UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD PARA REDES DE COMPUTADORAS LOCALES"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

ALEJANDRA BARTOLO GERVACIO

DIRECTOR DE TESIS:

ING. CRUZ SERGIO AGUILAR DÍAZ

Ciudad Universitaria 2007

A MIS PADRES

Le doy gracias a Dios por haberme dado unos padres que han estado conmigo desde el comienzo de mi vida, por sus cuidados, su amor incondicional y todo su apoyo a lo largo de este sueño.

Gracias por todos aquellos consejos y momentos en los cuales me veían desvanecer y aun así me animaron a seguir luchando en esta vida a pesar de las adversidades que encontraba en mi camino, les agradezco la educación que me impartieron a lo largo de mi vida ya que gracias a ello he logrado llegar hasta donde me propuse llegar.

No puedo estar más orgullosa de ustedes de lo que estoy en estos momentos de mi vida ya que gracias a su ejemplo de lucha incansable y trabajo me han enseñado que en esta vida hay que trabajar arduamente para conseguir lo que soñamos.

No me alcanzaría la vida para poder regresar un poco de todo lo que han hecho por esta hija suya, pero si se que estaré ahí junto a mis padres que han sido el pilar más grande de mi vida, espero estén orgullosos de mi y en este día de jubilo que es suyo también este presente hasta el ultimo día de nuestras vidas.

Con cariño, admiración y respeto

A MI MADRE

Eres la mujer mas excepcional que he conocido no podría describirte con palabras lo afortunada que he sido al tener una madre como tu, sin ti no hubiera podido llegar tan lejos me impulsaste y apoyaste en todos estos largos años de mi vida

Eres una mujer admirable por tu entrega, amor y comprensión conmigo, una mujer luchadora e incansable, tu ejemplo me ha dado las fuerzas para seguir adelante para no flaquear ante la adversidad.

Gracias Mamá por estar ahí siempre a mí lado, a pesar del arduo trabajo siempre has visto por tu familia dedicando tu amor y cuidados a nosotros, eres sin duda la mejor de las madres.

Eres el pilar más grande en mi vida deseo que estés orgullosa de mí y que esté triunfo también lo tomes como tuyo, porque sin ti no estaría aquí.

Te admiro y respeto mucho espero algún día llegar a ser como tu la mujer que ante todo se sacrifica cada día por mi y por mí hermana. Yo se que hay veces en que no te digo cuanto te quiero o lo mucho que te admiro, pero no te quede duda de todo esto que hoy lo puedo plasmar en unas cuantas líneas.

Con todo mi amor, respeto y admiración a la madre y a la mujer que es lo mas maravilloso del mundo.

A MI HERMANA

Guadalupe

Gracias mi pequeña hermana por estar ahí a mi lado en los buenos y malos momentos de mi vida, sabes te quiero mucho, Dios me dio una maravillosa hermana en la que puedo confiar, reír y llorar, se que te dará tanto gusto como a mí este triunfo, por lo cual doy gracias que estés a mi lado en este día.

A pesar de ser mi pequeña hermana siempre te he tenido una gran admiración y respeto, hemos pasado por muchos problemas pero hemos salido adelante gracias al amor incondicionable de nuestros padres, el día en que decidiste afrontar tu enfermedad y curarte a pesar de ser aun una niña me hizo darme cuenta de lo fuerte y valiente que eres, sabes que no podría verte sufrir y aun así tuvimos que hacerlo pero sabíamos que era por tu bien, además que así lo habías decidido. Y mírate ahora sigues adelante.

Espero ser para ti un buena hermana en todos los sentidos que siempre estaré ahí para ti, aunque se que habrá veces en que tendrás que afrontar tus propios problemas y miedos, aun así, siempre estaremos unidas.

Con esto quiero que tengas muy presente que todo lo que yo viví entre cansancio, desilusión, esfuerzo y sacrificios se plasma en la realización de una meta que me propuse, y te quede como enseñanza que se pueden lograr las metas si trabajas en ellas, se que algún día no muy lejano comprenderás estas palabras.

Con todo cariño y respeto tú hermana Alejandra

A MI NOVIO

Jose Luis

En alguna ocasión escuche decir que las personas como las cosas importantes de la vida no llegan antes ni después todo tiene un tiempo, y creo que en estos momentos de mi vida en el que haz llegado tu ha sido el momento preciso, para poder compartir a tu lado triunfos, derrotas, días buenos y días malos.

Gracias amor por todo el apoyo que me has brindado, por estar ahí, por tus cuidados y por compartir este momento.

Sabes te haz convertido en una persona muy importante en mi vida, espero q en este punto de nuestra vida en el cual hemos decidido estar juntos, tengamos la dicha de compartir muchos instantes.

Al hombre que ha llegado a llenar mi vida con su cariño y apoyo.

A MIS AMIGOS

IVETT

Amiguita hemos compartido estos años desde que iniciamos la carrera haz sido una de mis mas grandes amistades tu sabes bien que eres mi mejor amiga, recuerdo mucho el momento en que nos hablamos por primera vez y míranos ahora hemos fortalecido nuestra amistad a lo largo de estos años, no cabe duda de todo lo que hemos vivido juntas, hay veces en que talvez las situaciones sean difíciles pero estamos la una para la otra.

Gracias amiguita por estar cerca de mi, porque cuando me desilusionaba me dabas los ánimos necesarios para seguir y no abandonar mi meta te aprecio mucho no lo olvides, al igual que yo en este día yo se que te veré pronto lograr la misma meta esperando, me dejes compartir el jubilo de la ocasión. No olvides también que te admiro mucho por esa gran fortaleza y dedicación a no dejar las cosas por difíciles que sean sigue así porque se que vas a lograr muchos triunfos no desesperes.

VICTOR

Gracias por estos años en que nuestra amistad ha crecido incondicionalmente, no sabes cuanto te admiro eres un gran hombre y ser humano, nuestra amistad ha pasado por muchas situaciones se ha fortalecido a lo largo de los años, te agradezco el apoyo que me haz dado me diste tu mano y los ánimos necesarios para poder finalizar este proyecto.

Compartimos triunfos y derrotas pero estamos ahí siempre para apoyarnos en lo que ha surgido, solo quiero reiterarte mi amistad y aprecio hacia ti, el que estés aquí en estos momentos compartiendo esta meta para mi es muy importante, no hace mucho el verte lograr el mismo sueño compartiéndolo conmigo me lleno de mucho jubilo.

KAREN Y CLAUDIA

Amigas a pesar de que no estamos juntas se que este momento lo compartirán conmigo y les dará mucha alegría, nos conocemos ya hace muchos años que ahora ya hemos emprendido nuevos caminos pero seguimos apoyándonos a pesar de la distancia.

SAID, OMAR Y ALEJANDRO

Gracias por compartir este camino a mi lado, por todos aquellos momentos en los cuales reímos, lloramos y recordamos los momentos de la carrera, los aprecio mucho han estado ahí conmigo apoyándome e impulsándome a seguir mi camino y concluir mi sueño.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Un especial agradecimiento a mi universidad que me abrió las puertas del conocimiento, así como, me acogió brindándome la oportunidad que muy pocos tienen el de pertenecer a tí, para forjarme en tus aulas, siendo una de las bases de mi educación en la obtención de conocimientos para mi vida profesional.

Ser parte de ella en estos años me ha dado muchas satisfacciones, me ha dado los amigos y compañeros con los cuales emprendí este sueño, gracias mi querida Universidad por todo lo que haz brindado.

FACULTAD DE INGENIERÍA

Tus aulas, maestros y personas que forman parte de ti han sido parte fundamental de mi crecimiento como estudiante y persona, me abriste tus puertas hacia el conocimiento, estos años me has brindado todos los recursos necesarios para terminar este sueño que empecé algún día jamás haz dejado que el conocimiento en tus aulas se extinga, es más siempre has estado al pendiente de darle más ha tus estudiantes, gracias mi querida Facultad por todos estos años en los que me acogiste con gran cariño y dedicación para formar a un profesionista.

Jamás olvidare tus aulas, maestros, pasillos y personas en las cuales reí, conocí, recorrí, obtuve y realicé mis estudios.

UNICA

Unidad de Servicios de Cómputo Académico un agradecimiento en especial por brindarme la oportunidad de pertenecer a ella, gracias a mis compañeros y jefes que han sido parte fundamental de mi crecimiento profesional, me han dado la oportunidad de adquirir y desarrollar conocimientos sólidos.

Reitero un agradecimiento en especial al Jefe de UNICA el **Ing. Enrique Barranco Vite** quien ha sido una persona que se merece todo mi respeto y admiración por procurar a la gente que colaborar con el y la unidad, agradeciendo la oportunidad de formar parte de esta gran familia.

MARIAN

Ha sido un honor trabajar con una persona como tu, se que no tenemos mucho tiempo de conocernos pero en este tiempo le he tomado un aprecio a la mujer, a la profesionista y al ser humano tan maravilloso que eres, muchas gracias por tus consejos, compañerismo y apoyo.

ING. FRANCISCO JAVIER MONTOYA CERVANTES

Javier

El hombre, el amigo y el jefe son todas estas facetas las cuales he podido compartir a tu lado. Gracias por tu apoyo, comprensión, consejos y tu amistad eres un hombre maravilloso, con todo respeto y admiración hacia una de las personas que me han enseñado el valor del compañerismo, ha sido un privilegio el haber trabajado a tu lado, el que fueras mi jefe, de ti he obtenido muchos conocimientos.

El compartir esta faceta de mi vida en la cual me has apoyado y brindado una mano cuando más lo he necesitado, te tengo un gran cariño y respeto, son tantas palabras que quisiera decirte pero creo que no encuentro englobarlas todas pero sin duda espero estés orgulloso de mi en este día.

Eres un ser humano excepcional gracias por todo.

ESPERANZA

Espe

Agradecerte estos años en los que me haz brindado tu valiosa amistad y cariño aunque se que a veces te portas muy dura, en el fondo al igual que yo nos tenemos un cariño mutuo, gracias por tus consejos, por escucharme y aguantarme en esos ratos en los cuales a veces ni yo misma me comprendo.

Tu valiosa experiencia te hace una mujer muy valiosa no lo olvides, han sido unos años muy gratos Espe me la he pasado muy bien compartiendo muchas experiencias contigo, espero que tu opines lo mismo, el compartir este día tan especial contigo después de todo este esfuerzo.

ING. MARIA DEL ROSARIO PAZ BARRAGAN

Chary

Muchas gracias por dejarme conocer al ser humano ante todo, te agradezco mucho tu compañía, además de todos aquellos momentos de consejos y alegrías, de igual manera la oportunidad de trabajar a lado de una gran profesionista.

ING. BEATRIZ BARRERA HERNANDEZ

Bety

Muchas gracias por permitirme trabajar al lado de una gran mujer y profesionista ante todo de un ser humano.

Gracias por todos tus consejos y por poner tu confianza en mi, espero que en este tiempo en el cual he colaborado a tu lado haya reiterado dicha confianza.

Te he tomado mucho aprecio en este poco tiempo en que he conocido estas facetas tuya, gracias por los consejos que me haz dado, por alentarme acabar esta tesis y por todo el apoyo que he recibido de ti incondicionalmente.

Espero te sientas orgullosa de mi, siendo este día tan importante me llena de una gran alegría el poder compartirlo contigo.

Con cariño y respeto

ING. CRUZ SERGIO AGUILAR DÍAZ

Sergio

Has sido una de las personas más importantes en mi vida, el hombre, el amigo, el maestro, el padre, el profesionista en todas estas facetas he tenido la fortuna de haber compartido a tu lado, eres sin duda un ser humano maravilloso en toda la extensión de la palabra no pude haber tenido mayor suerte que haberte conocido a ti en estos momentos de mi vida.

Recuerdo el día en que emprendimos este sueño juntos yo como tu tesista y tu como mi director de tesis, a pesar de que había veces en que me desilusionaba o quería dejarlo todo me alentaste a seguir adelante, se que me ha costado mucho trabajo llegar hasta aquí pero detrás de todo este esfuerzo has estado tu apoyándome en todo momento.

Creo que no podría encontrar la manera de agradecerte tanto apoyo porque has estado en los momentos más difíciles de mi vida me has escuchado sin juzgarme, tus consejos han sido sin duda muy valiosos para mi, ha sido un privilegio el haber trabajado a tu lado sin duda eres un buen jefe pero ante todo un gran ser humano.

Tengo tantas cosas que decirte que la verdad no he encontrado una sola palabra para englobar todo, deseo que en un futuro sigamos siendo amigos como hasta ahora, que en este día me da mucho gusto el poder compartirlo contigo.

Con cariño, agradecimiento, respeto y admiración

EN MEMORIA DE

Recuerdo todos aquellos momentos en los que solíamos pensar en un futuro, emprendimos juntos un sueño, una meta y muchas otras cosas más, ojala pudiera regresar el tiempo atrás pero desgraciadamente no puede ser así.

Me gustaría que supieras todo lo que significas aun para mí, gracias por haber estado a mi lado, por haber compartido este pequeño lapso de vida en la que soñamos juntos, mi amigo, mi confidente y mucho mas que eso fuiste en mi vida.

Han sido años largos y difíciles en los que tuve que aprender muchas cosas ojala hubieras estado aquí para poder verme crecer como persona, pero se que donde quiera que estés lo estarás haciendo.

Déjame decirte que eras una persona admirable y maravillosa en todos los sentidos tu madre no pudría haber estado mas orgullosa de ti, tu empeño y dedicación a todo lo que hacías me hacia ver la vida de una manera diferente. Nunca olvidaré todos los momentos que pasamos juntos, en que reímos, lloramos, compartimos triunfos y derrotas.

Quiero que sepas que esta tesis es tanto tuya como mía espero que donde quiera que estés te sientas orgulloso de esto por que al final aunque ya no este aquí esta meta es nuestra

Señora Bernardina y Armando este es mi agradecimiento ha ustedes por haberme aceptado en sus vidas, los respeto y quiero mucho, se que con estas palabras no puedo regresarles a su hijo, si pudiera y estuviera en mis manos créanme lo haría, no se, si hice todo lo que podía hacer para hacer feliz a su hijo, pero en lo que cabe créanme que lo quise mucho.

Con cariño y respeto al hombre que compartió parte de mi vida

Descanse en Paz
Eligio Almazán González

Índice: **Página**

“Si te conoces a ti mismo y conoces a tu enemigo,
entonces no deberás temer el resultado de mil batallas”

Sun-Tzu

INTRODUCCIÓN

La seguridad hoy en día a cobrado una mayor fuerza, además de un avance significativo, las tecnologías de seguridad se han vuelto más robustas y menos complicadas que al principio cuando se hablaba de obtener seguridad, pero sin lugar a duda se puede tener una seguridad que sea integral con base a un buen análisis.

Pero cabe mencionar que como se sabe la seguridad es relativa y dinámica, por lo cual se puede decir que es todo un proceso continuo en donde lo que ahora es seguro mañana seguramente ya no lo será, no se puede confiar absolutamente en que lo implementado nos dará por siempre la seguridad por que en ese preciso momento no ha pasado nada, o seguramente no pasará nada esta es una falsa utopía de que no se requiere revisar continuamente los lineamientos de seguridad. Sin una estrategia integral y sin ser aislada, no se tendrá una visión de lo que realmente se requiere, la seguridad no se arregla si sólo se le invierte en tecnología ya que el factor humano es la base para resolver y solventar la seguridad en donde se requiera ser implementada.

La labor principal en **seguridad informática** es el aislamiento de los actos no deseables, y la prevención de aquellos que no se hayan considerado, de forma que si se producen hagan el menor daño posible. A su vez la **seguridad en sistemas de redes de computadoras** es la protección de la integridad, disponibilidad, y si es necesaria la confidencialidad de la información, así como los recursos que se emplean, para la entrada, almacenamiento, procesamiento y comunicación de los mismos. En la actualidad, la seguridad informática ha adquirido un gran auge, dadas las cambiantes condiciones y las nuevas plataformas disponibles. La posibilidad de interconectarse a través de las redes, ha abierto nuevos horizontes pero por otra parte se ha producido la aparición de nuevas amenazas para los sistemas informáticos. Lograr comprender la seguridad informática en toda su magnitud, desde aspectos como su objetividad, servicios, amenazas, hasta sus mecanismos, requiere de un profundo y detallado estudio.

