VNIVERSIDAD NACIONAL AVFNOMA DE MEXICO

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA

FACULTAD DE INGENIERÍA

ANALISIS Y DISEÑO DE UNA METODOLOGIA DE SEGURIDAD BASADA EN LA NORMA ISO 17799 PARA UNA RED DE DATOS CORPORATIVA

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN INGENIERÍA

ELÉCTRICA - TELECOMUNICACIONES

P R E S E N T A :

SILVIA GABRIELA FRANCO ESTRADA

DIRECTOR DE TESIS:
DR. FRANCISCO J. GARCÍA UGALDE

MÉXICO **2006**

JURADO ASIGNADO

Presidente:	Dr. Víctor Rangel Licea.
Secretario:	Dr. Ramón Gutiérrez Castrejón.
Vocal:	Dr. Francisco J. García Ugalde.
1er Suplente:	Dr. Javier Gómez Castellanos.
2º. Suplente:	Dr. Rogelio Alcántara Silva.

Lugar o lugares dónde se realizó la tesis:

DIVISIÓN DE ESTUDIOS DE POSGRADO
FACULTAD DE INGENIERÍA

DIRECTOR DE TESIS

DR. FRANCISCO J. GARCÍA UGALDE

A MI ABUE LUPE (Q.E.D.)

A quien dedico el presente ,
por haber sido una persona fundamental en mi vida.

A DIOS:

Por darme la vida y fortaleza para poder realizar un propósito más.

A MI MAMÁ:

GUADALUPE ESTRADA GARIBAY

Como un homenaje por su dedicación, apoyo y cariño incondicional para que cada día yo sea mejor.

A MI TUTOR Y DIRECTOR DE TESIS:

DR. FRANCISCO J. GARCIA UGALDE

Como un testimonio de gratitud por su amistad e inestimable ayuda para la culminación de este trabajo.

A LA UNAM:

Por darme la oportunidad de culminar otra meta en mi carrera profesional.

G R A C I A S

GABRIELA

I N D I C E

CAPITULO 2

2. NORMA ISO 17799 PARA LA GESTION DE SEGURIDAD DE LA INFORMACION

CAPITULO 3

3. METODOLOGIA DE SEGURIDAD PROPUESTA, BASADA EN LA NORMA ISO 17799 PARA UNA RED DE DATOS CORPORATIVA, ASI COMO SU APLICACION.

CAPITULO 4

4. EVALUACION Y RESULTADOS DE LA METODOLOGIA DE SEGURIDAD PARA UNA RED DE DATOS CORPORATIVA

Índice de Figuras y Tablas

Figuras:

Tablas:

OBJETIVOS:

Como objetivos se marcan:

Entender la situación de un medio ambiente interconectado en el ámbito de los negocios y de ahí fomentar la seguridad informática; presentando un problema real de seguridad en una red corporativa, identificando los aspectos relevantes sobre la vulnerabilidad de los sistemas de información, los posibles atacantes y la fuerza que estos pueden tener.

Adquirir conocimientos, metodologías y herramientas de implementación y control de medidas de seguridad de la información de acuerdo con el estándar internacional ISO 17799 para:

- La formación PROFESIONAL
- La IMPLEMENTACION PRACTICA en las organizaciones

Así como el estudio de una teoría relacionada con la Seguridad Informática, para diseñar una metodología que permita aumentar la seguridad en las redes corporativas.

R E S U M E N

La Seguridad hoy en día como materia académica no existe, y es considerada como una herramienta dentro del ámbito en que se le estudia: estudios de riesgo, prevención de crímenes y pérdidas, etc. Muchos sostienen que es una teoría tan amplia, compleja y abstracta que ni siquiera arriesgan su definición.

El amplio desarrollo de las nuevas tecnologías informáticas está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

Hoy día las empresas y organizaciones tienen un gran nivel de **dependencia informática** y esto implica que sean más **vulnerables a las amenazas de seguridad**. Además los sistemas de las empresas u organizaciones dialogan con otros sistemas. Por lo tanto, en lo relacionado con los parámetros de seguridad utilizados, es muy importante basarse en un estándar para poder ajustarse y ser compatibles con los otros sistemas.

Utilizar un estándar homologado, provocará que haya pocas posibilidades de tener que cambiar aspectos del manejo de seguridad informática cuando se establecen acuerdos con otras partes.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige como mínimo, la participación de todos los empleados de la organización.

A fin de lograr una mayor protección de la información surge la necesidad de definir pautas para resguardarla. La Norma ISO 17799 nace en respuesta a dicha necesidad. Esta norma es un estándar para manejo de la seguridad de la información reconocido internacionalmente.

Así mismo, en este trabajo se propone una Metodología de Seguridad, que engloba a los diez objetivos de control que define el estándar ISO 17799, tal metodología está conformada por 4 Fases trascendentales las cuales son:

Fase de Preparación. Esta ayuda a definir la arquitectura de Seguridad sobre la cual se va a trabajar, estableciendo diversos lineamientos básicos de Seguridad.

Fase de Análisis Preliminar. Ayuda a inventariar recursos de *hardware* y *software*, a clasificar la información así como realizar un análisis exhaustivo de riesgos y vulnerabilidades que pueden aquejar a la empresa.

Fase de Definición de políticas y estándares. Para manejar la normalización existente en la organización, identificar qué políticas y estándares existen y que tanto se llevan a cabo.

Fase de Implementación. Ayuda a implementar diversos controles de Seguridad así como fomenta la educación de Seguridad a usuarios de la información.

En este trabajo se evalúa y se muestra la efectividad de la metodología de Seguridad propuesta, aplicándola a una red de datos corporativa de una empresa pequeña. Así como también se muestran los resultados y se identifican las mejorías y beneficios que se obtienen. Haciendo un análisis y evaluación de posibles riesgos, dando como resultado un plan de contingencia. Posteriormente se dan a conocer algunas recomendaciones para cubrir ciertos puntos vulnerables que se encuentran en la red de estudio, siendo este el principal objetivo de la presente tesis.

Este estudio se lleva acabo, colocando un **IDS (Sistema de Detección de Intrusos)** en su red comprendida por 50 máquinas y así monitorear y encontrar posibles vulnerabilidades en la red, identificando así la falta de aplicación de políticas de Seguridad.

Como resultado de la implementación de tales fases, respaldadas por la buenas prácticas señaladas por la Norma ISO 17799, se obtiene toda una arquitectura de Seguridad a diferentes niveles, donde de igual manera se propone crear una **Dirección de Seguridad de la Información**, encargada de dar continuidad a tales recomendaciones, logrando con esto

permitir a cualquier organización obtener un mejor lugar en su mercado de desarrollo, minimizando sus vulnerabilidades y riesgos sobre su activo más importante: sus datos.

C A P Í T U L O 1

CONCEPTOS DE LA SEGURIDAD EN REDES

1. CONCEPTOS DE LA SEGURIDAD EN REDES

1.1 Introducción

A medida que las empresas han ido apoyando sus operaciones más confidenciales en la red de datos, la Seguridad en los sistemas informáticos se va tornando una preocupación cada vez más importante. Anteriormente, los ataques a la Seguridad eran sólo una circunstancia que provocaba pérdidas de tiempo, pero en la actualidad los riesgos para las empresas e instituciones son más graves, ya que la mayoría de las operaciones y transacciones se manejan vía redes de datos y telecomunicaciones. Hoy en día, una violación a la Seguridad de una red cableada o inalámbrica puede provocar el caos en las operaciones más sensibles de una empresa, afectando la productividad, poniendo en peligro la integridad de los datos, reduciendo la confianza de los clientes, interrumpiendo el flujo de información y llegando incluso hasta suspender las comunicaciones.

Hace no mucho tiempo, las redes de las empresas eran autónomas y su Seguridad constituía una tarea relativamente sencilla, es decir, cada área de la organización contaba con su propia red, pero no existía intercomunicación entre dichas áreas y mucho menos con redes externas. El perímetro de la red era fácil de delimitar y se podía brindar una protección adecuada con dispositivos de Seguridad simples.

Sin embargo, con el avance de *Internet* y la generalización del uso de las redes inalámbricas, las redes de las empresas han cambiado de tal modo que presentan nuevos y grandes desafíos para la Seguridad. A medida que las empresas abren sus infraestructuras para admitir dicha conectividad, desaparece el concepto de red tradicional. Las empresas han crecido en tal dimensión que actualmente los dispositivos de Seguridad diseñados no son suficientes para satisfacer sus necesidades de Seguridad y ahora son mucho más vulnerables a los ataques de “*hackers*” y otros agentes dañinos.

Un dispositivo, o paquete de *software,* de Seguridad individual ya no resulta adecuado como protección de redes abiertas, se necesita una solución de Seguridad robusta e integral, misma que se propondrá al final de la presente tesis.

La situación se complica aún más porque muchos sistemas de Seguridad no tienen capacidad para proteger redes ni están diseñados para trabajar en cooperación con servicios de red. Esto convierte a las empresas aún más vulnerables a los ataques cada vez más sofisticados que se llevan a cabo en la actualidad.

Esto significa que las soluciones de Seguridad se deben abordar como un proceso, aplicado con regularidad y metodología, ya que constantemente aparecen nuevas amenazas. El uso de un único producto, en su primera versión no será efectivo por mucho tiempo. Las organizaciones deben desarrollar dentro de un marco teórico general, su solución de Seguridad con base en un plan estratégico aplicado a sus redes y comunicaciones bien establecidas, y cubriendo las necesidades propias de la arquitectura que se maneje en forma regular y dinámica a medida que surgen nuevas amenazas y que su estructura de red cambie.

1.2 Evolución del término “Seguridad”

La “Seguridad es una necesidad básica. Estando relacionada con la prevención de la vida y las posesiones, es tan antigua como ella misma”. [1]

Los primeros conceptos de Seguridad de que se tiene registro, se inician con los sumerios en el año 3000 A.C. También se sabe que los primitivos reaccionaban con métodos defensivos similares a los de los animales. Así la lucha por la vida se convertiría en una parte esencial y los conceptos de evitar, detectar y reaccionar, ya eran manejados por ellos.

La Seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones. Se tuvieron que concebir nuevas estrategias de intimidación y alertas para la supervivencia de las mismas.

La Seguridad comenzó a especializarse surgiendo así la Seguridad Externa, como aquella que se preocupa por la amenaza de factores externos hacia la organización, y la Seguridad Interna, como aquella preocupada por las amenazas que se originan en la propia organización.

El concepto moderno de Seguridad se originó con la Revolución Industrial para combatir los delitos y movimientos laborales comunes de aquella época. Finalmente, Henry Fayol en 1919 [1] identifica la Seguridad como una de las funciones empresariales.

Este autor [1] manifiesta que el objetivo de la Seguridad es, salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas, y de forma amplia todos los disturbios sociales y naturales que puedan poner en peligro el progreso, e incluso la vida del negocio.

En la actualidad, la Seguridad se puede ver desde diversos puntos de vista, por ejemplo, desde el punto de vista técnico, la Seguridad esta en manos de la dirección de las organizaciones y en cada una de las personas que laboran en ellas, logrando cierta conciencia respecto a la importancia de la información y el conocimiento.

En este proceso de evolución del concepto de Seguridad se puede observar que no es nuevo y que actualmente se ha perfeccionado y acoplado al entorno tecnológico en donde se aplique.

1.3 La Seguridad como concepto

“La Seguridad es hoy en día una profesión compleja con funciones especializadas” [1]

El concepto de Seguridad tiene cierto grado de incertidumbre ya que tiene distinto significado para distintas personas y en situaciones diferentes.

Para dar una respuesta satisfactoria es necesario eliminar dicha incertidumbre y distinguir que es en si la Seguridad. Es por eso que ese autor se dio a la tarea de investigar dicho concepto, logrando resaltar que la Seguridad *se aplica a ciertos objetos, o mecanismos, que sirven para asegurar que estos se encuentren en perfecto funcionamiento.*

En nuestro dominio de trabajo, es importante resaltar no precisamente el concepto de Seguridad por si solo, sino asociarlo a problemas informáticos, surgiendo así el concepto de Seguridad Informática, originado a partir de la era de la Información. También

es de vital importancia demostrar que para las pequeñas y medianas empresas, ésta todavía no existe, o es muy escasa.

La Seguridad en la informática no puede ser vista como un producto que se instala una vez y se deja olvidado. La Seguridad debe ser un proceso de monitoreo, verificación, entrenamiento y actualización continuos, la mejor herramienta para prevenir ser victima de un incidente de Seguridad es el conocimiento de nuestros activos y los riesgos potenciales que enfrentan, así como los mecanismos con qué protegerlos.

La Seguridad requiere también de la participación de todos los usuarios. Si todos prestan su apoyo y colaboran en establecer las medidas de Seguridad y en ponerlas en práctica, cualquier sistema tendera a mejorar.

1.4 Concepto y Objetivo de la Seguridad Informática

La Seguridad Informática consiste en prevenir, impedir, detectar y corregir violaciones a la Seguridad durante la transmisión y almacenamiento de información, esta abarca la Seguridad de Sistemas Operativos, Bases de Datos y por supuesto Redes y Telecomunicaciones. Aquí se debe considerar la información esencialmente en forma digital y la protección se asegurara principalmente por medios formales lógicos, más que físicos.

A grandes rasgos se entiende que mantener un sistema seguro consiste básicamente en garantizar tres aspectos, surgidos de la teoría del cifrado de datos: *confidencialidad, integridad y disponibilidad.*

La **confidencialidad** establece que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados para ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades. La **integridad** significa que los objetos solo pueden ser modificados por elementos autorizados y de una manera controlada, y por ultimo, la **disponibilidad** indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados.

Se acaban de mencionar los aspectos básicos para garantizar la Seguridad Informática, pero también es importante hacer notar tres aspectos más, que también deben ser tomados en cuenta, como son: la **autenticidad**, que es la propiedad que permite asegurar el origen de la información, es decir, la identidad del emisor debe ser validada, de modo que se pueda demostrar que es, quien dice ser, de este modo se evita que un usuario envíe una información haciéndose pasar por otro; la **auditabilidad** que es la capacidad de determinar qué acciones o procesos se han llevado a cabo en el sistema y quién y cuándo los ha llevado a cabo, manteniendo un registro de las actividades del sistema, y considerando que este registro este altamente protegido contra modificaciones.

Y por ultimo, el **No repudio** que ofrece protección a un usuario frente a otro que niegue posteriormente que en realidad se realizo cierta comunicación, mediante una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. Las firmas digitales constituyen el mecanismo más empleado para este fin.

Con toda la información planteada con anterioridad, se puede decir, que el objetivo de la “Seguridad Informática es mantener la confidencialidad, integridad y disponibilidad, así como el control y la autenticidad de la información manejada por computadora”. [2]

1.5 Sistemas de Seguridad

Es de vital importancia conocer las distintas funciones que se deben asegurar en un sistema de red.

1. **Reconocimiento:** Cada usuario se debe identificar al usar el sistema y los recursos de red, y cada operación del mismo debe ser registrada con esta identificación. En este proceso se quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos, o que en su defecto, esta quede registrada.
2. **Integridad:** Una red integrada es aquella en la que todas las partes que la componen funcionan en forma correcta y en su totalidad, y en la que se tiene la confianza de que la información que circula no ha sido modificada por terceros.
3. **Aislamiento:** Los datos utilizados por un usuario deben ser independientes de los de otros, física y lógicamente, usando técnicas de ocultación y/o compartimiento.

También se debe lograr independencia entre los datos accesibles y los considerados críticos.

4. **Auditabilidad:** Es el procedimiento que se aplica al sistema para la elaboración de exámenes, demostraciones, verificaciones, o comprobaciones que servirán en la evaluación del mismo. Esta evaluación debe ser periódica y debe brindar datos precisos que aporten confianza al nivel estratégico de la organización.
5. **Controlabilidad:** Todos los sistemas y subsistemas que administren a una red deben estar bajo control permanentemente.
6. **Recuperabilidad**: En caso de emergencia, debe existir la posibilidad de recuperar los recursos de información perdidos o dañados.
7. **Administración y Custodia:** La vigilancia nos permitirá conocer en todo momento cualquier suceso para luego realizar un seguimiento de los hechos y permitir una retroalimentación del sistema de Seguridad, de tal forma que se mantenga actualizado contra nuevas amenazas.

1.6 ¿De quién se debe proteger?

Para entrar a este punto, se deben definir tres conceptos importantes para el desarrollo de este tema, que son: *amenaza, riesgo e intruso*.

Una **amenaza,** en el entorno informático, se puede definir como cualquier elemento que comprometa al sistema, el cual puede ser: de origen humano, o desastre natural.

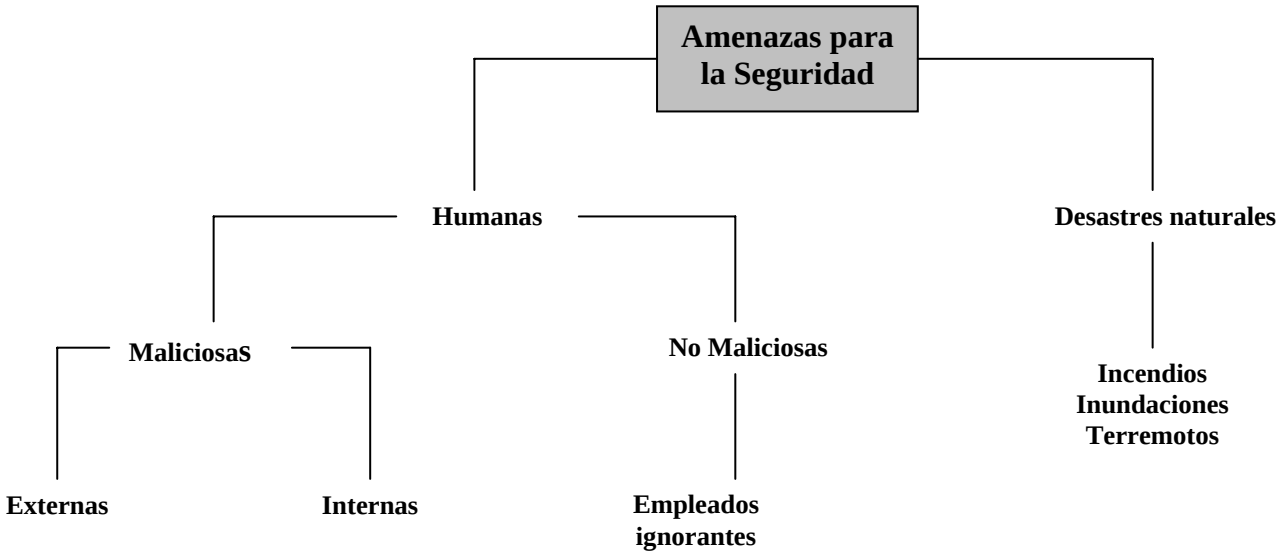


Figura 1.1 Amenazas para la Seguridad

Las amenazas pueden ser analizadas en tres momentos: antes, durante y después del ataque:

- **La prevención (antes):** consiste en mecanismos que aumentan la Seguridad de un sistema durante su funcionamiento normal. Ejemplo, el cifrado de información para su posterior transmisión.
- **La detección (durante):** son los mecanismos orientados a revelar violaciones a la Seguridad, generalmente son: programas de auditoria.
- **La recuperación (después):** están formados por mecanismos que se aplican, cuando la violación del sistema ya se ha detectado para retornar éste a su funcionamiento normal, por ejemplo, recuperación desde las copias de Seguridad realizadas previamente (*Back up*).

Un **riesgo** se puede definir como: la proximidad, o posibilidad de daño sobre un bien, ya sea por sucesos naturales, errores o actos intencionales humanos. Dependiendo de que tipo de riesgo se trate, será su tratamiento, ya sea:

1. Minimizando la posibilidad de ocurrencia
2. Reduciendo al mínimo el perjuicio producido

3. Diseñando métodos para la mas rápida recuperación de los daños experimentados
4. Corrigiendo las medidas de Seguridad en función de la experiencia recolectada

Como se menciono anteriormente, las amenazas y los riegos producen daños, pero también el daño es resultado de la no-acción, o una acción mal tomada. Ya sea por que no se supo identificar adecuadamente la amenaza, o en su defecto, se impusieron criterios no técnicos para sanear temporalmente alguna deficiencia de Seguridad. Es aquí donde se deben detectar cada una de las **vulnerabilidades,** o **debilidades,** del sistema que pueden ser explotadas, o empleadas, por las amenazas, y en consecuencia, saber como aplicar las contramedidas, o técnicas, de protección adecuadas.

Al analizar los conceptos mencionados anteriormente, se debe hablar de un sistema fiable de donde se puede resaltar que “la fiabilidad es la probabilidad de que un sistema se comporte tal y como se espera de él”. [3]

Ahora, es importante responder a la pregunta ¿De quién se debe proteger? Es en este punto donde entran los **intrusos**, o atacantes, como las personas que acceden o intentan acceder sin autorización a un sistema ajeno, ya sea de manera intencional o accidental.

Existen cuatro tipos de intrusos que menciona Julio C. Ardita, Director de una empresa de Seguridad (y *ex-hacker)*. [4] “Los tipos de intrusos se pueden caracterizar desde el punto de vista del nivel de conocimiento, formando una pirámide. Estos se clasifican en:

1. **Clase A.** El 80%, en la base de la pirámide son los nuevos intrusos que bajan programas de Internet, están jugando y son pequeños grupitos que se juntan y dicen vamos a probar.
2. **Clase B.** Es el 12% siguiente, son más peligros, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar el sistema

operativo que esta usando la victima, examinan las vulnerabilidades del mismo e ingresan a través de ellas.

3. **Clase C.** Corresponde al 5%, es gente que sabe, conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.
4. **Clase D.** El 3% restante en el pico de la pirámide, cuando entran a determinados sistemas buscan la información que necesitan.

Para llegar desde la Clase A hasta la D, se necesita en promedio de 4 a 6 años, por el nivel de conocimiento que se requiere asimilar: práctica, conocimiento, programación, tiempo dedicado." [4]

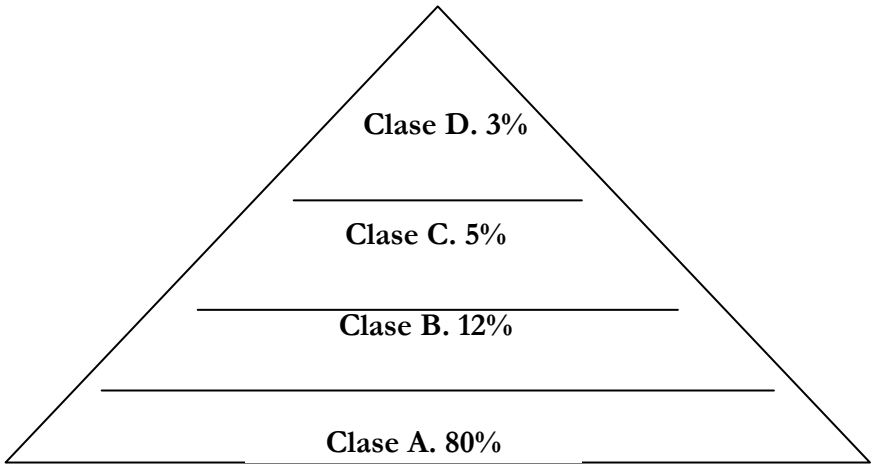


Figura1.2 Tipos de intrusos

1.7 ¿Qué se debe proteger?

Es prioritario conocer qué se debe proteger en cualquier sistema informático, es por eso que se mencionan tres elementos básicos a proteger, que son: el *hardware*, el *software* y los datos.

Por **hardware** se debe entender al conjunto de todos los elementos físicos de un sistema informático, ya sean internos, o externos.

El **software** es el conjunto de programas lógicos que hacen funcionar al *hardware*, ya sean sistemas operativos, lenguajes de programación, aplicaciones, etc.

Por último, los **datos** son el conjunto de información lógica que maneja el *software* y el *hardware*, como por ejemplo: archivos, bases de datos, documentos, etc. que nos ayudarán al mejoramiento de toma de decisiones; además es catalogado como el principal activo de toda organización.

Al ser el activo más importante de toda organización, los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y el más difícil de recuperar, es por eso que siempre se debe de pensar de manera obligatoria en un sistema de copias de Seguridad (*Back up*) que debe estar en constante actualización.

1.8 ¿Cómo se va a proteger?

A continuación se explicarán de manera breve algunos de los mecanismos de Seguridad más utilizados que proveen una protección contra amenazas, o ataques, costosos para las empresas; la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información, también poseen alguna información secreta como claves o contraseñas, algoritmos de cifrado y de descifrado, generación de números aleatorios, etc. Los más importantes son:

- **Intercambio de autenticación**: Corrobora que una entidad, ya sea origen o destino de la información, es la deseada. Por ejemplo, un protocolo utilizado es el siguiente: un usuario X envía una información aleatoria cifrada con una clave que solo el usuario Y conoce, Y lo descifra con esta clave y se lo reenvía a X, con esta técnica se demuestra que el usuario es quien pretende ser, más adelante se detallará un poco más este mecanismo.
- **Cifrado:** Garantiza que la información no es legible para usuarios, o procesos, no autorizados. Consiste en transformar un texto en claro, mediante un proceso de cifrado, en un texto cifrado.
- **Integridad de datos:** Este mecanismo implica el cifrado de una cadena comprimida (huella) de datos a transmitir, llamada Valor de Comprobación de Integridad (*Integrity Check Value,* o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la obtención de la huella y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, si ambos coinciden se da por buena la integridad.

- **Firma digital:** Este mecanismo implica el cifrado de una cadena comprimida (huella) de datos que se va a transferir por medio de la clave secreta del emisor. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar la firma.
- **Control de acceso:** Es el proceso que se lleva a cabo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema, o a la red, ya sea mediante contraseñas de acceso, o reconocimiento de patrones.
- **Tráfico de relleno:** Consiste en enviar tráfico basura junto con los datos validos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se están transmitiendo.
- **Control de encaminamiento:** Permite enviar determinada información por determinadas zonas clasificadas. También se posibilita solicitar otras rutas en caso de que se detecten posibles amenazas de integridad en una ruta determinada.
- **Unicidad:** Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores que se incluyen en una firma digital.

En la lista anterior, se acaban de mencionar mecanismos de Seguridad, pero también es importante dar a conocer métodos más elaborados de protección, estos métodos se deben ligar a las políticas de Seguridad que se vayan a implementar. Los principales métodos son:

- **Sistemas de detección de intrusos**. Son aquellos que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento, es decir, eventos que puedan considerarse sospechosos, con base en la información con la que han sido alimentados previamente. Se pueden considerar como sistemas de monitoreo.
- **Sistemas orientados a conexión de red**. Estos sistemas tienen la capacidad de monitorear las conexiones de red que se intentan establecer, siendo capaces de establecer una acción con base en ciertos criterios como pueden ser el origen y destino de la conexión, el servicio solicitado, el tiempo de conexión, etc. Las acciones que pueden emprender estos sistemas pueden ir desde el rechazo de la conexión hasta alertar al administrador mediante correo electrónico. Un ejemplo muy claro de este sistema son los llamados “muros cortafuegos” *Firewalls*.

- **Sistemas de análisis de vulnerabilidades**. Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. Existe una desventaja muy clara en este tipo de sistemas, ya que pueden ser utilizados por personas no autorizadas que busquen accesos malintencionados a la red, o a cualquier tipo de sistema.
- **Sistemas de protección a la privacidad de la información.** Estos sistemas utilizan criptografía para asegurar que la información solo es accesible para quien tiene autorización de usarla. Se utiliza principalmente en telecomunicaciones.
- **Sistemas de protección a la integridad de la información.** Son sistemas que mediante criptografía tratan de asegurar que no ha habido alteraciones no deseadas en la información que se intenta proteger.

Se quiere hacer notar que es realmente importante tener en cuenta que para implantar un sistema de Seguridad es necesario realizar un análisis interno y detallado, que comprenda desde los procesos, quién, cómo, cuándo y con qué frecuencia se realizan, de tal manera que dicho sistema se acople de la mejor manera a las necesidades de la organización. Realizar adecuadamente este análisis, proporciona a la organización una mejor perspectiva al tomar la decisión de cuánto vale la pena invertir en un sistema de Seguridad.

1.9 ¿Por qué Proteger?

Sin duda alguna, las redes han transformado y mejorado la forma de hacer negocios entre compañías. En contraparte, las redes y las tecnologías han abierto las puertas de una gran cantidad de amenazas de Seguridad de las cuales deben protegerse.

A pesar de que se supone que los ataques más graves a las redes suceden cuando afectan a negocios que manejan datos confidenciales, como datos financieros o antecedentes de la organización, las consecuencias de los ataques a cualquier entidad oscilan entre los que ocasionan un problema leve, o hasta completamente devastadores. Esto puede implicar pérdida de datos importantes, violación de la privacidad y hasta la paralización de las operaciones que se efectúan dentro de la red por tiempo ilimitado.

A pesar de los riesgos costosos de las potenciales violaciones a la Seguridad. Las redes pueden ser uno de los medios más seguros para realizar negocios, ya que las transacciones por *Internet*, para el comercio electrónico pueden estar protegidas con una tecnología de Seguridad.

El temor a los problemas de Seguridad puede ser tan perjudicial para los negocios como lo son las violaciones mismas a la Seguridad. Esta desconfianza puede limitar las oportunidades comerciales para las empresas, especialmente las que basan sus operaciones completamente en la *Web*. De este modo, las empresas deben crear políticas de Seguridad y estimular resguardos que sean efectivos para la organización.

Para las organizaciones lo más importante son sus clientes, y al utilizar tecnologías para sus procesos de negocio deben brindar al cliente protección para procurar una mayor confianza hacia la organización. Aparte de brindarle protección al cliente se debe proteger a los empleados y socios ante las violaciones a la Seguridad.

Internet, Intranet, Extranet permiten una comunicación rápida y efectiva entre empleados y socios. No obstante, tanto la comunicación como la eficiencia pueden verse impedidas por los efectos de un ataque a las redes.

Es evidente que la perdida de datos importantes y por añadidura de un tiempo valioso, puede ocasionar un gran impacto en la organización. Por eso a continuación se hará mención de la importancia de proteger los datos.

1.9.1 ¿Por qué proteger los datos?

En la actualidad, con toda la evolución de la tecnología las empresas han obtenido beneficios significativos respecto al manejo eficiente de sus datos, pero a su vez también esto ha traído consecuencias no muy benéficas ya que cualquier empresa es blanco perfecto de los ataques informáticos.

Por eso tener Seguridad en el manejo de su red ha sido vital para mantener la integridad de los datos, ya que son el activo más importante de toda organización y son también factores sumamente importantes. De su buen manejo e integridad depende el éxito de la empresa.

La imposición por parte de la Agencia de Protección de Datos que da importantes sanciones económicas a varias empresas, entre las que se incluye la reciente pena a un importante proveedor de acceso a Internet, ha contribuido a incrementar la sensibilidad de las compañías para la protección de los datos de carácter personal de sus clientes, personal, proveedores, etc.

El manejo de los datos requiere acatar políticas de Seguridad y estas especifican condiciones, derechos y obligaciones sobre el uso de los datos.

