de la organización, su cultura organizacional, su infraestructura actual, las políticas de seguridad requeridas en las tecnologías de información así como los controles que dicta la empresa en el manejo de la información confidencial, para poder responder a las siguientes preguntas: ¿Cómo puedo diseñar una estrategia de seguridad para su red corporativa de acuerdo a las necesidades particulares de la empresa? ¿Por qué es necesario implementarla ? ¿Quienes serán responsables de mantener la estrategia ?

Por todo lo anterior, el método de investigación utilizado fué el cualitativo.

La unidad de estudio fué solamente en una organización. La recolección de datos consistió en la observación de su cultura organizacional, consultando presentaciones ejecutivas e información anunciada en sus páginas de Internet (WWW) y entrevistando informalmente a algunos empleados de la empresa. También se revisó el organigrama de la misma para determinar su estructura departamental. La parte medular de la investigación consistió en el estudio de sus documentos relacionados con las políticas de seguridad localizados en sus páginas de Intranet (Red Interna), conocidas como ITCS's (*Information Technology Control Standards*) así como aquellos documentos que dictan el control del manejo de la información confidencial, además, se tuvieron entrevistas con el coordinador del programa IAS (*Information Asset Security*) de la empresa y con empleados de diferentes áreas para evaluar el conocimiento de las políticas de seguridad entre los mismos.

Por otro lado, se revisaron los procedimientos y actividades realizadas por el departamento de Tecnologías de Información, los servicios de ofrecidos a los diferentes departamentos así como sus acuerdos de nivel de servicio, se tuvieron entrevistas con las personas clave del departamento de TI así como con la gerencia del mismo para entender las responsabilidades de los diferentes puestos dentro del departamento. También se hizo el análisis de su infraestructura de comunicaciones externas actual, entrevistando a personal del área de Telecomunicaciones, revisando la documentación de su red, los controles y procedimientos de seguridad de la misma.

En base a la información obtenida, se desarrolló una estrategia para implementar un sistema de control de accesos para la protección y seguridad de su red que no impactara los servicios y niveles de servicio comprometidos con los diferentes departamentos y que no provocara un cambio radical en la forma de trabajo de la misma. Se adecuaron los procedimientos y controles a las necesidades de ella en lugar de cambiar a la empresa para adecuarse a la estrategia.

CAPITULO IV

RESULTADOS DE LA INVESTIGACION.

4.1 ENTORNO DE LA EMPRESA.

Historia.

La empresa inició sus operaciones manufactureras en 1957 fabricando máquinas de escribir electromecánicas en la ciudad de México. En 1975, en cooperación con el gobierno federal la planta de manufactura cambió sus instalaciones hacia Jalisco.

En 1982 marca un gran cambio, ya que inicia la evolución de productos electromecánicos a electrónicos.

En 1983 dentro de la rama de productos electrónicos, iniciaron con la manufactura de sub-ensambles, de tarjetas electrónicas la cual continuó durante 10 años hasta que fué transferida a los proveedores dentro de su estrategia de Desarrollo de los mismos.

En 1986, otro año clave en la historia de la empresa, ya que inició la manufactura y ensamble de la familia de computadoras personales y desde entonces ha sido un producto en expansión.

Durante 1989 dio inició los sub-ensambles para productos de almacenamiento, empezando por actuadores, los cuales sus volúmenes fueron incrementándose exponencialmente y posteriormente empezaron con la diversificación a otros ensambles como los de Suspensión de Cabezas, siendo estos productos de la más alta tecnología a

nivel mundial y requiriendo procesos y condiciones especiales para las líneas de ensamble, tales como cuartos limpios. Hoy en día es una de las misiones pilares de la empresa.

Continuando con la búsqueda de nuevas misiones y nuevas oportunidades, en 1990, se inició un laboratorio de desarrollo de software, trabajando en conjunto con un laboratorio de Rochester, MN.

Visión.

Su visión es: Ser la fuerza dominante del mercado que hemos elegido para servir cumpliendo con las expectativas de nuestros clientes y accionistas, con empleados, proveedores y socios de negocios altamente calificados y motivados.

Misión.

Su misión es: Proveer productos, soluciones y servicios de valor superior para el desarrollo de nuestros clientes y nuestro país, en un ambiente sin fronteras.

Cultura Organizacional.

La cultura organizacional de la empresa está enfocada a llegar a ser una cultura de clase mundial, está muy basada en la calidad, en el trabajo en equipo y en la ejecución. Para ello, realiza programas de calidad para que los empleados se sientan motivados en participar, por equipos, en la mejora de algún proceso.

La empresa ha logrado resultados como la certificación ISO9000 e ISO14000, Premio Nacional de Calidad y Premio Jalisco a la Calidad.

Entre sus estrategias principales están las de apoyar y ayudar a los clientes y proveedores a entrar en el comercio electrónico. Para esto, la empresa esta poniendo un enfoque muy amplio al cuidado de aspectos críticos en lo que se refiere a la transmisión de información como son la privacidad y la seguridad, para ello, la empresa tiene instrucciones bien definidas en cuanto a la seguridad en las tecnologías de información.

Políticas de seguridad en las TI de la empresa.

En un estudio realizado por la empresa sobre los ataques de seguridad en las tecnologías de información, se llegó a los siguientes resultados:

De 520 organizaciones estudiadas:

64% reportaron violaciones de seguridad.