La seguridad revelará el índice en que un sistema informático está libre de todo peligro daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas imposible) en un 100% por lo que sólo se habla de **fiabilidad** y se la define como “la probabilidad de que un sistema se comporte tal y como se espera de él” y, por lo general, se habla de sistema fiable en vez de sistema seguro.

Para hacer efectivo que un sistema sea fiable se deberá conocer y tomar en cuenta aspectos tales como: *¿Qué se quiere garantizar?, ¿Qué se quiere proteger?, ¿De Qué o De Quién se va a proteger? y ¿Cómo se va a proteger?*. La resolución, comprensión y el debido análisis de estos puntos con llevará al estudio de los riesgos, vulnerabilidades, amenazas y contramedidas; evaluar las ventajas o desventajas de la situación; y decidir medidas técnicas, así como tácticas metodológicas, físicas e informáticas, en base a las necesidades de seguridad. Como se puede observar, asegurar un sistema informático es una tarea difícil que requiere además de mucha capacitación, que sea de forma continua y siempre a la vanguardia de los más recientes avances tecnológicos.

El tener buenas bases de manera teórica nos permitirá tener los conocimientos necesarios para llevar acabo un análisis. Los fundamentos sobre redes de computadoras serán una parte de la base para tener presente todos aquellos conocimientos adquiridos previamente, obteniendo

conceptos básicos, requerimientos de una red, modelos de la misma, medios físicos, arquitecturas, estándares y protocolos que serán el punto de partida para poder entender los siguientes temas.

Adentrarse en la definición de la seguridad, obteniendo así varias definiciones de este concepto haciendo una introducción de cómo ha cambiado la seguridad en el tiempo, proporciona fundamentos básicos de seguridad por lo cual el definir de manera adecuada este concepto llevara a saber que es lo que se requiere implementar, además de saber los servicios de seguridad, criterios, modelos y estándares establecidos que deben de ser proporcionadas para poder definir de manera concreta cuales serán considerados en este punto, al hacer una énfasis referente a agujeros de seguridad existentes, escalas de vulnerabilidad, ataques a la seguridad y amenazas que son elementos básicos para poder entender el entorno de la seguridad.

Definir los tipos de seguridad existentes física, lógica y en redes, lo que cada una con lleva para obtener dicha seguridad, las herramientas de seguridad, sistemas de protección y reglas que permitirán tener la seguridad en todos estos entornos, el establecimiento de la definición de política de seguridad haciendo un énfasis en los elementos, parámetros y requerimientos para poder establecer una política

El software es un elemento fundamental, proporcionando una definición detallada de lo que es el software, su comportamiento, clasificación y función. Con el fin de tener una base teórica fundamentada en conceptos que permitirán llevar lo documentado a un problema real, por lo cual al realizar un análisis se tomarán en cuenta derivaciones de la misma para tener un mejor control del análisis global, definiendo claramente cual es el objetivo primordial de la organización nos llevará a realizar un análisis valuativo de todos los activos considerados. Tanto los análisis de hardware, software y de la red física en conjunto con herramientas que se utilizarán para realizar dichos análisis; arrojando la información suficiente para llevar acabo una definición más exacta de las vulnerabilidades que se presenten y de está manera obtener una arquitectura que permitieran especificar punto por punto que pasos deberán ser tomados.

Los problemas de seguridad han ido creciendo en los últimos 12 meses de forma alarmante, afectando también a las universidades tanto públicas como privadas del país. El 90% de empresas reportan un incremento de problemas de seguridad en sus equipos de cómputo, se reportan alrededor de un 80% de perdidas de origen monetario por dichos problemas de seguridad.

La complejidad de las redes ha ido en aumento debido a las cada vez más crecientes amenazas en la seguridad; pero también porque al tradicional equipo de switcheo y ruteo se le han agregado dispositivos para la seguridad. En este aspecto hay mucho por hacer, entre los usuarios para inculcarles el valor de estar comunicados con seguridad, y a las empresas habrá que explicarles lo fundamental que es mantener su información en un buen resguardo de amenazas. El diseño de una red de área local parte de requisitos mínimos de topología, dimensionamiento del número de usuarios, enlaces y ancho de banda necesario para los servicios que deben soportar. En la actualidad, estos requisitos no bastan. Se deben diseñar redes más fiables, estables, disponibles, seguras, escalables, y a la vez sencillas de operar y mantener.

La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. “Hackers”, “crakers”, entre otros, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes. Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención, vigilancia continua y sistemática por parte de los responsables de la red.

Como se ha visto hasta este momento el mundo actual ha tomado nuevas herramientas para la seguridad en las redes de computadoras, pero aun están en constante amenaza debido a que no existe realmente una cultura de seguridad, es por ello que no debemos tapar aquellos huecos con simples reglas que nos llevaran a que el costo de nuestra seguridad sobrepase lo esperado, la complejidad hoy en día de instalar nuevas redes traen como consecuencia la implementación de nuevos recursos de seguridad cuidando lo que es valioso para nosotros, pero sin dejar que la seguridad nos lleve a los casos extremos en donde sobrepase los objetivos principales. La historia nos ha enseñado con hechos como es que hoy en día la práctica de una buena seguridad hace que los riesgos y las amenazas disminuyan pero no están exentos a nuevas amenazas debido a que la Internet crece a pasos agigantados absorbiendo nuevas tecnologías de la información. Lo que nos conlleva a un solo punto que se ha remarcado la seguridad.

Objetivos Generales

Implementar una metodología para aplicar herramientas y políticas de seguridad con el propósito de fortalecer los servicios de cómputo que se proporcionan a los alumnos de la Facultad de Ingeniería; automatizando las actualizaciones de antivirus y parches para el Sistema Operativo, monitoreo de los equipos, así como de los servidores críticos e implementar un servidor de protección, estableciendo reglas de normatividad para la adecuada y eficiente utilización de los equipo.

Objetivos Particulares

- Proporcionar medidas de seguridad en un centro de cómputo que ofrece los servicios de una red local, así como servicios de Internet.
- Obtener una mejoría considerable en la seguridad del equipo de cómputo protegiendo las vulnerabilidades más importantes.
- El manejo y administración adecuada de las Salas de Cómputo.
- Emplear herramientas, técnicas, metodologías y políticas de seguridad con el fin de resolver la problemática de seguridad que se presenta en toda Sala de Cómputo.
- Establecer una arquitectura de seguridad que pueda ser general.
- Llevar acabo lo concientización y entrenamiento adecuado al personal de UNICA.

CAPÍTULO 1

PANORAMA GENERAL

1.1 Antecedentes Históricos

Hasta finales de 1988 muy poca gente tomaba en serio el tema de la seguridad en redes de computadoras de propósito general. Mientras que por una parte Internet seguía creciendo exponencialmente con redes importantes que se adherían a ella, como bitnet o hepnet, por otra parte el auge de la informática de consumo (hasta la década de los ochenta muy poca gente se podía permitir una computadora personal y un módem en casa) unido a factores menos técnicos.

Sin embargo, el 22 de noviembre de 1988 Robert T. Morris protagonizo el primer gran incidente de la seguridad informática: uno de sus programas se convirtió en el famoso worm o gusano de Internet.

Miles de computadoras conectadas a la red se vieron inutilizados durante días, y las pérdidas se estimaban en millones de dólares. Desde ese momento el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos. Poco después de este incidente, y a la vista de los potenciales peligros que podía entrañar un fallo o un ataque a los sistemas informáticos estadounidenses (en general, a los sistemas de cualquier país) la agencia DARPA (Defense Advanced Research Projects Agency) creo el CERT (Computer Emergency Response Team), un grupo formado en su mayor parte por voluntarios calificados de la comunidad informática, cuyo objetivo principal es facilitar una respuesta rápida a los problemas de seguridad que afecten a hosts de Internet .

Han pasado más de diez años desde la creación del primer CERT, y cada día se hace patente la preocupación por los temas relativos a la seguridad en la red y sus equipos, también se hace patente la necesidad de esta seguridad. Los piratas de antaño casi han desaparecido, dando paso a nuevas generaciones de intrusos que forman grupos. La seguridad de las redes de computadoras se ven continuamente afectadas, debido a la frecuente aparición de nuevos ataques, brechas de seguridad y la falta de cultura de los usuarios. Este último factor resulta determinante, debido a que por contar con los más actuales y eficaces mecanismos de protección no es sinónimo de tener una red segura sino existen especialistas capacitados y usuarios debidamente preparados.

Las redes de computadoras se han convertido en el soporte de cualquier entidad o institución que pueda considerarse de punta. Estás, además de la tecnología que involucran, brindan múltiples servicios con calidad, los cuales conllevan a más y mejores prestaciones, obteniéndose beneficios para la producción y el desarrollo. Estos servicios brindan información sensible y de vital importancia para la institución y/o empresa, generando diversas acciones relacionadas con la toma de decisiones, políticas de administración, informes económicos entre otros, siendo esta susceptible a cualquier variación, modificación o pérdida.

Gracias al rápido desarrollo de las telecomunicaciones, el mundo está avanzando hacia una única y gran comunidad global. Bajo este nuevo concepto de comunidad global podemos encontrar refugiadas nuevas interpretaciones o conceptualizaciones de procesos tradicionales, como la educación, trabajo y economía. El Internet es uno de los máximos protagonistas de esta revolución tecnológica digital, debido a su rápida aceptación y propagación, en donde las redes

de computadoras se han extendido a niveles jamás antes pensados, trayendo con ello desarrollo como también algunos serios problemas, como los fraudes informáticos y las brechas de seguridad, entre otros.

Es debido a esto que, existe una demanda constante y muy importante de seguridad informática que está esperando a que alguien la atienda. Aún así esta demanda está muy por debajo en relación a la cantidad de ataques y desastres en la seguridad informática que padecen los sistemas informáticos y las redes de computadoras.

Ambas situaciones están sujetas a la necesidad de educación tanto para los usuarios como para aquellos especialistas que entre sus propósitos de trabajo está mantener y hacer funcionar correctamente una red de computadoras así como sus servicios.

1.2 Seguridad en Cómputo

En la actualidad, la seguridad informática ha adquirido un gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Seguridad en cómputo y en redes son temas de discusión hoy en día en las coorporaciones que utilizan estas herramientas para la transmisión de información. Algunas veces los equipos de administración de las empresas, así como de las instituciones no están al tanto de los avances e innovaciones de la Internet y la tecnología que conlleva. Sin este conocimiento las empresas e instituciones no pueden tomar ventaja completa de los beneficios y capacidades de una red.

La seguridad en cada empresa e institución tiene diferentes requerimientos, características, culturas y una infraestructura tecnológica distinta. En las múltiples organizaciones se tienen diferentes necesidades para almacenar, enviar y comunicar información de manera electrónica. De la misma manera en la que un negocio está envuelto en un mercado cambiante, las políticas de seguridad cambian día con día de manera que emerge una nueva tecnología.

La creciente globalización de la economía en el mundo ha incrementado la necesidad en las organizaciones de poder abrir sus puertas al entorno que las rodea, disponer de la información íntegra y confiable en el momento adecuado. Debido al incremento en la complejidad de las operaciones de las organizaciones y a la disminución en los tiempos de respuesta requeridos, la única forma de disponer del recurso de la información es teniendo sistemas de información confiables que permitan a las organizaciones e instituciones estar a la vanguardia tecnológica y responder oportunamente a las exigencias de un mercado cada vez más competitivo.

Un sistema de información dentro de una organización juega el papel análogo al del sistema nervioso de un animal. En este sistema existen componentes que ejecutan funciones tales como la percepción, clasificación, transmisión, almacenamiento, recuperación, transformación. Su propósito primordial es proporcionar información (en el momento en que se solicite) para la toma de decisiones y coordinación. En el sentido más amplio el sistema de información incluye todos los componentes envueltos en la toma de decisiones, coordinación y advertencia tanto

humanas como automáticas. Dada la importancia que tiene hoy en día la información para la continuidad de los procesos en las organizaciones e instituciones, se deben enfrentar al tema de la seguridad de la información como un tema en el que esta en juego todos los componentes de una organización e institución.

La Seguridad en Cómputo la definiremos como el conjunto de metodologías, documentos, programas y dispositivos físicos, encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

El objetivo principal de la Seguridad Informática es proteger los recursos informáticos del daño, la alteración, el robo y la pérdida; incluyendo en esto los equipos, medios de almacenamiento, software, listados de impresora así como los datos. Todo esto enmarcado en un meta-objetivo que es el de mantener la continuidad de los procesos organizacionales que soportan los sistemas de información.

La seguridad en el ámbito de la computación o bien la llamada Seguridad Informática, se puede dividir en diversas ramas: seguridad de software y sistemas operativos, seguridad física, seguridad de hardware, seguridad de acceso y la seguridad en redes. Esta última será la más analizada y estudiada, ya que es un elemento crucial en la creación de los diseños de sistemas de información siendo este el objetivo principal de estudio que nos llevara al desglosamiento total de nuestro tema, pero sin olvidar que las otras ramas son de igual importancia en la columna vertebral de nuestro tema de estudio.

La Seguridad en Redes es la seguridad que se aplica en los componentes de red de una organización, y se puede definir también como los procesos necesarios en la implementación de políticas de seguridad y mantenimiento de los dispositivos de una red.

Los elementos que se pueden emplear para brindar Seguridad en Redes en una organización pueden ser muy diversos y adaptables. A la diversidad también se le puede agregar variabilidad, ya que se pueden emplear de manera conjunta diversos equipos para que trabajen a fin de conseguir un objetivo en común. Un esquema de seguridad tiene que ser adaptable y variable, es decir se le pueden eliminar y agregar ciertos elementos sin comprometer los requerimientos de seguridad en su totalidad; así mismo, se puede implementar un esquema de seguridad sin modificar la topología de red que una organización e institución estaban empleando previamente.

Existen diversas herramientas que pueden ser implementadas a fin de proveer seguridad en una red. Las aplicaciones de software y el hardware que proveen seguridad en una red de cómputo, necesitan interactuar con otros mecanismos para poder brindar los niveles necesarios de integridad que una organización requiere.

Las políticas y sistemas de seguridad seguirán desarrollándose, mientras existan elementos o personas que traten en cualquier momento de romper con la funcionalidad y la integridad de los sistemas de manejo de información (redes y equipos de cómputo) de las organizaciones.

La integridad, confidencialidad, confiabilidad y disponibilidad de la información sólo puede ser garantizada adoptando los mecanismos adecuados de seguridad en la organización. El aumento de la competencia incrementa la necesidad de establecer políticas y procedimientos de seguridad efectivas que disminuyan los riesgos que produzcan un escape, alteración o destrucción de datos que sean de vital importancia para cualquier organización e institución.

La seguridad es un elemento importante de cualquier servicio y sistema informático, aunque a menudo esta es postergada, basta tan sólo una brecha en la seguridad para crear graves daños. Por esto, el papel de la Seguridad Informática es cada vez más importante y no podrá ser ignorado, especialmente por el aumento de la exposición al riesgo que implica la cada vez mayor integración y globalización de los Sistemas Informáticos.

El tema de seguridad es complejo; y hay varias razones para ello, por ejemplo: la gran cantidad de información que manejan las organizaciones, la conectividad entre sistemas y equipos, pero por sobre todo, la falta de políticas globales al interior de la organización para enfrentarlo en forma clara y con las herramientas apropiadas.