Estas son importantes ya que previenen perdida de información, uso adecuado de las bases de datos y sistemas, ayudan a la adquisición eficaz de *hardware* y *software*, permite a las autoridades actuar en caso de violación a la Seguridad de los datos y sobre todo evita la ignorancia. [5]

Así para la protección de estos datos existen niveles de Seguridad que a continuación se explican.

1.9.2 Niveles de Seguridad Informática

"El estándar de niveles de Seguridad Informática más utilizado internacionalmente es el TCSEC *Orange Book*" [6], el cual fue desarrollado en 1983 como consecuencia de la creciente conciencia de la Seguridad por parte del gobierno de los Estados Unidos y de la industria, ambos con la necesidad de estandarizar el propósito y el uso de las computadoras del gobierno federal (en específico del Departamento de Defensa de los Estados Unidos).

Los niveles de Seguridad describen diferentes tipos de Seguridad del Sistema Operativo y pasan del mínimo hasta el máximo grado de Seguridad.

Estos niveles han sido la base del desarrollo de estándares europeos como (ITSEC o ITSEM) o de internacionales como (ISO 17799 e IEC).

Los propósitos principales del llamado *Orange Book* son:

- **Medición.** Proporciona aquellos elementos cuantificables, es un criterio con el cual se puede evaluar la confianza.

- **Dirección.** Son las características de Seguridad que se deben implementar en productos comerciales y así ofrecer sistemas que puedan satisfacer los requisitos de Seguridad.
- **Adquisición.** Es la base para especificar los requerimientos de Seguridad para adquisiciones determinadas.

Nivel D: Protección Mínima

Este nivel contiene solo una división reservada para sistemas que han sido evaluados y no pueden cumplir los requisitos para una clase más alta de evaluación. Son sistemas no confiables, no hay protección para el *hardware*, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información.

Algunos ejemplos de Sistemas Operativos que responden a este nivel son: MS-DOS y *Windows* de la compañía *Microsoft*.

Nivel C1: Protección Discrecional

Se requiere una identificación de usuarios que permita el acceso a distinta información y a través de capacidades de auditoria, exige la responsabilidad de los usuarios de las acciones que realiza. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, este último tiene el control total de accesos.

Muchas de las tareas cotidianas de administración del sistema solo pueden ser realizadas por el “Administrador”, quien tiene gran responsabilidad en la Seguridad del mismo.

A continuación se enumeran los requerimientos mínimos que debe cumplir el nivel C1:

- **Acceso de control discrecional.** Incorpora mecanismos de control y acreditación, hace cumplir las restricciones de acceso en una base, por lo que se realiza una distinción entre usuarios y recursos, de manera que se pueden

definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco). Garantiza que la información este protegida y evita que otros usuarios puedan leer o destruir datos.

- **Identificación y Autentificación.** Con el propósito de hacer cumplir más fielmente el acceso mediante acceso discrecional más fino; se hace responsable de manera individual a los usuarios de sus acciones a través de procedimientos de conexión, revisión de eventos relevantes y aislamiento de recursos. Se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. Los datos de un usuario no podrán ser accedidos por otro usuario sin autorización o identificación.

Nivel C2: Protección de Acceso Controlado

El propósito de este nivel es: reducir las debilidades del nivel C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se realiza una auditoria de accesos e intentos fallidos de acceso a objetos (archivos, directorios, disco). Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos, o se tenga acceso a ciertos archivos, así como permitir, o denegar, datos a usuarios en particular, con base en los permisos y los niveles de autorización.

Requiere que el sistema sea auditado, dicha auditoria se utiliza para llevar registros de acciones relacionadas con la Seguridad, como son: actividades efectuadas por el administrador del sistema y sus usuarios. La auditoria requiere de una autentificación adicional para asegurar que la persona que ejecuta determinada operación es quien debe ser. La gran desventaja radica en los recursos requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que cada usuario ejecuta el trabajo y no el administrador.

Nivel B1: Seguridad Etiquetada

Este subnivel, es el primero de los tres con los que cuenta el nivel B. Soporta Seguridad multinivel, secreta y ultra secreta. El dueño del archivo no puede modificar los permisos de un objeto que esta bajo control de un acceso obligatorio. A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de Seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nominas, ventas, etc.).

Cada usuario que accede a un objeto debe tener un permiso para hacerlo y viceversa, es decir que cada usuario tiene sus objetos asociados. Se establecen controles para limitar el derecho de accesos a distintos recursos.

Nivel B2: Protección Estructurada

Este nivel requiere etiquetado de cada nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de Seguridad, en comunicación con otro objeto a un nivel inferior.

El sistema es capaz de alertar a los usuarios si es que las condiciones de accesibilidad y de Seguridad son modificadas y es el administrador quien se encarga de fijar el almacenamiento y ancho de banda a utilizar para los demás usuarios.

Nivel B3: Dominios de Seguridad

El nivel B3 refuerza a los dominios complementándolos con la instalación de *hardware*. Como por ejemplo: el *hardware* de administración de memoria se utiliza para proteger el dominio de Seguridad de acceso no autorizado a la modificación de objetos, de diferentes dominios de Seguridad. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite, o las deniega, de acuerdo a las políticas de acceso que se hayan definido anteriormente.

Todas y cada una de las estructuras de Seguridad deben ser lo suficientemente pequeñas como para permitir un análisis ante posibles violaciones. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una conexión segura. Además cada usuario tiene asignado los lugares y objetos a los que puede acceder.

Nivel A: Protección Verificada

Es el nivel más elevado, este nivel engloba un proceso de diseño, control y verificación que se caracteriza por el uso de métodos formales para la verificación de la Seguridad y así poder garantizar los controles obligatorios, eficacia en la información clasificada, almacenada o procesada por el sistema, en términos generales permite asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de Seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de manera formal matemática y también se deben realizar análisis. El *software* y el *hardware* son protegidos para evitar infiltraciones ante traslados, o movimientos, del equipamiento.

1.10 ¿Qué es la Seguridad en Redes?

Hasta el momento se ha querido dar una perspectiva de la Seguridad Informática en general; ahora y en lo consiguiente, el tema será la Seguridad en Redes, pudiéndola *involucrar con todas y cada una de las actividades que las organizaciones asumen para proteger el valor y la facilidad de uso constante de los activos, la integridad de sus operaciones, mediante redes de comunicación.*

Un descuido en la Seguridad de la Red puede costarle muchas perdidas a una compañía en productividad, datos, trabajos de reparación y pérdida de confianza entre sus clientes, proveedores, socios y empleados.

Con el auge de *Internet* y del comercio electrónico las computadoras privadas y las redes de computadoras son cada vez más vulnerables a los ataques perjudiciales. *Hackers*, virus e incluso errores humanos representan peligros claros y actuales para las

redes. Además todos los usuarios de computadoras podrían verse afectados por descuidos en la Seguridad de las Redes. Es por eso que se debe de contar con una Estrategia de Seguridad en Redes bien definida, que se acople a la arquitectura de la red, para ofrecer un mapa general de los pasos que se deben seguir para proteger y garantizar que el viaje de los datos a través de la infraestructura de red, sea seguro.

La Seguridad en Redes, como ya se menciono en anteriores subtemas de esta tesis, engloba todos los conceptos de Seguridad Informática con el objetivo de prevenir, impedir, detectar y corregir violaciones a la Seguridad, durante la transmisión de información.

Resumiendo, enseguida se mencionan los principales pasos básicos que se deben tomar en cuenta al analizar la Seguridad de una red de cualquier organización, abarcando tanto a sistemas como a personas:

1. **Determinar los recursos a proteger y su valor.**
2. **Analizar las vulnerabilidades y amenazas del sistema de red.**
3. **Definir las medidas a establecer para proteger el sistema en todos sus niveles (físico, lógico, humano y logístico).**
4. **Definir estrategias a seguir en caso de fallos de cualquier nivel.**
5. **Monitorear el cumplimiento de la política y revisarla cada vez que se detecte un problema para su mejora.**

1.11 Ataques, Vulnerabilidades y Riesgos

Los ataques en el ambiente informático, son elementos que comprometen, o ponen en riesgo, la Seguridad del sistema de red. Existen ataques pasivos y ataques activos que se explican a continuación.

- **Ataques pasivos.** “El atacante no altera la comunicación, sino que únicamente la escucha, o monitorea, para obtener información que esta siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico”. [7] Generalmente se emplean para la obtención del origen y destinatario de la

comunicación, control de volumen de tráfico para obtener información acerca de la actividad, o inactividad, entre las entidades monitoreadas, y control de las horas habituales de intercambio de datos entre estas.

- **Ataques activos.** "Estos ataques implican algún tipo de modificación del flujo de datos transmitido, o la creación de falso flujo de datos. Generalmente son realizados por *hackers*, piratas informáticos, o intrusos remunerados y se les puede subdividir en cinco categorías:

  - *Interrupción:* Si hace que un objeto del sistema se pierda, quede inutilizable, o no disponible.
  - *Intercepción:* Si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
  - *Modificación:* Si además de conseguir el acceso, logra modificar el objeto.
  - *Fabricación:* Se consigue un objeto similar al original atacado, de forma que es difícil distinguirlos entre si.
  - *Destrucción:* Es una modificación que inutiliza el objeto". [7]

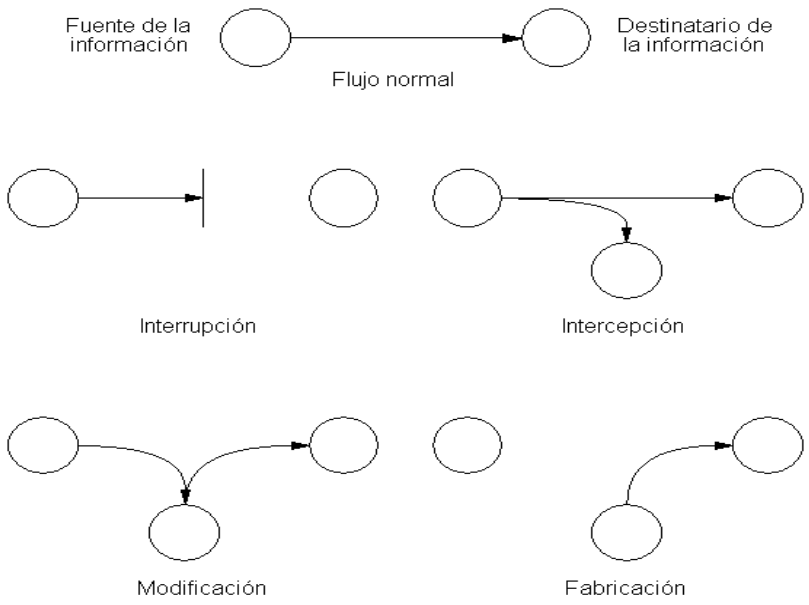


Figura 1.3 Representación de ataques pasivos y activos a la Seguridad del sistema de red

También se debe mencionar el concepto de vulnerabilidades como: aquellas debilidades del sistema que pueden ser explotadas y empleadas por las amenazas y riesgos para comprometerlo y en consecuencia tener el conocimiento de las contramedidas aplicables para cada una de ellas.

Como se mencionó anteriormente, un riesgo es la posibilidad de un daño sobre un bien, ya sea por actos naturales, errores u omisiones humanos, o actos intencionales.

Es difícil lograr la confidencialidad, integridad y disponibilidad para todo el sistema de red cuando no se tiene bien claro contra quién se debe proteger. Desgraciadamente, este es el caso de muchas empresas es decir, no existe un análisis de riesgos que permitan identificar los activos con que se cuenta y los riesgos que pudieran afectarlos y tampoco se tienen estimados de lo que costaría recuperarse de un incidente. Sin toda esta información, elegir mecanismos de protección no tiene mucho sentido, por lo que se adquieren soluciones contra riesgos que no existen, o donde se pasan por alto riesgos críticos.

Al implantar una estrategia de Seguridad se debe comenzar con la identificación de los riesgos potenciales. Este proceso debe ser desarrollado formalmente por personas de todas las áreas de la compañía y dar respuesta de la mejor manera a una serie de cuestionamientos para obtener información de estos riesgos. Las preguntas a responder para planear la protección serían:

- **¿Qué podría pasar?** Buscando identificar los activos existentes (*software*, *hardware*, datos, personas) y los eventos amenazantes.
- **¿Si pasará, qué tan dañino seria?** Buscando cuantificar el impacto en todos los ámbitos de la organización.
- **¿Qué tan frecuente podría pasar?** Identificando la frecuencia de ocurrencia de los eventos amenazantes.
- **¿Qué tan correctas son las respuestas a las tres preguntas anteriores?** Las respuestas estudiadas a estas preguntas permitirán tener un excelente conocimiento sobre los activos con los que se cuenta, así como conocer cual sería el impacto en caso de que sufran algún accidente de Seguridad

1.12 ¿Quiénes son los enemigos?

Actualmente las redes corporativas se han convertido en los objetivos más atractivos, la cantidad de amenazas potenciales internas y externas han aumentado.

La cantidad y variedad de ataques se han multiplicado enormemente y su difusión es cada vez más rápida a medida que avanzan las comunicaciones.

Virus nuevos, más poderosos, se difunden por sí mismos en infraestructuras de redes completas, asociándose a aplicaciones y archivos de datos y hasta multiplicándose entre ellos.

Actualmente, un virus sofisticado puede difundirse a millones de computadoras a través de *Internet* en cuestión de horas y erradicarlo provoca un gasto de miles de millones de dólares.

Los *Hackers* están accediendo con más facilidad que nunca al ataque de las redes. Las herramientas de ataque se descargan fácilmente desde *Internet*, lo que permite que los atacantes monitoreen una red para saber qué sistemas están activos y qué medidas de Seguridad se han implementado. La naturaleza “siempre activa” de las redes de banda ancha a menudo deja la puerta abierta para el ingreso a la red.

1.12.1 *Hackers*

“Este término, a menudo idealizado se aplica a los fanáticos de la computación a quienes les encanta acceder a las redes o computadoras de otras personas.” [8] A muchos *hackers* les agrada simplemente acceder sin autorización a las computadoras de escritorio y dejar sus “huellas” mediante mensajes, o aplicaciones ocurrentes, para probar su hazaña.

Otros *hackers*, generalmente conocidos como “*crackers*”, son más dañinos, producen la paralización de sistemas informáticos íntegros, hurtan, o estropean información confidencial, descompaginan páginas *Web* y básicamente desestabilizan los negocios.

Algunos *hackers* aficionados simplemente posicionan las herramientas de pirateo en paginas de *Internet* y algunos empleados de las organizaciones las implementan sin comprender demasiado cómo funcionan y cuáles son los efectos que producen, ya que esto es un nivel de riesgo alto para la organización.

1.12.2 Personal desprevenido

Debido a que los empleados se concentran en sus obligaciones laborales específicas, generalmente suelen descuidar políticas relacionadas con la Seguridad de la red. Por ejemplo, pueden elegir contraseñas que son fáciles de recordar, para poder conectarse a las redes fácilmente. No obstante, algunos usuarios de la misma organización pueden adivinar fácilmente estas contraseñas usando el sentido común, o con un programa de craqueo de contraseñas. Los empleados pueden inconscientemente ocasionar otras violaciones a la Seguridad, incluyendo la exposición y difusión accidental de virus informáticos. Una de las formas más comunes de contraer un virus es a través de un disco flexible, o de la descarga de archivos de *Internet*.

Los empleados que usan discos flexibles para transferir información pueden involuntariamente infectar las redes de la empresa con virus contraídos de computadoras de bibliotecas, o de cafés *Internet*. Es probable que ni siquiera ellos mismos sepan que los virus se encuentran en sus PC. Las empresas también se enfrentan al riesgo de infección cuando los empleados descargan archivos de *Internet*.

Las empresas también deben estar alertas ante errores humanos. Los empleados, ya sean principiantes, o expertos en computación, pueden cometer errores tales como instalar erróneamente un *software* de protección antivirus, o accidentalmente pasar por alto advertencias relacionadas con las amenazas a la Seguridad.

1.12.3 Personal descontento

Los empleados disgustados contra la empresa por alguna razón, pueden vengarse infectando las redes de la empresa con virus o eliminando archivos importantes. Estas personas son especialmente peligrosas porque en general tienen conocimientos de la importancia del contenido de la información, de la ubicación estratégica de la información

considerada de alta confidencialidad y de todas aquellas políticas de Seguridad establecidas para protegerla.

1.12.4 Curiosos

Los empleados identificados como “curiosos” participan en espionajes de la empresa, accediendo sin autorización a datos confidenciales a fin de facilitar a la competencia información que de otra forma no se puede obtener.

Otros empleados simplemente satisfacen su curiosidad personal accediendo a información personal y privada, como datos financieros, mensajes de correo electrónico entre compañeros de trabajo.

El revisar datos financieros o información de recursos humanos, son hechos mucho más graves, pueden ser perjudiciales y generar una responsabilidad económica por parte de la empresa.

1.13 ¿Cuál es la Metodología de Seguridad en red?

Una estrategia efectiva de Seguridad en red requiere identificar las amenazas y después seleccionar el conjunto de herramientas tecnológicas más efectivas para combatirlas, las amenazas más comunes a la Seguridad de una red se describen a continuación:

1.13.1 Virus

Los virus son las amenazas a la Seguridad más conocidas. “Los virus son programas informáticos generados por programadores malintencionados y están diseñados para que se reproduzcan solos, e infecten a las computadoras cuando un evento específico los active.” [8] Por ejemplo, los virus denominados virus de macro atacan a los archivos con instrucciones de macro (rutinas que se pueden repetir automáticamente) y se activan cada vez que la macro se ejecuta, por ejemplo la paquetería de *Office* utiliza macros.

Los efectos de algunos virus son relativamente benignos y provocan interrupciones molestas, tal como la presentación de un mensaje gracioso cada vez que se pulsa una determinada letra del teclado.

Otros virus son más destructivos y ocasionan problemas tales como la eliminación de archivos de un disco duro, o la inestabilidad de un sistema. Una red puede verse infectada por un virus sólo si el mismo ingresa a la red por una fuente externa: muchos virus suelen proceder de un disco flexible infectado, o de un archivo descargado de *Internet*. Cuando una computadora de la red está infectada, las demás computadoras son más propensas a contraer el virus.

1.13.2 Programas troyanos

"Los programas troyanos, o caballos de Troya, son instrumentos de distribución para código destructivo. Los troyanos parecen programas útiles, o inofensivos, por ejemplo juegos de computadora, pero en realidad son enemigos encubiertos. Estos programas pueden eliminar datos, enviar copias de sí mismos a listas de direcciones de correo electrónico y acceder a computadoras para realizar otros ataques. Los troyanos sólo pueden contraerse al copiar el programa a un sistema mediante un disco, al realizar descargas de *Internet*, o al abrir un archivo adjunto de correo electrónico." [8] Ni los troyanos ni los virus pueden difundirse por un mensaje de correo electrónico: sólo se propagan por los archivos adjuntos de correo electrónico.

1.13.3 Vándalos

"Los sitios *Web* se han vuelto más animados a partir del desarrollo de aplicaciones de *software* tales como *Active* X y *applets* (subprogramas) de Java. Estos dispositivos habilitan la animación y la ejecución de otros efectos especiales, logrando que los sitios *Web* sean más atractivos e interactivos." [9] Sin embargo, la facilidad de descarga y ejecución de estas aplicaciones ha proporcionado un nuevo medio para producir daños. Un vándalo consiste en un subprograma, o una aplicación de *software* que causa destrozos de diversas magnitudes. Un vándalo puede destruir un único archivo, o una gran parte de un sistema informático.

1.13.4 Ataques

"Se han dado a conocer gran cantidad de ataques a redes, que de acuerdo a la investigación realizada se pueden clasificar en tres categorías generales: ataques de reconocimiento, ataques de acceso y ataques de denegación de servicio (DoS)." [9]

Los ataques de reconocimiento consisten básicamente en actividades para reunir información, que permiten a los *hackers* recopilar datos, que se usan para luego poner en peligro las redes. Generalmente, las herramientas de *software*, como los *spyware* y buscadores, se emplean para delimitar los recursos de red y explotar las potenciales debilidades de las redes, los *hosts* y las aplicaciones objetivo. Por ejemplo, existe *software* específicamente diseñado para craquear contraseñas. Este *software* se creó para que los administradores de red puedan brindar asistencia a los empleados que hayan olvidado las contraseñas, o para descubrir las contraseñas de los empleados que dejaron la empresa sin informar a nadie cuáles eran sus contraseñas. Sin embargo, si cae en manos equivocadas, este *software* puede llegar a ser un arma peligrosa.

Los ataques de acceso se realizan para explotar vulnerabilidades en las áreas de red, tales como los servicios de autenticación y la funcionalidad del Protocolo de transferencia de archivos (FTP), a fin de poder acceder a las cuentas de correo electrónico, las bases de datos y otras clases de información confidencial.

Los ataques de denegación de servicios (DoS) impiden el acceso a todo el sistema informático, o a una parte del mismo. Generalmente se logran mediante el envío de una gran cantidad de datos mezclados, o incontrolables, a una máquina que está conectada a una red de la empresa, o a *Internet*, bloqueando el acceso del tráfico legítimo. Aún más perjudicial es el ataque de denegación de servicio distribuido (DDoS), mediante el cual el agresor compromete varias máquinas, o *hosts*.

1.13.5 Intercepción de datos

Los datos transmitidos a través de cualquier tipo de red pueden ser interceptados por personas no autorizadas. Los intrusos pueden escuchar comunicaciones, o incluso alterar los paquetes de datos que se transmiten.

Los intrusos pueden emplear diversos métodos para interceptar la información. Por ejemplo, el falseo de la dirección IP de origen (*IPspoofing*) “consiste en hacerse pasar por una persona autorizada en la transmisión de datos por medio del uso de la dirección IP (Protocolo de *Internet*) de uno de los receptores de la información.” [9]

1.13.6 Ingeniería social

La ingeniería social es utilizada para obtener información confidencial de Seguridad de la red por medios no técnicos. Por ejemplo, un ingeniero social podría darse a conocer como un representante de soporte técnico y llamar a los empleados para que reúnan la información de las contraseñas.

Otros ejemplos de ingeniería social incluyen sobornar a un compañero de trabajo para acceder a un servidor, o revisar la oficina de un compañero para encontrar una contraseña anotada en un sitio oculto.

1.13.7 Correo no solicitado (*Spam*)

“El término *spam* es comúnmente utilizado para referirse al correo electrónico no solicitado, o a la acción de difundir mensajes publicitarios no solicitados a través del correo electrónico.” [9] El *spam* generalmente es inofensivo, pero puede ser una molestia porque ocupa el ancho de banda, el espacio de almacenamiento y el tiempo del receptor.

1.14 En que consisten los 7 elementos de la Seguridad

En teoría una estructura con redes de datos, aplicaciones y herramientas de computaciones confiables, escalables, accesibles y manejables; son esenciales para lograr una implementación de Seguridad efectiva dentro de una organización.

Por lo tanto, básicamente cualquier red debe contar, como mínimo, con las siguientes herramientas de Seguridad de una red.

- *Paquetes de software antivirus.* Estos paquetes encuentran la mayoría de las amenazas de virus si se actualizan con regularidad y se les da un mantenimiento adecuado.
- *Infraestructura de red segura.* Los conmutadores y enrutadores tienen características de *hardware* y de *software* que soportan la conectividad segura, la Seguridad perimetral, protección contra intrusos, servicios de identificación y autenticación, y la administración de la Seguridad.
- *Hardware y software dedicados a la Seguridad de la red.* Herramientas como "muros cortafuegos" *firewalls* y sistemas de detección de intrusos ofrecen protección para la mayoría de las áreas de la red y permiten las conexiones seguras.
- *Redes privadas y virtuales.* Estas redes ofrecen control de acceso y encriptación de datos entre dos computadoras diferentes conectadas a una red. Esto permite que los trabajadores remotos se conecten a la red sin riesgo de que un *Hacker*, o un ladrón interprete los datos.
- *Servicios de identidad.* Estos servicios ayudan a identificar a los usuarios y a controlar sus actividades y transacciones en la red. Los servicios incluyen contraseñas, certificados digitales y claves de autenticación digital.
- *Encriptación* La encriptación garantiza que los mensajes no puedan ser interceptados, o leídos por nadie más que no sea el receptor autorizado.
- *Administración de la Seguridad.* Este es el "pegamento" que mantiene unidos a los otros bloques de construcción de una robusta solución de Seguridad.

Ninguno de estos enfoques por separado será suficiente para proteger toda una red, pero en conjunto pueden ser muy efectivos para mantener una red segura frente a los ataques y otras amenazas contra la Seguridad. Además, las políticas corporativas bien planeadas son críticas para determinar y controlar el acceso a varias partes de la red.

1.15 Beneficios de una solución de Seguridad

Los beneficios más importantes de una solución efectiva de Seguridad de red provienen de la ausencia de intrusiones y ataques. Toda la infraestructura de red, debe de estar protegida, y auxiliándose al mismo tiempo, por equipos especializados que cumplan con funciones específicas de Seguridad como: "muros cortafuegos" *firewalls*, redes privadas virtuales, detección de intrusos y *software* para el control de identificación de usuarios.

Al implementar una solución de Seguridad en red, se pueden evitar ataques costosos, reducir costos de infraestructura y ayudar a mejorar la productividad y confiabilidad de los procesos de información de la organización.

Logrando así beneficios como los siguientes:

- *Reducción de los costos.* Las inversiones en Seguridad dan como resultado un eficiente ahorro tanto en conectividad, infraestructura de comunicaciones, mantenimiento y soporte.
- *Mejoras en la Productividad.* Ayuda a la mejora en la actividad productiva de los empleados, disminuye los riesgos en los procesos obteniendo una mejor calidad, aumenta la confiabilidad de los clientes.
- *Evitar las intrusiones a la Seguridad.* El que la organización se recupere de un daño provocado por una mala administración en la Seguridad puede ser costoso. Además de la pérdida de datos, la pérdida de productividad y el tiempo que se dedica a la tecnología de información para corregir problemas, puede haber gastos no planeados, perdida de clientes y de confianza de los inversionistas, así como un daño a la imagen de la organización. La Seguridad puede evitar todos estos daños, lo cual beneficia la productividad, a la imagen y a las áreas críticas de éxito de la organización.

C A P I T U L O 2

NORMA ISO 17799 PARA LA GESTION DE SEGURIDAD DE LA INFORMACION

2. NORMA ISO 17799 PARA LA GESTION DE SEGURIDAD DE LA INFORMACION

2.1 Introducción. Gestión de la Seguridad

"Gestionar es llevar a cabo las diligencias necesarias para lograr un determinado fin." [10]

Durante muchos años, las organizaciones desarrollaron sus proyectos de Seguridad considerando la situación de su negocio y la de su competencia, teniendo que aprender muchas cosas en el camino, ya que no existía un modelo a seguir.

Se han manejado diferentes criterios de evaluación de la Seguridad: internos para una organización, sectoriales, nacionales, internacionales…

En la época científico-tecnológica actual, la información es el recurso más importante de cualquier compañía, por ser el único que no se puede, o es muy difícilmente, reemplazable. Al mismo tiempo, es el recurso que está sujeto a mayores vulnerabilidades. [11]

La Seguridad de la información pretende proteger a la información de amenazas, garantizando la continuidad del negocio, así como minimizar los posibles daños y maximizar el rendimiento de las inversiones y las oportunidades de un negocio.

Por lo que se debe contar con un sistema de gestión que permita, partiendo de la base de que la Seguridad absoluta no existe, ofrecer a empresas y organizaciones, instrumentos para garantizar al máximo posible la Seguridad de su información.

Es en este contexto que, gracias a las aportaciones de varias empresas alrededor del mundo, se creó el British Estándar 7799 (BS-7799), un primer esfuerzo por establecer una serie de lineamientos que cualquier empresa podía seguir para construir su arquitectura de Seguridad.

Para finales del año 2000, la ISO (*Internacional Organization for Standardization*) adoptó el BS-7799, e inició el camino para definir el estándar Internacional.

2.1.1 Modelo PHVA

El SGSI (Sistema de Gestión de Seguridad de la Información) está basado en el Modelo utilizado por las NORMAS ISO en general: **PHVA**

El PHVA puede describirse brevemente como:

- **Planificar** – Establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente y las políticas de la organización.
- **Hacer** – Implementar los procesos.
- **Verificar** – Realizar el seguimiento y la medición de los procesos y los productos respecto a las políticas, los objetivos y los requisitos para el producto, e informar sobre los resultados.
- **Actuar** – Tomar decisiones para mejorar continuamente el desempeño de los procesos.

Figura 2.1 Modelo PHVA: Mejora continua del sistema de gestión de calidad

2.2 Herramientas de Seguridad

Una vez identificadas las potenciales fuentes de amenazas y los tipos de peligros que pueden ocurrir, resulta mucho más fácil ordenar las políticas de Seguridad y los resguardos apropiados. Las organizaciones cuentan con una gran variedad de tecnologías, desde paquetes de *software* antivirus hasta *hardware* dedicado a la Seguridad de red, tal como los sistemas de detección de intrusiones y los servidores de Seguridad o *firewalls*, a fin de brindar protección a todas las áreas de la red.

Al igual que un edificio, una red requiere varios niveles de protección para ser completamente segura. Una vez establecidas estas soluciones, se pueden implementar herramientas que periódicamente detecten las vulnerabilidades en la Seguridad de la red garantizando una Seguridad proactiva y continúa. Además, se pueden contratar consultores profesionales de Seguridad de redes para que brinden asesoramiento en el diseño de la solución de Seguridad conveniente para la red, o para garantizar que la solución de Seguridad existente esté actualizada y sea efectivamente segura. Con todas estas opciones disponibles, es posible implementar una infraestructura de Seguridad que permita la protección suficiente, sin sacrificar demasiado la necesidad de acceder a la información en forma ágil y sencilla.

2.2.1 Paquete Antivirus

El *software* de protección contra virus viene con muchas computadoras y puede detener muchas amenazas de virus si se realiza una actualización periódica del mismo y su mantenimiento es óptimo.

La industria de los antivirus se basa en una amplia red de usuarios que le suministra advertencias oportunas ante la presencia de nuevos virus, de manera tal que se puedan desarrollar y distribuir los antídotos rápidamente. Debido a que todos los meses se generan miles de virus nuevos, es de vital importancia que la base de datos de virus se mantenga actualizada. El paquete de antivirus contiene una base de datos de los virus conocidos cuando intentan atacar. Los proveedores de *software* antivirus más conocidos publican en sus sitios Web las últimas novedades en antídotos y el *software* puede indicarles a los usuarios que periódicamente recopilen nuevos datos. La política de Seguridad de la red debería estipular que todas las computadoras de la red estén actualizadas y

preferentemente que todas tengan instalado el mismo paquete de antivirus, por compatibilidad, y para que los costos de mantenimiento y actualización sean mínimos.

Es también fundamental actualizar periódicamente el *software*. Generalmente, para los autores de los virus la prioridad fundamental es no ser detectados por el antivirus.

2.2.2 Contraseñas

La forma más simple y común de asegurarse de que sólo los individuos con la autorización accedan a una zona determinada de la red, es mediante la "protección con contraseña" de dichas áreas, lo que significa que sólo podrán acceder las personas que tengan contraseñas específicas para tal fin.