- 44% reportaron acceso no autorizado por empleados.
- 25 % reportaron negación del servicio.
- 24% reportaron penetración a los sistemas desde el exterior.
- 18% reportaron pérdida de información
- 15% reportaron fraudes financieros.
- 14% reportaron sabotaje
- 72% reportaron pérdidas financieras debido a las violaciones de seguridad.
    - Sólo el 46% (241 organizaciones) pudieron cuantificar sus perdidas.

- Las 241 organizaciones reportaron una pérdida total de $ 136 millones de dólares.

De ahí que la empresa se ha preocupado y ha desarrollado sus propias instrucciones de seguridad que mencionan lo siguiente:

a) Sistemas de cómputo.

1. Los sistemas de cómputo solo deberán de ser usados para fines de negocio o propósitos autorizados por la gerencia. Su uso puede ser auditado en cualquier momento.
2. La autorización del uso de los sistemas de cómputo debe basarse en una necesidad actual, determinada y aprobada por la gerencia.
3. Los sistemas de cómputo deben incluir controles designados para prevenir y detectar accesos no autorizados.
4. Los sistemas de cómputo deben estar protegidos físicamente y con accesos controlados.
5. La integridad de los sistemas de cómputo debe protegerse mediante controles designados para prevenir cambios no autorizados a los recursos del sistema operativo.
6. Los sistemas de cómputo deben incluir los controles necesarios para prevenir la propagación y ejecución de código dañino. (ej. virus, etc..)
7. La información almacenada en los sistemas de cómputo debe ser protegida contra accesos no autorizados.

b) Redes de telecomunicaciones.

Las redes de área amplia (WAN) y redes de área local (LAN) deben incluir el hardware y software apropiados, así como los procesos de control para proteger la intercepción no autorizada del tráfico en la red.

c) Servicios de conexión inter-empresariales. (IESC)

La conectividad en los sistemas de cómputo/redes de la empresa y sistemas de cómputo/redes de un tercero (ej. Internet, proveedores, subsidiarias, etc..) debe ser administrada con controles de seguridad designados para prevenir el acceso no autorizado a los sistemas de cómputo/redes de la empresa.

Estas instrucciones se encuentra en los documentos internos llamados ITCS (Information Technology Corporate Standard) 204 (Security standards for providers of network and computer services), ITCS 300 (Computer security and use guidelines for employees) y la ITCS 302 (Security guidelines for inter-enterprise services).

Clasificación y control de la información.

La empresa cuenta con una instrucción (116C Clasificación y control de la información de la empresa) en donde define la clasificación de la información confidencial y los controles que ella implica. El autor de la información decide si ésta se debe clasificar como confidencial, considerando su contenido, el carácter y el valor de dicha información.

Si el autor de la información decide que no es confidencial, se la considerará no reservada, de todos modos, la misma tiene valor para la empresa y sigue siendo propiedad de ésta. Por lo tanto, la información no confidencial que se origina dentro de la empresa no se debe divulgar fuera de ella, a menos que tal difusión la beneficie.

La instrucción menciona los siguientes puntos de interés para esta tesis:

a) Transmisiones electrónicas.

Las transmisiones electrónicas son intercambio de información, voz o datos mediante medios electrónicos, incluso teléfonos, videos, sistemas de conferencia y redes LAN o WAN.

La información confidencial no se debe transmitir por dispositivos de comunicación inalámbricos, que utilicen frecuencias radiales, a menos que la información esté encriptada.

b) Salvaguarda y almacenamiento.

La información confidencial siempre se debe guardar fuera de la vista de quienes no tienen necesidad de saber.

La información confidencial en forma física, incluso en medios electrónicos como diskettes, no debe quedar al descuido a menos que esté segura tras una puerta con llave o dentro de muebles de oficina cerrados, con cerradura aprobada por la empresa. La información confidencia en PC (*Personal Computer*), incluso de estaciones de trabajo, se debe proteger mediante mecanismos que aseguren el acceso a ella sólo por parte de personas autorizadas.

El acceso a los sistemas de información y bases de datos de la empresa que contengan información confidencial deben usar mecanismos de control de accesos o un proceso de autenticación para prevenir accesos no autorizados.

4.2. SERVICIOS DE TECNOLOGIAS DE INFORMACION (TI) DE LA EMPRESA.

Actualmente la Planta de Manufactura cuenta con cuatro áreas productivas principales, así como con diferentes áreas de servicio o soporte:

- Procurement
- Fulfillment (Distribución, IDC, Almacén, Logística de Materiales)
- Contraloría (Finanzas, Contabilidad)
- Materiales
- Recursos Humanos
- Servicios

Estas áreas, para su efectiva y eficiente operación están requiriendo actualmente de los servicios de Tecnologías de Información adecuados que garanticen el óptimo logro de sus resultados. Parte de ellos es el intercambio de información con los proveedores en cuanto a planes de producción, manejo de cotizaciones, pago a los mismos, etc.. y clientes de los cuales reciben ordenes interplanta y directos para surtir a diferentes mercados del continente. Los servicios requeridos están clasificados de la siguiente manera:

Operación.

- Disponibilidad de sistemas y de comunicación voz y datos el tiempo en que las áreas productivas y/o de soporte requieran de los mismos.