Definir los límites de seguridad en las organizaciones e instituciones es casi imposible porque involucra a toda la organización. No sólo se trata de protegerla del ambiente externo, si no que también del mal manejo que se puede producir en su interior. Y cada día se esta haciendo más común escuchar de Firewalls (Puerta de fuego), autentificación de usuarios, control de acceso, firmas digitales, etc.

A nivel nacional estamos en una primera etapa, donde las grandes organizaciones e instituciones han sido muy sensibles al tema de seguridad lo que se debe en gran medida, a los temores que existen sobre la inseguridad de la Internet tradicional, pero en el resto de las áreas de la informática se ha hecho muy poco.

1.2.1 La Seguridad como cultura

Una de las paradojas es que a pesar de que cada vez se destinan mayores recursos para el área informática y que ésta se ha vuelto esencial para la gestión de procesos de las empresas e instituciones, el presupuesto asignado específicamente al tema de seguridad, no ha crecido en la misma proporción. Por esto es fundamental crear una conciencia al interior de las organizaciones para que puedan dimensionar en su justa medida la relevancia del problema. Mientras más tecnología se incorpora, más se agranda la brecha en lo que son debilidades de seguridad. Actualmente basan sus procesos en la tecnología de la información y eso provoca que estén cada vez más involucradas con estas herramientas tecnológicas y paralelamente van creciendo los temas relacionados con la seguridad. Por esto es fundamental la creación de conciencia a nivel mundial.

1.2.2 La seguridad como proceso

Uno de los puntos de consenso en el tema es que la seguridad es un proceso y no una actividad particular que desarrolla una organización o institución, un proceso que barre todas las unidades funcionales de estos. Al hablar de seguridad hay que involucrar muchos aspectos que no solo están relacionados con herramientas tecnológicas. Abordar el tema de seguridad no sólo implica

una solución de hardware y software, también involucra un conocimiento sobre el riesgo que significa no dar confiabilidad a la información, lo que en ocasiones tiene que ver con un desconocimiento de parte de los administradores de sistemas sobre el tema.

El problema hay que enfrentarlo con tecnología, pero también debe involucrar a los tomadores de decisiones, que son finalmente quienes deciden, ellos deben comprender claramente la problemática para destinar los recursos necesarios y así garantizar la confiabilidad, disponibilidad e integridad de la información.

Cualquier amenaza que se materialice contra el flujo normal de la información en una organización o institución, pone de relieve la dependencia y la vulnerabilidad a esta en un grado que es consecuente con la gravedad de la amenaza.

El crecimiento de las redes y la consecuente conectividad entre sistemas representa nuevas oportunidades, no sólo positivas, sino también negativas al facilitar por ejemplo los accesos no autorizados y al reducir las facilidades de control centralizado y especializado de los sistemas de información.

Los sistemas de información de cualquier organización están sometidos a *amenazas* más o menos destructivas (como ampliamente difunden los medios de comunicación incluso los no especializados). Amenazas que van desde fallos técnicos y accidentes no intencionados (pero no menos peligrosos), hasta acciones intencionadas, lucrativas, de curiosidad, espionaje, sabotaje, vandalismo, chantaje o fraude. Todas las opiniones aseguran que las amenazas a la seguridad de los sistemas de información y a la información misma serán cada vez más ambiciosas y sofisticadas.

El objeto o propósito de la seguridad de los sistemas de información consiste sobre todo en mantener la *continuidad de los procesos* organizacionales que soportan dichos sistemas. Así mismo intentar minimizar tanto el *costo global* de la ejecución de dichos procesos como las *pérdidas* de los recursos asignados a su funcionamiento.

El sujeto global de la seguridad se determina como un dominio del conjunto de la organización, que suele considerarse compuesto por activos (como sujetos elementales de la seguridad), estructurados metódicamente de forma jerarquizada.

La seguridad siempre es barata a largo plazo (y lo es también cada vez más a corto plazo). El ahorro y la eficacia que proporciona son relativos, pues dependen de su costo propio y su implantación inteligente; pero siempre son muy superiores si los requerimientos y especificaciones de seguridad se incorporan en el propio desarrollo de los sistemas y los servicios de información. Cuanto más temprano se actúe para dar seguridad a los sistemas de información, más sencilla y económica resultará ésta a la organización.

La gestión de riesgos de los sistema de información constituye la principal forma de hacer frente al problema de la seguridad de la información en las organizaciones, ésta pasa ha ser una labor de vital importancia ya no a nivel funcional si no ha nivel corporativo. De ella se desprende la planificación de la seguridad de los Sistemas de Información, por ende las políticas y medidas de seguridad ha implantar como también los objetivos, estrategias, y

organización de la seguridad. La gestión de riesgos en los Sistemas de Información es una acción permanente cíclica y recurrente, es decir, se ha de realizar continuamente debido a los cambios del sistema y de su entorno.

Se ha dado un contexto de la seguridad en cómputo ya que es demasiado extenso abarca un todo que en este caso es global, pero sin olvidar que cada concepto es básico para el desarrollo de nuestro tema

1.3 Problemas de seguridad

En México, en lo que va del año, los ataques a los sistemas informáticos se han incrementado y nadie es inmune a la amplia gama de actos maliciosos, por tanto, la seguridad en cómputo debe apreciarse como un problema de personas y de procesos que puede solucionarse mediante la búsqueda de una solución, basándonos en nuevas tecnologías y tomando conciencia de la importancia del problema de seguridad. A continuación se muestra un esquema de procesos para la solución de problemas de seguridad.

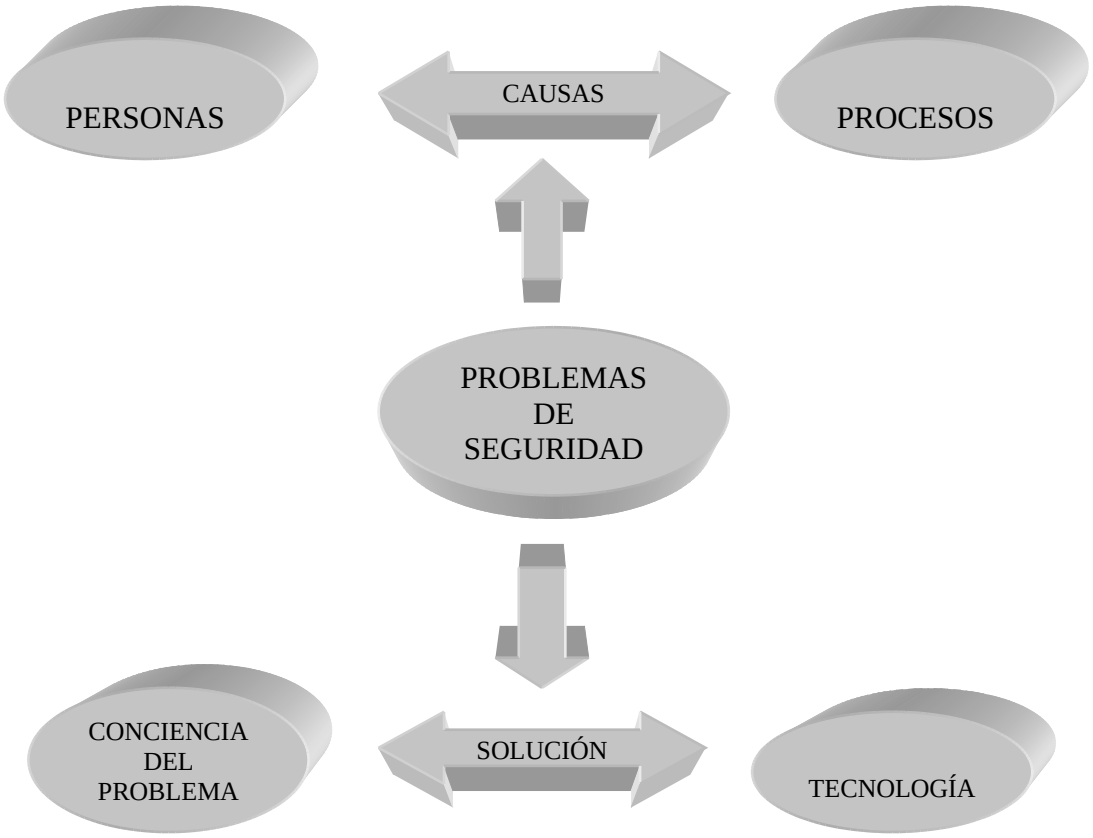


Figura 1.0 Esquema

Entre los ataques e incidentes más frecuentes que se deben tener en cuenta todos los días para garantizar la seguridad en cualquier equipo o sistema se pueden mencionar: robo de contraseñas, caballos de troya, virus y gusanos, puertas traseras, negación de servicios (DOS),

SPAM (correo basura) o correo no solicitado, Sniffers (“Husmeador”) de la red, Hoaxes (correos engañosos), Buffer Overflow e IP-Spooling (Cola de procesos), entre otros. En promedio, se crean y diseminan alrededor del mundo más de 100 virus cada semana, y éstos mutan, por lo que la multiplicación y replica de los virus informáticos es alarmante.

Por otro lado, en términos muy generales, podría decirse que existen tres objetivos primordiales para atacar un sistema o una red, y éstos son:

1. Las personas que sin buscar fines maliciosos o criminales, por curiosidad o reto atacan.
2. Los intrusos que quieren usar un sistema determinado como puente de acceso para atacar a otros sistemas.
3. Los intrusos que tienen, como único fin, atacar un sistema para provocar daño a la organización propietaria o que persiguen consultar, copiar, robar y vender información; existen también el crimen organizado y el espionaje industrial.

Sea cual sea el objetivo, los intrusos siempre causan un daño, voluntario o no, sea en términos de confianza o de un delito grave.

Las vulnerabilidades generales que los intrusos siempre buscan son cuentas sin contraseña, servicios mal configurados (Servicio de Correo, Web, etc.), contraseñas débiles, así como de los protocolos de comunicación y de transporte de información, además no proteger adecuadamente los sistemas operativos, ya que se aprovechan de la deficiente cultura de seguridad en cómputo que prevalece en términos generales.

Aquí, es importante destacar que cerca del 70% de los ataques informáticos los realiza personal especializado que trabaja dentro de la misma compañía o institución víctima. Si bien es cierto que en México no se han cuantificado, en términos económicos, las pérdidas que causan los ataques informáticos, el FBI (Oficina Federal de Investigación) estima que en Estados Unidos las pérdidas ascienden a cerca de los cinco billones de dólares.

Aunque existen intrusiones mayores y peligrosas, en México, además de la infección por “virus, gusanos y troyanos”, es común en materia de ataques, que los crackers[1] recurran al uso de organizaciones como computadoras personales, servidores, estaciones de trabajo y otros, para atacar a terceros con objeto de usar su infraestructura en cómputo y ancho de banda, etcétera.

Un problema central de la seguridad en cómputo es la poca capacidad de respuesta ante ataques de virus informáticos a un gran número de usuarios, por lo que es importante que todos ellos, tengan una cultura de seguridad. La seguridad informática no es un problema exclusivamente de las computadoras: las computadoras y las redes son el principal campo de batalla. Se debe de proteger aquello que tenga un valor para alguien, existe una gran variedad de herramientas que los intrusos usan hoy en día para tratar de introducirse a nuestros sistemas.

Entre los problemas más grandes que se tiene en cuestión de seguridad son los siguientes:

1. Robo de Información.
2. Fraude Financiero.

3. Penetración de los Sistemas por Intrusos.
4. Sabotaje de Datos o Redes.
5. Virus, Gusanos y Troyanos

Las vulnerabilidades e incidentes se han hecho más grandes, tan solo en el 2004 el CERT reporto 3,780 vulnerabilidades un poco menos que en el 2003 que fue de 3,784 pero aun así la suma es alarmante, con respecto a los incidentes se reportaron un total de 137,529 en el 2003 disparándose esta cifra ya que en el 2002 la cifra de incidentes reportados fue de alrededor de 82,094 esto debido al avance en la tecnología y la poca cultura de seguridad.

El CERT (Equipo de respuesta para Emergencias Informáticas), fue creado por DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa) en 1988 como respuesta a las carencias mostradas durante el incidente del gusano de ese mismo año el cual afecto a más de 6000 computadoras enlazadas al Internet. Entre los objetivos del CERT se encuentran; Trabajar en conjunto con la comunidad de Internet para generar recomendaciones y alertas en caso de problemas dentro de la Red.

Todo este contexto ha sido global debido al entorno en el que podemos manejar a la seguridad. Los problemas no vienen solos, son un conjunto de elementos, que a su vez forman la problemática de manera global como se mencionaba al principio, bajo este esquema debemos de tener las bases y la conciencia de que es un problema, él atacarlo será el siguiente paso para poder brindar seguridad.

1 Persona que viola la seguridad de los sistemas informáticos con fines personales

1.4 Niveles de seguridad

Existían desde el principio de la era de las computadoras sistemas que tenían sólo como meta establecer diferentes niveles de seguridad. En la micro-computación, con la llegada de las redes de área local (por sus siglas en inglés LAN), los sistemas operativos empezaron a implementar diferentes niveles de seguridad como:

- Establecer fiabilidad de los datos almacenados.
- Otorgar confiabilidad del sistema frente a diferentes configuraciones de hardware.
- Establecer restricciones de acceso ponderadas y selectivas a diferentes recursos, etc.

La seguridad absoluta no es posible y en adelante se entenderá que la seguridad informática es un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.
Además, la seguridad informática precisa de un nivel organizativo, por lo que se dice que:

Figura 1.1 Sistema de seguridad

En 1981 el departamento de Defensa de los Estados Unidos de Norte América formó el Computer Security Center, actualmente conocido como el National Computer Security Center (NCSC), para que fuera una organización formal y gubernamental para investigar la seguridad en las computadoras y así desarrollar métodos estándares de evaluación del nivel de seguridad ofrecido por un sistema en particular. La organización ha desarrollado un conjunto de criterios para abordar la fiabilidad de los sistemas de computadoras. El conjunto de criterios utilizados para evaluar sistemas comerciales esta disponible en una publicación titulada Trusted Computer System Evaluation Criteria, también conocida como el Libro Naranja (Orange Book).

El Libro Naranja clasifica los sistemas de informática en cuatro categorías D, C, B y A; siendo D la categoría menos segura y A la categoría más segura. Cada división consiste en una o más clases.

El Libro Naranja define seis requerimientos fundamentales:

- **Política de seguridad.** El sistema debe de proveer una implementación fiable de una política de seguridad bien definida.
- **Puntos de Seguridad (Marking).** El sistema debe de proveer una implementación fiable del control de acceso a los objetos para que el sistema sea capaz de asegurar que se cumple la política de seguridad.
- **Identificación.** Cada sujeto debe de ser identificado para que la política de seguridad sea capaz de forzar el control de acceso a los objetos. La información de identificación debe de ser segura.
- **Auditoría.** El sistema debe de proveer herramientas para auditar los sucesos relativos a la seguridad y para seleccionar el tipo de sucesos que se requieren auditar.
- **Garantía.** La implementación de todas las funciones de seguridad debe de ser identificable claramente y estar documentada para poder evaluar y verificar que es correcta.
- **Protección Continúa.** El sistema de seguridad debe de ser seguro en todo momento.

Los Niveles de Seguridad que propone el Libro Naranja son:

NIVEL D1: Protección Elemental

El Nivel D1 es la forma más elemental de seguridad disponible. Este estándar parte de la base que asegura que todo el sistema no es confiable. No hay protección disponible para el hardware; el sistema operativo, se compromete fácilmente y no existe la autentificación de usuarios con respecto a sus derechos para tener acceso a la información que se encuentra en la computadora. Algunos ejemplos de nivel D1 serian los sistemas operativos siguientes:

- MS-DOS.
- MS-Windows3.X y Windows 95 (sin grupo de trabajo).
- System7.x de Macintosh.

Estos sistemas operativos no distinguen entre usuarios y carecen de un sistema definido para determinar quien trabaja en el teclado. Tampoco tiene un control sobre los permisos en los archivos.