En la analogía de Seguridad física anterior, las contraseñas son comparables a las tarjetas de identificación para el acceso. No obstante, las infraestructuras más poderosas de Seguridad de redes son prácticamente ineficaces si las personas no protegen sus contraseñas. Muchos usuarios eligen como contraseñas palabras, o números, fáciles de recordar, como fechas de cumpleaños, números de teléfono, o nombres de mascotas y otros no cambian las contraseñas ni tienen la precaución de mantenerlas en reserva. Las políticas, o reglas de oro, para las contraseñas son:

- Cambiar las contraseñas en forma periódica.
- Elegir contraseñas con poco sentido.
- Nunca dar a conocer las contraseñas a nadie, aunque no se pertenezca más a la empresa.

En el futuro algunas contraseñas podrán reemplazarse por biométrica, que es la tecnología que identifica a los usuarios en base a características físicas, como huellas digitales, impresiones oculares, o de voz.

2.2.3 Certificados Digitales

Los certificados digitales, o los certificados de claves públicas, son los equivalentes electrónicos de los pasaportes, o las licencias de conductor, y se emiten por Autoridades certificadoras (CA) específicas.

Los certificados digitales comúnmente se usan para identificación al establecer túneles seguros por Internet, tal como sucede en la red privada virtual (VPN).

2.2.4 Servidores de Seguridad o *Firewall*

Un *firewall* es una solución de *software* o *hardware* implementada en la infraestructura de red para imponer las políticas de Seguridad de una organización mediante el acceso restringido a recursos de red específicos. En la analogía de Seguridad física, un *firewall* es el equivalente a la cerradura en la puerta exterior del edificio, o en la puerta de una sala dentro del edificio, ya que sólo los usuarios autorizados, es decir, los que tienen una tarjeta de acceso o llave, puedan ingresar. La tecnología del *firewall* también está disponible en versiones adecuadas al uso doméstico.

El *firewall* crea una capa protectora entre la red y el mundo exterior. De hecho, el *firewall* copia la red en el punto de entrada para que pueda recibir y transmitir datos autorizados sin una demora prolongada. No obstante, contiene filtros integrados que pueden impedir el acceso al sistema real de material potencialmente peligroso, o no autorizado. También registra una intrusión frustrada y la reporta a los administradores de red.

El propósito principal de un *firewall* es evitar los accesos no autorizados de redes y proporcionar un único punto de defensa con acceso controlado y auditado a los servicios, desde dentro y fuera de la red privada de una organización. Un *firewall* basa su funcionamiento en el examen de los paquetes IP que viajan entre el servidor y el cliente.

Las siguientes capacidades caen dentro de los alcances de un *firewall:*

1. Define un único punto de entrada y salida que deja fuera de la red protegida a los usuarios no autorizados, prohíbe que los servicios potencialmente vulnerables entren, o salgan de la red y proporcionan protección de varios tipos de *spoofing* y ataques de ruteo.
2. Proporciona una ubicación para monitorear los eventos relacionados a Seguridad. Auditorias y alarmas se pueden implementar en el firewall.
3. Es una plataforma conveniente para varias funciones de Internet no relacionadas a Seguridad. Estas incluyen la traducción de direcciones de red, la cual mapea direcciones locales a direcciones de Internet, y la administración de red que audita, o registra, el uso de Internet.

Entre los servicios que un *firewall* puede proporcionar están:

- Protección a los servicios vulnerables.
- Acceso controlado a los sistemas.
- Seguridad concentrada.
- Mejora de la privacía.
- Registros de *loggin* y estadísticas de uso, o mal uso, de la red.
- Ejecución de políticas de Seguridad.
- Alertar al administrador de intentos de violar las políticas.

También se debe mencionar los principales objetivos de diseño de un *firewall*:

1. Todo tráfico de adentro hacia fuera y viceversa, debe pasar a través del *firewall*. Esto se logra bloqueando físicamente todo acceso a la red local, excepto a través del *firewall*. Este tiene varias opciones de configuración.
2. Solo se permite el paso de tráfico autorizado, definido por la política local de Seguridad. Para esto se usan varios tipos de *firewall* los cuales implementan varios tipos de políticas.
3. El *firewall* mismo es inmune a penetración. Esto implica el uso de un sistema confiable con un sistema operativo seguro.

Existen cuatro técnicas generales que usan los *firewalls* para controlar el acceso y lograr implementar la política de Seguridad del sitio. Inicialmente los *firewalls* tenían como objetivo principal el control de servicio pero han evolucionado para proporcionar las siguientes técnicas:

Control de Servicio. Determina los tipos de servicios de Internet que pueden accederse hacia adentro, o hacia afuera. El *firewall* puede filtrar tráfico basándose en la dirección IP y en el número de puerto TCP.

Control de Dirección. Determina la dirección en la cual los servicios pueden iniciarse y se les permite fluir a través del *firewall*.

Control de Usuarios. Controla el acceso a los servicios de acuerdo al usuario que intenta el acceso. Este control se aplica a los usuarios internos que se encuentran dentro del perímetro de Seguridad.

Control de Conducta. Controla como se utilizan los servicios de red. Por ejemplo, se puede filtrar correo electrónico para eliminar *spam*, o puede habilitar acceso externo a solo una parte de la información en el servidor de *web* local.

Existen tres tipos comunes de *firewall* que son: filtrado de paquetes, *gateways* a nivel de aplicación y *gateways* a nivel de circuito.

Los *firewalls* pueden actuar en diferentes capas del modelo OSI.

Firewall por filtrado de paquetes

"Este tipo de *firewall* actúa en la capa de red del modelo OSI ya que se especifica el transito que pasa dentro del *firewall*, y eso es dependiendo de las políticas establecidas." [12]

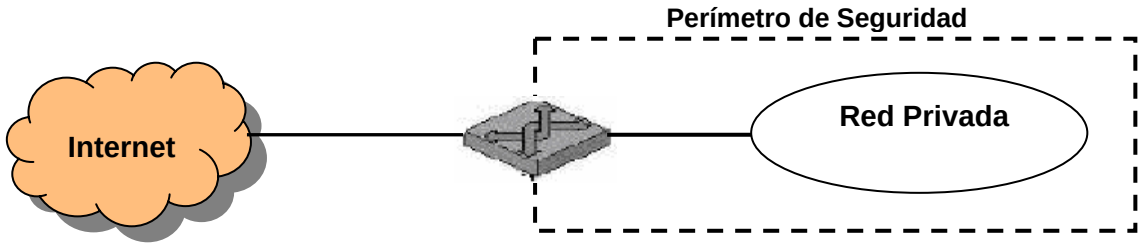


Figura 2.2 *Firewall* por filtrado de paquetes

Firewall a nivel de aplicación

"Este tipo de *Firewall* protege a nivel aplicación, también llamado servidor Proxy, actúa como regulador, o pasador, de tráfico de aplicación. El usuario se conecta a un *Gateway* usando una aplicación como TELNET o FTP." [12]

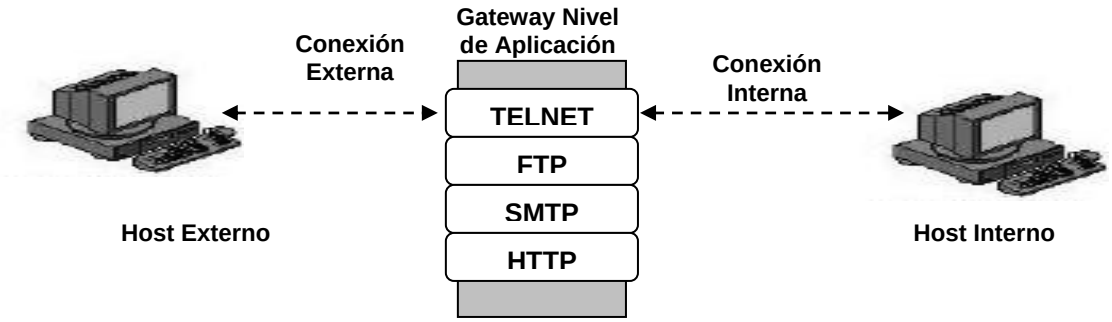


Figura 2.3 *Firewall* a nivel de aplicación.

Firewall a nivel circuito

"Este *Firewall* Funciona en la capa uno ya que se basa en conexiones uno a uno por medio de circuitos." [12]

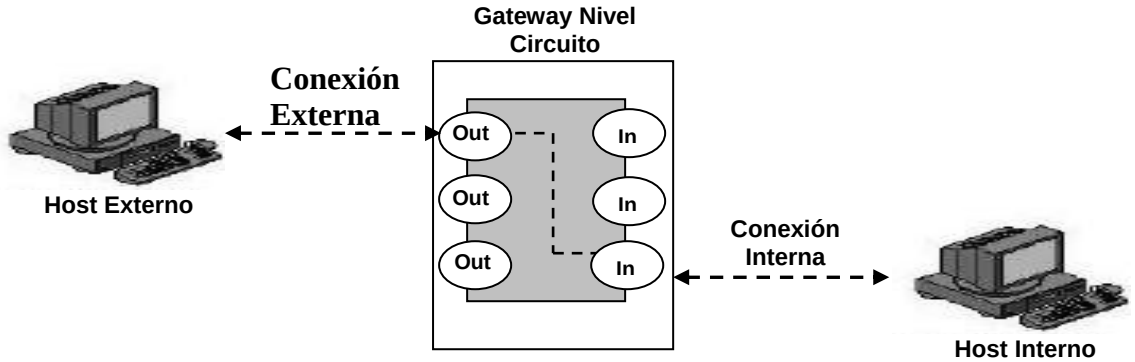


Figura 2.4 *Firewall* a nivel circuito.

2.2.5 Cifrado.

"Desde que el hombre ha necesitado comunicarse con los demás ha tenido la necesidad de que algunos de sus mensajes solo fueran conocidos por las personas a quien estaban destinados. La necesidad de poder enviar mensajes de forma que solo fueran entendidos por los destinatarios hizo que se crearan sistemas de cifrado, de forma que un mensaje después de un proceso de transformación, lo que llamamos cifrado, solo pudiera ser leído siguiendo un proceso de descifrado." [13]

Debido principalmente a su uso militar, los sistemas de cifrado fueron avanzando en complejidad, hasta llegar a nuestros días donde la informática ha entrado en las organizaciones y la necesidad de Seguridad al realizar operaciones aumenta.

En la actualidad, se está acostumbrado a enviar o recibir cartas postales que vienen encerradas en un sobre para que su lectura esté reservada solo a su destinatario. En el mundo virtual, en el caso del *e-mail* esto no es así, ya que lo que enviamos es la carta sin el "sobre" que lo contenga, es decir, sin nada que impida su lectura por parte de cualquiera que pudiera interceptarla. Es decir, quedan vulnerables nuestras confidencias, nuestros números de tarjeta de crédito, nuestros saldos en bancos, etc.

Sistemas de cifrado Los sistemas de cifrado se clasifican en:

Sistemas de cifrado simétrico: Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y descifrar un documento. El principal problema de Seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por lo tanto se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave. Es importante que dicha clave sea muy difícil de adivinar ya que hoy en día las computadoras pueden adivinar claves muy rápidamente, por lo que se requiere de un algoritmo de generación de números aleatorios eficiente.

Sistemas de cifrado asimétrico: También son llamados sistemas de cifrado de clave pública. Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella. Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje. Una vez que lo ha cifrado, solamente con la

clave privada del destinatario se puede descifrar, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfecto la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer.

Sistemas de cifrado híbridos: Es el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica. Funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico. En cada mensaje, la clave simétrica utilizada es diferente por lo que si un atacante pudiera descubrir la clave simétrica, solo le valdría para ese mensaje y no para los restantes. Existen programas llamados PGP y GnuPG que usan sistemas de cifrado híbridos. La clave simétrica es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave simétrica y acto seguido usa la clave simétrica para descifrar el mensaje.

La tecnología de cifrado garantiza que sólo el receptor autorizado pueda leer o interceptar los mensajes. Generalmente, el cifrado se utiliza para proteger los datos que se transmiten por una red pública y emplea algoritmos matemáticos avanzados para "codificar" los mensajes y los archivos adjuntos. Existen diversos tipos de algoritmos de cifrado pero algunos son más seguros que otros. El cifrado ofrece la Seguridad necesaria para sustentar la tecnología VPN cada vez más popular. Las VPN son conexiones privadas o túneles de las redes públicas, como Internet. Se utilizan para que trabajadores a distancia, empleados móviles, sucursales y socios de negocios puedan conectarse entre sí o a las redes corporativas.

Todos los dispositivos de *hardware* y *software* VPN admiten tecnología de cifrado avanzada para ofrecer la mayor protección para los datos que transfieren.

2.2.6 IDS (Detección de intrusos, Detección de Amenazas)

Las organizaciones siguen empleando *firewalls* como los dispositivos de control y administración central para impedir que usuarios no autorizados accedan a las redes. No obstante, la Seguridad de la red es en cierto modo similar a la Seguridad física en el hecho de que ninguna tecnología cubre todas las necesidades; en cambio, una defensa en capas proporciona los mejores resultados. Las organizaciones están considerando cada vez más tecnologías adicionales de Seguridad para contrarrestar el riesgo y la vulnerabilidad que los servidores de Seguridad no pueden resolver por sí solos. Un sistema de detección de intrusiones (IDS) basado en la red mantiene la red vigilada las veinticuatro horas del día.

"Los sistemas IDS, identifican los ataques que los *firewalls* y las redes VPN no pueden detectar, ya que monitorean las conexiones de Internet y extranet en tiempo real para proteger los sistemas y los recursos principales de la red. Un sistema IDS puede brindar avisos proactivos a los administradores, desconectar inteligentemente a un atacante malicioso e incluso reconfigurando dinámicamente la red para evitar futuros ataques." [12]

El IDS analiza las secuencias de datos de paquetes en una red, busca actividad no autorizada, como ataques de *hackers*, y permite que los usuarios reaccionen frente a las violaciones de Seguridad antes de que los sistemas se expongan al peligro. Cuando se detecta actividad no autorizada, el IDS puede enviar alarmas a una consola de administración con detalles de la actividad y es posible que ordene a otros sistemas, como los enrutadores, la interrupción de las sesiones no autorizadas.

La detección de intrusiones es similar a un sensor de movimiento, o a una cámara de vigilancia, que detecta actividad, activa alertas y genera una respuesta planeada. El análisis es como un guardia de Seguridad que controla y cierra las puertas, o ventanas, abiertas antes de que sean violadas.

Los productos IDS prestan servicios a organizaciones de todas las dimensiones, desde pequeñas empresas hasta entornos empresariales muy grandes. Están diseñados especialmente para brindar protección contra ataques de denegación de servicio (DoS), ataques de *hackers* y para la defensa de aplicaciones de comercio electrónico.

CARACTERISTICAS.

- Facilidad de implantación.
- Detección de amenazas.
- Investigación inteligente.
- Facilidad de administración.

En la figura 2.5 se muestra la secuencia del proceso de IDS.

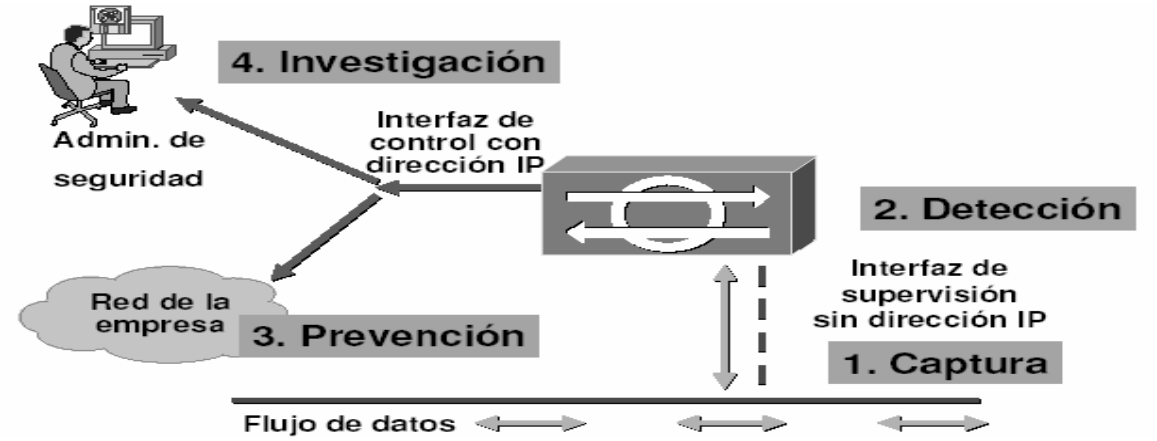


Figura 2.5 Proceso de IDS

CAPTURA

En esta primera etapa se encuentran los dispositivos IDS que son los equipos encargados de la captura de flujo de datos maliciosos.

En la figura 2.6 se muestran algunos ejemplos.

Figura 2.6 Ejemplos de equipos IDS del proveedor IDS 4250-XL y Dispositivo IDSM-2

DETECCION

Las firmas definen explícitamente qué actividad debe considerarse como maliciosa.

- Correspondencia de patrones sencillos.
- Correspondencia de patrones que conservan la información.
- Análisis basado en la decodificación de protocolos.
- Análisis heurístico.

PREVENCION

Para prevenir ataques con los sistemas IDS se aplican 2 técnicas generales que son, reinicio TCP y rechazo, que a continuación se muestra en la figura 2.7:

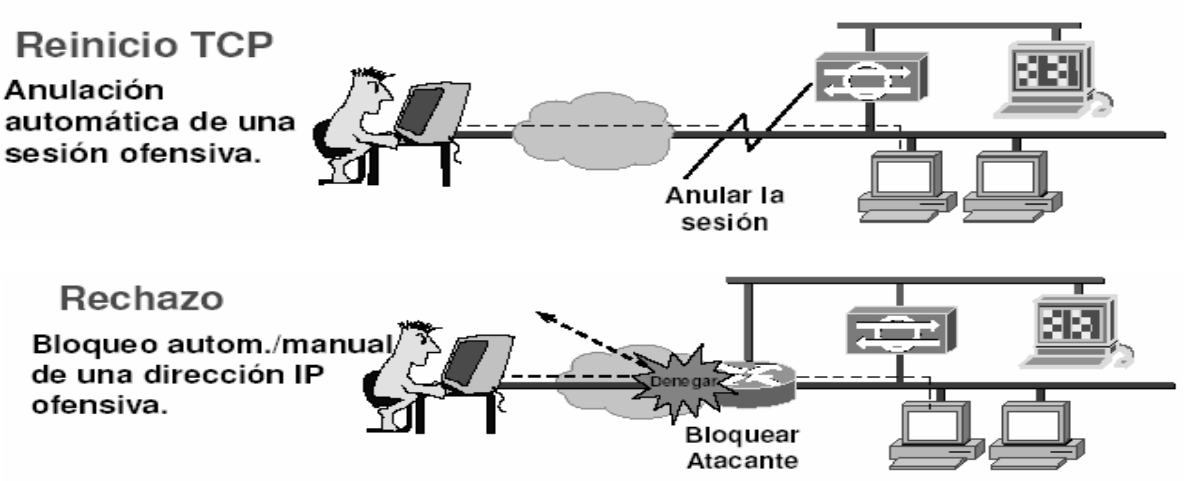


Figura 2.7 Prevención de ataques IDS

2.3 Prevención de Ataques

Como es bien sabido, las Empresas son blanco fácil de ataques informáticos, ya sea a sus sistemas o a sus telecomunicaciones, es por eso que se deben de tener siempre presente ciertos aspectos de prevención y estar siempre al día en la nueva tecnología de Seguridad informática.

En los puntos subsecuentes se presentan algunos de estos métodos de prevención de ataques.

2.3.1 Conectividad Segura (Confidencialidad, Integridad de datos y control de identidad)

Conectividad segura

La conectividad segura a través de Internet ofrece protección para las empresas que dependen de la conectividad a Internet, como empresas con sucursales y las que emplean trabajadores móviles y a distancia.

Al diseñar una solución de Seguridad de red, las organizaciones deben elegir entre la utilización de Seguridad integrada en un dispositivo de la red LAN o WAN, como un *switch* o *router* de acceso, o la utilización de un equipo funcional especializado. Las características de Seguridad integradas son generalmente atractivas porque se pueden añadir al equipo existente, o pueden mejorar una solución existente. Los equipos son una buena opción cuando la solución de Seguridad profunda necesaria es muy avanzada, o requiere de alto rendimiento.

Las empresas pueden tomar la decisión según la capacidad y funcionalidad del equipo, comparado con la ventaja de integración del dispositivo. Algunas organizaciones prefieren una solución integrada que podría resultar más rentable y más fácil de manejar, mientras que otras pueden requerir el mayor rendimiento y funcionalidad de un dispositivo dedicado.

Integridad de datos

En términos genéricos llamaremos “datos” a cualquier documento o información almacenada digitalmente. Se dice que la integridad de estos datos ha sido preservada cuando los datos *no han sido alterados (modificados, borrados) de una manera no autorizada desde el momento en que fueron creados, transmitidos o guardados por una fuente autorizada*. Para poder asegurar la integridad de los datos, se requiere la habilidad de detectar su manipulación por quien no posee la autorización para hacerlo. La manipulación o alteración de los datos incluye inserción, borrado o sustitución de partes o del todo.

2.3.2 Redes VPN

"Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte." [9]

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. Ver figura 2.8.

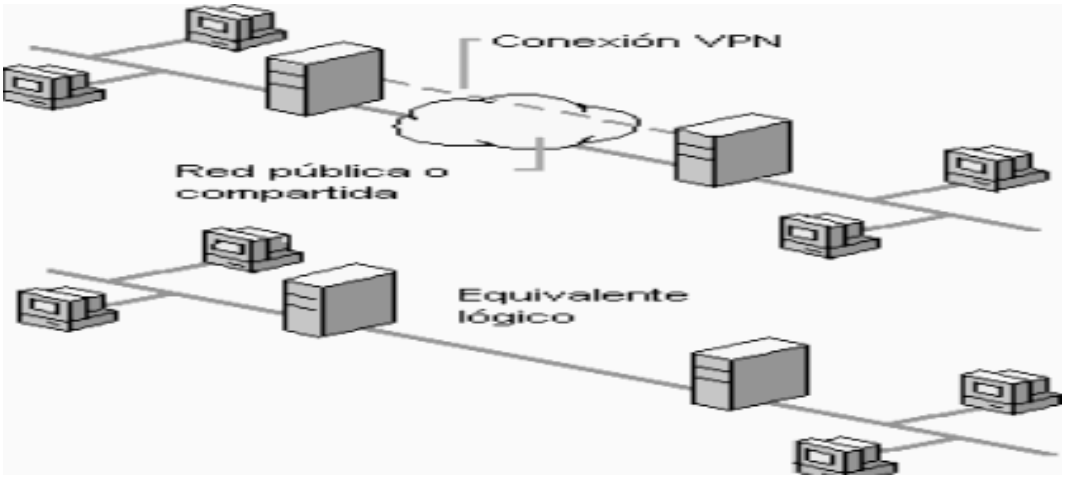


Figura 2.8 Red pública o compartida.

En la figura 2.9 se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a un *firewall* que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de Internet donde se genera un túnel dedicado únicamente para "nuestros datos" para que estos con una velocidad garantizada, con un ancho de banda también garantizado, lleguen a su vez al *firewall* remoto y terminen en el servidor remoto.

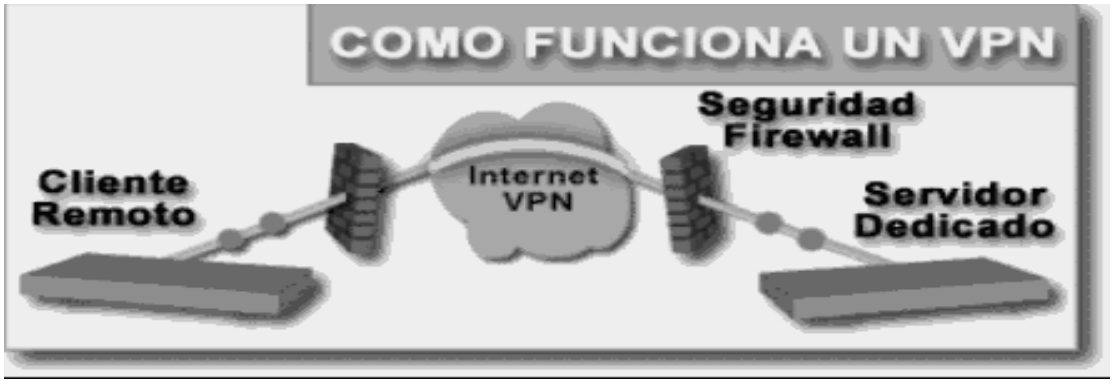


Figura 2.9 Función de una VPN

Las VPN pueden enlazar oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, Ipsec, Frame Relay, ATM.

2.3.3 Administración y Monitoreo de la red

Administración de la Seguridad

Una infraestructura de administración es el "integrador" de todas las tecnologías de Seguridad en redes. Esta administración brinda a los administradores la capacidad de administrar desde dispositivos individuales hasta sistemas completos. Y para las empresas de medianas a grandes puede admitir conjuntos más avanzados de reglas de Seguridad llamados "política de Seguridad".

En la actualidad existe *software* especializado para la administración de los dispositivos de Seguridad y esa administración se hace en función de las políticas de Seguridad que tenga implantada la empresa. Figura 2.10.

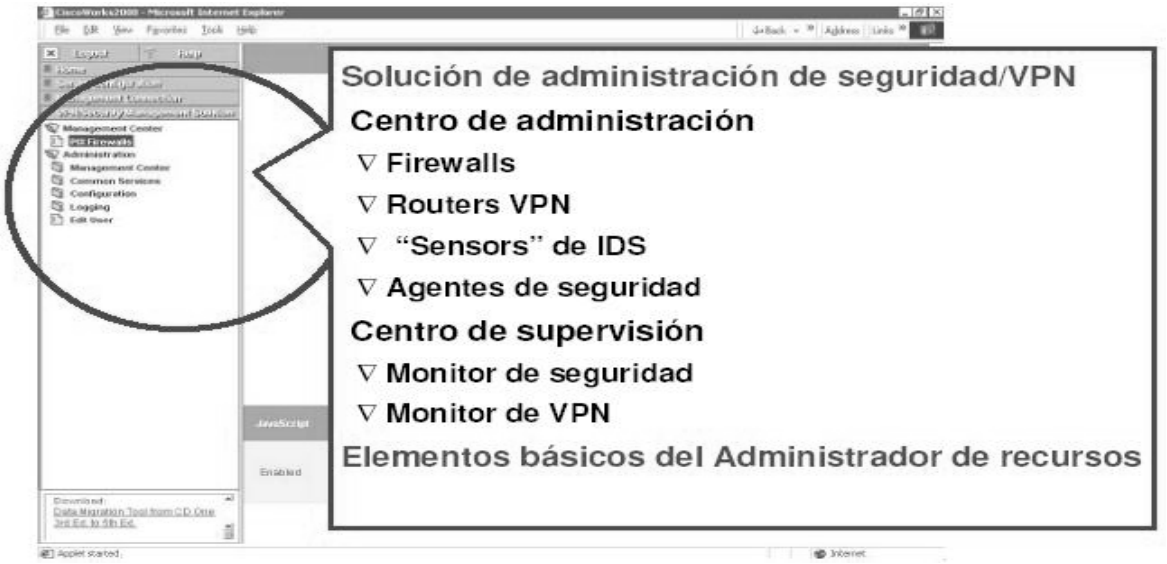


Figura 2.10 Administración Integral de dispositivos de Seguridad

Administración de un dispositivo

Las herramientas de administración de un solo dispositivo generalmente acompañan a un dispositivo de red individual, como un conmutador, un enrutador, un IDS, *firewall*, VPN y sistemas de autenticación y cifrado. Este *software*, que a menudo está

basado en Web, permite que los administradores instalen, configuren y monitoreen componentes de red individuales.

Administración de sistemas

Las herramientas de administración de sistemas son ideales para administrar VPN, sistemas de IDS y redes WLAN. Estos sistemas de administración se pueden adaptar para satisfacer las necesidades de diversas organizaciones. Además de proteger la red, estas herramientas actúan de forma eficaz de tal manera que bloquean el acceso a los recursos del servidor antes de que se produzcan daños graves. Contienen módulos de administración de políticas que admite la administración del cifrado, *firewall*, detección de intrusiones y política de control de acceso para grandes empresas.

Administración de sistemas para redes WLAN

En entornos inalámbricos, las redes WLAN admiten la administración basada en la Web y el Servicio de *Simple Network Management Protocol* (SNMP) para la ayuda en el monitoreo, la solución de problemas, la descarga de *software* y hasta en el registro. Los puntos de acceso inalámbricos se pueden instalar de manera rápida, precisa y segura.

Política de administración

La política de administración permite que los administradores definan, implementen y garanticen el cumplimiento de una política de Seguridad sin que los administradores de redes tengan que trabajar en los dispositivos individuales uno por uno.

2.3.4 Implicaciones de las nuevas tecnologías

Las implicaciones que trae consigo el implantar tecnologías de información se engloban en tres aspectos básicos: los **técnicos**, los **organizativos** y los **humanos**.

Los técnicos son los mas fáciles, baratos y rápidos a la hora de su implantación. Los organizativos y, sobre todo, los humanos representan siempre una formidable barrera y un reto sin precedentes para las empresas.

En la figura 2.11 se indican los aspectos que abarca la implantación de nuevas tecnologías de información, y el objeto que determina el beneficio que trae consigo esta nueva implementación.

Figura 2.11 Implantación de tecnologías de Información

Las organizaciones actuales están reorientándose hacia una infraestructura en red. Las nuevas tecnologías de información están revolucionando el aspecto laboral en las empresas, así se cuenta ahora con normas para manejar la Seguridad de forma integral como el ISO 17799.

2.4 ¿Qué es ISO 17799?

ISO 17799 es una Norma de Seguridad internacional que ofrece recomendaciones para realizar la gestión de la Seguridad de información dirigidas a los responsables de iniciar, implantar o mantener la Seguridad de una organización. [15]

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la Seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

Como se mencionó en el capítulo anterior, la Seguridad de la información se define como la preservación de:

- **Confidencialidad:** Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Integridad:** Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tienen acceso, cuando lo requieran, a la información y sus activos asociados.

Estos principios en la protección de los activos de información constituyen las normas básicas deseables en cualquier organización, sean instituciones de gobierno,

educativas e investigación; no obstante, dependiendo de la naturaleza y metas de las organizaciones, éstas mostrarán especial énfasis en algún dominio o área particular de la Norma ISO 17799.

El objetivo de la Norma ISO 17799 es proporcionar una base común para desarrollar normas de Seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la Seguridad.

ISO 17799 da la pauta en la definición sobre cuáles metodologías, normas o estándares técnicos pueden ser aplicados en el sistema de administración de la Seguridad de la información, se puede entender que estos estándares son auxiliares y serán aplicados en algún momento al implementar el mismo.