- Corridas de los diferentes procesos de manufactura de manera eficaz y efectiva que aseguren la continuidad y control de sus operaciones.

Comunicación voz y datos internas y externas.

Infraestructura y servicios de comunicación para:

- Comunicación voz internas (Planta)

- Comunicación voz llamadas locales

- Comunicación voz llamadas nacionales e internacionales

- Comunicación datos hacia sistemas locales.

- Comunicación datos hacia sistemas no locales

Sistema de Manufactura (Desarrollo y Mantenimiento)

- Sistema de Manufactura para su operación diaria.

- Interfaces del sistema de manufactura con otras aplicaciones.

- Sistema ERP (Enterprise Resource Planning) para la planeación de las operaciones de la planta.

Sistema de Oficina.

- Correo electrónico.

- Manejo de documentos (procedimientos)

- Servicios Generales (directorio, información general de negocio)

Equipo de cómputo y telefonía

Herramientas de usuario final para ingresar a las facilidades y servicios para el manejo de información tanto de voz como de datos.

Servicios Generales

- Impresión de reportes
- Educación a usuarios
- Accesorios (Consumibles equipo de cómputo)

Soporte TI

Siempre y cuando exista actividad de alguna de las áreas productivas y de servicio o soporte, o sea expresamente solicitado por algunas de éstas áreas a TI.

Todos estos servicios son suministrados y administrados por el departamento de tecnologías de información de la empresa compuesto por 52 personas. Dentro de dicho departamento, se encuentra un grupo de 10 personas que tienen a su cargo las comunicaciones internas y externas de voz y datos necesarias para las operaciones de la empresa.

4.3. CONTROL PARA EL ASEGURAMIENTO DE LOS SERVICIOS DE TI DE LA EMPRESA.

Manejo de Cambios

TI planeará, coordinará y monitoreará los cambios que afecten los servicios proporcionados asegurando que los cambios son hechos con un riesgo aceptable a los compromisos de servicio establecidos.

Los cambios que se realicen a la base instalada tanto de hardware y software se harán conforme al "Procedimiento de Manejo de Cambios" establecido.

Operación, rendimiento y administración de la capacidad

TI mantendrá una operación constante de los sistemas de producción los 365 días las 24 horas asegurando el uso y aprovechamiento eficiente de los recursos con los que se cuenta. Así mismo identificará de manera oportuna los recursos necesarios para mantener el nivel de servicio comprometidos.

Para esto TI analiza el rendimiento, cargas de trabajo y disponibilidad de cada uno de los sistemas locales y de comunicación (LAN/WAN) así como los procesos batch para identificar tendencias y detectar áreas de mejora en los servicios proporcionados.

El proceso que se sigue a través del *Management System* de TI es con el cual de manera mensual se revisan las operaciones y mediciones del servicio proporcionado estableciendo los planes necesarios en caso de existir alguna desviación con respecto de dichos servicios.

Seguridad de la Información

TI es responsable de:

- Protección física y lógica de la información y equipos del Centro de Cómputo de acuerdo con las instrucciones corporativas IAS (*Information Asset Security*) de seguridad de la información.

- Administradores de la seguridad de los sistemas de producción para actividades como altas, bajas y cambios de usuarios en los sistemas de acuerdo a requerimiento gerencial, etc..

Los sistemas de cómputo se encuentran localizados en un área de acceso controlado, sólo personal autorizado por la gerencia tiene permitido el acceso. El área es conocida como centro de cómputo, el cual cuenta con los sistemas de seguridad física que dicta la empresa como son detector de movimientos, detectores de humo, cámaras de video, etc..

En la empresa existe un programa llamado IAS que consiste en asegurar el cumplimientos de todas las normas de seguridad que dicte la empresa, para ello hay una persona encargada de dar seguimiento a todas y cada una de las actividades.

4.4. ANALISIS DEL CASO.

Manejo e importancia de la seguridad de la información.

La empresa tiene como parte de sus estrategias el compartir la información de los planes de producción con sus proveedores principales para acortar los tiempos de entrega de su materia prima directa, dicha información se encuentra tanto en los sistemas de manufactura como el sistema ERP de la planta, algunos de ellos necesitan tener acceso al correo electrónico de la empresa para mantenerse comunicados con personal de la empresa, otros necesitan accesar aplicaciones que se encuentran en Internet.

Esta comunicación entre la empresa y sus proveedores es conocida internamente como enlaces IESC (*Inter-enterprise Service Connection*), para los cuales la empresa cuenta con políticas de seguridad bien definidas en el estándar ITCS 302, las cuales indican que todos los enlaces IESC deben proveerse a través de un Firewall, además de la necesidad de definir claramente las responsabilidades de la gerencia así como los procedimientos de control.

Infraestructura actual.

La infraestructura actual con la que la empresa provee comunicación de datos entre ella y sus proveedores, mostrada en la figura 4.1, tiene un alto riesgo de seguridad debido a que no hay un sistema de control de accesos (Firewall) entre los proveedores y la empresa, por lo que cualquiera de los proveedores podría accesar cualquier sistema interno, a pesar de que no halla una necesidad de negocio, además pueden extender dicho acceso a los sistemas de la empresa ubicados en los Estados Unidos. Debido a que no hay un control de

accesos, se hace más difícil la detección de un "cracker" que esté accesando información confidencial y que pueda afectar a la empresa.