NIVEL C1: Protección Discrecional

El Nivel C tiene dos subniveles de seguridad: C1 y C2.

El Nivel C1: Sistema de Protección de Seguridad Discrecional.

El Nivel C1 describe la seguridad disponible, en un sistema típico UNIX, XENIX y NOVELL 3.X 0 superior. Existe algún nivel de protección para el hardware, puesto que no puede comprometerse tan fácil, aunque todavía es posible.

En este nivel los usuarios deberán identificarse así mismos con el sistema por medio de una clave (login) y una contraseña (password). Esta combinación se utiliza para determinar derechos de acceso a los recursos del sistema. Estos derechos de acceso son permisos para archivos y directorios. Estos controles de acceso discrecional habilitan al dueño del archivo o directorio, o al administrador del sistema, y evitar que algunas personas tengan acceso a programas e información de otras personas.

Sin embargo la cuenta del administrador del sistema no esta restringida a realizar cualquier actividad. En consecuencia un administrador descuidado o sin ética puede comprometer la seguridad del sistema sin que nadie se entere.

NIVEL C2: Protección de Acceso Controlado.

El segundo subnivel C2, fue diseñado para ayudar a solucionar tales hechos. Junto con las características de C1.

El nivel C2 incluye la característica de seguridad adicional que crea un medio de acceso controlado. Este medio es la capacidad de reforzar las restricciones a los usuarios en la ejecución de algunos comandos o acceso a algunos archivos basado no sólo en permisos, sino en niveles de autorización. Además este nivel de seguridad requiere de "auditarías del sistema". La Auditoría se utiliza para mantener los registros de todos los eventos relacionados con la seguridad, como aquellas actividades practicadas por el administrador del sistema. La auditoría requiere una autentificación adicional, de lo contrario ¿Cómo sabría el sistema de que la persona que esta logeada es realmente la persona que dice ser?.
Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

Algunos sistemas que pueden obtener el nivel C2 son: UNIX, XENIX, Novell 3.x o superior y Windows NT, Windows 2000 Server, Linux, etc.

NIVEL B1: Seguridad Etiquetada

El nivel B de seguridad cuenta con tres niveles de seguridad, que son los siguientes.

El nivel B1: Protección de Seguridad Encriptada.

Es el primer nivel que soporta seguridad de multinivel, como la secreta y la ultrasecreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que esta bajo control de 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, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe de poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

NIVEL B2: Protección Estructurada.

El nivel B2, conocido como Protección Estructurada, requiere que se etiquete cada objeto. Los dispositivos como discos duros, cintas o terminales podrán tener asignado un nivel sencillo o múltiple de seguridad. Requiere que se etiquete cada objeto de 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. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

NIVEL B3: Dominios de Seguridad.

El nivel B3, refuerza a los dominios con la instalación de hardware, por ejemplo el hardware de administración de memoria, se usa 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 según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben de ser lo suficientemente pequeñas como para permitir pruebas y 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 de seguridad más alto del Libro Naranja. Incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para 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 de incluirse. El diseño requiere ser verificado de forma matemática y también se deben de realizar análisis de canales encubiertos y de distribución confiable. El hardware y el software son protegidos para evitar infiltraciones ante translados o movimientos del equipo.

1.5 Fundamentos de redes de computadoras

La necesidad de que varios usuarios de un mismo servicio de telecomunicaciones, puedan comunicarse entre sí, y además optimizar los medios instalados para tal propósito, ha llevado al concepto de red de telecomunicaciones. Estas han evolucionado desde formas muy simples, diseñadas durante el siglo pasado para brindar el servicio telegráfico a redes más complejas, como son las redes que pueden brindar el servicio telefónico con computación o las actuales instalaciones que permiten una importante y más variada oferta, de servicios de telecomunicaciones.

Por otra parte, el crecimiento de las redes de telecomunicaciones es un fenómeno que se ha mantenido y se mantiene constante durante las últimas décadas; siendo este sector, uno de los más dinámicos en la economía en casi todos los países. La necesidad de comunicarse mas, mejor y con mayores facilidades técnicas esta haciendo al sector de los servicios de telecomunicaciones uno de los de mayor tasa anual de crecimiento en el mundo entero.

La aparición de la informática aplicada a los medios de comunicaciones ha reforzado y entremezclados ambos conceptos. Los problemas relacionados con el almacenamiento y recuperación de la información han estado presentes desde que el hombre comenzó a escribir por primera vez. En la década de los años 50, el hombre dío un significativo paso hacia el progreso con la invención de la computadora. A partir de entonces, los ambientes de oficina podían enviar lotes de información a una localidad central, disponer de la computadora para realizar el procesamiento de esta información. El problema era que la información, perforada en cajas repletas de tarjetas, todavía debía ser transportada manualmente a la localidad central de procesamiento.

La década de los años 60 fue la época de las terminales, situadas en los escritorios de los empleados de las oficinas. Las terminales permitían a los usuarios comunicarse directa e interactivamente con la unidad central de procesamiento a la que estaban conectados. Las líneas telefónicas constituían los medios más prácticos para efectuar la comunicación a larga distancia entre computadoras. A medida que se conectaban más terminales y otros periféricos a la unidad central de procesamiento de una compañía, esta unidad comenzaba a debilitarse ante la carga de entrada y salida de información. Otro problema era la naturaleza única de cada sistema operativo de las computadoras, lo cual hacía muy difícil la comunicación entre dos sistemas diferentes.

A mediados de los años 70, surgió la tecnología de los chips, o circuitos integrados de silicio. Esta nueva tecnología permitió a los fabricantes de computadoras integrar un mayor volumen de “inteligencia" en una máquina más pequeña. Estas microcomputadoras tomaron la agobiante carga de entrada / salida de las viejas unidades centrales de procesamiento, y la distribuían en porciones más manejables a los escritorios de cada trabajador.

Para comienzos de los años 80, las microcomputadoras habían revolucionado completamente el concepto de computación electrónica, así como sus aplicaciones y sus mercados. Los gerentes de sistemas de información estaban perdiendo control, ya que el ambiente de computación ya no era centralizado. Los precios fueron descendiendo, a tal punto que casi cualquier

presupuesto departamental podía absorber el costo de adquirir unas cuantas computadoras personales para uso del departamento.

La revolución de la computadora personal trajo consigo abundantes mejoras que beneficiaban directamente al usuario final. Aplicaciones en mayor cantidad y variedad, competencia entre fabricantes de hardware y software, menores costos e interfaces de usuarios mucho más sencillas.
La lista sigue indefinidamente, sin embargo, una desventaja evidente del microcomputador era la descentralización. Los primeros años de la década fueron la época de los disquetes. Los vendedores de computadoras decían: Estos 30 disquetes son capaces de almacenar toda la información de sus gabinetes de archivos y eso era cierto. Sólo que ahora, en lugar de cargar una pila de tarjetas perforadas de oficina en oficina, los empleados cargaban una pila de disquetes.

El disco duro con mayor capacidad de almacenamiento vino a minimizar la carga de disquetes. Una desventaja del sistema de disco duro era su elevado costo. Este elemento, así como el potencial de almacenamiento, generaron una vez más el movimiento de los engranajes creativos, y la gente comenzó a pensar: "Debe existir una forma de que varios usuarios puedan compartir el costo y el almacenamiento de los discos duros", este fue el nacimiento de las redes de área local.

1.5.1 Redes de computadoras

Una **Red de Computadoras** es un conjunto de terminales, nodos, servidores y elementos de propósito especial que interactuan entre sí con la finalidad de intercambiar información y compartir recursos.

Anteriormente la información se almacenaba en los llamados “Mainframes” (aunque existen todavía). Es decir, diferentes terminales eran conectadas con la finalidad de recibir información y compartir los recursos. El problema con este tipo de red, es que se basaba en un sistema centralizado, ya que del Mainframe se extraía toda la información, teniendo de esta forma la limitante en cuanto a la capacidad de almacenamiento de datos.

Por otro lado con la utilización de un Mainframe, el fallo del mismo provocaba el fallo de todo el sistema, lo cual traía consecuencias muy graves en el manejo de una organización.

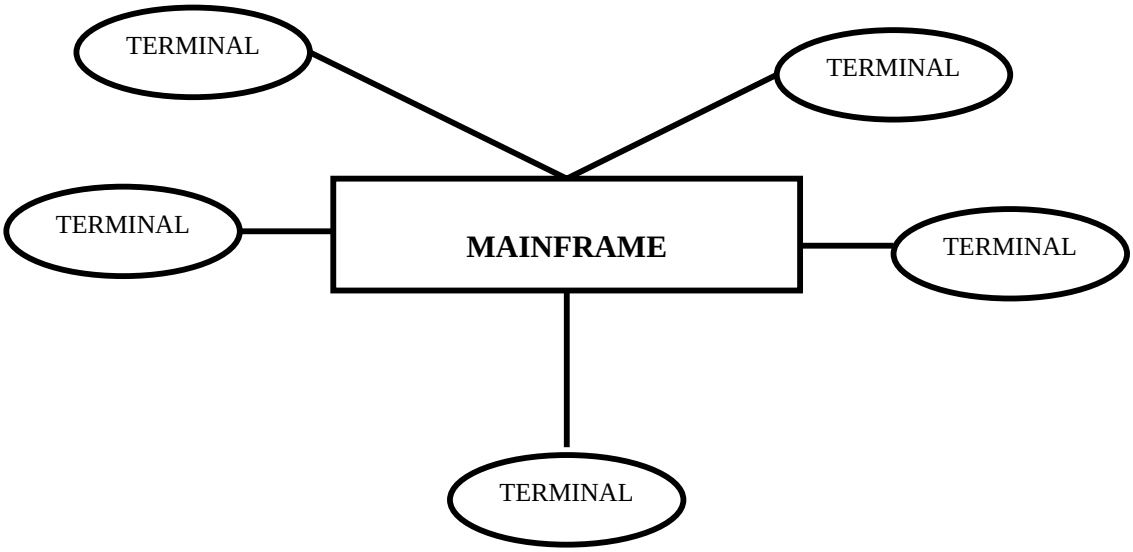


Figura 1.2 Mainframe

Con la introducción de las diferentes clases de redes de computadoras y tecnologías, surgió la posibilidad de utilizar diferentes servidores, que como su nombre lo indica, proveen servicios a un conjunto de nodos denominados clientes.

De esta forma, no existe limitante en cuanto almacenamiento de información, ya que nuevos servidores pueden ser instalados, dando así, la facilidad en la expansión de las redes. De esta forma, una **Red de Computadoras** se define como un sistema distribuido. En un sistema distribuido, la existencia de múltiples computadoras autónomas es transparente para el usuario. El usuario puede teclear una orden para ejecutar un programa y éste se ejecutará. La tarea de seleccionar al mejor o el correspondiente procesador y colocar los resultados en el lugar apropiado, corresponde al sistema operativo y a la red en sí.

En un sistema distribuido, el usuario no está consciente de que existen múltiples procesadores. El sistema se ve como un monoprocesador virtual, el sistema distribuido es un sistema de software construido encima de una red.

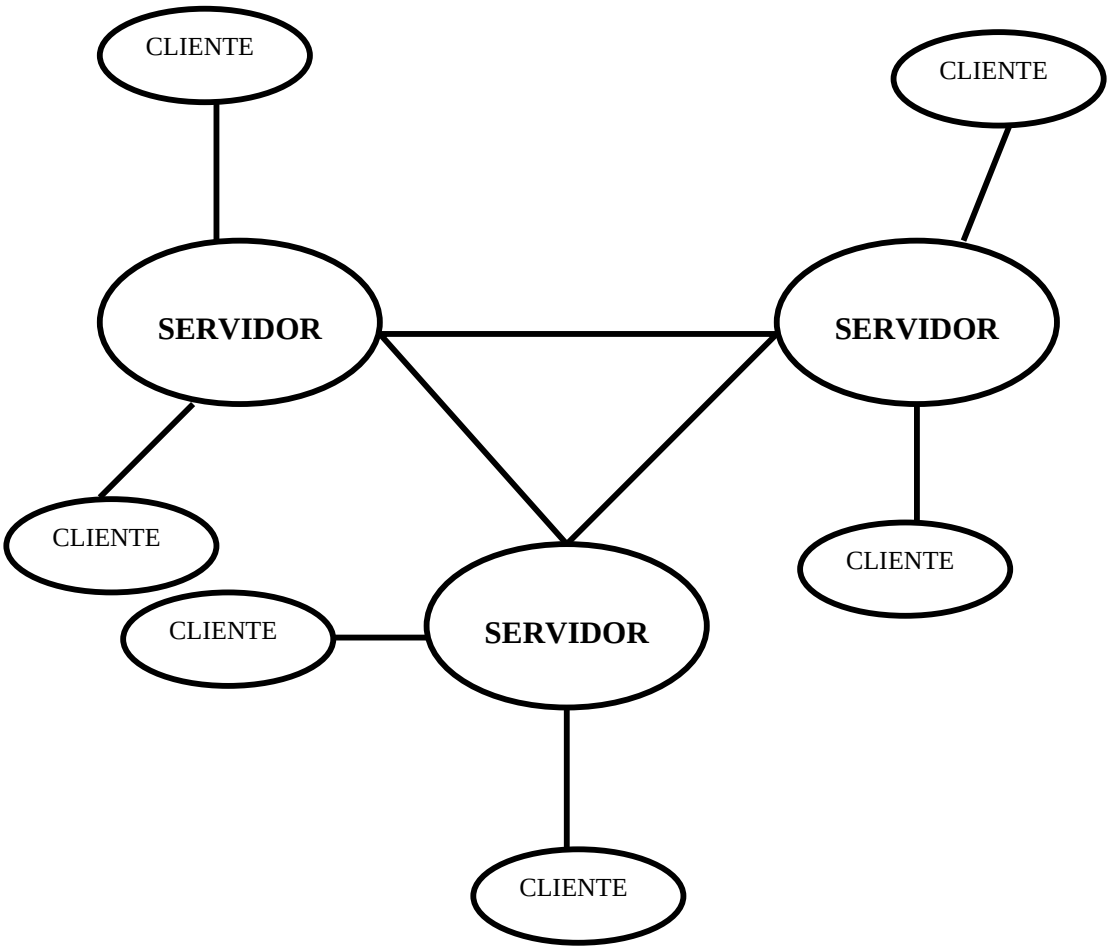


Figura 1.3 Sistema Distribuido

Las razones principales que se pueden tomar en consideración para la utilización de una red de computadoras es:

- **Integridad.** Hacer de un sistema de varios elementos una sola herramienta, en donde se utilicen las características y las aptitudes de cada uno de la mejor forma posible.

- **Flexibilidad.** Fácil de utilizar, rápida comunicación de datos en cualquier momento, etc.

1.5.2 Requerimientos de una red

Para poder lograr una conexión entre diferentes dispositivos que forman una red de datos, es necesario contar con algunos requerimientos básicos, basados en el tipo de conexión, transmisión de los datos, etc.

Los requerimientos mostrados a continuación, son los básicos para lograr una conexión apropiada, claro está, no son los únicos, pero nos da el inicio al conocimiento de todos los

problemas que se necesitan resolver, para realizar una conexión y un intercambio de información a través de una red de datos.

Conectividad. Para la realización de una red, es necesario conectar los diferentes elementos de la misma (link o enlaces). Dos tipos de conexión son básicos:

- Punto a Punto (Peer-to-Peer). Cada elemento es conectado a otro por medio de un enlace físico (cable o "link" en inglés).

Figura 1.4 Conectividad punto a punto

- Multipunto (multipoint). Todos los elementos están conectados a un solo enlace físico.