La aplicación de un marco de referencia de Seguridad basado en el ISO 17799 proporciona beneficios a toda organización que lo implemente, al garantizar la existencia de una serie de procesos que permiten evaluar, mantener y administrar la Seguridad de la información.

Las políticas, estándares locales y los procedimientos se encuentran adaptados a las necesidades de la organización debido a que el proceso mismo de su elaboración integra mecanismos de control y por último, la certificación permite a las organizaciones demostrar el estado de la Seguridad de la información, situación que resulta muy importante en aquellos convenios o contratos con terceras organizaciones que establecen como requisito contractual la certificación BS7799.

En resumen, esta Norma internacional cubre todos los aspectos de la Seguridad informática:

- *Equipos*
- *Políticas de gestión*
- *Recursos humanos*
- *Aspectos jurídicos*

ISO 17799 o BS 7799 UNE 71502

ISO 17799 (parte 1) [15] es una guía que contiene consejos y recomendaciones que permiten asegurar la Seguridad de la información de una empresa.

BS 7799 (parte 2) / UNE 71502 [15] proponen recomendaciones con el fin de establecer un marco eficaz de gestión de la Seguridad de la información. BS 7799-2 / UNE 71502 permiten establecer un sistema de gestión de Seguridad de la información (SGSI). [15]

2.4.1 Historia

Es importante entender los principios y objetivos que dan vida al ISO 17799, así como los beneficios que cualquier organización, incluyendo las instituciones públicas, privadas y ambientes educativos pueden adquirir al implementarlo en sus prácticas de Seguridad de la información.

En 1995 el *British Standard Institute* (BSI) publica la Norma B 7799, un código de buenas prácticas para la gestión de la Seguridad de la información.

En 1998, también el BSI publica la Norma BS 7799-2, especificaciones para los sistemas de gestión de la Seguridad de la información; se revisa en 2002.

Tras una revisión de ambas partes de BS 7799 (1999), la primera es adoptada como Norma ISO en 2000 y denominada ISO/IEC 17799, algunas de sus características son:

- Conjunto completo de controles que conforman las buenas prácticas de Seguridad de la información.
- Aplicable por toda la organización, con independencia de su tamaño.
- Flexible e independiente de cualquier solución de Seguridad concreta: recomendaciones neutrales con respecto a la tecnología.

En 2002 la Norma ISO se adopta como UNE con muy pocas modificaciones (UNE 17799) y en 2004 se establece la Norma UNE 71502, basada en BS7799-2 (no existe equivalente ISO).

Por la necesidad generalizada de contar con una Norma de carácter internacional que permitiera reconocer o validar el marco de referencia de Seguridad aplicado por las organizaciones, se elaboró la Norma ISO17799:2000, basada principalmente en la primera parte del BS 7799 conocida como Código de Prácticas. [16] Ver Figura 2.12.

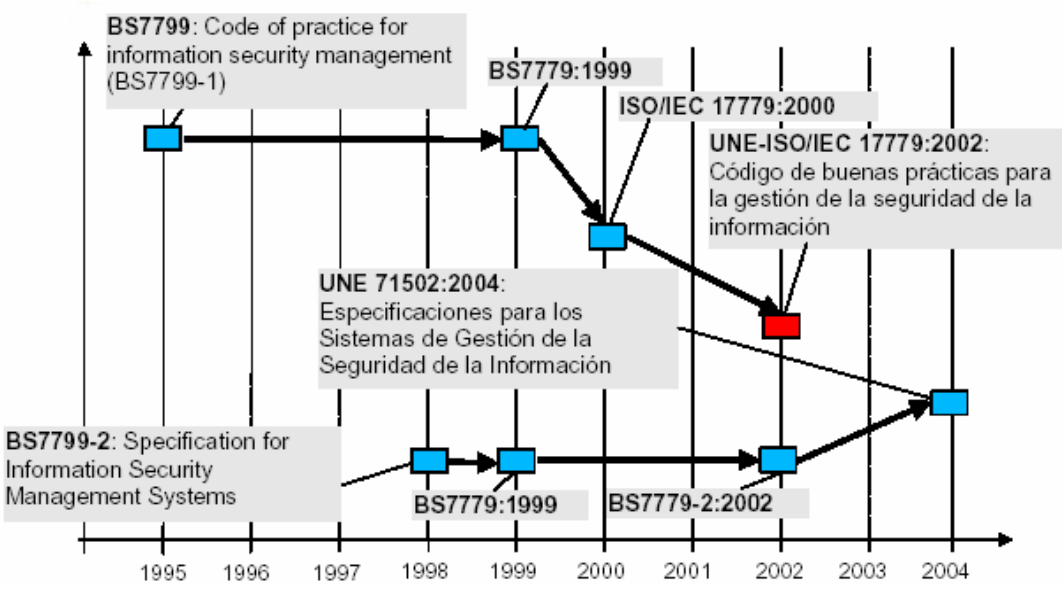


Figura. 2.12 Evolución de la Norma ISO 17799

2.5 Estructura de la Norma

2.5.1 Dominios de control

El éxito de la implementación de la Norma de Seguridad ISO 17799 requiere de una serie de procedimientos donde, inicialmente, el análisis de riesgos identificará los activos de la información y las amenazas a las cuales se encuentra expuesta.

El análisis de riesgos guiará en la correcta selección de los controles que se apliquen a la organización; este proceso se conoce en la terminología del estándar como *Statement of Applicability*, que es la definición de los controles que se aplican a la organización con objeto de proporcionar niveles prácticos de Seguridad de la información y medir el cumplimiento de los mismos.

Los diez dominios de control que cubren por completo la Gestión de la Seguridad de Información son de acuerdo a la (Figura 2.13):

1. Políticas de Seguridad
2. Aspectos organizativos para la Seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.
9. Gestión de continuidad del negocio.
10. Conformidad con la legislación.

Figura 2.13 Dominios de control de ISO 17799 [15]

De estos diez dominios se derivan 36 objetos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos, o mecanismos, que reducen el nivel de riesgo).

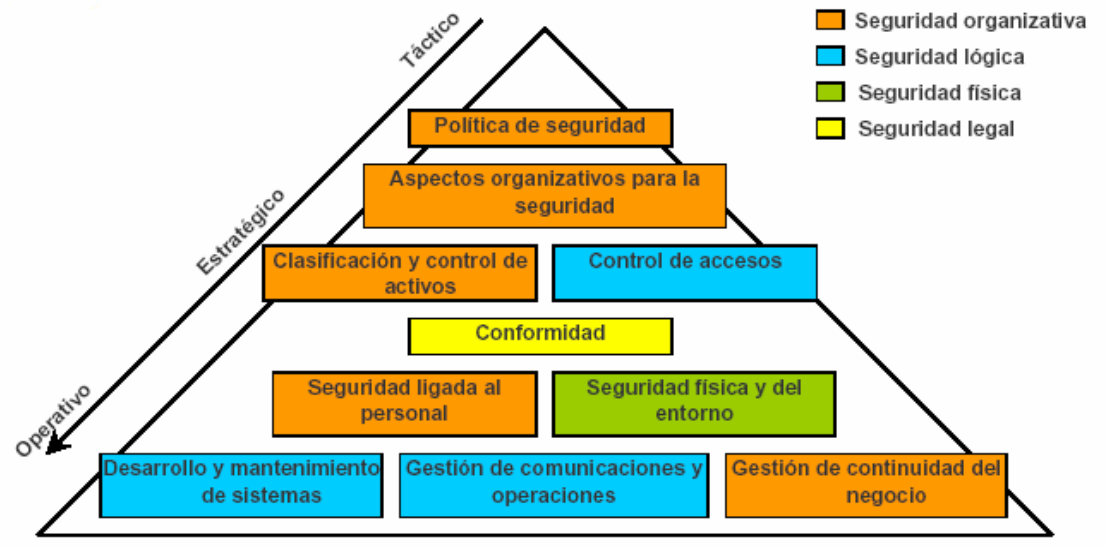


Figura. 2.14 Dominios de Control de ISO 17799 (Continuación)

2.5.2 Objetivos de control.

2.5.2.1 Políticas de Seguridad

Los activos de información y los equipos informáticos son recursos importantes y vitales de una Compañía. Sin ellos las empresas dedicadas a la Seguridad se quedarían rápidamente fuera del negocio y por tal razón su directiva tiene el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, *hackers*, interrupción de servicio, accidentes y desastres naturales.

Por lo que se deben de definir Políticas de Seguridad que tengan como finalidad proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de La compañía (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias.

Una vez definidas estas políticas deben ser aprobadas y publicitadas de la forma adecuada a todo el personal implicado en la Seguridad de la información.

La Norma define como obligatorias las políticas de Seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad.

2.5.2.2 Aspectos Organizativos para la Seguridad

Establece el marco formal de Seguridad que debe integrar una organización, tales como un foro de administración de la Seguridad de la información, un contacto oficial de Seguridad ISSO (*Information System Security Officer*), revisiones externas a la infraestructura de Seguridad. Donde se deben tomar en cuenta los siguientes puntos importantes:

- Administrar la Seguridad de la información dentro de la organización.
- Mantener la Seguridad de los recursos de tratamiento de la información y de los activos de la organización que son accedidos por terceros.
- Mantener la Seguridad de la información cuando la responsabilidad de su tratamiento se ha exteriorizado a otra organización.

Debe diseñarse una estructura organizativa dentro de la compañía que defina las responsabilidades que en materia de Seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de alguna forma.

Dicha estructura debe poseer un enfoque multidisciplinario, dado que los problemas de Seguridad no son exclusivamente técnicos.

2.5.2.3 Clasificación y Control de Activos

El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad. Por lo que se deberá hacer lo siguiente:

2.5.2.4 Seguridad Ligada al Personal

Contrario a lo que uno se puede imaginar, en este contexto no se orienta a la Seguridad del personal desde la óptica de protección civil, sino a proporcionar controles a las acciones del personal que opera con los activos de información.

El objetivo de esta área de la Norma es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, es decir, establecer claras responsabilidades por parte del personal en materia de Seguridad de la información.

Para lo cual, se debe tomar en cuenta lo siguiente:

- Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios.
- Asegurar que los usuarios sean conscientes de las amenazas y riesgos en el ámbito de la Seguridad de la información, y que deben estar preparados para sostener la política de Seguridad de la organización en el curso normal de su trabajo.
- Minimizar los daños provocados por incidencias de Seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

Las implicaciones del factor humano en la Seguridad de información son muy elevadas. Todo personal, tanto interno como externo a la organización, debe conocer tanto las líneas generales de las políticas de Seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la Seguridad global.

Se deben conocer las diferentes relaciones con los sistemas de información: operador, administrador, guardia de Seguridad, personal de servicios, etc.

Los procesos de notificación de incidencias deben ser claros, ágiles y conocidos por todos.

2.5.2.5 Seguridad Física y del Entorno

En este aspecto se debe identificar los perímetros de Seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de Seguridad establecida.[11]

Lo que se debe evitar:

- Accesos no autorizados, daños e interferencias contra los locales y la información de la organización.
- Pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.
- Riegos o robos de información y de recursos de tratamiento de información.

Las áreas de trabajo de la organización y sus activos deben ser clasificadas y protegidas en función de su importancia jerárquica, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, incendio…). [17]

2.5.2.6 Gestión de Comunicaciones y Operaciones

En este punto se debe procurar lo siguiente:

- Integrar los procedimientos de operación de la infraestructura tecnológica y de controles de Seguridad documentados, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, administración de aceptación de sistemas, hasta el control de código malicioso. [17]
- Asegurar la operación correcta y segura de los recursos de tratamiento de información.
- Minimizar el riesgo de fallos en los sistemas.
- Proteger la integridad del *software* y de la información.
- Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.
- Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.
- Evitar daños a los activos e interrupciones de actividades de la organización.

- Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

Se debe garantizar la Seguridad de las comunicaciones y la operación de los sistemas críticos para el negocio.

2.5.2.7 Control de Acceso

Para garantizar un acceso seguro se debe:

- Habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de Seguridad y el control de acceso a las aplicaciones. [11]
- Controlar los accesos a la información.
- Evitar accesos no autorizados a los sistemas de información.
- Evitar el acceso de usuarios no autorizados.
- Protección de los servicios en red.
- Evitar accesos no autorizados a ordenadores.
- Evitar el acceso no autorizado a la información contenida en los sistemas.
- Detectar actividades no autorizadas.
- Garantizar la Seguridad de la información cuando se usan dispositivos de informática móvil y tele trabajo.

Se deben establecer los controles de acceso adecuados para proteger los sistemas de información críticos para el negocio, a diferentes niveles: sistema operativo, aplicaciones, redes, etc.

2.5.2.8 Desarrollo y Mantenimiento de Sistemas.

La organización debe disponer de procedimientos que garanticen la calidad y Seguridad de los sistemas desarrollados para tareas específicas de la organización.

- Asegurar que la Seguridad está incluida dentro de los sistemas de información.
- Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

- Proteger la confidencialidad, autenticidad e integridad de la información.
- Asegurar que los proyectos de Tecnología de la Información y las actividades complementarias sean llevados a cabo de una forma segura.
- Mantener la Seguridad del software y la información de la aplicación del sistema.

Debe contemplarse la Seguridad de la información en todas las etapas del ciclo de vida del *software* en una organización: especificación de requisitos, desarrollo, explotación, mantenimiento…. [17]

2.5.2.9 Gestión de Continuidad de las operaciones de la organización.

El sistema de administración de la Seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

2.5.2.10 Requerimientos legales. Conformidad

La organización establecerá los requerimientos de Seguridad que deben cumplir todos sus proveedores, socios y usuarios; éstos se encontrarán formalizados en los contratos o convenios.

Cada una de las áreas establecerá una serie de controles que serán seleccionados dependiendo de los resultados obtenidos en el análisis de riesgos, además, existen controles obligatorios para toda organización, como es el de las políticas de Seguridad cuyo número dependerá más de la organización que de la Norma, el cual no establece este nivel de detalle.

2.6 Trabajando con la Norma ISO 17799

2.6.1 Auditoria

En una auditoria de ISO 7799 se debe de valorar el nivel de adecuación, es decir, implementación y gestión de cada control del estándar en la organización.

- Seguridad Lógica
- Seguridad Física
- Seguridad Organizativa
- Seguridad Legal

Así mismo, se debe referenciar la Seguridad de la información estándar y aceptada internacionalmente.

Una vez conociendo el estado actual de la Seguridad de la información en la organización, se puede planificar correctamente su mejora o su mantenimiento.

Una auditoria ISO 17799 proporciona información precisa acerca del nivel de cumplimiento de la Norma a diferentes niveles: Global, por dominios, por objetivos y por controles. (Figura 2.15)

1	1			Información sobre la política de Seguridad		100%		1.60%	
		1			Documento de la política de Seguridad			80%	1.30%	Nulo
		2			Revisión y evalución			20%	0.30%	Nulo
2	3	10	***Seguridad Orgnizativa, Organización de la Seguridad***			7.90%				
	1			Infraestructura de la Seguridad de la Información			60%		4.70%	
		1			Foro de Gestión de la Seguridad			20%	0.90%	Nulo
		2			Coordinación de la Seguridad de Información			10%	0.50%	Nulo
		3			Asignación de responsabilidades en materia de Seguridad de la Información			15%	0.70%	Nulo
		4			Proceso de autorización para instalaciones de proceso de información			20%	0.90%	Muy Bajo
		5			Asesoramiento especializado en materia de Seguridad			15%	0.70%	Nulo
		6			Cooperación entre organizaciones			10%	0.50%	Nulo
		7			Revisión independiente de la Seguridad de información			10%	0.50%	Nulo
	2			Seguridad frente al acceso por parte de terceros			20%			
		1			Identificación de riesgos del acceso de terceras partes			40%	0.60%	Muy Bajo
		2			Requerimientos de Seguridad en contratos con terceros			60%	0.90%	Nulo
	3			Externalización Outsourcing			20%			
		1			Requerimientos de Seguridad en la subcontratación de servicios			100%	1.60%	Nulo
3	2	3	***Clasificación y control de activos***			2.40%				
	1			Responsabilidades en los activos			60%			
		1			Inventario de activos			100%	1.40%	Muy Bajo
	2			Clasificación de la Información			40%			
		1			Pautas de clasificación			70%	0.70%	Nulo
		2			Rotulado y manejo de la Información			30%	0.30%	Nulo
4	3	10	***Seguridad de Personal***			7.90%				
	1			Seguridad en la definición de puestos de trabajo y la asignación de recursos			40%			
		1			Inclusión de responsabilidades de seguridad en el puesto de trabajo			40%	1.30%	Nulo
		2			Selección y política de personal			20%	0.60%	Nulo
		3			Acuerdos de confidencialidad			20%	0.60%	Nulo
		4			Términos y condiciones de empleo			20%	0.60%	Nulo
	2			Entrenamiento de usuarios			30%			
		1			Formación y educación en materia de Seguridad			100%	2.40%	Nulo
	3			Respuesta ante incidentes y anomalías en materia de Seguridad			30%			

Figura 2.15 Formato de auditoria ISO 17799

2.6.2 Consultoría

Conociendo el nivel de cumplimiento actual, es posible determinar el nivel mínimo aceptable y el nivel objetivo en la organización (Figura 2.16):

- *Nivel mínimo aceptable:* Estado con las mínimas garantías de Seguridad necesarias para trabajar con la información corporativa.

- *Nivel objetivo:* Estado de Seguridad de referencia para la organización, con un alto grado de cumplimiento de la Norma ISO 17799.

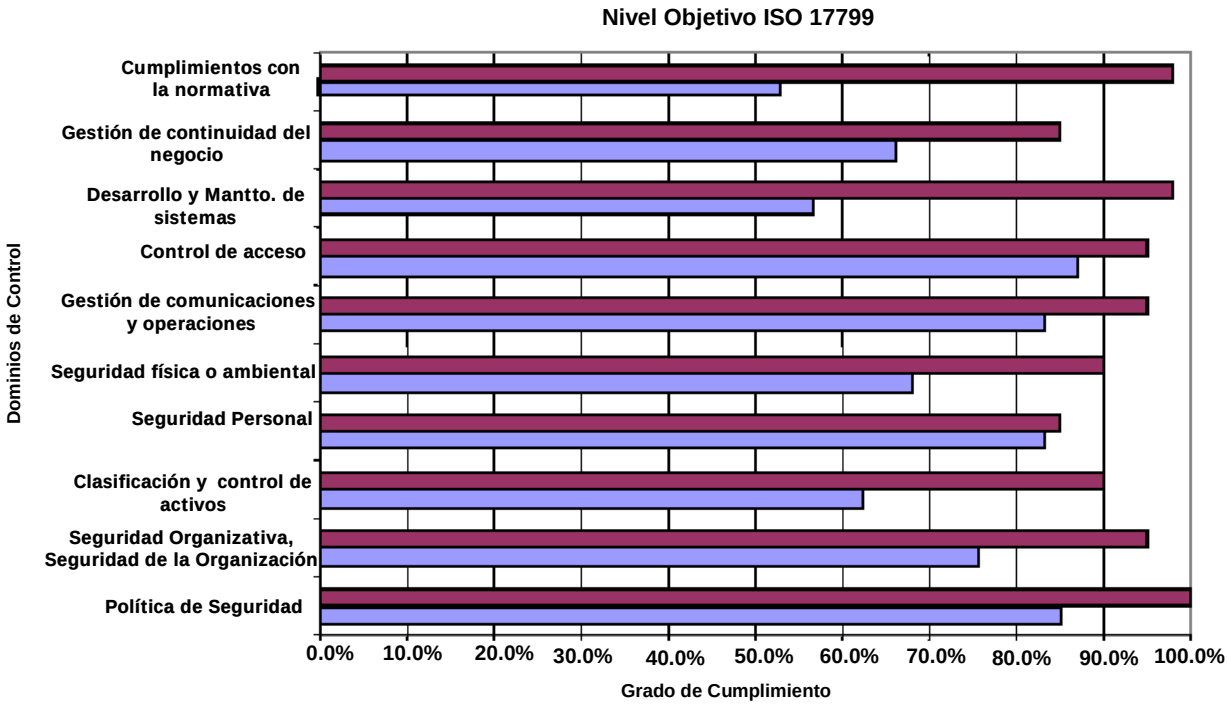


Figura 2.16 Relación de los Dominios de Control con el Grado de Cumplimiento Objetivo ISO 17799

A partir del nivel mínimo aceptable y el nivel objetivo, se puede definir un plan de trabajo para alcanzar ambos a partir del estado actual (figura 2.17).

- *Nivel mínimo aceptable:* Implantación de los controles técnicos más urgentes, a muy corto plazo.

- *Nivel objetivo:* Se desarrolla en el tiempo dentro del Plan Director de Seguridad corporativo, y es el paso previo a la certificación UNE 71502.

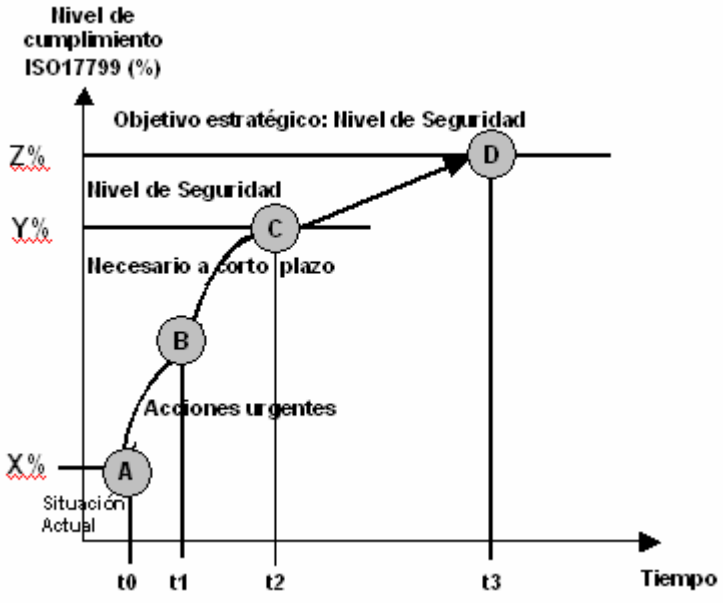


Figura 2.17 Nivel de cumplimiento ISO 17799

2.6.3 Implantación

ISO 17799 no es una Norma tecnológica, más sin embargo, involucra la Seguridad tecnológica. Ha sido redactada de forma general, flexible e independiente de cualquier solución de Seguridad específica.

Proporciona buenas prácticas neutrales con respecto a la tecnología y a las soluciones disponibles en el mercado.

Estas características posibilitan su implantación en todo tipo de organizaciones, sin importar su tamaño o sector de negocio, pero al mismo tiempo son un argumento para los detractores de la Norma.

Un ejemplo de Implantación sería el siguiente:

Dominio de control: Gestión de comunicaciones y operaciones.

- **Objetivo de control:** Proteger la integridad del *software* y de la información.

Control: Controles contra *software* malicioso.

"Se deberían implantar controles para detectar el *software* malicioso y prevenirse contra él, junto a procedimientos adecuados para concienciar a los usuarios" [12]

Consultoría

- Normativa de uso de *software*: definición y publicación en la Intranet.
- Filtrado de contenidos: **X**
- Antivirus de correo: **Y**
- Antivirus personal: **Z**

2.6.4 Ventajas

La adopción de la Norma ISO 17799 proporciona diferentes ventajas a cualquier organización como son:

- Conformarse a las normas en materia de gestión del riesgo.
- Aumento de la Seguridad efectiva de los sistemas de información.
- Una reducción de riesgos de ataques
- Correcta planificación y gestión de la Seguridad
- Garantías de continuidad del negocio.
- Una recuperación más rápida y más fácil de las operaciones después de un ataque
- Mejora continua a través del proceso de auditoria interna.
- Aumento del valor comercial y mejora de la imagen de la organización.
- Una metodología de Seguridad estructurada y reconocida internacionalmente
- Una confianza mutua aumentada entre socios estratégicos de negocios
- Una disminución potencial de las primas de seguro contra los riesgos informáticos
- Un mejoramiento de las prácticas sobre la vida privada y una conformidad con las leyes sobre las informaciones personales.

C A P I T U L O 3

METODOLOGÍA DE SEGURIDAD PROPUESTA, BASADA EN LA NORMA ISO 17799 PARA UNA RED DE DATOS CORPORATIVA, ASI COMO SU APLICACIÓN

3. METODOLOGIA DE SEGURIDAD PROPUESTA, BASADA EN LA NORMA ISO 17799 PARA UNA RED DE DATOS CORPORATIVA, ASI COMO SU APLICACIÓN

3.1 Introducción

El motivo de desarrollo de la presente tesis, es la de proponer una Metodología de Seguridad basada en los principios la Norma ISO 17799 que sirva de base para la implantación de políticas, procesos y tecnologías de Seguridad en redes, que permita a cualquier organización obtener un mejor lugar en su mercado de desarrollo, minimizando sus vulnerabilidades y riesgos sobre su activo más importante: sus datos.

Para lograr lo dicho anteriormente, se ha estudiado y documentado acerca del tema e investigado algunos casos de empresas que por descuidar este aspecto, han caído en errores sumamente costosos, que si bien se han podido recuperar es por que cuentan con planes alternos o de contingencia y recuperación, pero en el caso de algunas pequeñas empresas, desgraciadamente no es así, cosa que les puede costar su presencia dentro del mercado.

En capítulos anteriores, se ha mencionado que la Seguridad es un problema de educación de los usuarios principalmente, en donde también se ha identificado de donde provienen más comúnmente los riesgos. Es en este punto, donde se debe tener la claridad de donde se debe partir para lograr el objetivo de la tesis.

Se necesita proteger y controlar la información corporativa, para preservar el negocio. Y ser más sensibles a las buenas prácticas de protección de información, para que los clientes mantengan un alto nivel de confianza hacia la organización. Para lograrlo, se necesita primordialmente eliminar los riesgos de Seguridad, lo cuál es sumamente difícil, casi imposible al 100%, es por eso que para empezar se debe tener muy claro que lo importante es minimizarlos al máximo. Se realizará el análisis de las aplicaciones corporativas, elementos tecnológicos y recursos humanos necesarios para identificar los activos: elementos *hardware*, elementos *software*, recursos humanos e información.

Antes de comenzar cualquier punto de este capítulo, se debe tener en cuenta lo siguiente:

- Recordar los servicios básicos de Seguridad.
    - **Confidencialidad**
    - **Integridad**
    - **Disponibilidad**
- Obtener Estadísticas de problemas en la corporación
    - Robo de Equipos
    - Riesgos de entidades externas (WWW, Virus & *Worms*)
    - Riesgos de entidades internas
        - Empleados deshonestos
        - Errores u Omisiones
        - Modificaciones a los sistemas sin control
        - Empleados no capacitados, con iniciativa

3.2 Justificación de la metodología

El establecimiento de un conjunto eficaz de políticas y controles de Seguridad requiere el uso de un método para determinar los puntos vulnerables que existen en los sistemas que manejamos y en las directivas y controles de Seguridad que los protegen. Ideando un plan de Seguridad en donde se identifiquen métodos, herramientas y técnicas de ataques probables.

Para lograr lo anterior descrito, uno de los objetivos de esta tesis es el de establecer una serie de lineamientos propuestos y probados, apoyados en el estándar ISO 17799, que cualquier empresa pueda seguir para construir su arquitectura de Seguridad y compararla con las mejores prácticas internacionales.

3.3 La Metodología

Para poder establecer una Metodología de Seguridad se debe de incluir tanto estrategias proactivas como reactivas.

La estrategia *proactiva* (ver Anexo A) o de previsión de ataques contiene una serie de pasos que ayudan a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de Seguridad y a desarrollar planes de contingencia; así como la determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque, el cual ayudará a desarrollar tal estrategia.

La estrategia *reactiva* (ver Anexo A), o estrategia posterior al ataque, ayuda al personal de Seguridad a evaluar el daño que ha causado un ataque, a repararlo, o a implementar el plan de contingencia desarrollado en la estrategia proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Haciendo una integración de las dos estrategias anteriores, la metodología que se propone consta de 4 Fases las cuales engloban a los diez objetivos de control que define el estándar ISO 17799, dichas Fases se listan a continuación:

Fase de Preparación. En esta primera Fase se define la arquitectura de Seguridad sobre la cual se va a trabajar, estableciendo diversos lineamientos básicos de Seguridad. Toda esta información se debe de presentar a los niveles estratégicos de la organización para autorizar el presupuesto de implementación.

Fase de Análisis Preliminar. En esta Fase se inventarían recursos *hardware* y *software*, a clasificar la información así como realizar un análisis exhaustivo de riesgos y vulnerabilidades que pueden aquejar a la empresa.

Fase de Definición de políticas y estándares. Esta Fase es de especial atención, ya que maneja la normalización existente en la organización, que políticas y estándares existen y que tanto se llevan a cabo. En caso de que no existan se deben de plantear éstas en un plan de acción que las contenga.

Fase de Implementación. Esta Fase implementa diversos controles de Seguridad vistos en capítulos anteriores,[18] así como fomenta la educación de Seguridad a usuarios de la información y lleva una buena documentación de cada uno de los controles aplicados.

Se debe hacer notar que las tres últimas Fases se pueden englobar en lo que llamamos análisis de riesgos (parte de la evaluación del ciclo de implementación del estándar ISO 17799), en donde se debe definir una estrategia de Seguridad completa, retroalimentando al grupo de Seguridad que implementa el plan de proyecto. Los resultados que arrojara esta metodología serán recomendaciones sobre: Políticas, Procesos y Tecnología de Información como primer resultado. El análisis de riesgos también proporcionara un plan de contingencia y recuperación. Estos aspectos serán vistos a detalle en el Capítulo 4.

Todo lo mencionado anteriormente se puede representar en la figura 3.1, que nos explica el flujo que sigue esta metodología de Seguridad, y en la tabla 3.1 se muestra la relación con la Norma ISO 17799.