Por otro lado, si la empresa se vieran en una auditoria de seguridad estaría en problemas ya que no cumple con la norma ITCS 302, trayendo como consecuencia, posibles pérdidas competitivas, pérdida de proyectos asignados o incluso hasta el cierre de la localidad.

Por todo lo anterior, existe la necesidad de establecer una estrategia de seguridad que nos permita contar con una infraestructura más segura y que cumpla con el estándar ITCS 302.

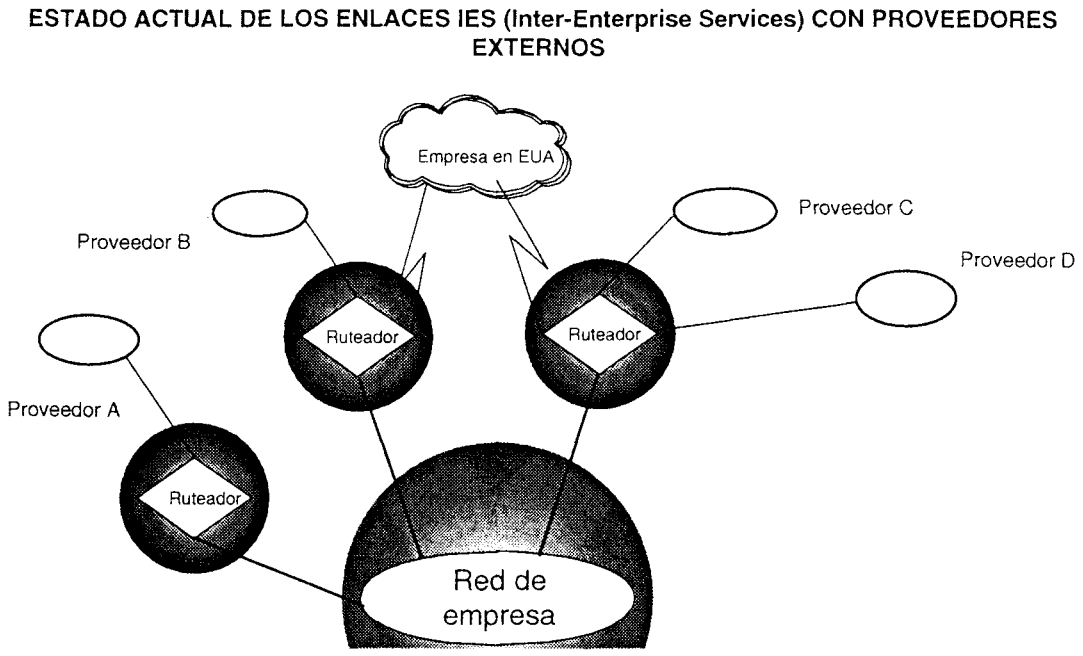

Figura 4.1: Infraestructura actual.

Ambiente Interno.

DEBILIDADES FORTALEZAS

	La empresa, en esta localidad, cuenta con un departamento de tecnologías de información.	La empresa cuenta con políticas de seguridad de red bien definidas que pueden aplicar para cualquier localidad.	Es una empresa basada en procesos.	La empresa tiene fácil acceso a la tecnología.
No hay un sistema que controle los accesos a la red de la empresa.	Aprovechar el skill de la gente para hacer un estudio de las diferentes tecnologías de seguridad que permitan controlar los accesos.	Implementar un sistema que controle los accesos a la red de la empresa		Obtener información como apoyo al estudio de las diferentes tecnologías de seguridad .
No existe formalmente una persona responsable de implementar y mantener la seguridad en la red de esta localidad.	**Asignar a una persona o personas del grupo de comunicaciones para formalizar la responsabilidad.**	Documentar las responsabili-dades de la gerencia en cuanto a la seguridad de la red.		
Existe un escaso conocimiento de las políticas de seguridad de red en la localidad.		Fortalecer la publicación de las políticas de seguridad de red		Hacer uso de las tecnologías de información para dar a conocer las políticas de seguridad de red.
No existen procedimientos de seguridad específicos para esta localidad.		**Elaborar los procedimien tos basados en las políticas de seguridad de la empresa.**	**Continuar con el estándar y aprovechar el skill de procesos para elaborar los correspondientes a la seguridad de red.**	

Tabla 4.1: Ambiente Interno

Ambiente Externo.

AMENAZAS OPORTUNIDADES.

	Crecimiento del comercio electrónico.	Tecnología de seguridad de red disponible.	Empresas consultoras en seguridad de redes.
Competencia.	Implementar soluciones informáticas que permitan compartir información electrónicamente.	Proteger la información que pueda ser competitiva para la empresa.	
Crackers	Proveer seguridad para generar confianza y acelerar el uso del comercio electrónico.	Implementar tecnologías de seguridad de red para evitar accesos inválidos.	Elaborar métodos de detección y prevención de accesos. Pedir consulta externa en casos necesarios.

Tabla 4.2: Ambiente Externo.