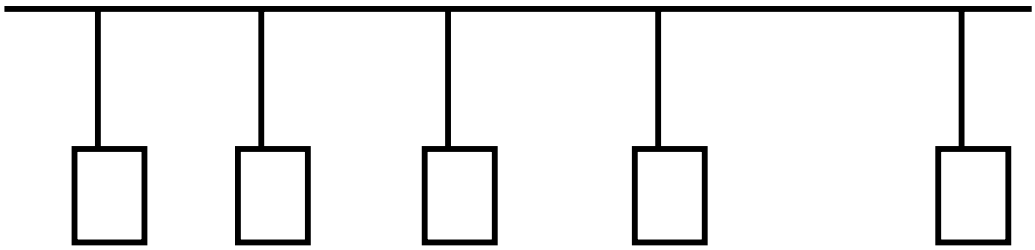


Figura 1.5 Conectividad Multipunto

Ruteamiento. Por el hecho de ir de un elemento (cliente) a otro (servidor), o viceversa, es necesario seguir una ruta entre diferentes elementos (routers, bridges, gateways, etc.).

Estas rutas pueden seguir dos modelos diferentes para llegar a su destino final:

- **Circuito Conmutado (Circuit Switched).** Trabaja como la línea de teléfono, haciendo una conexión estática virtual mientras exista conexión, primeramente se hace la petición del canal y una vez tenida la dirección a seguir, realiza la comunicación siguiendo la misma ruta. No hay pérdida de datos y se espera que lleguen en forma secuencial.

- **Paquete Conmutado (Packet Switched).** Cada paquete de información (conjunto de bytes) sigue una ruta determinada por la dirección destino almacenada en cada paquete, pudiendo usar diferentes caminos. En este tipo de ruteamiento, no existe la seguridad de que los paquetes lleguen al destinatario, así como tampoco se asegura que éstos lleguen en forma secuencial.

Por otro lado, la ventaja con relación a Circuit Switched es que en Packet Switched la información se transmite a una velocidad mayor ya que no se tiene que esperar a tener un enlace creado antes de transmitir datos. Se puede hacer la comparación con el servicio de correo

postal, en donde uno tiene la seguridad de que la correspondencia llegue al destinatario únicamente por la dirección que uno anota en la misma.

- **Dirección.** Debido a que los enlaces físicos pueden ser utilizados para una comunicación entre múltiples nodos, los nodos intermedios deben ser capaces de determinar el camino a seguir para llegar al nodo destino. De esta forma, la identificación de cada nodo por una dirección única permite realizar dicha tarea (igual que el servicio postal). Por ejemplo en internet, se trabaja bajo el protocolo IP (Internet Protocol), cada nodo tiene una dirección denominada "dirección IP".

- **Multiplexión.** Si un nodo cualquiera A desea comunicarse con otro nodo B, es necesario de alguna manera hacer saber a la línea (la línea se define como el enlace físico por el cual se transmite la información) que se estará enviando información de A a B, y de compartir la línea con otras comunicaciones.

Existen tres métodos para hacer esto:

- **Multiplexión por División de Tiempo (TDM).** A diferentes tiempos se envían diferentes comunicaciones.

- **Multiplexión por División de Frecuencia (FDM).** A diferentes frecuencias (portadora) se envían diferentes comunicaciones.

- **Multiplexión por División de Código (CDMA)**. Cada subcanal utiliza un código para la transmisión de su información.

- **Multiplexión Estadística por División de Tiempo.** La comunicación que requiere enviar más datos se le asigna mayor tiempo de envío.

- **Multiplexión por Polarización.** Cada subcanal se transmite con una polarización determinada.

Con los requerimientos mostrados en este apartado, es posible lograr una conexión básica entre los diferentes dispositivos que forman una red de computadoras. Primeramente, la conectividad nos da la conexión física entre los dispositivos; el ruteamiento nos da el camino a seguir, así como la identificación de todos los dispositivos involucrados en la comunicación de acuerdo a la dirección que sea asignada a cada uno de ellos y el multiplexaje nos dará la forma de compartir un enlace físico entre múltiples dispositivos que generarán múltiples conexiones.
Para la realización de una red de computadoras, y partiendo de que el mundo no es perfecto, diversos problemas producidos por errores al envío de datos, de ruteamiento, de calidad de servicio, costo, etc. Hace posible que surjan diversas técnicas a diferentes niveles para solucionar los problemas.

1.5.3 Conceptos básicos

Servidor. Es una computadora especial a la que están asociados todos los recursos de uso compartido, tanto de hardware como de software, incluyendo el software encargado de supervisar la operación de la red.

Estaciones de Trabajos. Son las computadoras en los que trabajan los usuarios, también llamados Clientes.

Elementos de Conexión. Es el equipo utilizado para conectar las estaciones de trabajo al servidor de la red, bien sea directa o indirectamente. Esta categoría incluye las tarjetas de interfaz de red instaladas tanto en el servidor como en las estaciones, cableado, y otros equipos de conexión, dependiendo del sistema.

Las redes pueden también disponer de una variedad de dispositivos periféricos opcionales los cuales pueden o no estar conectados directamente al servidor de archivos.

Entre éstos se incluyen:

- Modem.
- Impresoras.
- Subsistemas de discos (para Incrementar la capacidad de almacenamiento en el servidor).

Nodo. Término genérico usado para dispositivos que forma parte de una red. Los nodos incluyen computadoras de propósito general, de propósito especial, switches, routers, bridges, etc.

Bandwidth. Velocidad de transmisión de bits por unidad de tiempo, típicamente por segundo. Por ejemplo, en una red Ethernet, el ancho de banda es de 10Mbps o 100Mbps, en Token Ring de 4Mbps o 16Mbps. El ancho de banda de un canal es el mínimo de los anchos de banda de los contribuyentes.

Latency (Delay). El Latency es el tiempo que tarda un bit en propagarse de un nodo a otro.

Round Trip Time (RTT). Es el tiempo que tarda un bit en ir de un nodo A a un nodo B y regresar. Es decir, RTT = 2 x Latency.
¿Cuándo basarnos en el parámetro Latency y cuándo en Bandwidth?.

Esto depende de la aplicación y de la información que se envía. Por ejemplo, cuando el paquete de información es muy grande, es más útil utilizar el ancho de banda, en caso contrario, el delay es más útil.

Info. Transmitida	*1 Byte*	*1 Byte*	*1.25MB=10Mb*	*1.25MB=10Mb*
Latency *Bandwidth*	*1ms.*	*25ms.*	*1ms.*	*25ms.*
1Mbps	*1.008*	*25.008*	*10.001s*	*10.025s*
100Mbps	*1.00008*	*25.00008*	*0.101s*	*0.125s*

Figura 1.6 Tabla comparativa

Como se observa, cuando la información transmitida es muy pequeña, el Latency es quien define el tiempo de transmisión de la información (Figura 1.6, casos 1 Byte). Cuando la cantidad de información es grande (la tabla nos muestra casos de 1.25 MB), el Bandwidth es quien definirá el tiempo de propagación de la información.

Delay x Bandwidth. Es el número de bits en tránsito o el número de bits mandados antes de recibir información.

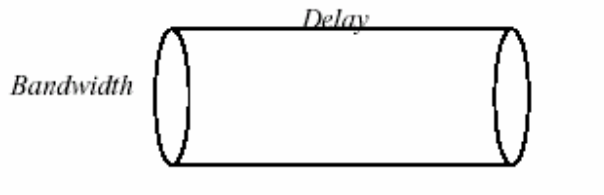


Figura 1.7 Delay x Bandwidth

Troughput. Bits transmitidos por unidad de tiempo, típicamente por segundo.

% Utilización. Porcentaje de una red que está siendo utilizada para enviar y recibir datos. Es decir, el troughput dividido por el bandwidth, idealmente en una red Ethernet el porcentaje de utilización no debe sobrepasar el 40%.

% de Utilización= Troughput / Bandwidth

Baudio. Cantidad de información que se transmite por unidad de tiempo, dependiendo de los niveles de cuantización es el número de bits que se transmiten por segundo.

Baud Rate. Número de señales enviadas por unidad de tiempo.

- **Comunicación Simplex.** Comunicación entre dos puntos (nodos) en un solo sentido únicamente.

Figura 1.8 Comunicación Simplex

- **Comunicación Half Duplex.** Comunicación entre dos puntos (nodos) en un solo sentido a la vez.

Figura 1.9 Comunicación Half Duplex

- **Comunicación Full Duplex.** Comunicación entre dos puntos (nodos) en los dos sentidos a la vez.

Figura 1.10 Comunicación Full Duplex

Modos de Transferencia. La comunicación entre nodos de una red, se realiza de dos maneras distintas que a continuación se describen.

- **Difusión.** Comunicación a un conjunto de nodos (Broadcast).

- **Conmutación.** Comunicación de información de un nodo a otro (Punto a Punto).

Control Transmisión: La forma de controlar la transferencia de información en una red, se puede manejar de dos formas ya sea centralizada o distribuida

- **Centralizado.** Un nodo único almacena y distribuye procesos.

- **Distribuido.** Varios nodos ejecutan los procesos.

Modelos de Interconexión:

- **Conexion Oriented.** Se hace una conexión lógica y después se envían los datos siguiendo la misma ruta durante toda la conexión. Basado en el método de ruteamiento de Circuit Switched. Como ejemplo de dicha conexión se encuentra el protocolo TCP (Transfer Control Protocol).

- **Conectionless.** La información es enviada por paquetes, en donde cada uno puede seguir rutas diferentes. Basado en el método de ruteamiento de Packet Switched. Un ejemplo de un protocolo que trabaje bajo este modelo es UDP (Unit Datagram Protocol).

1.5.4 Topologías de red

Una topología de red va relacionada con el tipo de conexión entre los diferentes dispositivos que forman la red de computadoras, es decir, la forma como se interconectan todos los

dispositivos para formar la red. Existen tres topologías básicas que son utilizadas para formar redes: Estrella (Star), Anillo (Ring) y Bus. De estas tres topologías principales, es posible generar diferentes topologías "híbridas", logrando así, una integración entre las topologías básicas, expandiendo las redes de computadoras hacia redes de cobertura global.

Hay que hacer notar que en este apartado, las topologías definidas van relacionadas con el tipo de interconexión física para unirlas. Es posible hablar de topologías con relación a una interconexión física y a una interconexión lógica, es decir, la forma como comparten físicamente el medio transmisor y la forma como lógicamente comparten este medio.

Cada topología, independientemente de la forma o apariencia geométrica que pueda tener, cuenta con características propias que definen el material a utilizar como medio de transmisión, distancia máxima entre estaciones, grado de dificultad para realizar el cableado, así como para su mantenimiento, ya que la disposición de las estaciones en la red puede determinar si una falla afecta a uno o más elementos; favorece también determinados métodos de acceso.

Topología Tipo Bus

En esta topología no existe un CPU o similar que controle la comunicación entre los nodos. Cada nodo está conectado a un bus, donde cada nodo actúa como si fuera parte de una red anillo, pero ninguno depende del nodo siguiente para que el flujo de información continúe, ni tampoco depende del nodo anterior para que la información llegue a él.

Las características más importantes son:

- Los nodos no retransmiten ni amplifican la información.
- El tiempo de retención de la información en los nodos es nulo.
- Todos los mensajes llegan a todos los nodos.
- No es necesario ningún encaminamiento de la información.
- La fiabilidad de la comunicación depende únicamente del bus (punto crítico).
- La configuración es flexible y modular.
- Es una tecnología de bajo coste que todavía se utiliza frecuentemente.

Ofrece facilidad para interceptar la información circulante.

La tecnología común que trabaja bajo una topología Bus es denominada Ethernet fue desarrollada por Digital, Intel y Xerox, normalizada con IEEE 802.3.

Ethernet distribuye paquetes de datos de longitud variable con una velocidad de 10 Mbps a los diferentes nodos dispersos a lo largo de un bus que comúnmente es cable coaxial. Los nodos separados hasta una distancia de 50m de largo pueden ser también unidos por cable par trenzado. Una red Ethernet puede estar formada hasta por 1024 nodos.

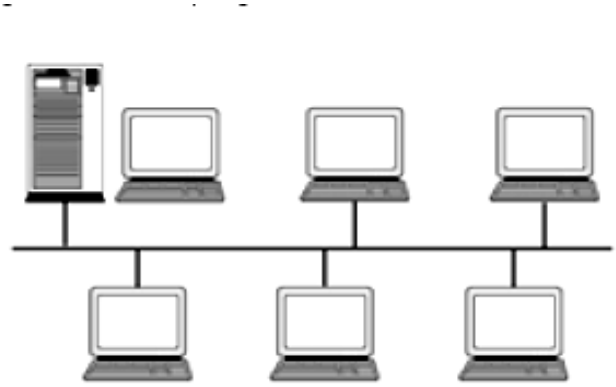


Figura 1.11 Topología Tipo Bus

Topología Tipo Anillo (Ring)

Una de sus características importantes es que está formado por un conjunto de enlaces punto a punto, lo cual es una topología bien entendida y probada, en donde la información es pasada a través de los nodos de uno a uno en una comunicación peer-to- peer. La ventaja que tiene esta topología es que no se requiere un cuarto de control central, aunque la desventaja es que si uno de los enlaces punto a punto que la forman se rompe (o se desconecta debido a errores en la transmisión, etc.), la red deja de funcionar.

El control de transmisión que usa esta topología es distribuido y su modo de transferencia es de conmutación.

Las características más importantes son:

- Cada nodo amplifica y repite la información que recibe.
- Los mensajes viajan a través del anillo nodo a nodo, de forma que todas las informaciones pasan por todos los módulos de comunicación de los terminales (facilidad para interceptar la información).
- No es necesario dirigir el encaminamiento de la información.
- La fiabilidad del anillo depende de cada uno de los nodos y de la vía de comunicación que forma el anillo. La caída de una sola terminal podría provocar que la red entera dejara de funcionar.

La tecnología común que utiliza dicha topología es denominada Token Ring.

Token Ring es una tecnología desarrollada por IBM, corresponde al estándar IEEE 802.5. El diseño básico es un anillo de nodos que no superan 256, operando a 4 ó 16 Mbps. En Token Ring se utiliza un código de autorización llamado Token que actúa como método de acceso al medio denominado Token Passing.

El método de acceso al medio Token Passing trabaja de la siguiente forma. Si no hay mensaje, el token (tres bytes) es enviado a través del anillo. Cuando un nodo A con un mensaje a enviar recibe el token, retiene éste y envía el mensaje, el cual incluye un código de identificación del destinatario. Los nodos ignoran el mensaje si no es para sí mismo, en caso contrario, obtienen la información. La información sigue viajando hasta que se completa su trayectoria alrededor del anillo hasta que llega al nodo A. Dicho nodo suelta el token para que pase nuevamente alrededor del anillo para futuros envíos de información.

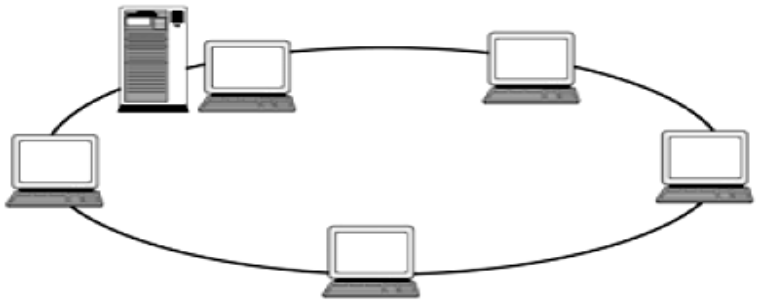


Figura 1.12 Topología Tipo Anillo (Ring)

Topología Estrella (Star)

La topología Estrella consta de una unidad central que controla el flujo de información a través de la red. La topología Estrella tiene limitaciones en cuanto a rendimiento y confiabilidad, ya que el tamaño de la red depende directamente de la capacidad del controlador central (número de conexiones que puede soportar) y en caso de fallar éste, todo el sistema deja de funcionar. Por otro lado, tiene la ventaja de poderse administrar de forma centralizada.

En la topología Estrella se tiene un control de transmisión centralizada y una forma de transferencia de conmutación.