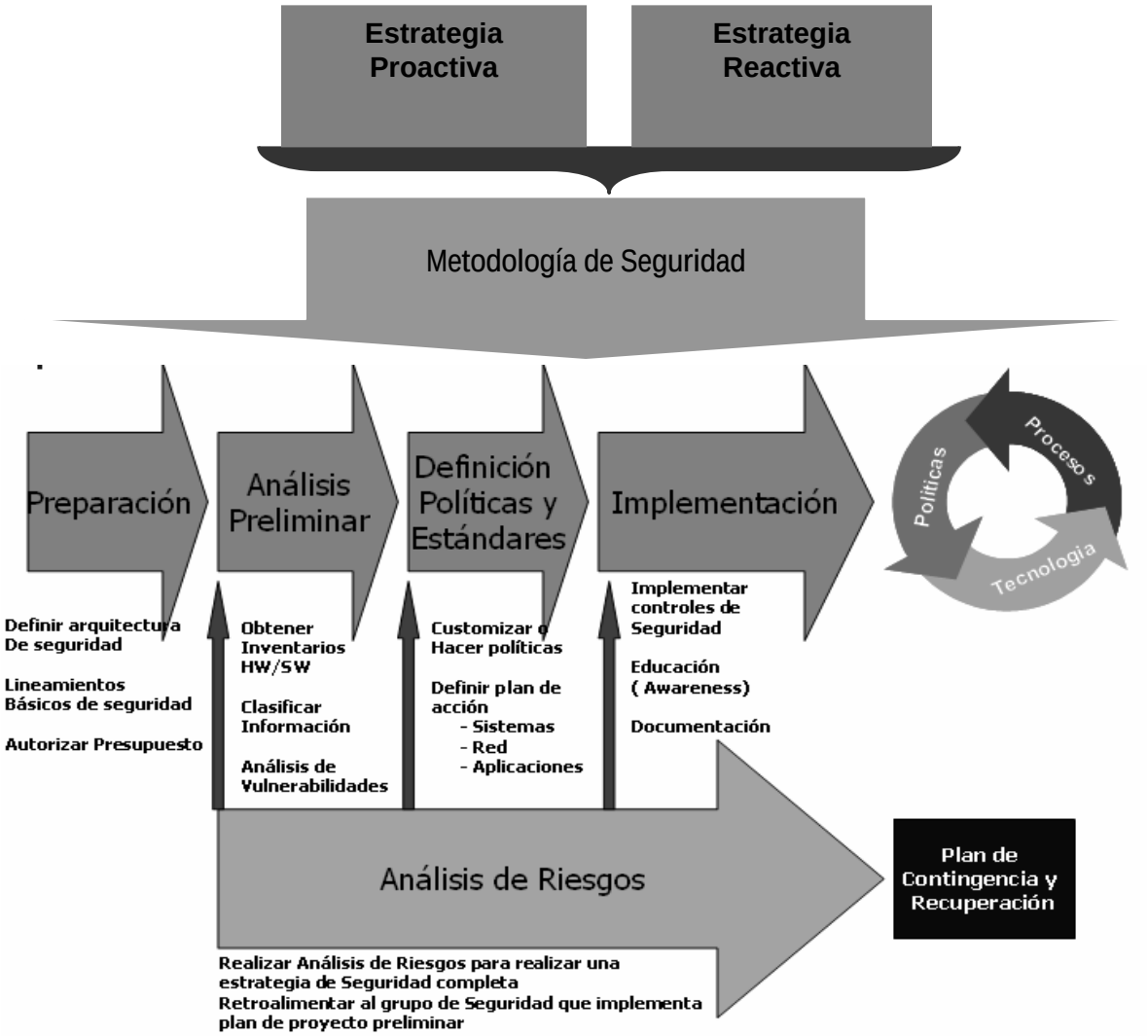


Figura 3.1 Metodología de Seguridad

Metodología	Pasos y ciclo para implementar el estándar ISO17799	Descripción
FASE DE PREPARACION	Iniciación del Proyecto	• Asegurar el compromiso de la dirección • Seleccionar y entrenar a los miembros del equipo inicial de proyecto
	Definición del SGSI (Sistema de Gestión de la Seguridad de la Información)	• Identificar el alcance y los límites del marco de dirección de Seguridad de la información. • Este paso es crucial para el éxito del proyecto
FASE DE ANALISIS PRELIMINAR	Evaluación de Riesgos	• Realizar el inventario y evaluar el activo a proteger • Identificar y evaluar amenazas y vulnerabilidades • Diagnosticar el nivel de cumplimiento con ISO 17799 • Calcular el valor de riesgos asociados
	Administración de Riesgos	• Encontrar como seleccionar e implantar los controles correctos que le permitan a la organización reducir el riesgo a un nivel aceptable
DEFINICION DE POLITICAS Y ESTANDARES	Entrenamiento y concienciación	• Los empleados pueden ser el eslabón más débil en la Seguridad de la información de su organización. Aprenda a establecer un programa de concienciación de la Seguridad de la información, implementando políticas.
FASE DE IMPLEMENTACION	Auditoria	• Aprender más sobre los pasos realizados por auditores externos y averiguar sobre los cuerpos de certificación.
	Control y mejora continua	• Aprender a mejorar la eficiencia de SGSI conforme al modelo de administración reconocido por la ISO.

Tabla 3.1 Relación de la Metodología de Seguridad con el Ciclo de Implementación de la Norma ISO 17799

Para evaluar y medir la efectividad de esta Metodología de Seguridad se aplicará cada Fase a una red corporativa, de una empresa pequeña dedicada al reclutamiento y selección de profesionales en TI; que aunque cuenta con una vasta

infraestructura de comunicación, tiene sin embargo una gran deficiencia en el aspecto de Seguridad, además de que uno de sus principales problemas es la desinformación hacia sus usuarios, acerca de toda una cultura de protección y prevención de la información.

3.4 Fase de Preparación

Como se mencionó anteriormente, en esta Fase se debe de tener planteada la arquitectura de Seguridad sobre la cuál se trabajará, es decir, el medio para establecer las estrategias a seguir dentro de la Metodología de Seguridad y los mecanismos de cómo se administrará la misma, y su final aprobación de desarrollo por parte de la empresa a la cuál se le aplique el método de mejora de la Seguridad.

Para conformar esta Fase, es necesario seguir ciertas actividades dentro de la Preparación para cada uno de los niveles de la empresa, es decir, identificar los procesos administrativos. En la figura 3.2 se mencionan estas actividades, separadas por nivel de la organización.

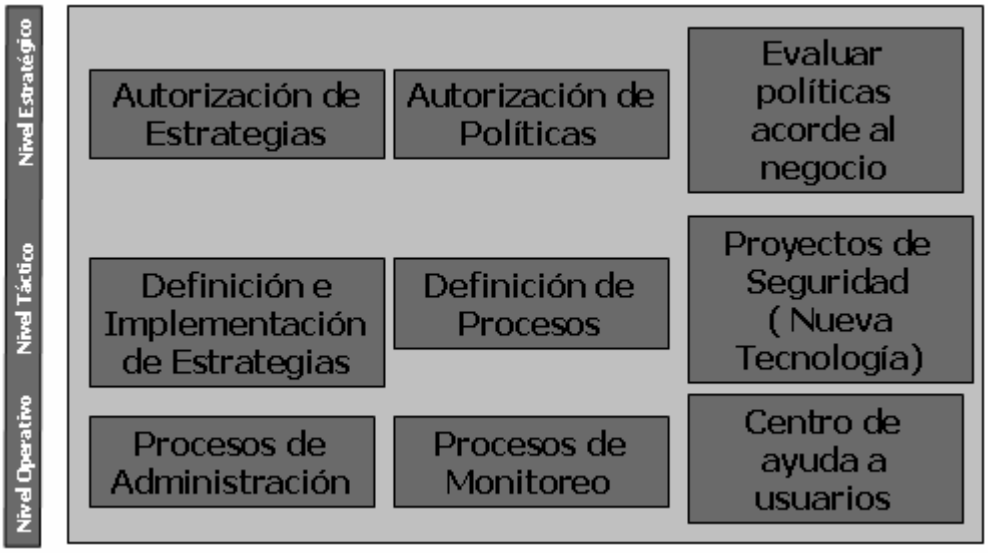


Figura 3.2 Procesos de tipo administrativo que son requeridos en la Fase de Preparación

Para el **Nivel Estratégico** debemos tener en cuenta lo siguiente:

- Para los planes y proyectos de Seguridad se requiere que las estrategias, directrices y normas sean autorizadas a nivel dirección.
- Se requiere un análisis de las políticas, las cuales deben ser contempladas, para reforzar y no ir en contra de las necesidades del Negocio.
- Hoy en día, como factor de éxito para la Seguridad Informática se requiere una dirección de Seguridad de la información.
- Se necesita recopilar información estadística de los problemas organizacionales causados por las malas prácticas de Seguridad en cómputo.
- Realizar un análisis tomando en cuenta los factores de Disponibilidad, Confidencialidad, Integridad y Autenticidad.

Para el **Nivel Táctico** se debe:

- Identificar que Infraestructura de cómputo y comunicaciones existente en la corporación.
- Se requiere conocer detalles del negocio, y que tipo de aplicaciones existen.
- Preparar un chequeo general (*Checklist*) con controles mínimos de Seguridad para Asegurar la infraestructura de cómputo y comunicaciones (asegurar Unix, Windows, Enrutadores, *Firewalls*, *Mainframes* etc.)
- Identificar y desarrollar procesos para la administración de toda la Infraestructura de Seguridad
- No olvidar que es necesario actualizarse constantemente respecto a la nueva tecnología del mercado

Y para el **Nivel Operacional:**

- Contar con procesos de administración de la Infraestructura de Seguridad
    - Proceso de Administración de usuarios.
    - Proceso de Auditoria y Manejo de Alertas.
    - Proceso de Operación.
    - Educación continúa de Seguridad para los usuarios.

- No se debe olvidar que los centros de ayuda a usuarios suelen ser un área muy vulnerable para la Infraestructura de Seguridad (debido al uso de la Ingeniería Social).

3.4.1 Tipos de estándares básicos que se requieren al iniciar

En la Fase de Preparación se considerarán tres tipos de estándares básicos o controles a tres niveles:

- Controles de Aplicaciones
- Controles de Seguridad en Sistemas
- Controles de Seguridad en Comunicaciones

Dichos controles deberán ir acorde a las técnicas de Seguridad que se deben implementar, o con las que se cuente actualmente en la organización. En la figura 3.3 se muestra un esquema que resume lo dicho anteriormente.

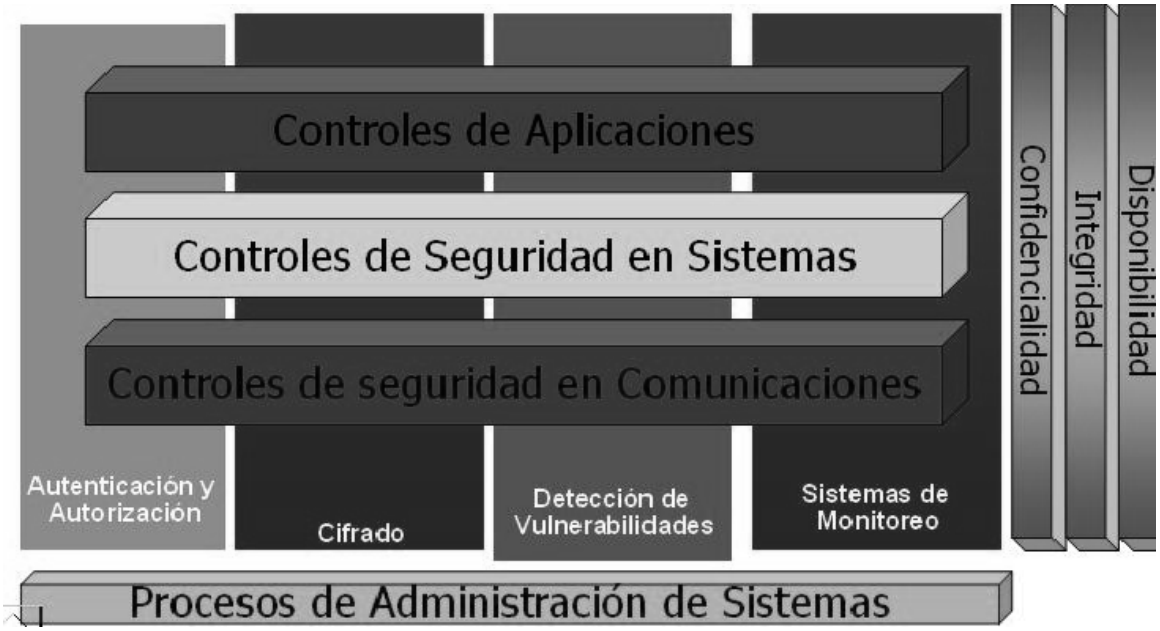


Figura 3.3 Controles básicos al iniciar la Metodología de Seguridad

Controles de Aplicaciones. Principalmente las aplicaciones que corren a nivel de red, es decir, aquellas que tienen que ver con la administración de la misma. Dentro de este tipo de controles se recomienda:

- Preparar las Mejores Prácticas para asegurar las Aplicaciones
    - Técnicas de Programación Segura (Java, Crypto, API's)
    - Nunca usar *javascript* para realizar funciones de Seguridad
    - Consultar Seguridad para desarrollo de aplicaciones
    - Evitar practicas de codificación de contraseñas en código aplicativo

- Revisar código para evitar "caballos de Troya"

- Evaluar recomendaciones de Seguridad cuando se trata de productos comerciales, tales como:
    - Sistemas Bancarios
    - SAP
    - Prácticas en bases de datos

- Control de programas en producción
- Evitar compartir ambientes de desarrollo y producción

Controles de Seguridad de Sistemas. Todos aquellos sistemas que maneje la organización a nivel general, es decir, sistemas que sean de gran relevancia en el desarrollo del negocio, así como los Sistemas Operativos de Red más utilizados. Dentro de este tipo de controles se recomiendan:

- Identificar que tipo de sistemas tiene la Corporación
- Preparar las Buenas Prácticas de Seguridad para la Infraestructura de cómputo utilizada
    - Controles mínimos para Unix, LINUX
    - Controles mínimos para Windows NT, Windows 2000
    - Sistemas Centrales (As400 y *Mainframe*)

- Con base en los inventarios, realizar el plan de implementación de controles por cada uno de los equipos
- Incorporar controles para servidores de :
    - Aplicaciones
    - Correo Electrónico
    - Servidores de Archivos (*File Servers*)
    - Servidores Web (*Web Servers*)

- Servidores de Correo (*Mail Servers*), etc.

Controles de Seguridad en Comunicaciones. Poner toda la atención en la arquitectura de red con la que se cuente y a que nivel de Seguridad pertenezca. Se recomienda:

- Identificar el tipo de Infraestructura de Comunicaciones que tiene la Corporación.
- Preparar inventarios de equipos de comunicaciones (Enrutadores, *Firewalls*, *Switches*, etc.)
- Preparar las Buenas prácticas de Seguridad para la Infraestructura de cómputo utilizada.
- Consultar con el proveedor:
  - Recomendaciones de Seguridad para *firewalls*.
  - Recomendaciones de Seguridad Enrutadores.
  - Definir los servicios de Cifrado que son soportados por la Infraestructura
  - Evaluar la necesidad de instalación de detectores de intrusos
  - Preparar un chequeo general (*Checklist*) para control de puertos a restringir y/o autorizar
  - Preparar buenas practicas servicios remotos
  - Planear una actividad de escaneo para detección de módems (*war dialer*)

3.4.2 Aplicación

Para la aplicación de esta Fase se identificaron los procesos que se llevarán a cabo en el nivel operativo de la red corporativa, tomada como caso de estudio, para así determinar la arquitectura de Seguridad con la que cuentan, y poder establecer la puesta en marcha de las Fases subsecuentes.

Al aplicar los controles básicos de esta Fase; se identificaron ciertos problemas, a los cuales se les propuso la solución más adecuada. Ver la tabla 3.2:

CONTROLES BASICOS	SITUACION	PROBLEMA	SOLUCION PROPUESTA
SEGURIDAD EN APLICACIONES	La empresa maneja diversas aplicaciones que corren directamente en las máquinas del usuario final, es decir, no todas están alojadas en los servidores centrales	No se lleva un control de los sistemas instalados.	Es necesario revisar y evaluar todas las recomendaciones de Seguridad que vienen anexas con la licencia del mismo, además de revisar el código de las demás aplicaciones para evitar la posible intrusión de "Caballos de Troya"
EN SEGURIDAD SISTEMAS	La empresa cuenta para administrar sus recursos de red con el Sistema operativo Windows 2003 Server	No está implementada ninguna política de seguridad	Evaluar y corregir fallas identificadas en dichos servidores.
EN SEGURIDAD COMUNICACIONES	La infraestructura con la que cuenta la empresa se basa en topología en estrella corriendo a una velocidad de 10/100 mbps, con topología lógica Ethernet. Además, cuenta con salida a Internet de banda ancha de hasta 2 mbps. En la figura 3.4 se muestra tal infraestructura.	No existen políticas de seguridad sobre actualizaciones de parches de seguridad	Identificar los puntos vulnerables.

Tabla 3.2 Inventario

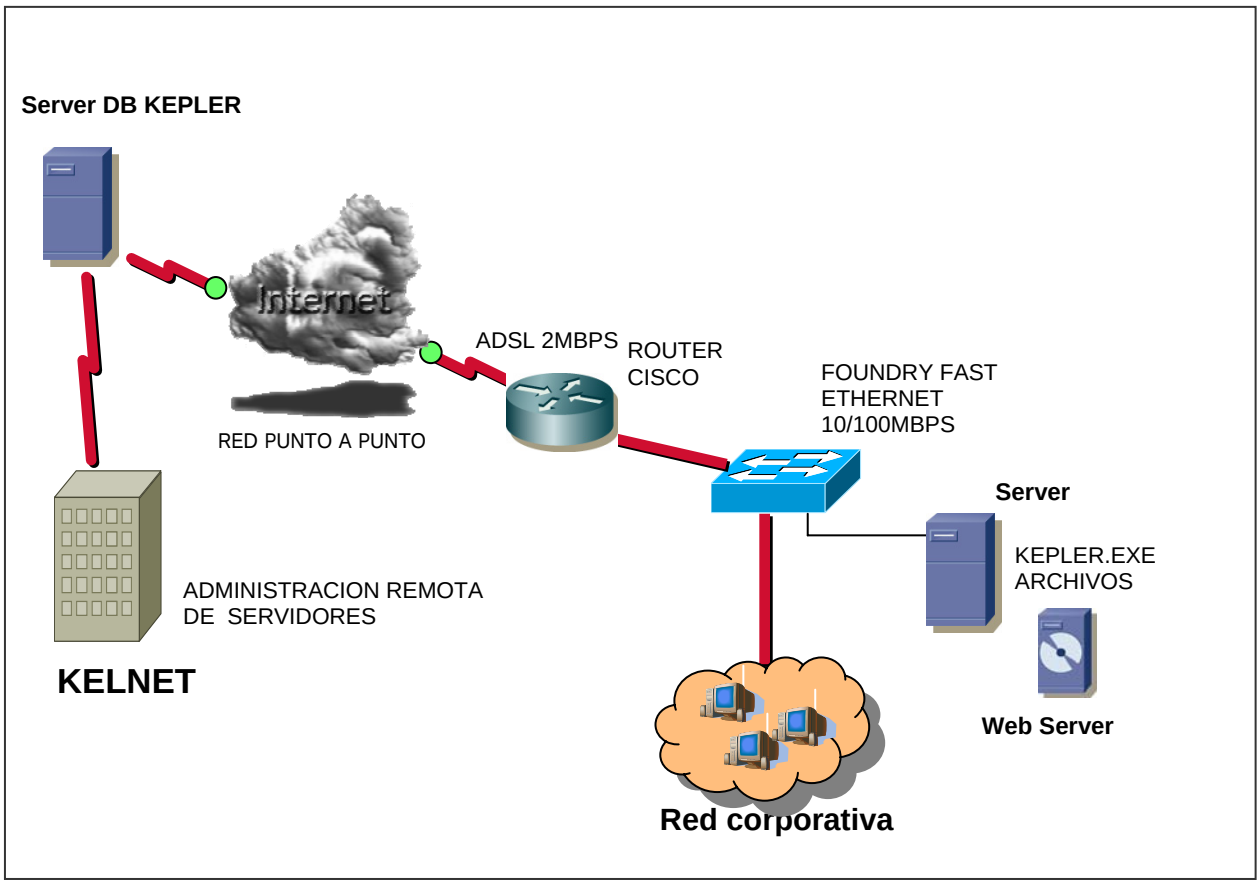


Figura 3.4 Infraestructura actual de comunicación.

Las comunicaciones de la empresa comienzan con una conexión ADSL a 2 Mbps de velocidad proveída por Telmex, la conexión llega a un ruteador y después pasa por el *switch* el cual provee la conexión a todas las estaciones de trabajo.

3.5 Fase de Análisis Preliminar

En esta Fase se propone realizar inventarios sobre recursos *hardware* y *software*, así como clasificar la información obtenida y por último realizar un análisis exhaustivo de riesgos y vulnerabilidades que puedan aquejar a la empresa.

Además de seguir las siguientes actividades:

- Promover el análisis de estrategias de Seguridad en los tres niveles siguientes:
  - Sistemas
  - Redes
  - Aplicaciones
- Realizar entrevistas para determinar la clasificación de la información, tomando en cuenta a:
  - Líderes de aplicaciones
  - Líderes de Administración de Sistemas
  - Grupos de Soporte Técnico
  - Usuarios propietarios de la información

- Realizar una evaluación del valor de los datos
- Realizar un Análisis de Vulnerabilidades con distintas Herramientas (ejemplo: ISS, NESSUS)
- Documentar Riesgos y Vulnerabilidades
- Revisar con Administradores y dar continuidad al Plan de corrección (si existe)

Los resultados al finalizar las actividades anteriores, serán:

- Contar con matrices con las aplicaciones más importantes para el negocio
- Identificación de los sistemas en donde se encuentra la información
- Información clasificada en directorios, archivos, medios de Impresión etc.
- Situación actual de las políticas de Seguridad en las tres Capas (sistemas, redes y aplicaciones)
- Se conocerán los sistemas más importantes para el negocio y se determinará:
  - ¿Cuáles requieren confidencialidad?
  - ¿En dónde es más importante la integridad?
  - ¿Qué sistemas deben estar disponibles al 100%?
- Se tendrá el análisis de las políticas actuales en cuanto a Seguridad de la información de la organización a nivel de: sistema, red y aplicativo.
- Se cotejará un inventario con el que cuenta la empresa contra el recopilado.

3.5.1 Aplicación

Para la aplicación de esta Fase se identificó la Arquitectura de Tecnología de Información de la empresa en cuestión, realizando un inventario de activos; que se muestran a continuación.

Hardware	-SERVIDORES: Tres servidores (A,B y C) marca Proliant 3000 Pentium 4 a 2 Ghz. 3 Discos Duros de 9 GB, dos de ellos están de espejo. y 512 Mb en RAM. - USUARIOS: 50 computadoras marca HP: Procesador Pentium IV a 1.7 Ghz de velocidad Disco duro de 60 G y 256 Mb en RAM. -IMPRESIÓN: 4 Impresoras marca *Lexmark* conectadas en red.

Software	**-SERVIDORES** Los tres servidores (A, B y C) cuentan con Sistema Operativo Windows 2003 Server. Los servidores A y B se encuentran en la empresa y C es proporcionado por el *outsourcing* de una empresa externa. El servidor remoto C además del S.O., cuenta con una Base de datos del sistema *KEPLER* que es soportada por *SQL SERVER.* El servidor B soporta la página Web de la empresa, para publicaciones de servicios de la empresa, así como de nuevas vacantes de trabajo y cuentan también con un sistema llamado *Netstat* para obtener estadísticas de las operaciones de la página. El servidor A soporta el *DBMS SQL SERVER* para tener conexión con el servidor C de Base de Datos de *KEPLER*, además de la aplicación que permite manipular dicha *BD* y también comparte archivos e impresoras de la empresa. Los datos almacenados son procesados y manejados por una base de datos llamada *SQL SERVER* que les permite manejar un gran número de datos para *Kepler* que es con el que operan. -**USUARIOS:** Las 50 computadoras cuentan con el S.O. Windows XP, además de un cliente *SQL* para la conexión con el servidor *C* de la base de Datos.
Red	La Empresa cuenta con un *SITE* el cual contiene un *Router* marca Cisco y dos *Switches* marca *Foundry* los cuales tienen 24 puertos cada uno. Además del cableado estructurado que es el medio por el cual se conecta la red y pasan los datos. La topología física con la que cuentan es en estrella, y la topología lógica es *Ethernet* con una velocidad de 10/100 Mbps. Cuentan con conexión a Internet por medio de *Telmex Infinitum* con un ancho de banda de 2Mb.

Seguridad	La Seguridad con la que cuentan es muy básica: un *Firewall* físico que está incluido en el *Router* y cuenta con un software *Trend Micro* antivirus para cada PC, que se actualiza cada semana. Cuenta con una conexión punto a punto "*peer-to-peer"* la cual consiste en escribir un *login* y contraseña del usuario y con eso se entra al sistema, los datos se actualizan en tiempo real, entre el servidor C de la Base de datos del sistema KEPLER y los clientes de la conexión que cuenta cada usuario de la empresa. Ya que maneja sistema de autenticación para la conexión al servidor. Las contraseñas al inicio de sesión de cada usuario son otras herramientas de Seguridad que ocupa la empresa.

Tabla 3.3 Inventario de activos

3.6 Fase de Definición de Políticas y Estándares

Esta Fase de la Metodología de Seguridad, tiene por objetivo el llevar a cabo una exhaustiva investigación de documentación impresa, revisada y autorizada de todas aquellas reglas, políticas o estándares existentes en la empresa en estudio. Éstas, deben ser minuciosamente analizadas conjuntamente con el personal encargado de los sistemas en la organización. En caso de no existir políticas documentadas, se deben de establecer éstas, en un plan o manual de acción que vaya de la mano con la misión de la empresa.

Todas y cada una de las políticas y estándares contenidos en el manual, deben atender tres aspectos fundamentales:

- Ser autorizadas por la alta dirección y el departamento de sistemas.
- Dar a conocer cuales son las que conforman la base normativa de todos los sistemas que se encuentran dentro de la organización.
- Considerar que se implantarán, tomando como base la arquitectura y la infraestructura de la tecnología de información.

Además de lo mencionado anteriormente, el manual de políticas y estándares debe contener lo siguiente:

- Política general.
- Procesos para el manejo de la Seguridad (de administración, de auditoria y alertas)
- La evaluación del riesgo.
- Recuperación en caso de que se presente alguna anomalía.

Aquí, se deben de retomar los inventarios recopilados en la Fase del análisis preliminar, para realizar el desarrollo e implementación de cada una de las políticas y estándares de Seguridad. Tomando en cuenta: *hardware*, *software* e información que maneje la compañía.

En esta parte se recomienda:

- Implementar controles de Seguridad en todos y cada uno de los equipos.
- Verificar que se instalen antivirus actualizados en cada uno de los equipos y de ser posible implantar una consola de administración de los mismos, para su constante y fácil monitoreo.
- Implementar controles en enrutadores, *firewalls* y demás dispositivos de Seguridad con los que cuente la empresa.
- Proponer unas políticas de control de información tales como: filtrado de paquetes, cierre de puertos, *backups*, etc.
- Instalar detectores de intrusos (IDS) y redes privadas (VPN's) en donde se requiera.
- Análisis e implantación de servidores RAS para autenticación.
- Llevar un correcto inventario de los módems existentes y si son o no autorizados.
- Verificar nombres de servicios del Protocolo de Administración de Servicios de Red (SNMP), en toda la red.
- Implementar cifrado para medios de comunicación donde se identificó información altamente confidencial.
- Tomar en cuenta políticas para servidores Web.
- Implementar manejo de alertas en caso de posibles ataques.

Las recomendaciones que este plan da en cuanto a establecimiento de políticas y estándares, son:

- Apoyarse con los administradores de los recursos de la red.
- Negociar, que las claves de administración estén custodiadas y delegadas.
- Auditar periódicamente el uso de las claves de administración.
- Mantener siempre las últimas actualizaciones de “parches” de Seguridad.
- Tener mayor cuidado con la infraestructura de Internet.
- Practicar detección de vulnerabilidades externas e internas con mayor frecuencia.
- Monitorear constantemente los servidores RAS.
- Verificar que se implementen y revisen archivos *logs* en aplicaciones con información confidencial.
- Participar desde la Fase de diseño hasta la Fase de implementación de políticas de Seguridad conjuntamente con personal del departamento de sistemas.

Es de vital importancia mantener siempre una cultura de Seguridad y difundirla a todo el personal usuario de la compañía, es por eso que en esta Fase se toma en cuenta la educación de los usuarios, realizando programas para tal objetivo, en los cuales se debe de especificar los siguientes puntos:

- Definir las señalizaciones y *logs* de Seguridad.
- Llevar a cabo programas de orientación hacia la Seguridad a nuevos empleados.
- Conducir programas de conducta y ética profesional.
- Programar y aplicar anualmente cuestionarios de conocimientos sobre las políticas de Seguridad.
- Crear alguna publicación interna con boletines de Seguridad de reciente creación.
- Crear y distribuir material adicional para la educación a los usuarios, tales como: *posters*, videos, conferencias, etc.

Si no se educa a los usuarios y se difunden las políticas, la infraestructura técnica de Seguridad pierde efectividad.

3.6.1 Aplicación

Para esta Fase se estudiaron que tipo de políticas de Seguridad estaban implementadas en esta empresa, encontrándose la siguiente problemática.

- No se lleva a cabo el adecuado manejo de políticas de Seguridad, puesto que no se encuentran documentadas, son desconocidas por el personal, o no hay una correcta difusión de las mismas.
- No existe un buen uso de las contraseñas personales, debido que son del conocimiento de todo el personal.
- Acceso al SITE por el personal no autorizado.
- Mala administración por parte del proveedor de Internet, lo cual causa un retraso en las actividades de la empresa.
- El envío masivo de correo SPAM y virus afecta constantemente al servidor de correo, que maneja la empresa, con lo cual se corre el riesgo de infectar los equipos con los cuales se trabajan.

Debido a esta problemática, se hace la siguiente propuesta; colocar las políticas y estándares preestablecidos por la empresa, aunados a los propuestos en la tesis, para así lograr un mejor funcionamiento dentro de la Seguridad ya establecida.
Para tal fin, se comenzará con establecer una política general la cual se enuncia a continuación:

"Todas las políticas existentes y por crear, deben encontrarse documentadas en el Manual de Políticas de Seguridad para la protección de información en la empresa en estudio, para que sean del conocimiento de los usuarios y aplicables en todo momento"

Además de proponer las siguientes políticas de Seguridad en diversos puntos vulnerables: Ver tabla

Políticas para el uso del correo electrónico *(e-mail)*	***Propósito:*** Prevenir el deterioro de la imagen pública de la empresa, cuando un correo sale de la misma. ***Alcance:*** Uso apropiado de cualquier correo electrónico que se envía desde la empresa y se aplica a todos los empleados. ***Restricción:*** No será autorizado el uso del correo electrónico de la empresa para la creación o distribución de mensajes que contengan comentarios ofensivos acerca de raza, nacionalidad, género, etc. Los empleados que reciban algún e-mail con esta clase de comentarios de parte de otro empleado, deberán reportarlo al supervisor inmediato. ***Uso Personal*.** Usar un número considerable de recursos de la empresa para mandar o recibir *e-mails* personales es aceptable, pero los correos no relacionados con el trabajo deben de guardarse en otra carpeta aparte. Mandar cadenas o bromas desde dentro de la empresa queda prohibido. ***Monitoreo*.** Los empleados de la empresa no gozan de privacidad en los archivos almacenados, enviados o recibidos, en el sistema de *e-mails*, es decir que el departamento de Seguridad puede monitorear en cualquier momento y sin previo aviso. ***Aplicación.*** Cualquier empleado que sea sorprendido violando estas políticas será sometido a las medidas impuestas de parte de la empresa o el área encargada de la Seguridad en la red, e incluso corre el riesgo de ser despedido.
Políticas para el buen uso y creación de contraseñas	***Propósito.*** Establecer un estándar en la creación de contraseñas que no sean fáciles de atacar, la protección de los mismos así como cambios frecuentes en éstos. ***Alcance.*** El alcance de estas políticas incluye a todo el personal que tiene o es responsable de una cuenta de usuario o cualquier medio de acceso que requiere de una contraseña en un sistema que resida en recursos de la empresa y que tiene acceso a su red. **Políticas Generales para la creación de contraseñas:** - Todas las contraseñas a nivel del área de sistemas deben cambiar por lo menos cada tres meses. - La generación de contraseñas a nivel de área de sistemas debe ser una tarea del área de Seguridad de la red, administrados mediante el manejo de la base de datos. - Las contraseñas a nivel usuario como son *e-mail, web, desktop computer,* deberán cambiar cada cuatro meses. - Las contraseñas no deberán escribirse o almacenarse dentro de correos o medios electrónicos.