4.5. ESTRATEGIA

Objetivo: La estrategia de seguridad tiene como objetivos proponer una infraestructura que elimine el riesgo de accesos inválidos, que sólo permita que los proveedores accesen aquellos sistemas internos que sean una necesidad de negocio y que estén aprobados por la gerencia; definir las responsabilidades en esa infraestructura así como procedimientos y controles para llevar a cabo la estrategia y cumplir con la norma ITCS 302.

Política general de seguridad.

Como vimos anteriormente, existen dos vertientes en cuestión del control de accesos a la información, estas son:

1.- Lo que no se permite expresamente está prohibido.

2.- Lo que no se prohibe expresamente está permitido.

La política a utilizar para nuestro caso y de acuerdo con la norma ITCS 302 de la empresa es: **LO QUE NO SE PERMITE EXPRESAMENTE, ESTA PROHIBIDO.**

Desarrollo de la estrategia.

1.- Infraestructura propuesta.

La propuesta consiste en la implementación de un dispositivo de seguridad entre la empresa y sus proveedores para poder tener un control de los accesos y permitir aquellos que son estrictamente necesarios para el negocio, además que nos facilita la detección de accesos inválidos. Hoy en día, el concepto de Firewall nos puede ayudar a lograr nuestro objetivo.

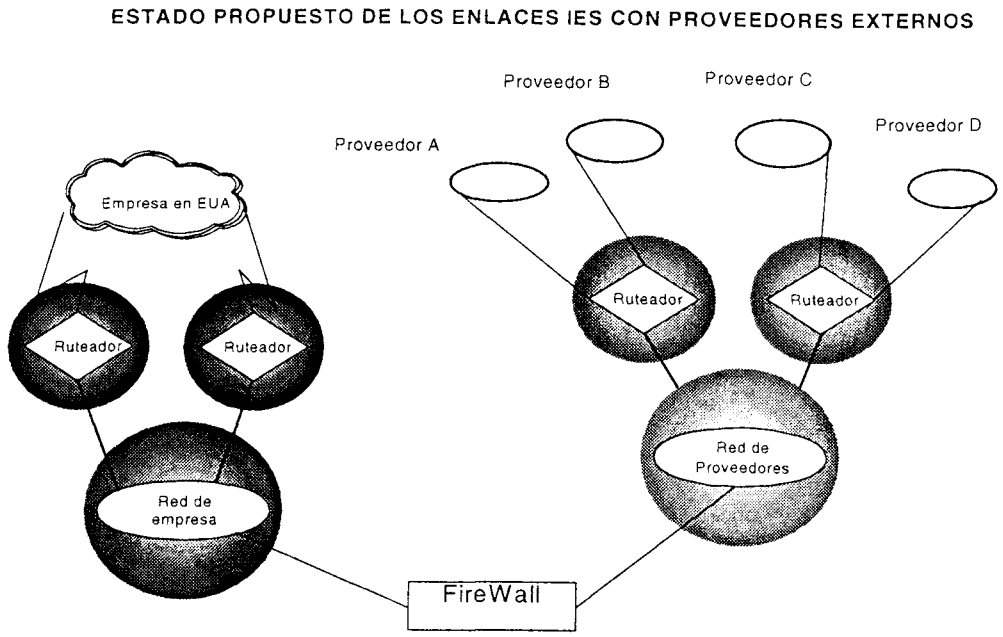

Figura 4.2: Infraestructura propuesta.

2.- Responsabilidades.

La norma ITCS 302 indica que por cada enlace IESC debe existir un requisitor y un administrador, los cuales se definen de la siguiente manera:

El gerente de la empresa que define la necesidad de negocio de proveer un IESC será el IESC Requierement Owner (IESC RO)

- El IESC RO usará el Firewall existente que satisfaga la necesidad de negocio y cumplirá con los procedimientos establecidos para autorización y revalidación de accesos y uso de los IESC Firewalls existentes.
- Si la necesidad de negocio no es ofrecida con el IESC Firewall existente, entonces el IESC RO es responsable de solicitar un nuevo IESC Firewall.

Cuando se establece la necesidad de un nuevo IESC Firewall, el IESC RO y el IESC Firewall Manager definirán los procedimientos a seguir para la autorización y revisión periódica de los accesos y usos del IESC Firewall. Los procedimientos usados para la autorización de accesos a los servicios de TI internos de la empresa por parte de empleados de empresas externas, deberán cumplir con la carta de instrucción 116 C.

El gerente responsable de las operaciones y soporte del IESC Firewall es el IESC Firewall Manager.

- El IESC Firewall Manager implementará los controles de seguridad requeridos en el IESC Firewall y verificará que los controles sean de acuerdo al procedimiento de "Revisión de la Certificación de Seguridad del IESC Firewall"
- El IESC Firewall Manager se apegará a los procedimientos de autorización y revalidación de accesos establecidos en el "proceso de autorización y revalidación de accesos y uso a través del IESC Firewall".