Las características más importantes son:

- Todos los terminales se comunican entre sí mediante un nodo central.
- El dispositivo central puede ser activo o pasivo.
- Los fallos tienen una repercusión muy diferente, según dónde se produzcan.

Desde el punto de vista de su forma física, este tipo de topología es utilizada en redes Ethernet y Token Ring, aunque la topología lógica continúa siendo bus y anillo, respectivamente.

Figura 1.13 Topología Tipo Estrella (Star)

En el momento de elegir una topología de red, es necesario tener en cuenta los siguientes aspectos:

- Distancia máxima que se puede obtener.
- Número máximo de terminales.
- Flexibilidad a la hora de añadir o eliminar terminales de trabajo.
- Tolerancia a caídas de los terminales.
- Retraso de los mensajes.
- Costo.
- Flujo de información que puede circular a través de la red.

Las topologías de bus y de anillo son las más utilizadas en redes locales, aunque por motivos de flexibilidad, fiabilidad y seguridad, el diseño físico en estrella también se ha convertido en muy popular con redes que, lógicamente pueden funcionar en bus o anillo, pero que tienen una topología física de estrella.

1.5.5 Arquitectura de red

Para la realización de una red de computadoras, y para tener una comunicación eficiente entre diferentes nodos que forman a una red a nivel de aplicación, es útil (y así se ha hecho) la utilización de una Arquitectura de Red, la cual, tiene la finalidad de separar el problema de la comunicación en diferentes capas, en donde cada una se encargue de una comunicación a diferentes niveles. Por ejemplo, en una comunicación telefónica, la comunicación se transmite por medio del cable sin tener conocimiento el usuario de la forma de comunicación (analógica o digital, half duplex o full duplex, etc.), mientras que el usuario se comunica por medio de la voz, lo cual no es importante para el medio (ya que no interesa si se comunica voz, fax, email, etc.).

Una arquitectura básica está formada por cuatro capas.

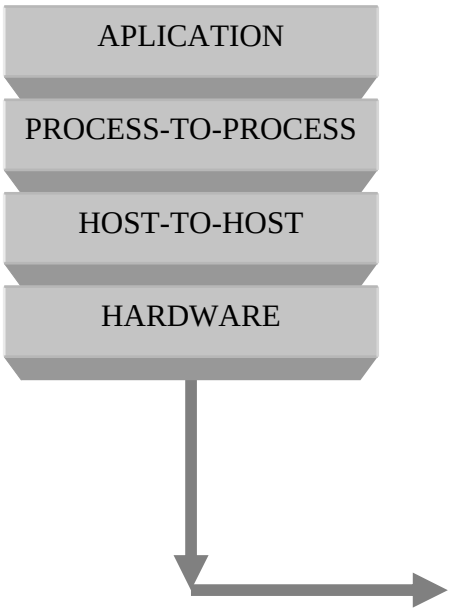


Figura 1.14 Esquema de Arquitectura de Red básica

Un protocolo provee un servicio de comunicación entre nodos en los diferentes niveles. Es el software de cada capa.

.

Un protocolo provee dos interfaces:

- **Interfaz de Servicio.** Define las operaciones que los objetos locales pueden desarrollar en el protocolo (qué funciones/operaciones exporta).

- **Interfaz punto a punto.** Define los mensajes que se pueden intercambiar en puntos remotos. Define la estructura y significado de la comunicación.

Se dice que los protocolos permiten una comunicación punto a punto entre las diferentes capas (layers), es decir, dada la arquitectura mostrada anteriormente, la comunicación punto a punto es representada de la siguiente manera

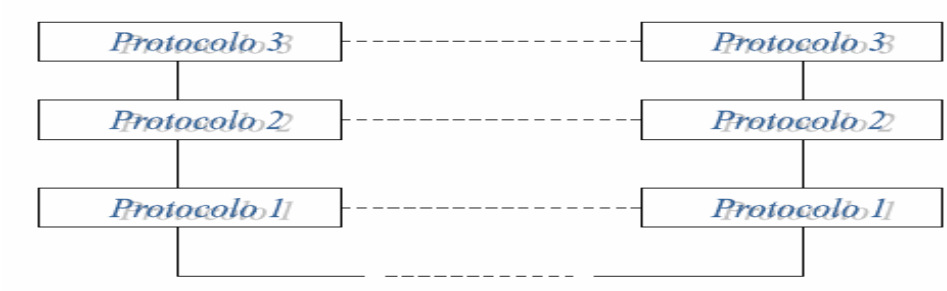


Figura 1.15 Comunicación punto-a-punto de los protocolos

Con la utilización de Arquitecturas de Computadoras, tres nuevas definiciones serán vistas:

Gráfica y Pila (Graph and Stack). Generalmente el número posible de protocolos que se pueden usar en cada capa es más de uno. De esta forma la gráfica representa todos los protocolos posibles (el diagrama), el cual, es llamado Protocol Graph (Gráfica de protocolos).

El conjunto de protocolos utilizados para realizar una conexión específica es llamado Protocol Stack (pila de protocolos).

Encapsulación (Encapsulation). Cada capa recibe datos de las capas superiores y un protocolo no conoce nada acerca del contenido de los datos que recibe (pudiendo ser un email, una transacción bancaria, etc.). El único requerimiento es que los datos lleguen al nodo destino sin alteración. Para hacer esto, cada protocolo necesita mandar controles de información para ser reconocido en el otro nodo.

Para hacer posible la comunicación punto a punto, es necesario colocar una cabecera (header) a cada mensaje, los cuales son alrededor de 10 Bytes. De esta forma se dice que los datos son encapsulados por el protocolo. La ventaja de utilizar una Arquitectura de Red es la estandarización entre diferentes tipos y marcas de dispositivos como son los servidores, terminales, bridges, routers, etc.

Dos de los estándares más utilizados, y que explicamos a continuación son: el modelo OSI y el modelo TCP/IP.

El Modelo OSI

Uno de los estándares más utilizados y del cual prácticamente se basan los posteriores estándares, así como las diferentes tecnologías de red es el modelo OSI (Open System Interconnection), desarrollado por ISO (International Standard Organization). El modelo OSI está formado por siete capas (Layers).

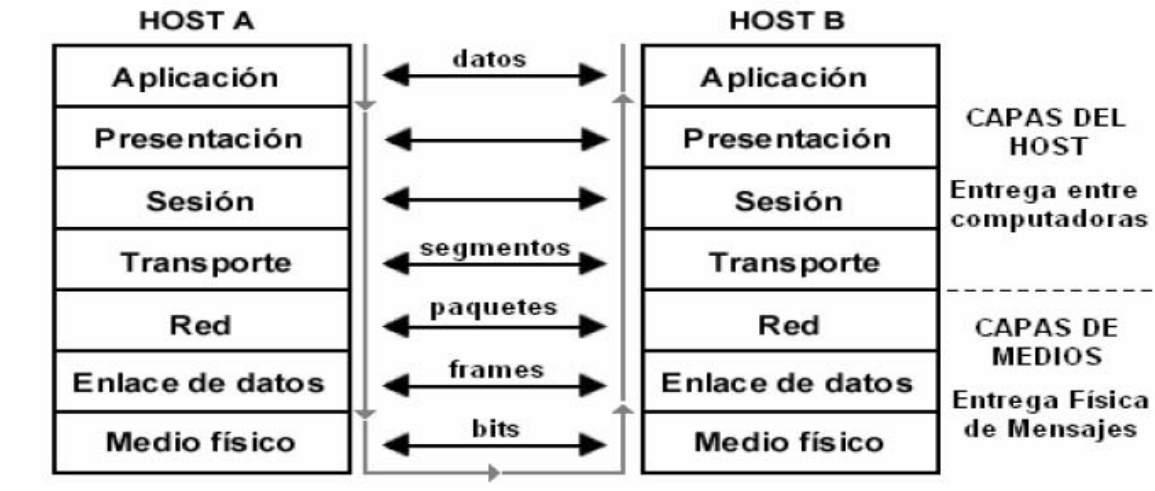


Figura 1.16 Modelo OSI.

1. Capa Física *(*Physical Layer)

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio (cable conductor, fibra óptica o inalámbrico); características del medio (tipo de cable o calidad del mismo; Tipo de conectores normalizados o en su caso tipo de antena, etc.) y la forma en la que se transmite la información (codificación de señal, niveles de tensión / corriente, modulación, tasa binaria, etc.).

Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es uni o bidireccional (simplex, duplex o full-duplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable); o electromagnéticos. Estos últimos, dependiendo de la frecuencia / longitud de onda de la señal pueden ser ópticos, de micro-ondas o de radio. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica, etc.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

2. Capa de Enlace de Datos *(*Data Link Layer)

La capa de enlace de datos proporciona tránsito de datos a partir de cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También debe incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

Ejemplos de protocolos usados: Ethernet, Token Ring, ATM (Modo de Transferencia Asíncrona).

3. Capa de Red (Network Layer)

La capa de red se encarga de hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir que se encarga de encontrar un camino manteniendo una tabla de enrutamiento y atravesando los equipos que sean necesarios, para hacer llegar los datos al destino. Los equipos encargados de realizar este encaminamiento son llamados encaminadores, o también llamados Routers y, en ocasiones enrutadores.

Adicionalmente la capa de red debe gestionar el tráfico en la red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad).

Ejemplos de protocolos usados: IP, IPX(Intercambio de paquetes en red interna)

4. Capa de Transporte (Transport Layer)

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas unidades si es necesario, y pasarlos a la capa de red. En el caso del modelo OSI, también se asegura que lleguen correctamente al otro lado de la comunicación. Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes. Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío.

Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión finalice. De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas 1 a 3, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir. Para finalizar, podemos definir a la capa de transporte como: Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando.

Ejemplos de protocolos usados: Transfer Control Protocol (TCP), User Datagram Protocol (UDP), Sequenced Packet Exchange (SPX), etc.

5. Capa de Sesión (Session Layer)

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son:

- Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta).

- Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo).
- Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio.

Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

Ejemplos de protocolos usados: Real Time Streaming Protocol (RTSP), Session Initiation Protocol (SIP), Server Message Block (SMB) , etc .

6. Capa de Presentación (Presentation Layer)

El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres American Standard Code for Information Interchange (ASCII), unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes; los datos lleguen de manera reconocible.

Para conseguir este objetivo se describió una posible notación de sintaxis abstracta (ASN.1), que en realidad se utiliza internamente el Manager Information Base (MIB) de SNMP (protocolo de gestión de red, para supervisar equipos de comunicaciones a distancia).

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Son ejemplos claros los datos transmitidos en ASCII a un receptor que utiliza EBCDIC, como en el caso de los mainframes de IBM, o la utilización de diferentes normas de punto flotante o aritméticas de complemento para representar los enteros.

Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.

Ejemplos de protocolos usados: HiperText Markup Language (HTML), Extensible Markup Language (**XML**), etc.

7. Capa de Aplicación (Application Layer)

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico, gestores de bases de datos y servidor de ficheros. Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml.
Entre los protocolos más conocidos destacan:

- HTTP (Hipertext Transfer Protocol) el protocolo bajo la WWW.
- FTP (File Transfer Protocol) (FTAM, fuera de TCP/IP) transferencia de ficheros.
- SMTP (Simple Mail Transfer Protocol) (X.400 fuera de TCP/IP) envío y distribución de correo electrónico.
- POP (Post Office Protocol) / IMAP (Internet Message Access Protocol): reparto de correo al usuario final.
- SSH (Secure SHell) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otro terminal remoto, ha caido en desuso por su inseguridad intrínseca, ya que las claves viajan sin cifrar por la red.

Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:

- SNMP (Simple Network Management Protocol).
- DNS (Domain Name Server).

Casi todas las aplicaciones descritas comparten la arquitectura cliente-servidor, aunque hay otros paradigmas minoritarios como las redes Punto a Punto (P2P), los sistemas maestro-esclavo o el modelo Remote Procure Call (RPC) de Sun.

Modelo OSI	
Capas	**Protocolos**
7) Aplicación	FTAM, X.400, X.500
6) Presentación	ASN.1, Videotex, Unicode, MIME, HTML, XML, ...
5) Sesión	RTSP, H.323, H.248, SIP, RPC, ...
	NetBT, SMB, SSL, TLS, ...
4) Transporte	TCP, UDP, SCTP, RTP, SPX, TCAP, DCCP, ...
3) Red	NetBEUI, OSPF, ...
2) Enlace	MPLS, SNA, ...
	Ethernet, Token Ring, LocalTalk, FDDI, X.21, X.25, Frame Relay, BitNet, CAN, ATM, Wi-Fi, HDLC, SDLC, CSMA/CD, CSMA/CA, ...
1)Física ISO 10022 CCITT X.211	RS-232, RS-449, EIA-422, EIA-485, V.21-V.23, V.42-V.90, ...
	Códigos NRZ, Codificación Manchester, Cable coaxial, Par trenzado,10Base2, 10BASE5, 10BASE-T, 100BASE-TX, PDH, SDH, T-carrier, E-carrier, SONET, DSSS, FHSS, ...

Figura 1.17 Protocolos utilizados en las diferentes capas del Modelo OSI

El Modelo TCP/IP

El TCP/IP es actualmente el protocolo más ampliamente utilizado por su independencia del Sistema Operativo y hardware utilizado. Es un eficaz protocolo orientado por paquetes; es particularmente adecuado como plataforma para protocolos de los más distintos servicios y aplicaciones que se pueden conseguir a través de la red.

TCP/IP no es un único protocolo, sino que en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y le IP (Internet Protocol), que son los que dan nombre al conjunto. Se diferencian cuatro capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI como se muestra la Figura 1.17.

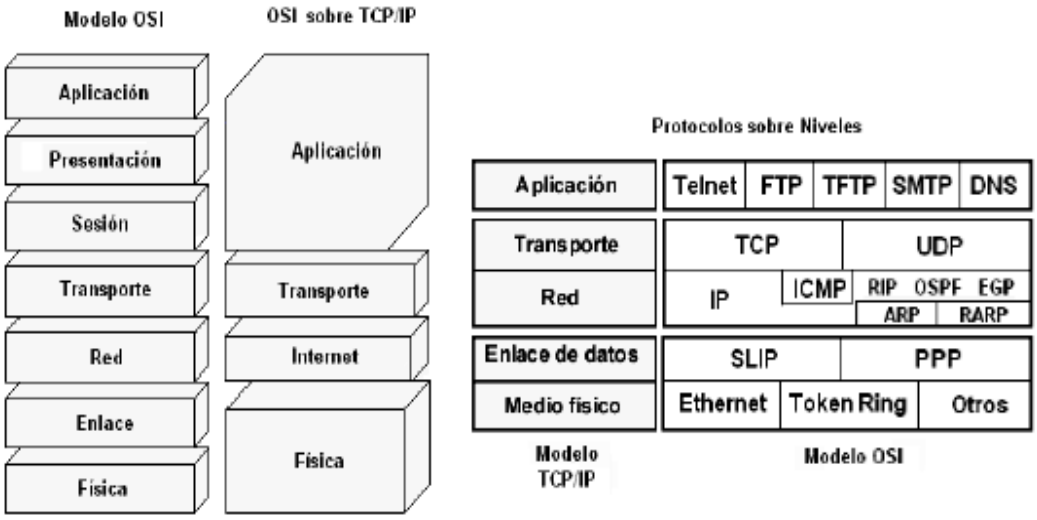


Figura 1.18 Comparación Modelo OSI-TCP

Las capas del Modelo TCP/IP serán descritas a continuación:

Interfaz de red. Correspondiente al nivel de Enlace Físico del Modelo OSI. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada Host, como puede ser una línea punto a punto o una red Ethernet.

La capa inferior, que podemos nombrar como Física respecto al modelo OSI, contiene varios estándares (conocidos con el nombre del IEEE 802.X) que establecen las reglas para enviar datos por cable coaxial delgado (10Base2), cable coaxial grueso (10Base5), par trenzado (10Base-T), fibra óptica (10Base-F) y su propio método de acceso.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y

ventajas principales del TCP/IP es proporcionar una abstracción del medio; de forma que sea posible intercambiar información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, esta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren. En TCP/IP cada una de estas unidades de información recibe el nombre de "Datagrama" (datagram), y son conjuntos de datos que se envían como mensajes independientes.