Políticas Éticas	***Propósito*.** Guiar el comportamiento en los negocios y poder asegurar la conducta de a quienes se les aplica: empleados, contratistas, consultores, empleados temporales y demás trabajadores de la empresa. ***Alcance:*** Establecer una cultura de confianza e integridad en las labores cotidianas de la empresa. La ética en un equipo de trabajo proporciona un ambiente de apoyo y participación de cada empleado de la compañía, por lo tanto cada uno de los empleados deben estar familiarizados con el código ético de la empresa.
Políticas Extranet	***Propósito***: Describir las políticas sobre las cual otras organizaciones se conectan a la red de la empresa con el propósito de compartir información y/o realizar negocios. ***Alcance.*** Las conexiones entre terceros que requiere acceso a la red de la empresa caen dentro de esta política, sin tener en cuenta tecnologías como ISDN o VPN. Aquellos como *ISPs* que proveen Internet a la empresa no se encuentra dentro de esta política. Se realizará la descripción de políticas de la red interna hacia redes externas que se conectan a la empresa.

Políticas para los Servidores	***Propósito.*** Establecer estándares para la configuración del equipo interno de los servidores que pertenece y es manipulado por la empresa. La implementación efectiva de estas políticas minimiza el acceso de personal no autorizado. ***Alcance:*** Utilización de los servidores de manera eficiente por el grupo de administración de sistemas ***Políticas Generales Propuestas*** - Los administradores deben contar con una localización y con los respaldos correspondientes de cada servidor. - Control de las versiones del Sistema Operativo. - Así como también un control de las funciones y aplicaciones principales. - La información administrativa de la empresa debe ser actualizada y respaldada. - Tener un adecuado control de cambios de administración de servicios. ***Políticas para el Protocolo General de Configuración de los Servidores:*** - La configuración del sistema operativo se realizara de acuerdo con el protocolo establecido, aprobado por el área de Seguridad de información. - Los servicios y las aplicaciones que no son utilizados deben de ser desactivados. - Para tener acceso a los servicios será necesario tener una cuenta y una contraseña, protegidos mediante el control de accesos con métodos como TCP o *wrappers* si es posible. - Los parches mas recientes deberán instalarse en el sistema para que sea más práctico, excepto cuando este proceso interfiera con las actividades de la empresa . - Siempre deben utilizarse principios de Seguridad estandarizados. - Si esta disponible una metodología segura para el canal de conexión, se deberán desarrollar accesos con permisos sobre los canales seguros con técnicas como encriptación a través de la red usando *SSH o IPSec.* - Los servidores deberán estar localizados alrededor dentro un ambiente donde sea fácil controlar los accesos. - Los servidores no serán operados por personal ajeno al área de sistemas. Cualquier empleado que sea sorprendido violando estas políticas será sometido a las medidas impuestas por parte de la empresa, o el área encargada de la Seguridad en la red, e incluso corre el riesgo de ser despedido

Tabla 3.4 Políticas de Seguridad

La evaluación del desempeño de estás políticas, así como la efectividad lograda por las demás Fases, serán tratadas en el capítulo 4.

C A P I T U L O 4

EVALUACION Y RESULTADOS DE LA METODOLOGIA DE SEGURIDAD PARA UNA RED DE DATOS CORPORATIVA

4. EVALUACION Y RESULTADOS DE LA METODOLOGIA DE SEGURIDAD PARA UNA RED DE DATOS CORPORATIVA

4.1 Introducción

En este capítulo se evaluará y mostrará la efectividad de la metodología de Seguridad propuesta, aplicada en el capítulo anterior, a una red de datos corporativa de una empresa pequeña. Se concluirá con las fases finales, mostrando así los resultados e identificando las mejorías y beneficios que se obtuvieron. Así como también, un análisis y evaluación de posibles riesgos, dando como resultado un plan de contingencia. Posteriormente se darán a conocer algunas recomendaciones para cubrir ciertos puntos vulnerables en la red en estudio, siendo este el principal objetivo de la presente tesis.

Para cumplir con lo anteriormente descrito, es necesario hacer un recuento de las actividades realizadas hasta el momento:

Primeramente se identificaron todos los accesos a la información y a todos aquellos recursos *Hardware* y *Software* que forman parte de la infraestructura de comunicación de datos de la empresa en estudio. Se revisaron además, accesos al sistema *Kepler,* al sistema Operativo, accesos a las bases de datos, accesos a los archivos, y a los servidores que los contienen, encontrándose que no existe limitación alguna para el uso de estos.

En segunda instancia se desarrollaron estrategias de control en donde, por medio de un inventario se identificaron los recursos a proteger, mencionados en la fase de análisis preliminar, así como los requerimientos de Seguridad implícitos en los procesos y flujos de la información.

Se depuraron todas las políticas de Seguridad establecidas por la empresa (no documentadas) y se complementaron con políticas propuestas en la tercera fase de la Metodología. Dichas políticas deben de llevar una revisión periódica para corroborar que se estén cumpliendo cabalmente. Es por esta razón que se propone esta revisión cada seis meses como periodo mínimo.

4.2 Fase de Implementación

Esta fase es la culminación de la Metodología de Seguridad, con la cual se tendrán de manera concreta todas las políticas, procesos y tecnologías de información, que la organización requiere para un óptimo y seguro flujo de información.

Esta última fase fue llevada al caso práctico, y representa la ejecución de las acciones tomadas de las fases anteriores, pero ya bien establecidas en sub-fases que a continuación se describen y que se siguieron durante toda la metodología.

1ª. **Administración de la Seguridad**.- Identificar todos los accesos a la información, al software y al hardware, tales como: accesos al sistema, accesos a las bases de datos, accesos a archivos y directorios, accesos a compiladores protegidos, etc.
2ª. **Desarrollo de Estrategias de Control**.- Identificar los recursos a proteger así como sus propietarios para su autorización.
3ª. **Atención de Requerimientos de Seguridad**.- Tener perfectamente identificado cuales son los flujos y procesos de solicitudes de acceso a información.
4ª.**Depuración de los Datos de Seguridad**.- Actualizar todas y cada una de las políticas implementadas en la fase anterior cuando existe alguna creación o modificación en alguna de ellas.
5ª. **Rectificación de los identificadores de usuario (userid's) y sus privilegios**.- Validar que los recursos a los que accedan los usuarios sean solo los autorizados, para el desarrollo de sus actividades laborales.
6ª. **Análisis de *logs***.- Explotar los archivos *logs* de auditoria con herramientas predefinidas.
7ª. **Monitoreo de Políticas de Seguridad**.- Llevar una revisión periódica de cada una de las políticas de Seguridad implementadas en la infraestructura de cómputo y comunicaciones.
8ª.**Implementación y Administración de Alertas**.- Llevar un perfecto control de alertas emitidas por todos aquellos dispositivos encargados de la Seguridad interna y externa de la infraestructura de cómputo y comunicaciones, tales como: IDS, archivos *logs,* actualizaciones a antivirus, *firewalls*, etc.
9ª.**Detección de vulnerabilidades periódicamente**.- Aplicar un escaneo de posibles vulnerabilidades con herramientas de Seguridad *ISS*.

10ª.**Educación y comunicación continua con el usuario**.- Implementar una educación y cultura continua de Seguridad a los usuarios de la infraestructura de cómputo y comunicaciones.

4.3 Evaluación y Resultados de la Metodología de Seguridad Aplicada

Las primeras fases de esta metodología de Seguridad como se mencionó en el capítulo 3 fueron aplicadas para su evaluación (durante 5 meses) en una empresa pequeña dedicada a la selección y reclutamiento de profesionales en Tecnología de Información (TI).

Mediante los resultados arrojados se pudo observar a lo largo de este período de tiempo la viabilidad y efectividad de tal metodología, a razón de la identificación de vulnerabilidades de red, detección de códigos maliciosos, virus y caballos de Troya; así como también mejoramiento de control en las políticas de Seguridad de la empresa.

Aunque con estas fases queda cubierta la Seguridad en solo una parte de la arquitectura de Seguridad de la red de datos corporativa en cuestión, en este capítulo también se propondrán mejoras para dicha arquitectura.

4.3.1 Resultados del monitoreo a nivel red

Al aplicarse esta política de tener un monitoreo continuo en la red, en conjunción con las demás políticas involucradas, se obtuvieron los siguientes resultados durante los meses de evaluación.

Marzo – Abril

PROBLEMA	No. de incidencias	%
TRAFICO MALICIOSO	120	38%
GATOR	90	28%
HOTBAR	50	16%
NTBIOS -137UDP	22	7%
BROADCAST 53UDP	2	1%
NETBIOS-135TCP	27	8%
CHATAOL	4	1%
BROADCAST 25TCP	3	1%
CODERED	1	0%

(a)

Mayo - Junio

PROBLEMA	No. de incidencias	%
TRAFICO MALICIOSO	85	37%
GATOR	72	32%
HOTBAR	36	16%
NTBIOS -137UDP	10	5%
BROADCAST 53UDP	2	1%
NETBIOS-135TCP	21	9%
CHATAOL	1	0%
BROADCAST 25TCP	1	0%

(b)

Julio – Agosto

PROBLEMAS	No. de incidencias	%
TRAFICO MALICIOSO	68	47%
GATOR	43	30%
HOTBAR	15	10%
NETBIOS-137UDP	6	4%
BROADCAST 53UDP	0	0%
NETBIOS-135TCP	12	9%
CHATAOL	0	0%
BROADCAST 25TCP	0	0%

(c)

Tablas. 4.1 (a),(b),(c) Número de incidencias reportadas en los 5 meses de evaluación

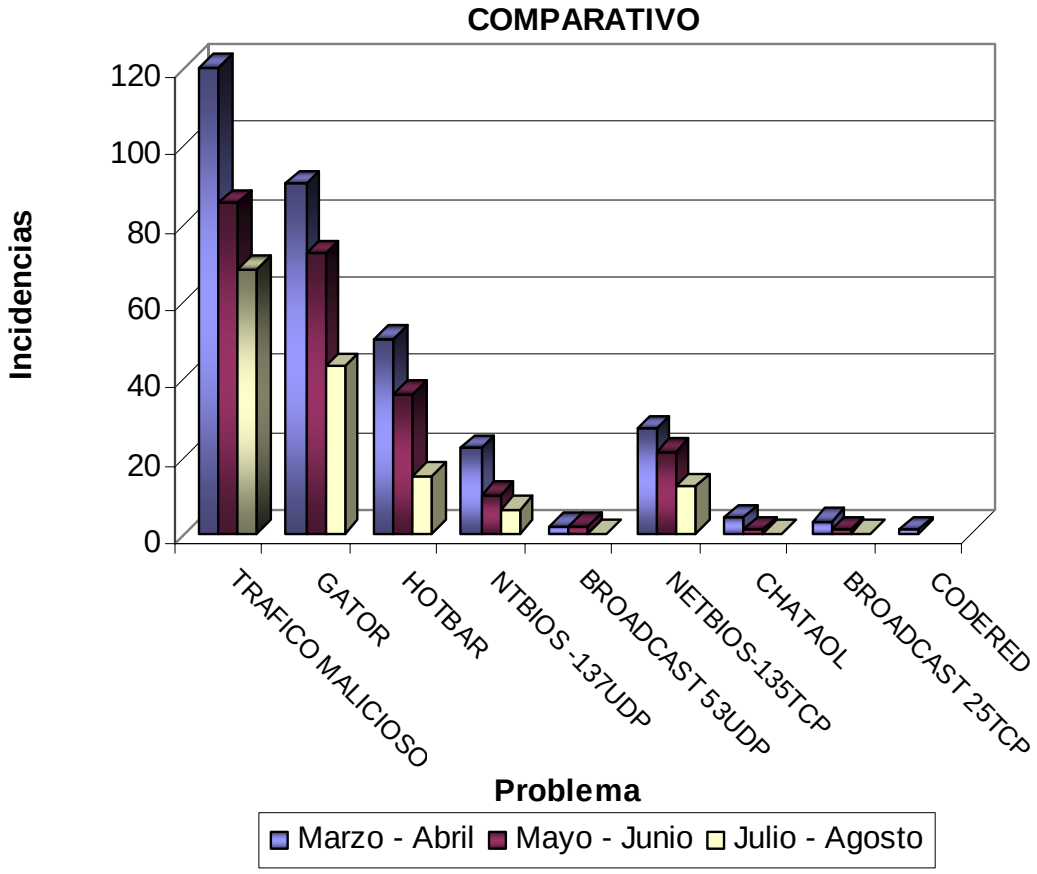


Figura 4.1 Número de Incidencias reportadas en los meses de evaluación

Tales resultados fueron proporcionados al actualizar el *software* de antivirus y al aplicar filtros de Seguridad de contenido, por lo que de acuerdo a la gráfica mostrada, se puede observar una significativa reducción de estas incidencias.

4.3.2 Resultados de detección de vulnerabilidades

Durante los 5 meses de evaluación, se utilizó un *IDS (Sistema de Detección de Intrusos),* como se muestra en la Figura 4.2 tal dispositivo fue colocado en el inicio del segmento de red, el cual reportaba a una consola de administración, donde se generaron reportes para poder identificar posibles vulnerabilidades y ataques externos y así poder aplicar las políticas de Seguridad correspondientes.

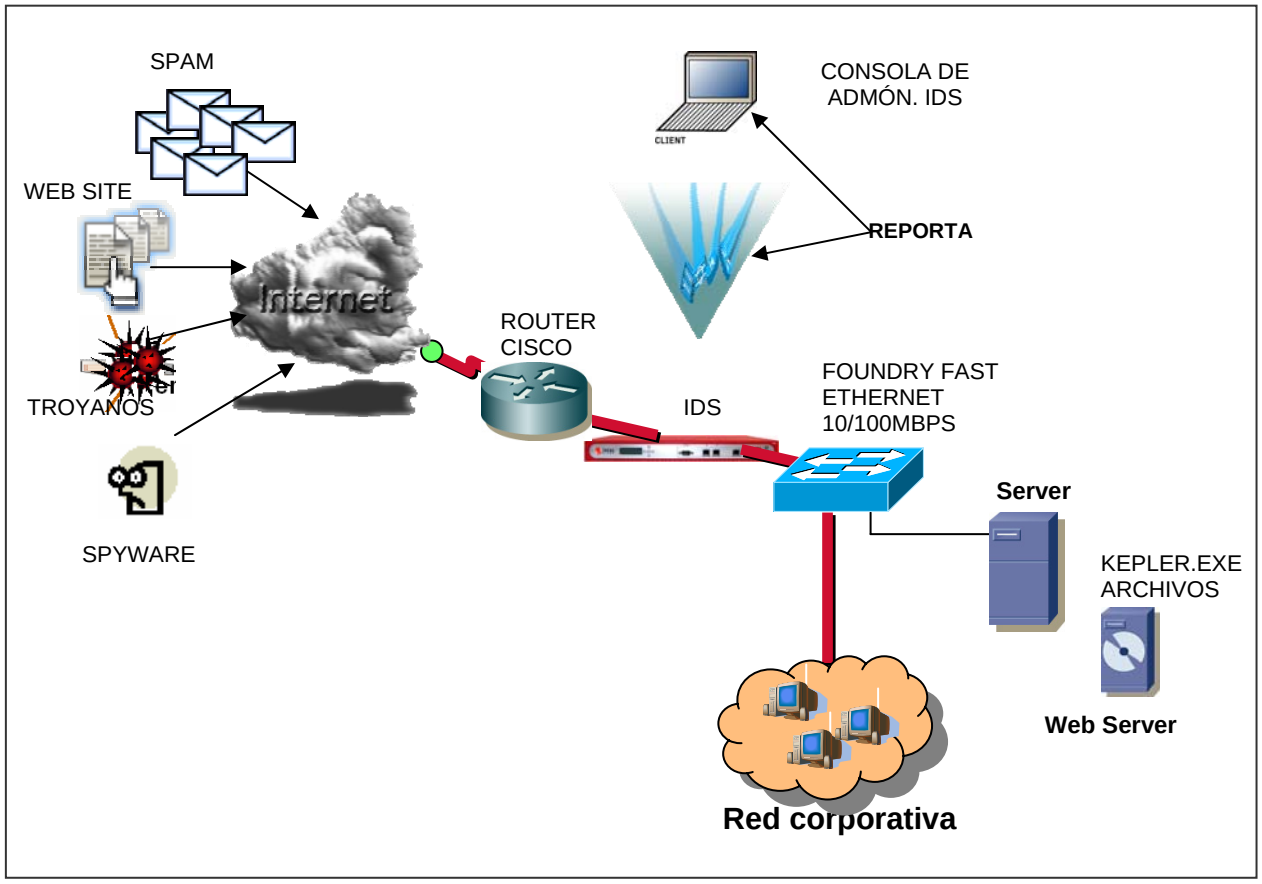


Figura 4.2 Monitoreo de la red corporativa mediante el IDS

Los reportes que se obtuvieron al monitorear las 50 estaciones de trabajo en operación fueron los siguientes:

VULNERABILIDADES IDENTIFICADAS

MARZO-AGOSTO DE 2005

	ALTAMENTE CRITICAS		CRITICAS	
Fecha	**Nombre**	**vulnerabilidad**	**Nombre**	**vulnerabilidad**
25 de Marzo de 2005	PC-02	MS02-072, MS03-001	PC-08	MS04-011,MS04-012
	PC-10	MS02-072, MS03-001	PC-10	MS01-028
	PC-14	MS02-072, MS03-001	PC-45	MS04-011,MS04-012
	PC-20	MS02-072, MS03-001	PC-09	MS04-011,MS04-012
	PC-03	MS02-072, MS03-001	PC-06	MS04-011,MS04-012
	PC-26	MS02-072, MS03-001	PC-19	MS01-028
	PC-05	MS02-072, MS03-001	PC-11	MS01-028
	PC-10	MS02-072, MS03-001	PC-27	MS01-028
	PC-33	MS02-072, MS03-001	PC-30	MS04-011,MS04-012
	PC-46	MS02-072, MS03-001	PC-22	MS04-011,MS04-012
	PC-09	MS02-072, MS03-001	PC-17	MS04-011,MS04-012
	PC-27	MS02-072, MS03-001	PC-48	MS03-030
	PC-32	MS02-072, MS03-001	PC-36	MS04-011,MS04-012
	PC-34	MS02-072, MS03-001	PC-05	MS04-011,MS04-012
	PC-18	MS02-072, MS03-001	PC-15	MS04-011,MS04-012
	PC-23	MS02-072, MS03-001	PC-35	MS03-030
			PC-42	MS03-030
			PC-04	MS03-030
15 de Abril de 2005	PC-03	MS02-072, MS03-001	PC-09	MS04-011,MS04-012
	PC-26	MS02-072, MS03-001	PC-06	MS04-011,MS04-012
	PC-05	MS02-072, MS03-001	PC-19	MS01-028
	PC-10	MS02-072, MS03-001	PC-27	MS04-011,MS04-012
	PC-33	MS02-072, MS03-001	PC-35	MS04-011
	PC-46	MS02-072, MS03-001	PC-30	MS03-030
	PC-14	MS02-072, MS03-001		
	PC-20	MS02-072, MS03-001		
	PC-24	MS02-072, MS03-001		
22 de Abril de 2005	PC-26	MS02-072, MS003-001	PC-09	MS04-011,MS04-012
	PC-15	MS02-072, MS003-001	PC-06	MS04-011,MS04-012
	PC-05	MS02-072, MS003-001	PC-19	MS01-028
	PC-10	MS02-072, MS003-001	PC-27	MS04-011,MS04-012
	PC-33	MS02-072, MS003-001	PC-35	MS04-011
	PC-46	MS02-072, MS003-001	PC-30	MS03-030
	PC-14	MS02-072, MS003-001	PC-36	MS04-011
	PC-20	MS02-072, MS003-001	PC-28	MS04-011,MS04-012

	PC-24	MS02-072, MS003-001		
29 de Abril de 2005	PC-03	MS02-072,MS03-001	PC-20	MS04-013
	PC-26	MS02-072,MS03-001	PC-27	MS04-012,MS04-013
	PC-05	MS02-072,MS03-001	PC-28	MS04-004,MS04-012
	PC-10	MS02-072,MS03-001	PC-30	MS03-030
	PC-33	MS02-072,MS03-001	PC-35	MS04-011
	PC-46	MS02-072,MS03-001	PC-19	MS01-028
	PC-14	MS02-072,MS03-001	PC-02	MS04-013
	PC-24	MS02-072,MS03-001		
6 de Mayo de 2005	PC-11	MS02-072,MS03-001	PC-33	MS04-018,MS04-022
	PC-26	MS02-072,MS03-001	PC-39	MS04-018,MS04-022
	PC-05	MS02-072,MS03-001	PC-16	MS04-018,MS04-022
	PC-10	MS02-072,MS03-001	PC-41	MS04-018,MS04-022
	PC-33	MS02-072,MS03-001	PC-05	MS04-018,MS04-022
	PC-46	MS02-072,MS03-001	PC-13	MS04-018,MS04-022
	PC-14	MS02-072,MS03-001	PC-12	MS04-018,MS04-022
	PC-24	MS02-072,MS03-001	PC-47	MS04-018,MS04-022
	PC-42	MS02-072,MS03-001	PC-17	MS04-018,MS04-022
	PC-04	MS02-072,MS03-001		
	PC-12	MS02-072,MS03-001		
	PC-18	MS02-072,MS03-001		
13 de Mayo de 2005	PC-10	MS02-072,MS03-001	PC-33	MS04-027,MS04-028
	PC-33	MS02-072,MS03-001	PC-39	MS04-018,MS04-022
	PC-46	MS02-072,MS03-001	PC-16	MS04-018,MS04-022
	PC-14	MS02-072,MS03-001	PC-41	MS04-018,MS04-022
	PC-24	MS02-072,MS03-001	PC-05	MS04-018,MS04-022
	PC-42	MS02-072,MS03-001	PC-13	MS04-018,MS04-022
	PC-04	MS02-072,MS03-001	PC-12	MS04-018,MS04-022
27 de Mayo de 2005	PC-10	MS02-072,MS03-001	PC-33	MS04-027,MS04-028
	PC-33	MS02-072,MS03-001	PC-39	MS04-018,MS04-022
	PC-46	MS02-072,MS03-001	PC-16	MS04-018,MS04-022
	PC-14	MS02-072,MS03-001	PC-41	MS04-018,MS04-022
	PC-24	MS02-072,MS03-001	PC-05	MS04-018,MS04-022
	PC-42	MS02-072,MS03-001	PC-13	MS04-018,MS04-022
			PC-12	MS04-018,MS04-022
3 de Junio de 2005	PC-46	MS02-072,MS03-001	PC-12	MS04-018,MS04-022
	PC-14	MS02-072,MS03-001	PC-16	MS04-018,MS04-022
	PC-24	MS02-072,MS03-001	PC-41	MS04-018,MS04-022
	PC-42	MS02-072,MS03-001	PC-05	MS04-018,MS04-022
	PC-04	MS02-072,MS03-001		
17 de Junio de 2005	PC-46	MS02-072,MS03-001	PC-12	MS04-018,MS04-022
	PC-14	MS02-072,MS03-001	PC-16	MS04-018,MS04-022
	PC-24	MS02-072,MS03-001	PC-41	MS04-018,MS04-022
	PC-42	MS02-072,MS03-001		
	PC-04	MS02-072,MS03-001		

24 de Junio de 2005	PC-46	MS02-072,MS03-001	PC-24	MS04-018,MS04-022
	PC-14	MS02-072,MS03-001	PC-16	MS04-018,MS04-022
	PC-42	MS02-072,MS03-001	PC-38	MS04-018,MS04-022
	PC-04	MS02-072,MS03-001	PC-16	MS04-018,MS04-022
			PC-45	MS04-018,MS04-022
			PC-05	MS04-018,MS04-022
			PC-13	MS04-018,MS04-022
			PC-12	MS04-018,MS04-022
15 de Julio de 2005	PC-46	MS02-072,MS03-001	PC-16	MS04-018,MS04-022
	PC-14	MS02-072,MS03-001	PC-41	MS04-018,MS04-022
	PC-42	MS02-072,MS03-001	PC-03	MS04-018,MS04-022
	PC-04	MS02-072,MS03-001	PC-13	MS04-018,MS04-022
			PC-12	MS04-018,MS04-022
22 de Julio de 2005	PC-14	MS02-072,MS03-001	PC-02	MS04-018,MS04-022
	PC-42	MS02-072,MS03-001	PC-11	MS04-018,MS04-022
	PC-46	MS02-072,MS03-001	PC-48	MS04-018,MS04-022
			PC-44	MS04-018,MS04-022
			PC-16	MS04-018,MS04-022
29 de Julio de 2005	PC-42	MS02-072,MS03-001	PC-44	MS04-018,MS04-022
	PC-47	MS02-072,MS03-001	PC-11	MS04-018,MS04-022
			PC-18	MS04-018,MS04-022
12 de Agosto de 2005	PC-18	MS02-072, MS003-001	PC-12	MS04-027,MS04-028
	PC-42	MS02-072, MS003-001		
	PC-38	MS02-072, MS003-001		
26 de Agosto de 2005	PC-38	MS02-072, MS003-001	0	0

Tabla 4.2 Identificación de vulnerabilidades clasificadas como altamente críticas y críticas

En la Tabla 4.2 se muestran las principales vulnerabilidades que fueron detectadas en el sistema *Windows* y están clasificadas de acuerdo al grado de peligrosidad que presentan al sistema.

Es decir tales vulnerabilidades son consideras de la siguiente manera:

Críticas: Si el año en el que fueron descubiertas es más reciente y es más probable se puedan cubrir mas rápidamente.

Altamente Críticas: Entre menor sea el año en que fueron descubiertas y se tenga un poco más de dificultad para poder ser cubiertas.

Graficando tales resultados se puede observar en la Figura 4.3 la disminución de las PC's con tales vulnerabilidades; ya que se aplicó la política de Seguridad de mandar

actualizaciones cada semana, así como la aplicación de *"parches"* de Seguridad al Sistema Operativo.

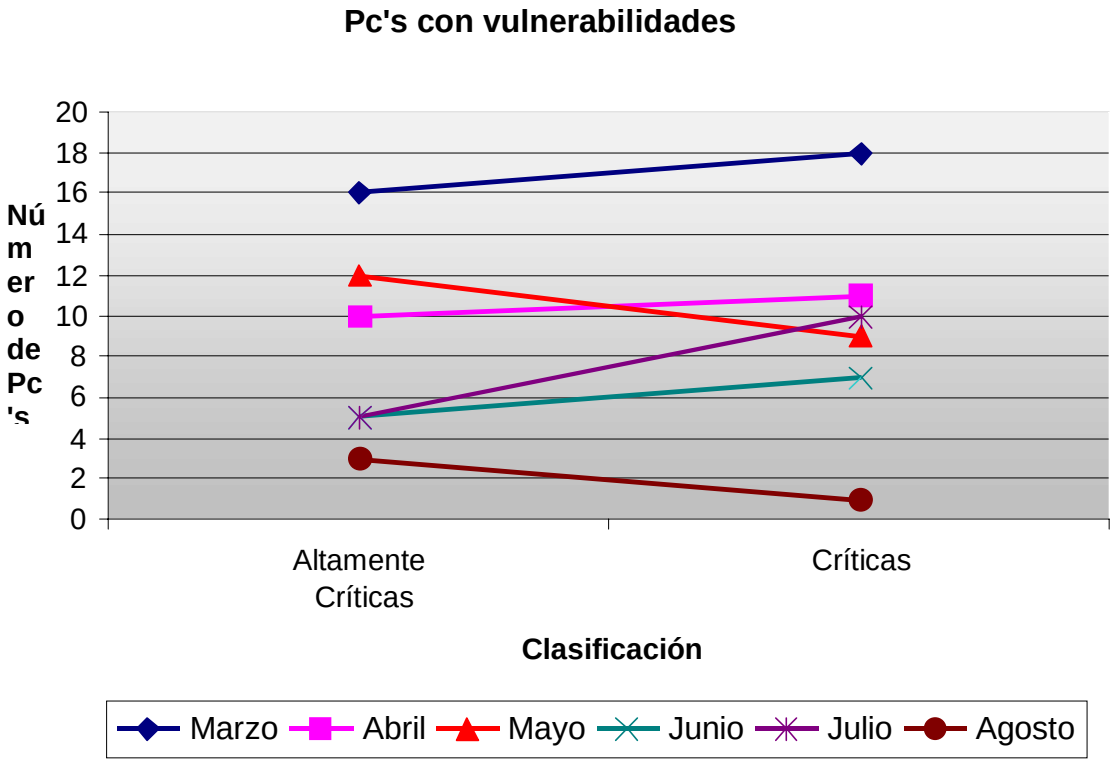


Figura 4.3 PC's reportadas con vulnerabilidades

4.4 Arquitectura de Seguridad Propuesta

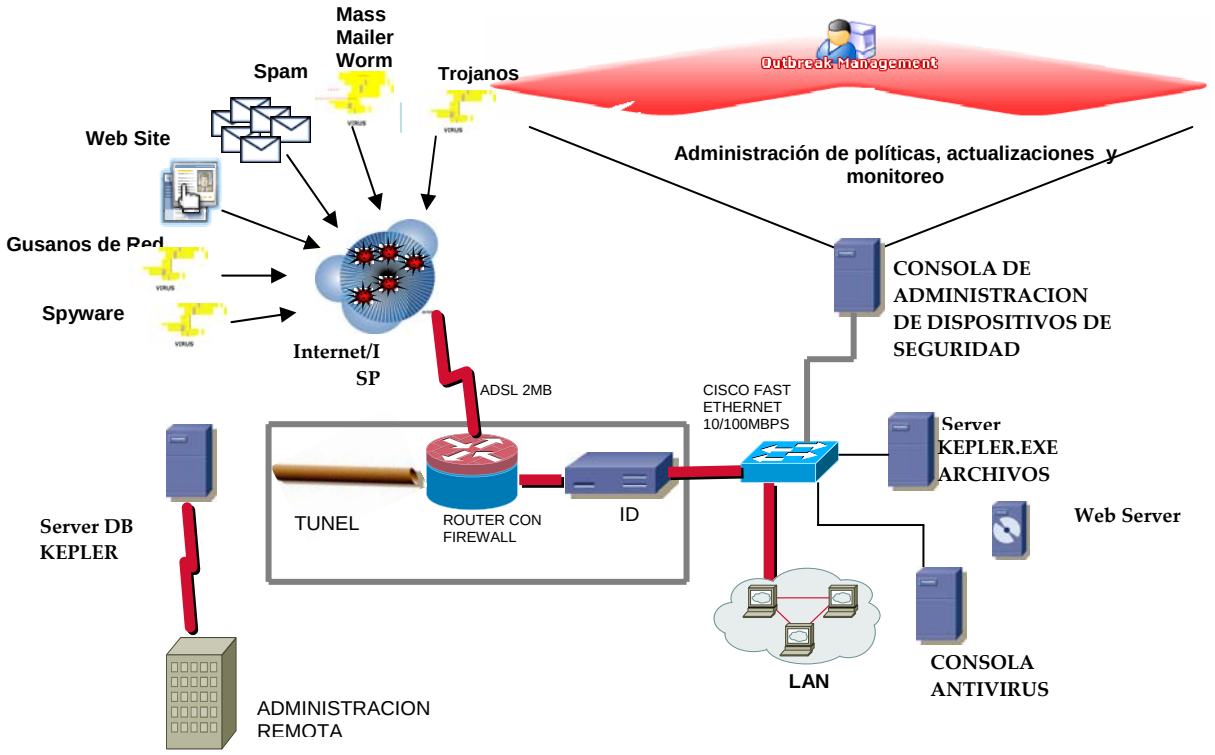


Figura 4.4 Arquitectura de Seguridad propuesta

En la figura 4.4 se muestra la arquitectura propuesta de Seguridad para la empresa en estudio, la cual consta de una arquitectura más robusta y se está protegiendo al 100% todos los recursos de la red.