Organigrama del departamento de IT

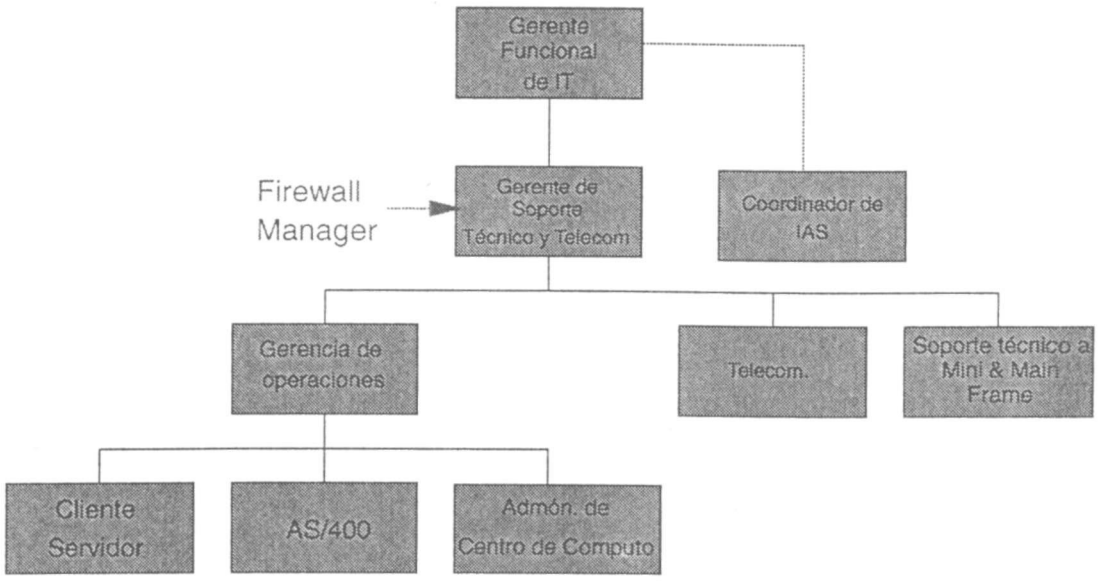

Figura 4.3 Organigrama de TI

En esta empresa, el Gerente de Soporte Técnico y telecomunicaciones será el IESC Firewall Manager.

3.- Control de la estrategia.

El control de la estrategia se lleva a cabo a través de procedimientos que establecen un proceso de detección y reporteo de incidentes de seguridad que nos permita actuar de manera inmediata; controlan los cambios realizados en el IESC Firewall para evitar que dichos cambios pongan en riesgo la integridad del mismo y garantizar los servicios comprometidos; asegurar que los servicios ofrecidos a través del IESC Firewall continúan siendo una necesidad de negocio y están aprobados por el IESC Requester Owner y por el

IESC Firewall Manager; pruebas de penetración periódicas así como un plan de contingencia.

Los procedimientos son los siguientes:

a) Detección y reporteo de incidentes de seguridad.

Cada vez que se viola la política de seguridad, el sistema está sujeto a amenazas. Si no se producen cambios en la seguridad de la red cuando ésta sea violada, entonces debe modificarse la política de seguridad para eliminar aquellos elementos que no sean seguros.

Cuando se detecte una violación a la política de seguridad, se debe determinar si esta ocurrió debido a la negligencia de un individuo, a un accidente o error, por ignorancia de la política vigente o si deliberadamente la política fué pasada por alto. En cada una de estas circunstancias, la política de seguridad debe contar con lineamientos acerca de las medidas que se deben tomar.

Existen dos tipos de estrategias de respuesta ante incidentes de seguridad:

- Proteger y continuar.
- Perseguir y demandar.

Si los administradores de la política de seguridad sienten que la compañía es bastante vulnerable, quizá se decidan por la estrategia de proteger y continuar. El objetivo de esta política es proteger de inmediato a la red y restablecerla a su situación normal para que los usuarios puedan seguir usándola. Para hacer esto, se tendrá que interferir activamente con las acciones del intruso y evitar mayor acceso. La desventaja de este procedimiento es que los intrusos saben que ya fueron detectados y tomarán medidas para evitar que sean rastreados, asimismo, el intruso puede reaccionar a su estrategia de

protección atacando el sitio con otro método. Por lo menos, es probable que el intruso continúe su vandalismo en otro sitio.

La segunda estrategia, adopta el principio de que el objetivo principal es permitir que los intrusos continúen sus actividades mientras usted los vigila. Deben registrarse las actividades de los intrusos para que haya pruebas disponibles en la fase de demanda de esta estrategia. Este es el enfoque recomendado por las dependencias judiciales y los fiscales, ya que rinde evidencias que pueden usarse para demandar a los intrusos. La desventaja es que el intruso seguirá robando información o haciendo otros daños.

El procedimiento para la detección y reporteo de incidentes de seguridad para el IESC Firewall es el siguiente:

- El administrador del IESC Firewall recibirá vía electrónica el reporte de intentos fallidos de acceso al IESC Firewall de acuerdo al límite definido localmente.
- En caso de que el administrador sospechara o detectara cualquier incidente de seguridad, notificará inmediatamente al IESC Firewall Manager.
- El administrador deberá generar una bitácora (en papel o en otro sistema) para identificar toda información relacionada al evento con fecha, hora y fuente de información.
- Si el IESC Firewall es penetrado, desconecte físicamente de los demás sistemas o redes de la empresa al cuál está conectado. No lo conecte hasta que el incidente haya sido aclarado.

- Respalde el IESC Firewall e identifique el respaldo con fecha, hora, nombre del sistema y nombre de la persona que realizó el respaldo.
- El IESC Firewall Manager seguirá el proceso de reporteo indicado en la sección de IESC Security Incidents de la Norma ITCS302.

b) Control de cambios.