Internet. Es el nivel de Red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a los destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

Transporte. Coincide con el nivel de Transporte de modelo OSI. Esta capa está implantada por dos protocolos: el Transmission Control Protocol (TCP) y el User Datagram Protocol (UDP). El primero es un protocolo confiable y orientado a conexiones, lo cual significa que ofrece un medio libre de errores para enviar paquetes. El segundo es un protocolo no orientado a conexiones (connectionless) y no es confiable (unreliable) el TCP se prefiere para la transmisión de datos a nivel red de área amplia y el UDP para redes de área local.

Aplicación. Se corresponde con los niveles OSI de Aplicación, Presentación y Sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de archivos (FTP), conexión remota (Telnet) y otros más recientes como el protocolo HTTP (Hipertext Transfer Protocol).

Funcionamiento

Las aplicaciones de red presentan los datos a TCP. Este divide los datos en trozos o paquetes, y le otorga a cada uno un número. El conjunto de paquetes ordenados pueden representar imágenes, documentos, videos, o cualquier otra información que el usuario desee enviar.

Luego, TCP presenta los datos a IP, quien agrega su información de control (como su dirección de origen y destino). Si por algún motivo IP no puede entregar algún paquete, TCP pedirá el reenvío de los faltantes. Por último TCP se encarga de reensamblar los paquetes en el orden correcto, basándose en los números asignados previamente.

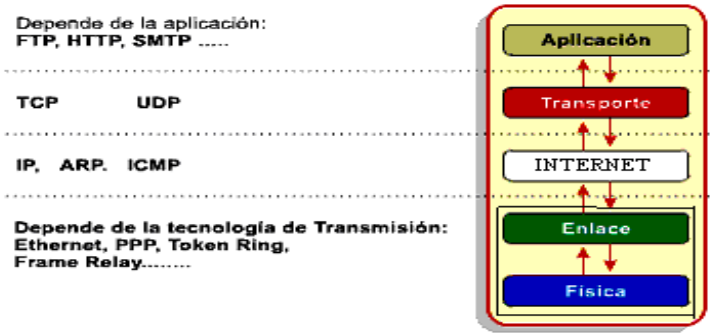


Figura 1.19 Diagrama de bloques del Modelo TCP/IP

Comparación con el Modelo OSI

Si bien TCP/IP está basado en el Modelo OSI, este último no tuvo éxito debido a causas como el momento de su introducción, la tecnología existente en ese momento, malas implementaciones y políticas por parte de los investigadores. Sin embargo el Modelo OSI es un buen modelo y TCP/IP es un buen conjunto de protocolos y la combinación de ambos es la que permite contar con las comunicaciones que se tienen hoy.

El modelo TCP/IP no tiene bien divididas las Capas de Enlace de Datos, Presentación y Sesión y la experiencia ha demostrado que en la mayoría de los casos son de poca utilidad.

Los estándares 802.X junto con el protocolo IP realizan todas las funciones propuestas en el modelo OSI hasta la Capa de Red. Los protocolos TCP y UDP cumplen con la Capa de Transporte.
Finalmente, las aplicaciones ya mencionadas son ejemplos prácticos y reales de la funcionalidad de la Capa de Aplicación.

Gráficamente pueden apreciarse las siete capas del modelo y su relación directa en su implementación sobre el protocolo TCP/IP como lo muestra la Figura 1.19.

1.5.6 Clasificación por cobertura.

Una de las principales características de las redes, es su cobertura, ya que de acuerdo al número de clientes y los diferentes dispositivos (elementos) que la componen definen a la misma, Las redes son clasificadas de la siguiente manera.

- **Redes de Área Locales (LAN)**

LAN son las siglas de Local Área Network (red de área local), y su utilidad primordial radica en el hecho de poder enlazar microcomputadoras originalmente aisladas, permitiendo a las personas que las utilizan establecer un nivel de comunicación y compartir recursos. El poder compartir eficiente los recursos y la comunicación efectiva redunda normalmente en un ahorro sustancial de tiempo y de dinero, provee una comunicación de alta velocidad (10-100 Mbps) y corta distancia entre dispositivos inteligentes como PC’s, ver figura 1.20.

Mientras más rápidamente puedan comunicarse los individuos, mucho mejor podrán trabajar. Cuando las computadoras en las que trabajan las personas están enlazadas, es más fácil establecer la comunicación, y de esa forma pueden trabajar eficientemente. Imaginemos, por ejemplo, el tratar de manejar una empresa sin teléfonos.

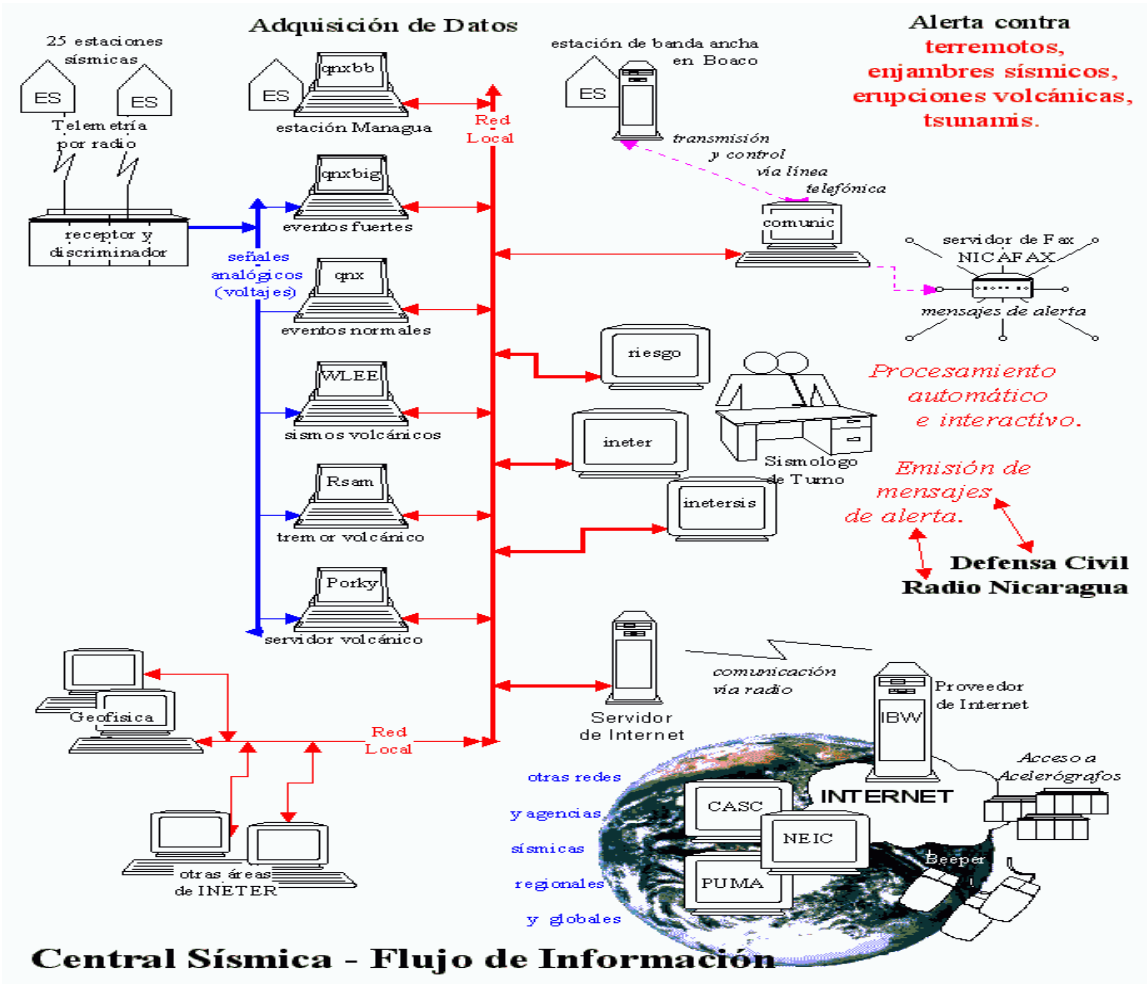


Figura 1.20 Red de Área Local (LAN)

- **Redes de Área Metropolitana (MAN)**

Son redes con cobertura urbana concebidas inicialmente para vincular distintas redes LAN entre ellas, formando lo que se denomina una internet. Sirve como la red principal (backbone) que interconecta varias LAN'S distribuidas o puede proveer acceso a la red metropolitana o a una red pública de cobertura amplia. Al decir cobertura urbana, decimos que su extensión (el largo del cable que las vincula) se mide en metros, pudiendo llegar a ciudades grandes en segmentos de 50 kilómetros. Transportan señales a velocidades de 102 Mbps (por ejemplo, 100 Mbps FDDI y 155 Mbps DQDB), utilizando para ello fibra óptica, 101 Mbps (por ejemplo, en Trama de 2 Mbps) usando fibra óptica, coaxial y par no trenzado y 10-1 Mbps (por ejemplo, conexiones en 64 Kbps y 128 Kbps) usando recursos generalmente telefónicos. Prestan servicios de transporte para interconexión de redes, telefonía con PBX, etc. Pueden ser de conmutación de circuitos o de paquetes con servicios orientados o no a la conexión (Figura 1.21).

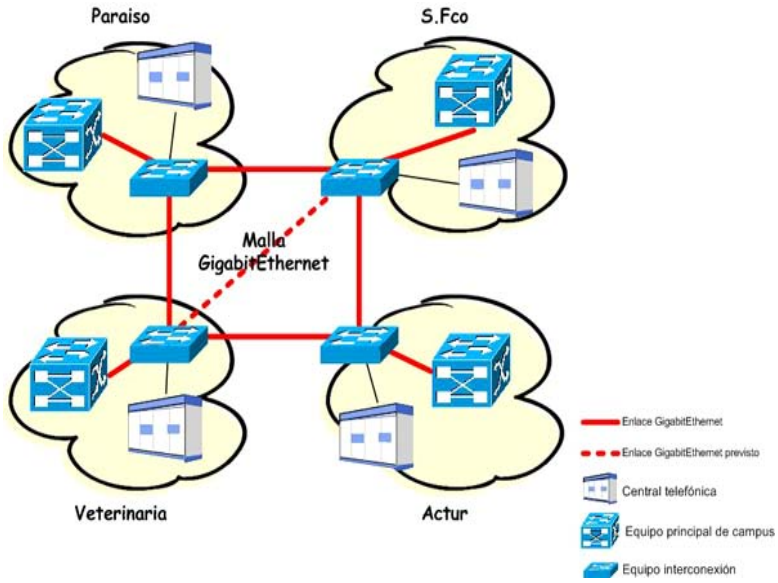


Figura 1.21 Red de Área Metropolitana (MAN)

- **Redes de Área Amplia (WAN)**

Estas redes también son llamadas de área extendida o área extensa, y en la práctica son de cobertura ilimitada, ya que encadenan diferentes redes de cobertura menor. Para poder hacerlo, se valen generalmente de redes públicas y privadas, utilizando todo tipo de vínculos: no tangibles, como satélite y radio enlace, y tangibles, como pares de cobre, coaxiales y fibras ópticas. Son necesariamente utilizadas para poder comunicarse más allá de un edificio, cuando no existe una MAN, o más allá del alcance de la misma, y por lo tanto dan servicios de todo.

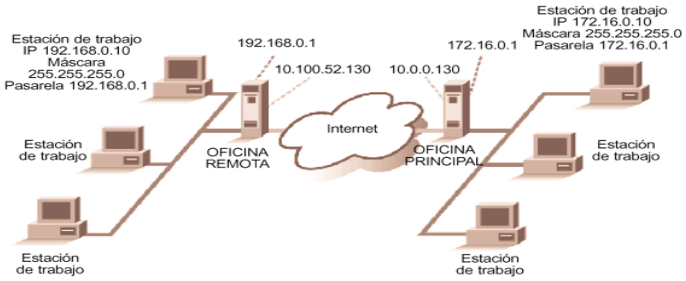


Figura 1.22 Red de Área Amplia (WAN)

1.5.7 Señalización de LAN's

- **Banda Base (BaseBand)**

Es la técnica de señalización más difundida dentro de las redes de computadores. Es una técnica de señalización digital. Las transmisiones se hacen por impulso, son pulsos discretos, el ancho de banda es utilizada en su totalidad. La comunicación utilizada es bidireccional.

Para la regeneración de la señal se utiliza un dispositivo bien conocido llamado repetidor, el cual trabaja solamente con señales digitales y además de un umbral.

- **Ancho de Banda (BroadBand)**

La señalización es analógica y puede representar como una curva ovulante. La comunicación es unidireccional, no se puede transmitir en el mismo medio.
También necesita de un dispositivo para la regeneración de la señal cuando se llega al límite de distancia, este dispositivo se llama amplificador. Esta señalización se utiliza por la tecnología 10Broad-36, es una tecnología que está englobada por Ethernet.

1.5.8 Medios de Transmisión

Introducción

El medio de transmisión es por donde viajan las señales de información, los estándares hoy en día sólo se especifican para redes de área local. Sin embargo también existen medios de transmisión inalámbricas implementadas mediante la utilización de tecnologías de Spread Spectrum o Radio Frecuencias, Infrarrojo y Láser.

El medio de transmisión consiste en el elemento que conecta físicamente las estaciones de trabajo al servidor y los recursos de la red. Entre los diferentes medios utilizados en las Redes Locales se puede mencionar: el cable de par trenzado, el cable coaxial, la fibra óptica y el espectro electromagnético (en transmisiones inalámbricas).

Su uso depende del tipo de aplicación particular ya que cada medio tiene sus propias características de costo, facilidad de instalación, ancho de banda soportado y velocidades de transmisión máxima permitidas.

Tipos de Medios de Transmisión

Cable de Par Trenzado. Esta clase de cableado se encuentra formada por diferentes hilos conductores que se trenzan entre sí para protegerse del ruido ambiental. Es el cableado más económico y fácil de instalar. Puede alcanzar los 100m de distancia (sin experimentar amortiguamientos de la señal) y una velocidad que oscila entre los 10 y los 100 Mbps.

A continuación se mencionaran los tipos de cables y sus características:

- **Cable UTP o Unshielded Twisted Pair**. Cable sin apantallar, formado por cuatro pares de hilos conductores. Además, los cables UTP se pueden subdividir en diferentes categorías:

    - **Categoría 3.** Este tipo de cables puede alcanzar velocidades de transmisión de 30 Mbps.
    - **Categoría 5.** Es el tipo de cable que se utiliza más a menudo. Puede alcanzar velocidades de transmisión de 100 Mbps.

Podemos observar en la figura 1.23, el aspecto de un par trenzado UTP, el conector hembra y el conector macho, respectivamente:

Figura 1.23 Aspecto de un cable UTP

Por ejemplo, al conectar todas las computadoras a un concentrador mediante un par trenzado, y sin necesidad de utilizar un servidor principal, podemos diseñar una red muy sencilla, perfectamente válida para compartir recursos y que se puede ampliar con facilidad hasta ocupar todos los puertos del concentrador.

Cable STP o Shielded Twisted Pair. Cable de cuatro pares de conductores trenzados con impedancia nominal de 100 Ohms. Están certificados por estándares internacionales para soportar aplicaciones que trabajan desde 10Mhz hasta 100 Mhz según la clasificación particular para cada frecuencia de trabajo. Este tipo de cable permite reducir el porcentaje de error, es un tipo de cable blindado, el cual proporciona cierta inmunidad al ruido y permite extender la longitud del cable a instalar.