Esta arquitectura consta de una conexión segura de túnel VPN entre la empresa y el *Hosting* de la empresa *outsourcing;* los datos que cruzan a través del túnel llevan un proceso de autenticación y cifrado, esta *VPN* pasa los datos de *KEPLER.*

El nivel de Seguridad se refuerza por medio de un *router* que contiene un *firewall* integrado, el cual puede decidir que tráfico pasa y que tráfico no pasa, además de contar con un IDS para prevenir ataques al proporcionar herramientas de valoración de vulnerabilidades integradas con los productos y servicios y para ayudar a reforzar las políticas de Seguridad,

bloquear el acceso de dispositivos no regulados, y aislar vulnerabilidades relacionadas con amenazas.

Esta información correlaciona vulnerabilidades con debilidades del sistema para evaluar los riesgos. Ayudando a aislar sistemas vulnerables y asegurar la red.

Las medidas que pueden ser tomadas son las siguientes:

- *Bloqueos en la capa de Red*
- *Monitoreo y Limpieza*
- *Análisis de Paquetes*
- *Políticas Forzadas (Antivirus y vulnerabilidades de MS)*
- *Logs y Reportes*
- *Topología*
- *Administración*
- *Notificaciones*
- *Actualizaciones (Updates)*

Así, una vez que las amenazas sean identificadas, el conocimiento específico de estas y las políticas de prevención de epidemias deben ser proporcionados como alerta temprana para ayudar a prevenir o contener epidemias.

4.5 Algunas Recomendaciones

De acuerdo a los resultados anteriormente vistos, y en conjunto con la Metodología de Seguridad Propuesta, se hacen las siguientes recomendaciones:

Además de lo mencionado acerca de las políticas, también se debe de poner en práctica las detecciones de posibles vulnerabilidades (como se hizo para la evaluación), es aquí donde se recomienda la utilización de herramientas propias para este fin tales como *ISS y NESSUS*. Y por ultimo, y no por eso menos importante, esta Metodología de Seguridad propone la educación y comunicación continua con el usuario donde se debe implementar una cultura continúa de Seguridad de la infraestructura de cómputo y telecomunicaciones.

Como esta empresa cuenta con una infraestructura administrativa y organizacional básica, se propone que se evalué la posibilidad de crear una **Dirección de Seguridad de**

la Información, que a nivel estratégico coordinara y ejecutara cada una de las actividades relacionadas al desarrollo y mantenimiento de procesos, políticas y tecnologías de información, encaminadas a la Seguridad en *software, hardware* y sobre todo de datos.

Es importante llevar siempre una documentación eficaz de todas las implementaciones, esta actividad también estará cubierta por la dirección antes mencionada.

4.5.1 La importancia de la Dirección de Seguridad de la Información

Como se sabe, muchas empresas no cuentan con un departamento especializado en Seguridad, lo único con lo que cuentan son con un encargado o gerente de sistemas, quien se encarga de llevar a cabo todas las funciones relacionadas al área.

Dicha dirección contará con una gerencia a nivel táctico, denominada “Gerencia de Arquitectura de Seguridad” y tres más a nivel operacional que serán: “Gerencia de Administración de Seguridad”, “Gerencia de Seguridad de Red (*Networking*)” y “Gerencia de Monitoreo y Alertas”.

En la siguiente figura 4.5, se muestra una propuesta para el organigrama de la Dirección de Seguridad de la Información, en ella se puede observar las diversas actividades que se llevarían a cabo por parte de cada Gerencia encargada.

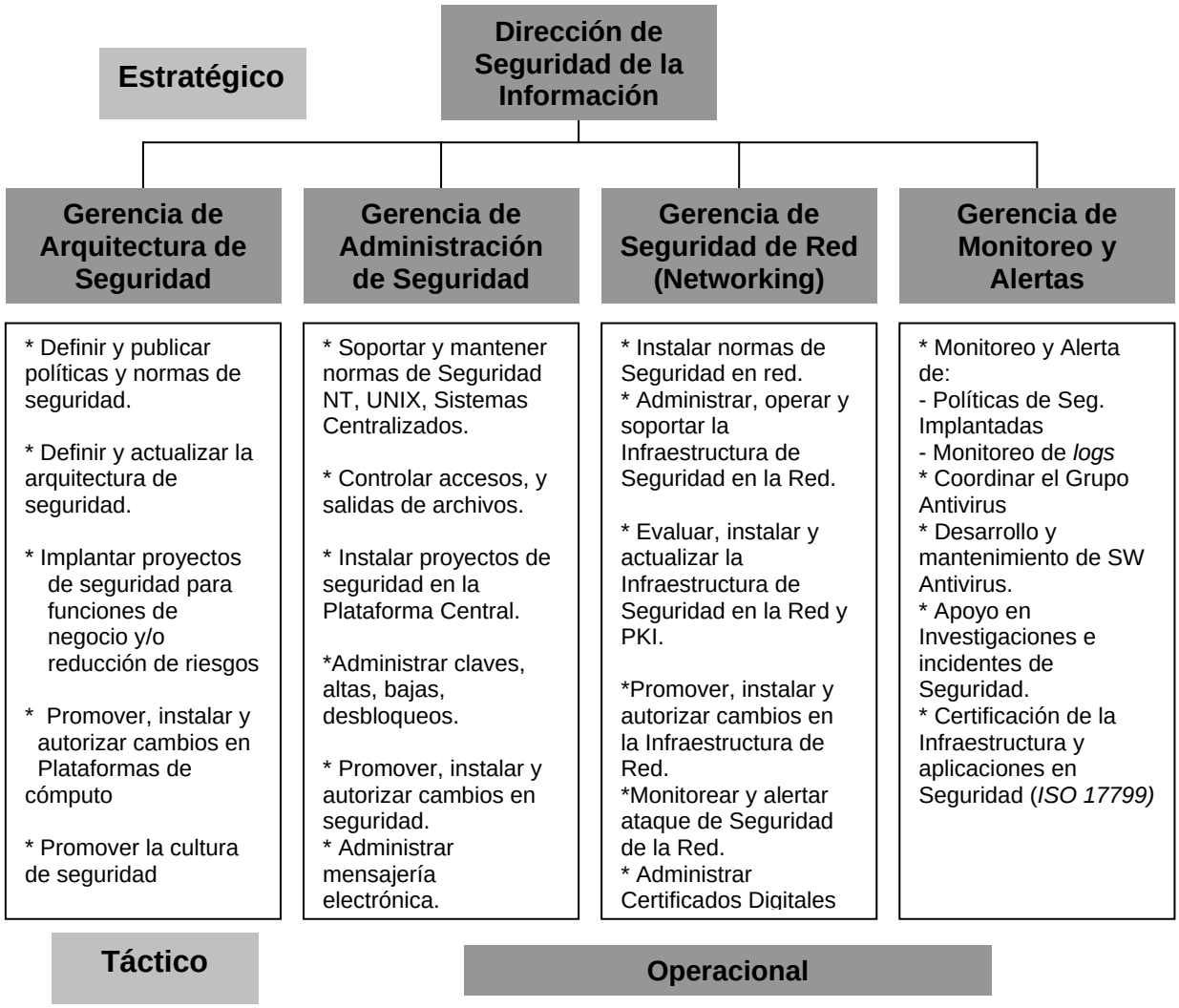


Figura 4.5 Dirección de Seguridad de la Información

4.6 Análisis de riesgos.

Basándonos en lo que dice la Norma ISO 17799, esta establece que; Para "**evaluar los riesgos en materia de Seguridad**", el análisis de los riesgos realizado a toda la organización, o sólo a partes de la misma, debe ser de tipo "cualitativo" y no "cuantitativo" y que la evaluación de los mismos es una consideración sistemática de los siguientes puntos:

a) Impacto potencial de una falla de Seguridad en los negocios, teniendo en cuenta las potenciales consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos;

b) Probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados.

Los resultados de esta evaluación ayudarán a orientar y a determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes a Seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos. Puede resultar necesario que el proceso de evaluación de riesgos y selección de controles deba llevarse a cabo en varias ocasiones, a fin de cubrir diferentes partes de la organización o sistemas de información individuales.

El análisis de los riesgos debe ser dinámico y cíclico. Debe efectuarse periódicamente sin importar si hubo o no modificaciones tecnológicas u operativas. Con los sucesivos análisis de riesgo realizados, se evalúan los problemas que ocurrieron debido a la falta de medidas tomadas, para luego implementar contramedidas. Esto hace posible que el análisis de riesgo se vaya ajustando progresivamente a la realidad de la organización y forme parte del mantenimiento del sistema de Seguridad informático.

Por lo tanto es importante llevar a cabo revisiones periódicas de los riesgos de Seguridad y de los controles implementados a fin de reflejar los cambios en los requerimientos y prioridades de la empresa, considerar nuevas amenazas y vulnerabilidades (lo cual debe hacerse permanentemente y debe estar a cargo de personal especializado) y corroborar que los controles siguen siendo eficaces y apropiados.

Las revisiones deben llevarse a cabo con diferentes niveles de profundidad según los resultados de evaluaciones anteriores y los niveles variables de riesgo que la gerencia está dispuesta a aceptar.

Frecuentemente, las evaluaciones de riesgos se realizan primero en un nivel alto, a fin de priorizar recursos en áreas de alto riesgo, y posteriormente en un nivel más detallado, con el objeto de abordar riesgos específicos.

El análisis de riesgos involucra la determinación de qué se necesita proteger, qué se necesita para protegerlo y cómo. Es el proceso de examinar los posibles riesgos y clasificarlos por nivel de severidad, esto involucra hacer decisiones costo-beneficio.

Haciendo este análisis más preciso, y tomando como ejemplo la red de datos corporativa que se ha estudiado, el primer paso para mejorar la Seguridad en un sistema es responder a las siguientes preguntas básicas.

- ¿Qué es lo que estoy tratando de proteger?
  Todos los datos que son generados por la organización y los flujos de información de la misma.
- ¿Qué es lo que necesito para protegerlo?
  Gracias a la Metodología de Seguridad, nos brindará las herramientas necesarias para poder proteger los datos y los flujos de información.

- ¿Cuánto tiempo, esfuerzo y dinero estoy dispuesto a dedicar para obtener un nivel adecuado de protección?
  La Empresa en estudio esta convencido que la Seguridad es un punto muy importante dentro de su organización, es por ello que esta dispuesto a brindar todo el apoyo necesario para la puesta en marcha de la Metodología de Seguridad.

Estas preguntas forman la base del proceso del Análisis de Riesgos. Existen tres pasos básicos en el análisis de riesgos:

1.- Identificación de recursos.
2.- Identificación de amenazas.
3.- Cálculo de riesgos.

1. Identificación de recursos

Para lograr esto, se necesita enlistar los recursos con los que se cuente en la organización. Es posible que se requiera conocer más detalladamente los procedimientos, leyes, políticas de la organización, recursos disponibles e inclusive si se cuenta con seguro sobre los bienes inmuebles. Existen recursos tangibles (monitores, computadoras, impresoras, etc.), e intangibles (privacidad de los usuarios, contraseñas de los usuarios, imagen pública, etc.)

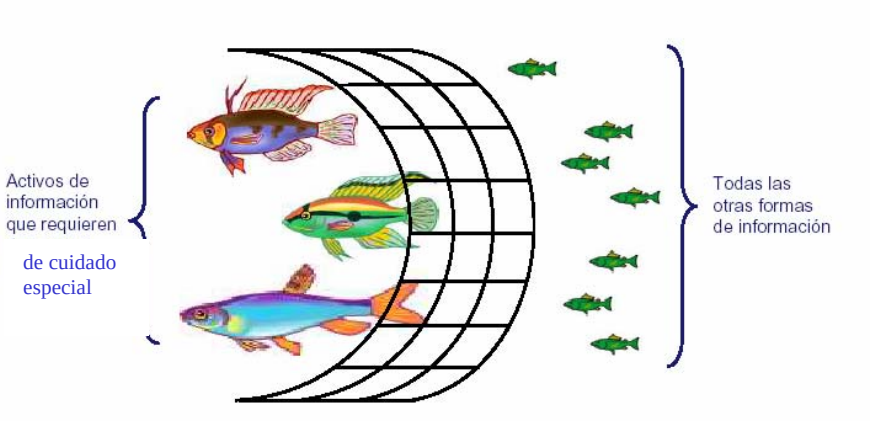


Figura 4.6 Identificación de Recursos

2. Identificación de las amenazas.

El siguiente paso es hacer una lista de amenazas que afecten los recursos, dichas amenazas pueden ser ambientales como: incendios y terremotos, amenazas extrañas como: fallas estructurales del edificio, relámpagos, inundaciones, pérdida del servicio telefónico, etc., amenazas de introducción de virus informáticos y "*bugs*" en el *software*. Después de determinar las amenazas es necesario estimar qué tan factible es que suceda cada una de ellas, esta es una tarea difícil por la cantidad de información a recabar, por ejemplo: informes estadísticos, seguros, daños, etc.

3. Cálculo de la revisión de los riesgos

El análisis de riesgos no debe ser hecho una sola vez y olvidarlo, sino por el contrario debe ser actualizado periódicamente. Además el análisis de amenazas debe ser realizado cada vez que se observe un cambio importante en la operación o la estructura del inmueble por ejemplo: un cambio de oficinas, la construcción de una oficina cerca de nuestro centro de cómputo, remodelaciones, etc.

El concepto de riesgo puede ser visto desde una ecuación:

$$\frac{\text{Amenaza} * \text{Vulnerabilidad} * \text{Impacto}}{\text{Mitigación}} = \text{Riesgo}$$

- **Tabla de análisis de riesgos**

Se debe de realizar el análisis de acuerdo a los riesgos: muy alto, alto, medio, bajo y muy bajo y de acuerdo al impacto y a las vulnerabilidades que se presenten. En la tabla se muestra un ejemplo del como se puede armar una tabla de este tipo.

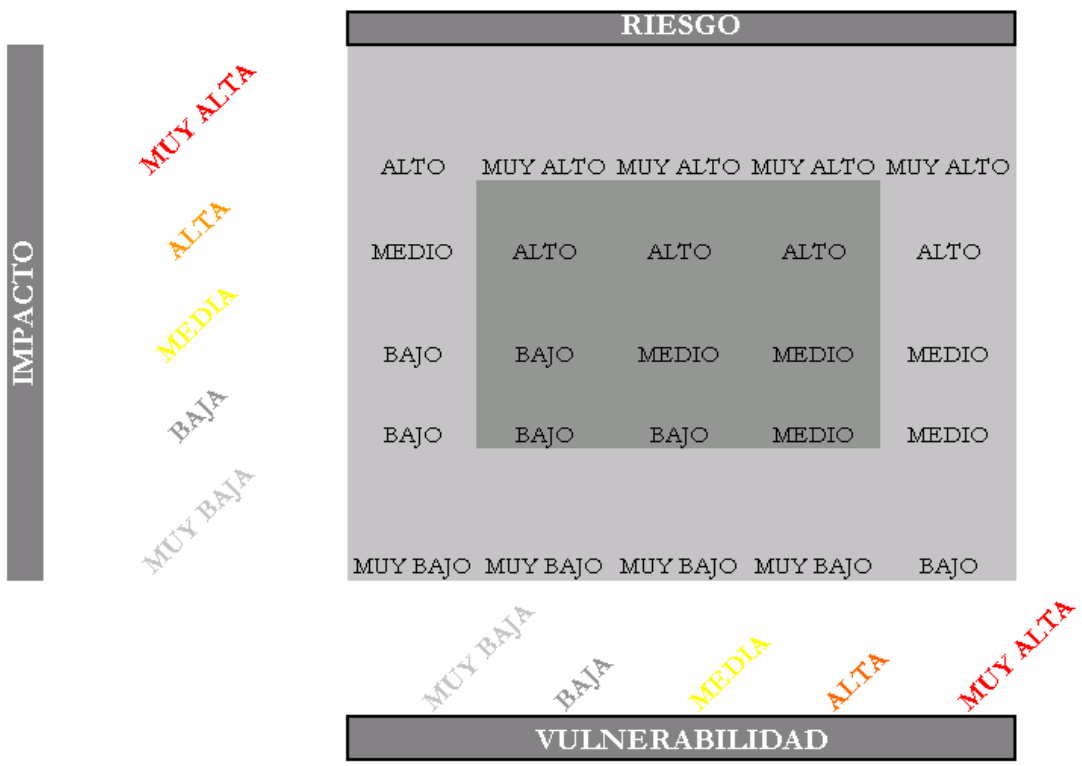


Tabla.4.3 Tabla de análisis de riesgos

- **Análisis costo-beneficio**

Después de completar el análisis de riesgos, es necesario asignar un costo a cada riesgo, esto es, si sucede algo saber cuánto le cuesta a la organización la pérdida, y determinar el costo de prevención de riesgos, el costo de recuperación, etc.

- **El costo de pérdida**

Los costos de pérdidas en computación pueden ser bastante difíciles de averiguar puesto que muchas veces se trata con beneficios intangibles. Supongamos un servicio cualquiera, cuáles serian los costos de:

- Negación de un servicio en determinado tiempo
- Pérdida permanente del bien que presenta el servicio
- Daño parcial del servidor

- **El costo de prevención**

Finalmente es necesario calcular el costo de prevención para cada una de las pérdidas, es decir, lo que nos cuesta en dinero el contar con algún tipo de plan de contingencia y prevención y ponerlo en marcha.

4.6.1 Proceso de identificación de Riesgos

Este proceso sirve para lograr identificar el riesgo dentro de una organización, evaluando su magnitud, así como también identificando áreas, para minimizar el riesgo encontrado, utilizando contramedidas. Ver figura 4.7.

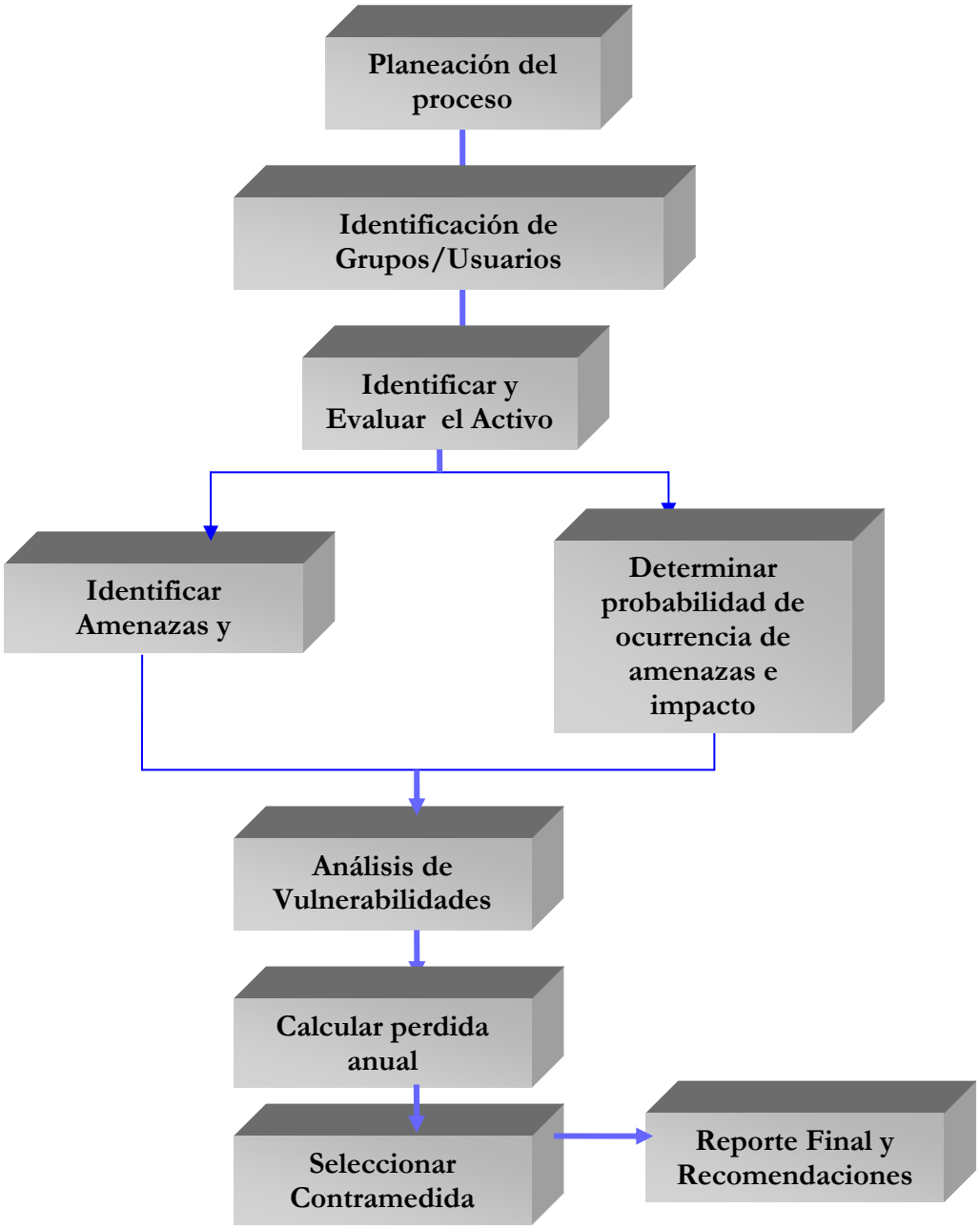


Figura 4.7 Proceso de identificación del riesgo

Pasos del proceso de análisis de riesgos

1- Planear, cuestionarios de entrevistas, metodologías de probabilidad e inventarios.

2- Identificar propietarios de aplicaciones/servicios con amplio conocimiento del negocio así como de la operación de los servicios.

3- Cada servicio se debe evaluar identificando cuento vale en dinero, o cuanto perdería el negocio ante una perdida total o por divulgación de la información.

4- Estadísticas de cada cuando se presenta el problema (Amenazas naturales, accidentales e intencionales).

5- Analizar cuan vulnerable somos ante las amenazas identificadas.

6- Calcular cuanto perdemos en dinero anualmente.

7- Seleccionar contramedidas evaluando costo/beneficio.

4.6.2 Herramientas para el análisis de riesgos

Una de las herramientas de auditoria que se recomienda para el análisis de riesgos más utilizada es: el "*checklist*". Un ejemplo del contenido de éste se muestra en la tabla 4.4.

Activo	Valor intrínseco	Valor adquirido		
		Disponibilidad	Integridad	Confidencialidad

HW
SW
Información/Datos
Personal
Procedimientos
Comunicaciones
Instalaciones Físicas

Tabla. 4.4 Herramienta *Checklist*

4.7 Fase Final

En esta fase final, se concluyeron siguientes resultados:

- Decisión de comprar componentes de Seguridad adicionales.

  - Inversión de *Hardware* y *Software*
- Decisión requerida para aplicaciones prioritarias a ser consideradas en planes de contingencia.
  - Costos del Centro alterno
  - Compra de Seguro de daños materiales
  - Costos por *Hardware* y *Software* requeridos para recuperación
  - Costos de *Software* y mecanismos de "espejo"
- Análisis Costo-Beneficio

4.8 Plan de Contingencia

Un plan de contingencia es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. Este plan se sigue si el sistema no se puede restaurar a tiempo, su objetivo final es mantener la disponibilidad, integridad y confidencialidad de los datos.

Debe haber un plan para cada tipo de ataque y tipo de amenaza. Cada plan consta de un conjunto de pass que se han de emprender en el caso de que un ataque logre pasar las directivas de Seguridad. El plan de contingencia debe:

- Determinar quién debe hacer qué, en qué momento y en qué lugar para que la organización siga funcionando.
- Ensayarse periódicamente para mantener al personal informado de los pasos de la contingencia actual.
- Abarcar la restauración de las copias de Seguridad.
- Explicar la actualización del software antivirus.
- Abarcar el traspaso de la producción a otra ubicación o sitio.

Los siguientes puntos resaltan las distintas tareas que deben evaluarse para desarrollar un plan de contingencia:

- Evaluar las directivas y controles de Seguridad de la organización para utilizar todas las oportunidades destinadas a reducir los puntos vulnerables. La

evaluación debe tratar el plan y los procedimientos de emergencia actuales de la organización y su integración en el plan de contingencia.

- Evaluar los procedimientos actuales de respuesta ante emergencias y su efecto en el funcionamiento continuo de la organización.
- Desarrollar respuestas planeadas a taques, integrarlas en el plan de contingencia y anotar hasta qué punto son adecuadas para limitar el daño y reducir el impacto del ataque en las operaciones de procesamiento.
- Evaluar planes de recuperación de desastres para determinar su adecuación con el fin de proporcionar un entorno operativo temporal o a largo plazo.

C O N C L U S I O N E S

CONCLUSIONES

La Metodología de Seguridad que se propuso durante esta tesis, fue diseñada para ayudar a las organizaciones a desarrollar un plan de seguridad para proteger la *disponibilidad, integridad y confidencialidad* de los datos de los sistemas informáticos y de la red de datos corporativa en general. Basándose en recomendaciones para las prácticas exitosas de Seguridad de Información manejadas por la Norma ISO 17799.

Los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo, que hay que invertir para desarrollar las directivas y controles de seguridad apropiados. Cada organización debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación. Cada sistema informático, entorno y directiva organizativa es distinta, lo que hace que cada servicio y cada estrategia de seguridad sean únicos. Sin embargo, los fundamentos de una buena seguridad siguen siendo los mismos.

Aunque la Metodología de Seguridad aquí propuesta, puede ahorrar tiempo a la organización y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad no es una actividad puntual. Es una parte integrante del ciclo de vida de los sistemas. Las actividades que se describieron a lo largo de la tesis suelen requerir actualizaciones periódicas, o las revisiones correspondientes. Estos cambios se realizan cuando las configuraciones y otras condiciones y circunstancias cambian considerablemente o cuando hay que modificar las leyes y normas organizativas. Éste es por tanto un proceso *iterativo*. Nunca termina y debe revisarse y probarse con periodicidad y metodología.

Los principales ataques a los sistemas y a la información, provienen de la red. Proteger la misma de intrusiones no deseadas es, por tanto, uno de los objetivos prioritarios que un administrador de red debe proponerse. Es por eso que a lo largo de esta tesis, se desarrollaron aspectos que se deben de tomar en cuenta a la hora de proteger la red.

Este trabajo dio una visión profunda de los riesgos que se presentan en las redes de la mayoría de las empresas conectadas, o no, a Internet, así como de los principales sistemas de seguridad existentes y las nuevas tecnologías de información que operan

actualmente en referencia a este tema. El objetivo de este estudio se centró precisamente en el análisis de los peligros y amenazas más comunes que existen en seguridad, así como en los nuevos mecanismos de seguridad que pretenden darles solución.

En México, para las empresas, la existencia de recursos humanos especializados en Seguridad Informática es extremadamente escasa, es por ello, que se dio a la tarea de profundizar sobre el tema y desarrollar una serie de pasos y actividades, englobados en una metodología de Seguridad, que pretende dar una solución óptima a ciertos problemas de seguridad de información y en general de infraestructura de comunicaciones y cómputo.

Creando una cultura de seguridad eficiente que permita el desarrollo óptimo de todas y cada una de las actividades que este ámbito necesita, proponiendo una ***Dirección de Seguridad*** a nivel estratégico, que coordinará a través de sus gerencias todas aquellas actividades encaminadas a esto.

Así como también proponer el desarrollo de las políticas de seguridad, que bien, se pueden tener, es también de vital importancia que se encuentren documentadas, especificando objetivos y actividades a desarrollar, así como monitorear que sean cumplidas al pie de la letra.

Por último, al tomar las guías para implementar las mejores prácticas en la Seguridad de la Información que predica la Norma ISO 17799 como base, la Metodología de Seguridad estudiada queda respaldada por esta Norma, pudiéndola llevar acabo en cualquier empresa u organización no importando su tamaño, lo importante es el grado de “dependencia informática” que se tenga.

GLOSARIO DE TERMINOS

GLOSARIO DE TERMINOS

-A-

Active X: Componente que se puede insertar en una página Web para proporcionar una funcionalidad que no está directamente disponible en HTML como secuencias de animación. Los controles *Active X* se pueden implementar en diversos lenguajes de programación. Pequeños programas que permiten mostrar páginas Web dinámicas en el PC y que suplen las limitaciones que, al respecto, tiene el lenguaje HTML. Los controles *Active X* tienen que descargarse al disco duro del ordenador para que los documentos que los utilizan puedan visualizarse.

Actualización: Es el término que se utiliza para identificar todos los diferentes tipos de paquetes que pueden hacer que un sistema esté al día (actualizado), incluyendo *hotfixes*, acumulados, *Service Packs*, y otros paquetes que incluyan características. Las actualizaciones se caracterizan por la severidad del tema que tratan. Algunas actualizaciones son críticas mientras que otras son recomendadas.

Administrador: Es la persona o programa encargado de gestionar, realizar el control, conceder permisos, etc. de todo un sistema informático o red de computadoras.

ADSL *(Asymetric Digital Subscriber Line).* Línea de usuario Digital Asimétrica. Este sistema permite transmitir información en formato digital a través de las líneas normales de teléfono. Para acceder a este sistema tenemos que contratarlo con nuestro operador de telefonía.

Antispyware: Tecnología de seguridad que ayuda a proteger a un equipo contra *spyware* y otro software potencialmente no deseado. Este software ayuda a reducir los efectos causados por el *spyware* incluyendo el lento desempeño del equipo, ventanas de mensajes emergentes, cambios no deseados en configuraciones de Internet y uso no autorizado de la información privada.

Auditoria informática: Actividad que consiste en la emisión de una opinión profesional sobre si un sistema sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas. La auditoria se fundamenta y justifica a través de procedimientos específicos basados en la opinión profesional del auditor. El alcance, la amplitud y la profundidad de la auditoria informática está especificado en su propia metodología.