El procedimiento de cambios para el IESC Firewall es el siguiente:

- Todo requerimiento de cambio en el IESC Firewall necesita usar la forma de requerimiento anexa.
- El cambio deberá ser aprobado por el IESC Requirement Owner y por el IESC Firewall Manager.
- Se efectuará un análisis de implicaciones y autorizaciones a nivel Técnico y de Negocio para garantizar que no afecte la integridad del IESC Firewall.
- Deberán guardarse dichas formas por el tiempo que viva el IESC Firewall como parte de la documentación

Forma de manejo de cambios en el IESC Firewall.

NOMBRE DEL REQUISITOR:

_____

FECHA _____ IESC AFECTADO

_____

DESCRIPCION DEL CAMBIO:

_____

_____

_____

_____

NECESIDAD DEL CAMBIO:

_____

_____

_____

PREREQUISITOS (SI APLICAN) :

_____

_____

_____

IMPACTO:

_____

_____

_____

FECHA REQUERIDA: _____

CRITERIO DE INSTALACION EXITOSA:

_____

_____

_____

PLAN DE REGRESO EN CASO DE FALLA:

_____

_____

_____

AUTORIZACIONES:

_____	_____	_____
Requisitor	IESC Requester Owner	IESC Firewall Manager.

c) Autorización y revalidación de accesos.

Los servicios ofrecidos a través del IESC Firewall deberán ser revisados y aprobados anualmente por el IESC Requester Owner, IESC Firewall Manager y por el coordinador de IAS de la empresa.

El IESC Firewall Manager elaborará un reporte anual con los servicios ofrecidos a través del IESC Firewall y se lo entregará al IESC Requester Owner.

El IESC Requester Owner revisará y aprobará aquellos servicios que sigan siendo una necesidad de negocio.

La documentación de cada servicio deberá ser revisada y autorizada por el IESC RO, el IESC Firewall Manager, por el gerente de la empresa que aprueba la relación con la empresa externa y por el coordinador de IAS de la empresa.

Los reportes deberán ser guardados por el tiempo que viva el IESC Firewall como parte de su documentación.

Si en el ínter dejara de existir una necesidad de negocio para algún servicio existente, el IESC Requester Owner notificará inmediatamente por correo electrónico al IESC Firewall Manager, quién dará la baja de dicho servicio en el IESC Firewall.

El formato generado por el IESC Firewall Manager será el siguiente:

==========

Fecha:

Revalidación de servicios a través del IESC Firewall

Nombre del IESC Firewall

Empresa exterior	Relación con nuestra empresa	Servicios y aplicaciones autorizadas

Nota: Los servicios y aplicaciones que NO estén explícitamente autorizados, están PROHIBIDOS.

IESC Requester Owner

IESC Firewall Manager.

d) Revisión de la certificación de seguridad del IESC Firewall.

El objetivo es la realización de pruebas de penetración constantes en el FireWall, que permita la detección de fisuras en el mismo para actuar de manera inmediata.

Existe software especializado para hacer estas pruebas, las cuales se deberán realizar mensualmente y en cada cambio realizado en el Firewall.

Una vez obtenido los resultados de la prueba se deberá analizar y verificar que, en caso de que existan servicios expuestos, estos sean solamente los autorizados. En caso contrario se deberá revisar y en su caso deshacer el cambio hasta encontrar el motivo de la falla.

e) Plan de contingencia.

Debido a la importancia que es para la empresa la constante comunicación con sus proveedores y clientes, es recomendable contar con un Firewall de respaldo con las mismas características, de manera que en caso de que el Firewall que esté en producción falle, entre automáticamente el de respaldo.

Si esta alternativa resultara costosa para la empresa, la otra opción sería contar con filtros en los ruteadores que hagan la función de un firewall. Cabe mencionar que en la actualidad existen Firewalls que ya manejan alta disponibilidad.

F) Costos.

Los costos para la implementación de la estrategia son los siguientes:

Hardware	$ 25 Kusd
Software	$ 6 Kusd
Capacitación	$ 4 Kusd
Total	**$ 35 Kusd**

ANEXO.

ORGANIZACIONES CONSULTORAS EN SEGURIDAD.

(Karanjit, 1997) menciona que algunas organizaciones han formado grupos de especialistas en seguridad que manejan los problemas de seguridad de las computadoras. Estos equipos recaban información acerca de las posibles lagunas de seguridad en el sistema y la difunden y reportan a las personas adecuadas. Dichos equipos pueden ayudar a rastrear intrusos y proporcionar ayuda y lineamientos para recuperarse de una violación de seguridad.

1.- CERT

El Equipo de Respuesta a Emergencias de Cómputo / Centro de Coordinación (CERT/CC) fué establecido en diciembre de 1988 por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA). El objetivo de este equipo es abordar las preocupaciones acerca de seguridad de cómputo de los investigadores de Internet. El CERT es coordinado por el Instituto Nacional de Estándares y Tecnologías de Estados Unidos (NIST) y existe para facilitar el intercambio de información entre diversos equipos.