Autenticación: Es el proceso de verificar que alguien o algo es quien o lo que dice ser. En redes de equipos públicos y privados (incluyendo Internet), la autenticación se lleva a cabo comúnmente a través de contraseñas de inicio de sesión.

Autocifrado: Operación mediante la cual un virus codifica (cifra) parte de su contenido, o éste en su totalidad. Esto, en el caso de los virus, dificulta el estudio de su contenido.

Autorización Con referencia a la computación, especialmente en los equipos remotos en una red, es el derecho otorgado a un individuo o proceso para utilizar el sistema y la información almacenada en éste. Típicamente la autorización es definida por un administrador de sistemas y verificado por el equipo basado en alguna identificación del usuario, como son un código o una contraseña.

-B-

Backup. Recursos adicionales o copias duplicadas de datos como prevención contra emergencias.

Base de datos: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su uso posterior.

Bug: Término aplicado a los errores descubiertos al ejecutar un programa informático. Fue usado por primera vez en el año 1945 por *Grace Murray Hooper*, una de las pioneras de la programación moderna, al descubrir cómo un insecto (bug) había dañado un circuito de la

computadora. Hoy en día, muchos programas son creados y puestos a disposición del público en las conocidas versiones beta, para que los propios usuarios detecten los errores o *bugs*.

-C-

Caballo de Troya: Del inglés *TrojanHorse*. También llamado comúnmente como *Troyano*. Programa de computadora que aparenta tener una función útil, pero que contiene código posiblemente malicioso para evadir mecanismos de seguridad, a veces explotando accesos legítimos en un sistema.

Cifrado. Técnica de seguridad que utiliza un valor corto usado al cifrar datos para garantizar la intimidad. En algunos esquemas de cifrado, el receptor debe usar la misma clave para descifrar los datos. Otros esquemas usan un par de llaves: una para cifrar y otra diferente para descifrar.

Contraseña: Es una cadena de caracteres que el usuario escribe para verificar su identidad en una red o en una PC local.

Cracker: Persona que trata de introducirse a un sistema sin autorización y con la intención de realizar algún tipo de daño u obtener un beneficio.

Crackeador de contraseñas: Programa utilizado para obtener las contraseñas cifradas de los archivos de contraseñas

Credenciales: Información que incluye la identificación y prueba de identificación que se utiliza para obtener acceso a los recursos locales y de red. Ejemplos de credenciales son el nombre de usuario y contraseñas, tarjetas inteligentes y certificados.

Criptografía: Es la utilización de códigos para convertir información por medio de una clave para que sólo un receptor específico pueda leerla. La criptografía es utilizada para permitir la autenticación y el no repudio, y para ayudar a preservar la confidencialidad y la integridad de datos.

-D-

Derechos de administrador: Conjunto de acciones u operaciones, que sólo uno o varios usuarios concretos pueden realizar dentro de una red de computadoras

DDoS: Acrónimo de *DistributedDenialofService* (Negación de Servicio Distribuido). Un tipo de ataque de *Negación de Servicio* en el cual un intruso utiliza código malicioso instalado en varias computadoras para atacar un solo objetivo. Un intruso podría utilizar éste método para tener un efecto mayor en el objetivo que el que se obtendría con un ataque desde una sola computadora.

DoS: Acrónimo en inglés de *DenialofService* (Negación de Servicio). Es un asalto computarizado llevado a cabo por un intruso, que no afecta a la información de equipo y cuya finalidad es sobrecargar o congelar un servicio de red, como un servidor Web o de archivos. Por ejemplo, un ataque puede causar que el servidor esté tan ocupado tratando de responder, que ignorara cualquier petición legítima de conexión.

Dropper: Es un archivo ejecutable que contiene varios tipos de virus en su interior.

-E-

Ethernet:

Extranet: Una Extranet en una red de colaboración que utiliza la tecnología Internet. La tecnología Extranet puede ser concebida como parte de una Intranet que es accesible para otras empresas o como una herramienta que permite la colaboración entre empresas, la información compartida puede ser sólo para aquellos miembros colaboradores de la empresa que poseen Intranet y en algunos casos éstos podrían ser públicos.

-F-

Firewall: Elemento físico ó lógico en una red cuyo fin es prevenir el acceso no autorizado a recursos ó información.

FTP: *File Transfer Protocol.* Protocolo de Transferencia de Archivos. Uno de los diversos protocolos de la red Internet. Es el ideal para transferir grandes bloques de datos por la red

-G-

Gusano: Del término en ingles *Word*.Código malicioso autopropagable el cual puede distribuirse a sí mismo a través de una conexión de red. Puede tomar acciones dañinas tales como consumir recursos de sistemas de red o locales, causando posiblemente un ataque de negación de servicio.

-H-

Hacker: Persona que deliberadamente viola la seguridad informática, normalmente para causar desconcierto o conseguir información confidencial como datos financieros. Originariamente, la palabra "hacker" hacía referencia a cualquier persona interesada en la informática; hoy en día, el término es usado por el público y la prensa para designar a las personas maliciosas.

Host: Cualquier computadora que tenga acceso total de dos direcciones a otras computadoras y a la Internet.

Hostname Denominación otorgada por el administrador a una computadora. El hostname es parte de la dirección electrónica de esa computadora, y debe ser único para cada máquina conectada a Internet. Comúnmente conocido como *Nombre de equipo*.

Hub:

-I-

IDS: Acrónimo en inglés de *Intruder Detection System* (Sistema de Detección de Intrusos). Administración de seguridad para redes y computadoras. Se encarga de obtener y analizar información dentro de una computadora o una red para identificar posibles huecos de seguridad, que incluyen intrusiones (externas) y uso inapropiado (internas).

IIS: *Internet Information Service (o Server),* serie de servicios para los ordenadores que funcionan con Windows. Originalmente era parte del *Option Pack* para *Windows NT*. Luego fue integrado en otros sistemas operativos de Microsoft destinados a ofrecer servicios, como *Windows 2000* o *Windows Server 2003*. Windows XP Profesional incluye una versión limitada de IIS. Los servicios que ofrece son*: FTP, SMTP, NNTP y HTTP/HTTPS.*

Internet: Es una red de redes a escala mundial de millones de computadoras interconectadas con el conjunto de protocolos TCP/IP.

Intranet: Infraestructura basada en los estándares y tecnologías de Internet que soporta el compartir información dentro de un grupo bien definido y limitado. Red privada.

IP: Acrónimo en inglés de *Internet Protocol* (Protocolo de Internet).Método por el cual información es enviada de una computadora a otra en el Internet.

IPSec: Acrónimo en inglés de *Internet ProtocolSecurity*(Seguridad del Protocolo de Internet). Un estándar en desarrollo para seguridad en redes ó en la capa de procesamiento de paquetes en comunicaciones por redes.

ISO: Acrónimo en inglés de*InternationalOrganizationforStandardization* (Organización Internacional de Normalización). Organización voluntaria con miembros votantes que son organismos designados de naciones participantes.

ISO 17799: Estándar para el manejo de la Seguridad de la Información reconocido internacionalmente. Norma que contiene una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar.

ISP: Siglas para identificar al Proveedor de servicios de Internet.

ISS: Siglas de Internet Security Scáner. Es una herramienta de dominio público que revisa una serie de servicios para comprobar el nivel de Seguridad que tiene esa máquina. Es capaz de revisar una dirección IP o un rango de direcciones IP.

-K-

KEPLER: Sistema Integral de Información. Sistema ERP mexicano que soporta y ayuda la toma de decisiones. Tiene como objetivo el control de información de su empresa; buscando así el aumento de su productividad. Cumple con las necesidades actuales de cualquier empresa. Es un sistema 100% integrado, que cuenta con una herramienta de flexibilidad la cual le permite adaptar la totalidad de sus partes de su empresa.

Kerberos: Sistema desarrollado en el Instituto Tecnológico de Massachusetts que basado en contraseñas y en el cifrado simétrico DES e implementa un sistema de tickets, autenticación de entidades y control de acceso en un ambiente cliente-servidor.

Kernel : Centro del sistema operativo de una computadora, que provee servicio a todas las otras partes de este. Sinónimo de *Núcleo*.

-M-

Malware: Proviene de una agrupación de las palabras *mal*icious soft*ware*. Este programa o archivo, que es dañino para el ordenador, está diseñado para insertar virus, gusanos, troyanos o spyware intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí.

-N-

NESSUS: Potente escáner de Seguridad libre. Consta de dos partes (cliente/servidor) que pueden estar instaladas en la misma máquina por simplicidad.

-O-

OSI: Acrónimo en inglés de *OpenSystemsInterconection* (Interconexión de Sistemas Abiertos). Descripción estándar o modelo de referencia de como se deben llevar a cabo las transmisiones de mensajes entre dos puntos en una red de telecomunicaciones. Refiere siete capas de funciones que toman lugar a cada extremo de la comunicación. A su vez estas capas se dividen en dos, las *Cuatro Capas Superiores* y las *Tres Capas Inferiores*. Las primeras actúan cuando un mensaje pasa hacia o desde un usuario, en el caso de las segundas es cuando pasan a través de una computadora o ruteador.

Ocultamiento de contraseñas: Del término en inglés *ShadowPassword*. Mecanismo que consiste en impedir que los usuarios sin privilegios puedan leer el archivo donde se almacenan las contraseñas cifradas.

Outsourcing. Es un tipo de relación contractual que permite a una organización cualquiera el uso de las instalaciones físicas de otra que, además, provee a la primera de mantenimiento y desarrollo de aplicaciones, proceso de datos, gestión de comunicaciones, etc. Así, una empresa (la segunda, según la definición anterior), aprovecha, por ejemplo, el sobrante de potencia de proceso de sus máquinas, o rentabiliza su experiencia en la gestión de sus propias aplicaciones, o comparte su estructura de comunicaciones, etc. La primera, en estas circunstancias, no necesita acometer costosísimas inversiones para resolver sus necesidades de operación.

-P-

PAP: Acrónimo en inglés de *PasswordAuthenticationProtocol* (Protocolo de Autenticación de Contraseña) Es un mecanismo de autenticación simple en donde un usuario ingresa una contraseña y esta es enviada a través de la red en texto simple.

PGP: Acrónimo en inglés de *PrettyGoodPrivacy*. Marca de Network Associates, Inc., que describe al programa de computadora y protocolos relacionados que usa criptografía para proveer seguridad en correo electrónico y otras aplicaciones de Internet.

PKI: Acrónimo en inglés *PublicKeyInfrastructure*(Infraestructura de Llave Pública)**.** Mecanismo que permite a usuarios de una red insegura intercambiar información de manera segura a

través del uso de dos llaves (Llave Pública y Llave Privada) que son obtenidas desde y distribuidas por una Entidad Certificadora. Así esta infraestructura provee soporte a servicios de certificados que pueden identificar a una entidad, por medio de una entidad que almacena y cuando es necesario revoca estos certificados.

PPP: Acrónimo en inglés de *Point-to-PointProtocol* (Protocolo Punto a Punto). Protocolo para la comunicación entre dos computadoras usando interfases seriales, i.e. una computadora personal conectada a un servidor por medio de la línea telefónica. Empaqueta los paquetes TCP/IP y los envía al servidor para su salida a Internet.

Proxy: Método que permite ocultar datos por medio de enrutamiento de las solicitudes.

-Q-

QFE: Acrónimo en inglés de *QuickFixEngineering* (Ingeniería de Corrección Rápida)**.** Equipo de desarrollo de Microsoft encargado del desarrollo de los *hotfixes*, también se les llega a llamar así a estos últimos.

-R-

Riesgo: Se le considera así al valorar el nivel de una amenaza, con el nivel de una vulnerabilidad, así se determina la posibilidad de que un ataque sea exitoso.

RAS Servidor: (Remote Access Server) Servidor de Acceso Remoto. Servidor para autenticación de usuarios, sirve para identificar usuarios y contraseñas que acceden a los recursos de red.

-S-

Seguridad: Es la necesidad de asegurar a quienes están involucrados en una organización (empleados, clientes y visitantes) que están protegidos contra cualquier daño.

Servidor: Entidad de un sistema que provee de servicios en respuesta a peticiones de otras entidades del sistema llamadas clientes.

SITE: Espacio físico acondicionado para albergar equipo informático. Contiene todas las facilidades para la conexión y preservación de equipo (aire acondicionado, piso falso, canaletas para cables, conexiones de red, racks, etc.)

SNMP: *Simple Network Management Protocol.* Protocolo para Administración Simple de Redes. Protocolo de gestión de red más importante y usado en la actualidad. Forma parte del conjunto de protocolos TCP/IP y está definido en la capa de aplicación del mismo.

SP (*ServicePack*): Es un conjunto acumulado de todos los *hotfixes* creados y las correcciones para errores encontrados internamente desde la publicación del producto. Los *Service Packs* pueden contener también un número limitado de peticiones del cliente para cambios de diseño o características. Éstos son ampliamente distribuidos y por tanto probados arduamente.

Spam: Envío indiscriminado y no solicitado de publicidad, principalmente a través de correo electrónico, aunque últimamente han aparecido nuevos tipos (mensajería instantánea, mensajes de celular, correos de voz).

Spoofing: Se produce cuando grupos de *spammers* falsifican una dirección de correo electrónica para ocultar el origen del mensaje de spam. Grupos de spammers o creadores de virus también utilizan este método. Los primeros falsifican las direcciones para hacer creer a los usuarios que el correo electrónico procede de una fuente legítima, como por ejemplo un banco online. Del mismo modo, los creadores de virus han circulado supuestas actualizaciones de seguridad pretendiendo que proceden del soporte técnico de Microsoft.

Spyware Son aplicaciones que vienen incorporadas en algunos programas. Estos programas recopilan información sobre el usuario que lo utiliza, las páginas Web que visita, la computadora que tiene, etc. de forma oculta para, posteriormente, enviarla a empresas a través de Internet.

SSH: Acrónimo en inglés de *SecureShell*. Programa para establecer conexiones cifrados entre equipos, ejecutar comandos en un equipo remoto o transferir archivos de un equipo a otro.

-T-

TCP: Acrónimo en ingles de *Transfer Control Protocol* (Protocolo de Control de Transferencia). Conjunto de protocolos que son usados junto con el protocolo de Internet para enviar datos en forma de unidades de mensaje entre computadoras. Mientras que IP se encarga del envió de los datos, TCP se encarga de vigilar cada unidad de datos (paquetes) en los que un mensaje se divide. Así IP se encarga de los paquetes y TCP establece la conexión y el intercambio de datos entre los dos equipos. TCP garantiza la entrega de los paquetes y que sean entregados en el mismo orden en que fueron enviados.

TCPWrappers: Herramienta simple para monitorear y controlar el tráfico que llega a un servidor.

Troyanos: Instrumento de distribución para código destructivo, estos programas parecen útiles e inofensivos pero en realidad son enemigos incubiertos, pueden eliminar datos y envían copias de sí mismos a listas de direcciones de correo electrónico y acceder a computadoras para realizar otros ataques.

Túnel: Del término en inglés *Tunneling*. Canal de comunicación creado en una red de computadoras encapsulando los paquetes de un protocolo en un segundo protocolo que normalmente seria llevado en una capa superior o en la misma que el original. Frecuentemente es una conexión punto a punto. Así se puede transportar información que use un protocolo que no sea soportado por la red en la que viajara.

-V-

Valoración de riesgos: Del inglés *RiskAssesment*.Es la forma en la que son determinados los riesgos a los que un sistema puede verse sujeto y el daño que causarían en este.

Virus: Sección de un programa, oculta y auto replicante usualmente malicioso, que se propaga o infecta insertando una copia de sí mismo en otro programa para convertirse en parte de él. Un virus no puede ejecutarse por si mismo, requiere que el programa que lo aloja sea ejecutado para poder realizar sus operaciones.

VPN: Siglas de *Virtual Private Network* (Red Privada Virtual) que es aquélla que mediante un proceso de encapsulación o encriptación de los procesos de datos envía los paquetes de datos a distintos puntos remotos mediante el uso de una infraestructura pública de transporte (túnel).

Vulnerabilidad: Una falla o debilidad en el diseño, implementación u operación de un sistema que puede llevar a que sea explotado para violar las políticas de seguridad por parte de un intruso.

-W-

Wardialer: Programa de cómputo que automáticamente marca una serie de números telefónicos para encontrar líneas conectadas a sistemas de cómputo y catalogarlos para que un intruso pueda intentar comprometer los sistemas

Wrapper. Programa para controlar el acceso a un segundo programa. El *Wrapper* literalmente cubre la identidad del segundo programa, obteniendo con esto un más alto nivel de seguridad.

R E F E R E N C I A S

R E F E R E N C I A S

[1] Manunta, Giovanni, (2003) *Seguridad: Una introducción. Universidad de Cranfield.* http://www.Seguridadcorporativa.org.

[2] Aldegani, Gustavo.(1997) *Seguridad Informática.*

[3] Huerta, Antonio. (2004) *Seguridad en Unix y Redes.* http://www.kriptopolis.com

[4] Ardita, Julio César.(2001) *Entrevista CYBSEC, SA*. http://www.cybsec.com

[5] http://Seguridad.internet2.ulsa.mx/congresos/2002/esime/impseg_polleg.pdf

[6] Orange Book. (1985) *Department Of Defense*. EEUU. http://www.doe.gov

[7] Howard, Jonh. (1995) *Analysis of Security on the Internet*. Carnegie Mellon University.

[8] Quittner Jeremy. (1999) *Hackers: Methods of Attack and Defense*. http://www.all.net

[9] Pérez Mercado Luis Enrique. (2001) *Seminario de Seguridad "Prevención de Ataques". Cisco Systems.*

[10] Villalón Huerta, Antonio. (2004) *"Seguridad de los Sistemas de Información"*

[11] Villalón Huerta, Antonio.(2004) *"El Sistema de Gestión de Seguridad de la Información"*

[12] Otero Javier, Ing.(2003) *Diplomado en Seguridad Informática*.

[13] Asociación de Internautas. (2003.) *http://www.seguridadenlared.org*

[15] Callio Technologies. (2004) *Presentación: ISO 17799 y Callio Segura*. http://www.callio.com.es

[16] (BS 7799 Part 1: Code of Practice). (2003) *Documentos BSI* http://www.bsi.org.uk/index.html

[17] ABASTsystems, (2005) *"Auditoría de Seguridad Basada en la Norma ISO 17799"*

[18] Franco, S. Gabriela, (2006) CAPITULO 2 "*Norma ISO 17799 para la Gestión de Seguridad de la Información"*

B I B L I O G R A F Í A

B I B L I O G R A F I A

- **Aldegani, Gustavo Miguel,** *Seguridad en Informática*
  MP Ediciones, Argentina, 1997

- **Cebrian Ruz, Antonio,** *Guía Práctica de Comunicaciones y Redes Locales*
  Colección de Informática, Ed. Gustavo Pili

- **Cooper, Frederic,** *Implementing Internet Security*
  New Riders Publishing, E.E.U.U., 1995, 1ª. Edición.

- **Howard, John,** *Analisis of Security on the Internet*
  Carnegie, Mellon University, 1995

- **Lucena, Manuel J.** *Criptografía y Seguridad en Computadoras*
  4ª. Edición V 0.62

- **Morant, Ramón J.L., Ribagorda Garnacho A.,** *Seguridad y Protección de la Información*
  Barcelona, España, 1994.

- **Pérez Mercado, Luís Enrique,** *Seminario de Seguridad "Prevención de Ataques"*
  Cisco Systems, 2001

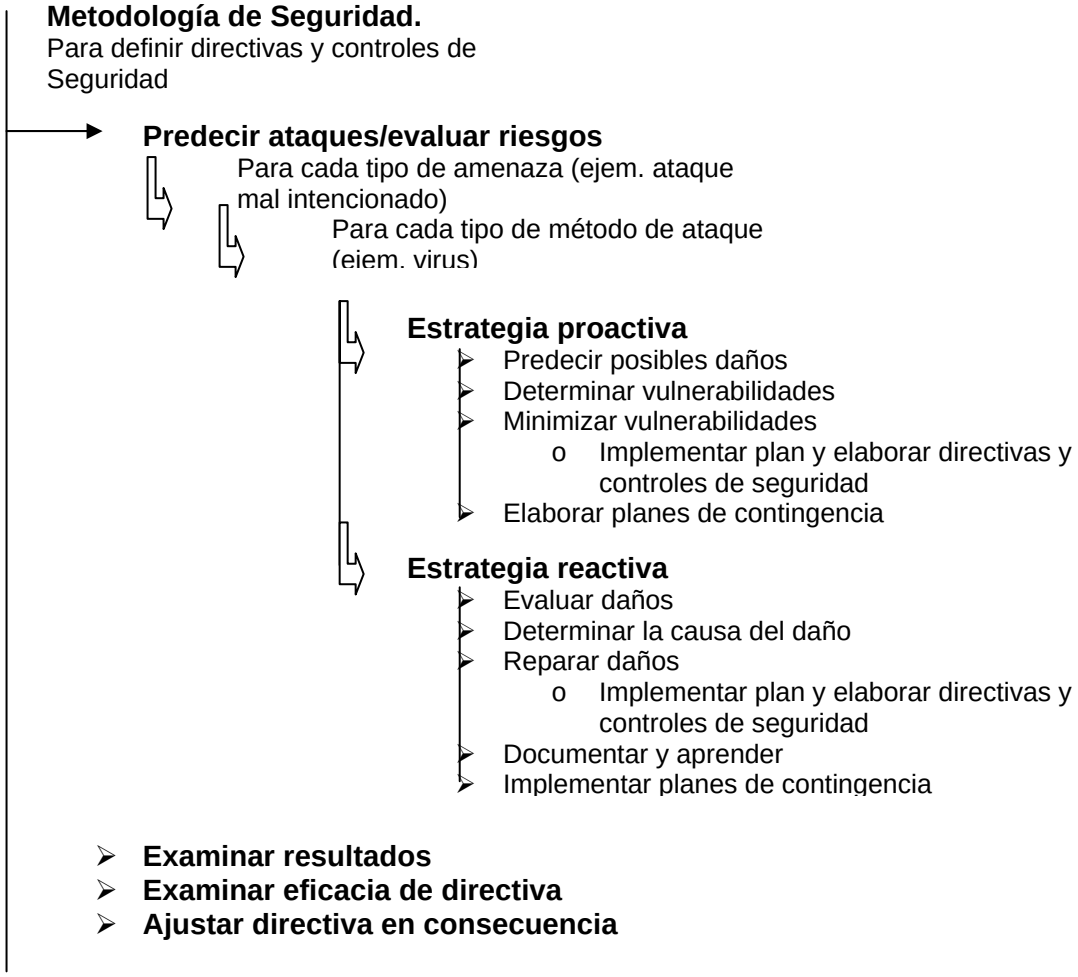
- **Ramió Aguirre, Jorge,** *Libro Electrónico de Seguridad en Informática*
  Barcelona, España, 2005

- **Stalling, William,** *Cryptogtaphy and Network Security, Principles and Practices*
  Prentice Hall, Third Edition, 2003

- **Tanenbaum, Andrew S.** *Redes de Computadoras*
  Editorial Prentice Hall, México, 1997 3ª. Edición

ANEXO A
Aplicación de Metodología para la solución de problemas comunes mediante estrategias de seguridad.

En esta sección se muestra una metodología para definir estrategias de seguridad informática, que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los métodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales y, por consiguiente, se puedan volver a utilizar en distintos casos de ataque. La metodología se basa en los distintos tipos de amenazas, métodos de ataque y puntos vulnerables. El siguiente diagrama de flujo describe la metodología.



Ejemplo 1: Amenaza no intencionada.

Un empleado, Juan Domingo, no desea perder la información que ha guardado en el disco duro. Desea hacer una copia de seguridad de esta información, así que la copia a su carpeta particular del servidor que resulta ser también l servidor principal de aplicaciones de la organización. No se ha definido cuotas de disco para las carpetas particulares de los usuarios que hay en el servidor. El disco duro de Juan tiene 6,4 GB de información y el servidor tiene 6,5 GB de espacio libre. El servidor de aplicaciones deja de responder a las actualizaciones y peticiones porque se ha quedado sin espacio en el disco. El resultado es que se deniega a los usuarios los servicios del servidor de aplicaciones y la productividad se interrumpe. A continuación, se explica la metodología que se debería haber adoptado antes de que Juan decidiera hacer una copia de seguridad de su disco duro en su carpeta particular.

Metodología de Seguridad.
Para definir directivas y controles de Seguridad

→ **Predecir ataques/evaluar riesgos**
Denegación de Servicios cuando el usuario abusa de los recursos.

⇩ **Para cada tipo de amenaza.**
Empleado sin malas intenciones. Juan Domingo.

⇩ **Para cada tipo de método de ataque.**
Juan no tenía ningún motivo ni objetivo para interrumpir los servicios, por lo que no se utilizó ningún método ni herramienta

Estrategia proactiva

- Predecir posibles daños
  - *Si no hay espacio en disco duro, se puede perder productividad.*
- Determinar vulnerabilidades
  - *Sin cuotas de disco, sin entrenamiento del personal.*
- Minimizar vulnerabilidades
  - *Implementar cuotas de disco y elaborar un entrenamiento sobre la seguridad.*
- Elaborar planes de contingencia
  - *Tener posiblemente un servidor en espera.*

Estrategia reactiva

- Evaluar daños
  - *Pérdida de producción*
- Determinar la causa del daño
  - *El servidor se quedó sin espacio en díscola copiar el usuario su carpeta particular.*
- Reparar daños
  - *Eliminar información de la carpeta particular del usuario.*
- Documentar y aprender
- Implementar planes de contingencia
  - *Implementar un servidor en espera hasta que vuelva a estar operativo el servidor de producción.*

- **Examinar resultados** *Pérdida de producción*
- **Examinar eficacia de directiva** *De recursos y entrenamiento del personal.*
- **Aiustar directiva en consecuencia**

Ejemplo 2. Amenaza mal intencionada (agresor externo)

Cristina Martínez es aficionada a crear virus y entrar ilegalmente en sistemas. Cristina crea un virus nuevo que altera los sistemas de correo electrónico de todo el mundo.

Metodología de Seguridad.
Para definir directivas y controles de Seguridad

Predecir ataques/evaluar riesgos
Si se deniegan los servicios al utilizar correo electrónico para comercio electrónico y otras funciones empresariales, y el servidor de correo no funciona

Para cada tipo de amenaza
Atacante mal intencionado Juan Domingo.

Para cada tipo de método de ataque
Virus de correo electrónico

Estrategia proactiva

- Predecir posibles daños
  Si se detiene el correo electrónico, también se detiene la productividad
- Determinar vulnerabilidades
  No hay búsqueda o firma de virus en la base de datos actual del explorador antivirus.
- Minimizar vulnerabilidades
  - *Implementar la exploración antivirus o actualizar la BD de firma de virus poniéndose en contacto con el proveedor.*
- Elaborar planes de contingencia
  Teniendo posiblemente un servidor en espera.

Estrategia reactiva

- Evaluar daños. *Pérdida de producción.*
- Determinar la causa del daño
  El servidor de correo tuvo un error debido a un virus.
- Reparar daños
  - *Implementar un servidor en espera hasta que vuelva a estar operativo el servidor.*
- Documentar y aprender
- Implementar planes de contingencia
  Implementar un servidor en espera

- **Examinar resultados**
- **Examinar eficacia de directiva**
- **Ajustar directiva en consecuencia**

Examinar la directiva de detección y la exploración de virus

Ejemplo 3. Amenaza mal intencionada (agresor externo)

Un empleado, Enrique Barreda, trabaja para una empresa que se diseña naves espaciales. Una organización competidora se pone en contacto con Enrique para ofrecerle una gran suma de dinero por robar información del diseño de la organización más reciente. Enrique no tiene los derechos necesarios para tener acceso a la información. En una conversación telefónica con un empleado que tiene derechos de acceso, simula que es uno de los administradores. Enrique dice al empleado que está realizando un trabajo administrativo habitual le solicita su nombre de usuario y contraseña para comprobarlos con los registros del servidor. El empleado accede a dar a Enrique dicha información.

Metodología de Seguridad.
Para definir directivas y controles de Seguridad

→ **Predecir ataques/evaluar riesgos**
Información que se puede robar mediante ingeniería social

Para cada tipo de amenaza
Empleado atacante malintencionado. Enrique Barrera.

Para cada tipo de método de ataque
Ingeniería Social

Estrategia proactiva

- Predecir posibles daños
  Si se roba información confidencial hay pérdida de beneficios.
- Determinar vulnerabilidades
  Concienciación por la seguridad entre los empleados
- Minimizar vulnerabilidades
  - *Implementar entrenamiento sobre concienciación por la seguridad.*
- Elaborar planes de contingencia

Estrategia reactiva

- Evaluar daños.
  Pérdida de beneficios e información confidencial
- Determinar la causa del daño
  El empleado reveló un nombre de usuario y una contraseña.
- Reparar daños
  - *Implementar entrenamiento sobre concienciación por la seguridad y ponerse en contacto con las autoridades correspondientes.*
- Documentar y aprender
- Planes de contingencia

- **Examinar resultados**
  La información confidencial se puede robar por la existencia de poca concienciación por la seguridad, lo que producirá pérdida de ingresos.
- **Examinar eficacia de directiva**
  Examinar la directiva de entrenamiento sobre concienciación por la seguridad
- **Ajustar directiva en consecuencia**

Ejemplo 4. Amenaza no intencionada (desastre natural)

La organización XYZ, no tiene sistemas de detección y protección contra incendios en la sala de servidores. Un administrador de los sistemas de la organización deja un par de manuales del aparato de aire acondicionado. Durante la noche el acondicionador de aire se calienta y comienza un incendio que arrasa la sala de servidores y un para de despachos.

Metodología de Seguridad.
Para definir directivas y controles de Seguridad

Predecir ataques/evaluar riesgos
Incendio

Para cada tipo de amenaza
Desastre natural: incendio

Para cada tipo de método de ataque
Ningún método

Estrategia proactiva

- Predecir posibles daños
  Los incendios pueden causar pérdida de información.
- Determinar vulnerabilidades
  No hay protección o detección contra incendios instalada, o los sistemas de detección de incendio no funcionan correctamente.
- Minimizar vulnerabilidades
  - *Implementar directivas parta la detección y prevención de incendios y/o mantto .periódico de los sistemas de protección contra incendios.*
- Elaborar planes de contingencia
  Asegurarse de que se realizan periódicamente copias de seguridad y se almacenan fuera de las instalaciones. Si es posible, tener HW de repuesto.

Estrategia reactiva

- Evaluar daños
  Pérdida de información, HW y productividad.
- Determinar la causa del daño
  Incendio causado por el bloqueo del aparato de Aire Acondicionado.
- Reparar daños
  - *Volver a construir los servidores y restaurar las copias de seguridad mas recientes*
- Documentar y aprender
- Implementar planes de contingencia

- **Examinar resultados** — ***Los incendios pueden tener efectos desastrosos sobre los sistemas informáticos***
- **Examinar eficacia de directiva** — ***Examinar o implementar directivas de detección de incendios.***
- **Ajustar directiva en consecuencia**