El CERT es manejado por el Instituto de Ingeniería de Software (SEI) de la Universidad de Carnegie Mellon (CMU). Este equipo tiene la capacidad de hablar inmediatamente con expertos para diagnosticar y resolver problemas de seguridad. También pueden ayudar a establecer y mantener la comunicación entre un sitio y las autoridades de gobierno. También funciona como centro de intercambio para identificar y reparar puntos vulnerables en los principales sistemas operativos. También puede proporcionar

evaluaciones informales de sistemas existentes y orientar para mejorar la capacidad de respuesta a emergencias.

2.- Centro de Coordinación de Seguridad DDN

Para los usuarios de la Red de Datos de Defensa (DDN), el Centro de Coordinación de Seguridad (SCC) sirve como una oficina central para discutir problemas y soluciones de seguridad para usuarios y hosts, y trabaja en combinación con la Oficina de Seguridad de Redes DDN.

3- Centro de Recursos y Respuestas de Seguridad en Computadoras del NIST.

El Instituto Nacional de Estándares y Tecnología (NIST), además de manejar las cuestiones de estándares, también tiene la responsabilidad, dentro del gobierno estadounidense, de actividades de ciencia y tecnología de computación.

El NIST maneja el Centro de Recursos y Respuestas de Seguridad en Computadoras (CSRC), el cual ofrece ayuda e información acerca de incidentes de seguridad de computadoras

4.- Capacidad de Asesoría en Incidentes de Computadoras del DOE (Departamento de Energía)

La CIAC es la Capacidad de Asesorías en Incidentes de Computadoras del Departamento de Energía y se formó para construir un capacidad de respuesta centralizada y un centro de asistencia técnica para los sitios del DOE. La responsabilidad básica de este grupo es ayudar a los sitios del DOE que se enfrentan a incidentes de seguridad, como

ataques de intrusos, infecciones de virus, etc.. La CIAC mantiene a los sitios informados de los eventos actuales relacionados con la seguridad y mantiene enlaces con otros equipos y agencias de respuesta.

5.- Equipo de Respuesta de Seguridad de Red de Computadoras Ames en la NASA.

El Equipo de Respuesta de Seguridad de Red de Computadoras (CNSRT) fué formado por el Centro de Investigación Ames de la NASA en agosto de 1989. El objetivo primordial del equipo es ofrecer ayuda a los usuarios de Ames, pero también se ha involucrado para ayudar a otros centros de la NASA y agencias federales

BIBLIOGRAFIA

AHUJA, Vijay, Network and Internet security, Ap professional, primera edición, Estados Unidos, 1996.

ANONIMO, "How to develop your security policy", URL http://www.frus.com/index.cgi?file=frus/sec-policy-howto.html, Noviembre 1998.

ANONIMO, "FIRST security papers", URL http://www.alw.nih.gov/Security/first-papers.html, Diciembre 1998.

ANONIMO, "Keeping Internet access manageable" URL http://www.cyberpatrol.com/cpwp.htm Noviembre 1998.

AVOLIO, Frederick M., "Firewalls are not enough", URL http://www.tis.com/prodserv/gauntlet/FirewallsNotEnough.html, Noviembre 1998.

BOLDEN, Darren, "Network Security, Filters and Firewalls", URL http://www.acm.org/pubs/periodicals/crossroads/xrds2-1/security.html, Noviembre 1998

COMER, Douglas, Internetworking with TCP/IP, Prentice Hall, Tercera edición, Estados Unidos, 1995

CHAPMAN, D. Brent, Elizabeth, Building Internet Firewalls, O'Reilly & Associates, Inc., Primera edición, Estados Unidos, 1995.

CHESWICK, William R., Steven, Firewalls and Internet Security, Addison-Wesley, Quinta edición, 1995.

DAFT, Richard, Management, International Edition, Tercera edición, Estados Unidos, 1993.

FORCHT, Karen A, "Privacy, confidentiality, security and control issues relating to the wide-spread use of the information highway", URL http://lattanze.loyola.edu/lattanze/research/wp0996.031.html, Octubre 1998

FRASER, Barbara, "RFC 2196", URL http://sunsite.auc.dk/RFC/rfc/rfc2196.html, Diciembre 1998.

GARFINKEL, Simson; Gene, Web security & Commerce, O'Reilly & Associates, Inc., Primera Edición, Estados Unidos, 1997.

McGEE, James, Laurence, Managing Information Strategically, John Wiley & Sons, Primera edición, Estados Unidos, 1993

KARANJIT, Siyan, Firewalls y la Seguridad en Internet, Traductor: Jorge Luis Gutiérrez, Prentice Hall, Segunda edición, México, 1997.

KAUFMAN, Charlie, Radia, Network Security: Private communication in a public world, Prentice Hall PTR, Primera edición, Estados Unidos, 1995.

RUSSELL, Deborah; Gangemi, Computer Security Basics, O'Reilly & Associates, Inc., Primera Edición, Estados Unidos, 1991.

SOS Corporation, "An introduction to firewalls", URL

STALLINGS, William. Network and Internetwork Security Principles and Practice, Prentice Hall, Primera edición, Estados Unidos, 1995.

TELLEEN, Steven, "Intranet Organizations: Strategies for managing change", URL http://www.iorg.com/intranetorg/, Noviembre 1998

WACK, John, Lisa, "Keeping your site confortably secure: An introduccion to Internet Firewalls", URL http://csrc.ncsl.nist.gov/nistpubs/800-10/, Noviembre 1998.