Cable coaxial. Dispone de un único conductor interno y de varias capas de protección. Se puede encontrar cable grueso y delgado (RG-58A/U). En distancias no superiores a los 300m con 30 nodos en normativa extendida y de 150m con 15 nodos en normativa estándar, permite velocidades de transmisión de 20 Mbps, y en distancias cortas (no superiores a un lm) puede alcanzar los 100 Mbps. El cable coaxial, en comparación con el par trenzado, reduce los problemas de amortiguamiento de la señal en largas distancias, y el porcentaje de potencia que se pierde en forma de radiación. Es muy sensible a las acciones de posibles espías y susceptible al ruido producido por los aparatos eléctricos (por ejemplo, un motor).

Para conectar diferentes segmentos de cable coaxial se utilizan conectores BNC. Para conectar una computadora a la red, se utilizan conectores BNC en forma de T.

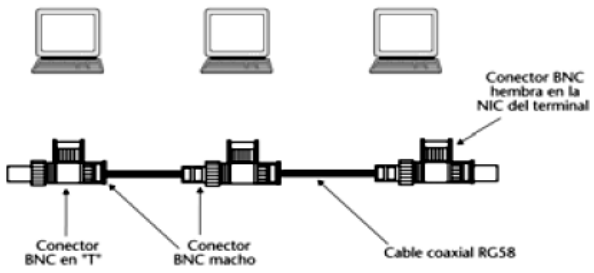


Figura 1.24 Conexión de una computadora a la red con cable coaxial

Fibra óptica. Consiste en un tubo de vidrio o plástico muy delgado a través del cual viaja información en forma de energía luminosa, es decir, la información es convertida de un formato digital a la luz para ser transmitida, lo que permite manejar un ancho de banda muy alto y puede conseguir velocidades de transmisión del orden de centenares de Mbps e incluso Gbps. La fibra óptica experimenta una reducción mínima de la señal, es inmune a las interferencias electromagnéticas y resulta difícil de interceptar y espiar, dado que no emite ninguna señal que pueda ser monitorizada. Por lo general, se utiliza conjuntamente con otros tipos de cableado.

1.5.9 Conectividad de redes

La conectividad de redes se refiere a los métodos de acceso que son las reglas que deben seguir las estaciones de trabajo para accesar al medio y transmitir su información en forma ordenada, evitando así colisiones con la consecuente pérdida de datos. Permiten también el direccionamiento de la comunicación entre estaciones. Los métodos utilizados se detallan a continuación:

Acceso Múltiple con Sensibilidad de Portadora, con Detección de Colisión (CSMA/CD): Es un método en el que la estación de trabajo sensa el medio antes de hacer una transmisión; si el medio está ocupado espera un tiempo determinado antes de volver a sensar, cuando detecta que ninguna estación está transmitiendo comienza su envío. Es posible que dos estaciones transmitan al mismo tiempo por hacer la detección simultáneamente, por lo tanto habrá una colisión. Cuando ocurre esto, ambas máquinas vuelven a esperar un tiempo aleatorio para iniciar el proceso. Se usa principalmente en redes con topologías bus.

Acceso Múltiple con Sensibilidad de Portadora Evitando Colisiones (CSMA/CA). Es una variante del CSMA/CD en el cual la característica principal es evitar las colisiones y no sólo detectarlas.

Token Passing. Se basa en el envío de paquetes de información que contiene tanto la dirección del destino como la información a transmitir. Una vez liberada la información, el paquete está libre y disponible para que otra estación pueda utilizarlo. El paquete viaja en una dirección definida por lo que no existen problemas por colisión y permite a todos los usuarios la posibilidad de accesar la red con más facilidad.

1.5.10 Estándares en LAN's

Dentro de las redes de área local se definen estándares. El Institute of Electrical and Electronics Engineers (IEEE) es un organismo, que data de 1980, quien elaboró las normas **IEEE 802.X**, las cuales definen los estándares con respecto al funcionamiento de las redes de área local.

IEEE 802.3. Estándar basado en la versión 2.0 de la red **Ethernet**. Define una red con topología de bus y método de acceso CSMA/CD (todos los terminales pueden acceder simultáneamente al medio y compiten por la utilización del canal de comunicación). Su campo de aplicación se encuentra en entornos técnicos, oficinas, universidades y hospitales.

Características	ETHERNET	10 BASE 5	10 BASE 2	10 BROAD 36	1 BASE 5	10 BASE T	10 BASE F
Medio	Coax. 50 Ohms Grueso	Coax. 50 Ohms Grueso	Coax. 50 Ohms Delgado	Coax. 75 Ohms	UTP	UTP	Fibra ptica
Señalización	Baseband	Baseband	Base band	Broadband	Base band	Base band	Base band
Topología	Bus	Bus	Bus	Bus	Estrella	Estrella	Estrella
Dist. Del Segmento	500 Mts	500 Mts	185 Mts	1800 Mts	250 Mts	100 Mts	<4 Kms
Velocidad de Transferencia	10 Mbps	10 Mbps	10 Mbps	10 Mbps	10 Mbps	10 Mbps	10 Mbps

Figura 1.25 Tabla comparativa

IEEE 802.4. Define una red con topología de bus y paso de testigo (sólo puede acceder al uso del canal el terminal que posea el testigo). Se utiliza en entornos industriales y se conoce con el nombre de *Token-bus*.

IEEE 802.5. Estándar basado en la red *Token-ring* de IBM. Define una red con topología de anillo y paso de testigo, la velocidad de transmisión de datos es de 4 Mbps ó 16 Mbps y método de acceso Token Passing. Se ha hecho popular en entornos de oficinas, con un nivel de implantación similar a las redes *Ethernet*.

Entre los estándares que han sido mencionados, posiblemente sean las redes *Ethernet* las que han gozado de más popularidad. La mayor parte de las implementaciones de redes *Ethernet* poseen velocidades de transmisión de 10 Mbps, las cuales serán mencionadas a continuación, según el cableado que se utilice (el primer número hace referencia a la velocidad en Mbps, y el segundo, a los metros que puede tener el segmento –multiplicado por cien, sin que la señal sufra debilitamientos–):

- **1Base-5.** Cable de par trenzado, con una velocidad de transmisión de 1 Mbps, y una longitud máxima de segmento de quinientos metros.
- **10Base-T.** Cable de par trenzado UTP, con una longitud máxima de segmento de cien metros, sobre una topología física de estrella.

- **100Base-T.** Similar al anterior, pero, con velocidades de transmisión de 100 Mbps (llamadas también, ***fast Ethernet***).

- **10Base-5 (*thick wire*).** Cable coaxial grueso, con una velocidad de transmisión de 10 Mbps. Acepta incluso cien estaciones de trabajo, en segmentos de longitud no superiores a los quinientos metros.

- **10Base-2 (*thin wire*).** Cable coaxial delgado, con una velocidad de transmisión de 10 Mbps. Acepta incluso treinta puestos de trabajo, en segmentos de longitud que no rebasen los ciento ochenta y cinco metros.

- **10Base-F.** Fibra óptica, con velocidades de transmisión de 10 Mbps.

100 VGAnyLAN. Definida por el estándar IEEE 802.12 para soportar tanto a topología Ethernet y Token Ring también es una tecnología para alta velocidad (100 Mbps). Introduce un nuevo concepto en cuanto al método de acceso llamado Método de Acceso Prioritario por Demanda (DPAM).

FDDI (**Interfaz de Datos Distribuida por Fibra)**. Es una tecnología más de MAN que de LAN, utiliza topología lógica de anillo y método de acceso Token Passing pero permite transmisión de datos a 100 Mbps y su medio de transmisión es la fibra óptica, por lo que accede a mayores distancias de operación. No está estandarizado por la IEEE sino por el Instituto Nacional de Estándares Americanos (ANSI) como X3T9.5.

FDDI define el uso de 2 tipos de fibra: monomodo y multimodo. En la monomodo da una mayor distancia debido a que maneja en su transmisor de luz un rayo láser, y en la fibra multimodo el generador de luz es un diodo emisor de luz (LED), lo que proporciona una distancia mucho menor.

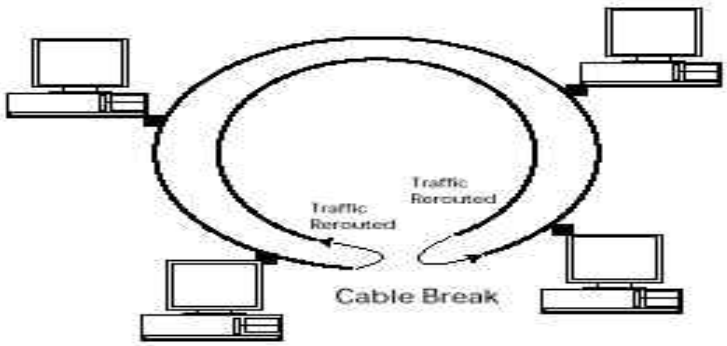


Figura 1.26 FDDI

1.5.11 Dispositivos de red

En la actualidad hay un gran número de dispositivos que conectan distintos tipos de redes, todos ellos cumplen una función muy importante dentro de una red. Además de que dependiendo del tipo de red, se necesitarán uno o varios dispositivos funcionando al mismo tiempo, A continuación se describen cada uno de estos dispositivos.

Repetidores. Son dispositivos “no inteligentes” que amplifican la señal y evitan los problemas de amortiguamiento que se producen cuando el cable alcanza cierta distancia (recordamos que, según el cableado que se utilice, estas distancias varían). Con la ayuda de repetidores es posible aumentar la longitud dentro de una red LAN, con la restricción del tipo de cable que se esté usando.

El repetidor es un dispositivo que trabaja en capa 1 (Physical Layer) dentro del modelo OSI.

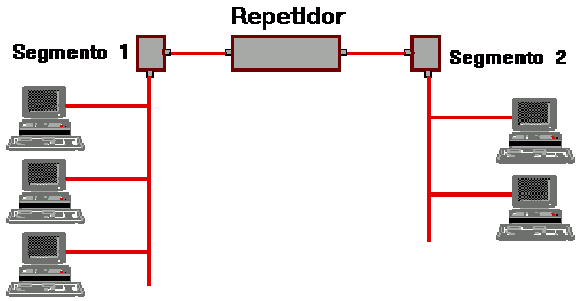


Figura 1.27 Repetidor

Uno de los problemas que surgen con los Repetidores, es que al unir dos segmentos se comparte el mismo ancho de banda. En cuanto a limitantes es que el número máximo de estos que pueden compartir el mismo ancho de banda es de cuatro.

Puente (Bridge). Conecta entre sí dos segmentos de red que pueden ser diferentes. A diferencia del repetidor, el puente resulta bastante “inteligente” para filtrar el tráfico de información entre los segmentos. Con la incorporación de un puente, cada segmento cuenta con una dirección distinta, de forma que la información siempre se direcciona hacia su destinación y se evitan los cuellos de botella habituales cuando todos los terminales de trabajo se conectan en el mismo segmento.

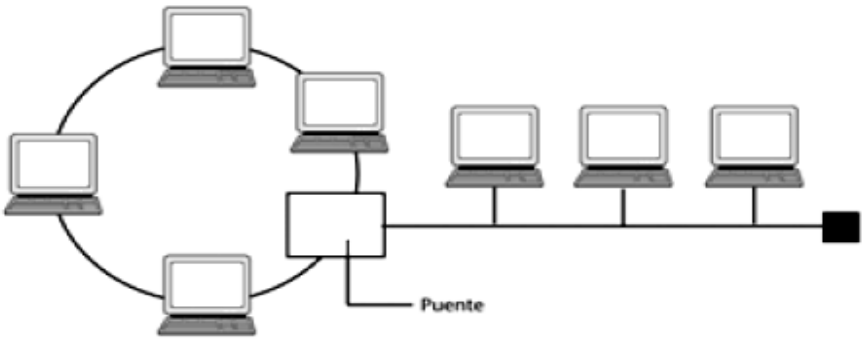


Figura 1.28 Interconexión de redes mediante un puente

Switch. El switch es la derivación de un Puente (Bridge). La diferencia primordial es que el Switch utiliza tablas estáticas a diferencia de tablas dinámicas como en el Puente (Bridge). Es un dispositivo que trabaja en la capa 2 y las direcciones son estáticas (no cambian). El Switch se usa en redes WAN.

Un Switch es muy similar a un Bridge Multipuerto. La diferencia es que un Puente (Bridge) aloja cada frame, lo examina y toma una decisión. El Switch únicamente ve el destinatario e inmediatamente toma una decisión del puerto por donde enviar el frame. Esto hace un decremento en el Delay. Un Switch es utilizado únicamente para una conexión Punto a Punto con respecto a la Red troncal (backbone) se denominan de esta manera los cables principales que conectan entre sí los segmentos de una red local. Habitualmente, funcionan como enlaces de alta velocidad (por ejemplo, fibra óptica).

Figura 1.29 Switch

Ruteador (Router). Dispositivos que gestionan el tráfico de paquetes que proviene del exterior de la red y se dirige al interior (y al revés). Un Ruteador (Router) ayuda a la unión de dos redes a nivel capa 3, pueden ser dispositivos muy sofisticados y capaces de actuar en calidad de cortafuego (Firewall). Son similares a los puentes (Bridges), pero al contrario que éstos, ofrecen servicios de encaminamiento de los datos que se transmiten; es decir, no sólo pueden filtrar la información, sino que también pueden encontrar la ruta de destinación más eficiente para los paquetes de información que se transmiten.

Un Router se compone de:

- Interfaz de Red. Conecta el Router a uno o más redes que usan protocolos de capa 3. Así, pueden unir redes Ethernet con redes Token Ring si ambas están trabajando sobre el mismo protocolo de capa 3 como pueden ser ambas sobre IP, sobre Novell, etc.
- Tabla de Ruteo.
- Algoritmo de Ruteo. Ejemplos de Algoritmos de Ruteo basados en Distance-Vector puede ser Protocolo de Información de Ruteo (RIP) o Open Shortest Path First (OSPF) para un algoritmo basado en Algoritmos de Ruteo (Link-State).

Para la utilización de algoritmos de ruteo, debe tomarse en cuenta:

- Velocidad de Convergencia. Convergencia lograda cuando todos los ruteadores han descubierto la mejor ruta posible.
- Memoria y Cómputo. Distance-Vector usa menos memoria que Link-State, pero misma capacidad de cómputo.
- Bandwidth: Velocidad de transmisión de bits por unidad de tiempo, típicamente por segundo
- Tolerancia a errores. Ambos son propensos a fallas.
- Funcionalidad. Link-State ofrece mayor flexibilidad en términos de resolución de problemas que Distance Vector.

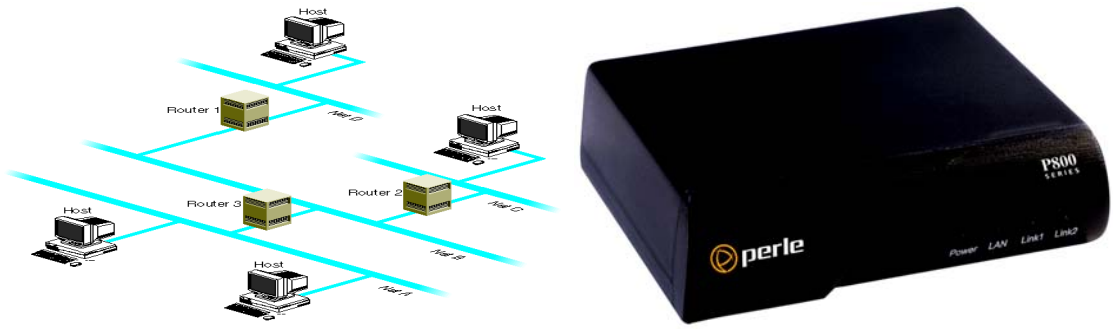


Figura 1.30 Ruteador (Router)

Concentrador (Hub). Son dispositivos que permiten compartir una línea de comunicación entre diferentes computadoras que tienen la finalidad de crear Grupos de Trabajo (Workgroup). Repiten toda la información que reciben, de manera que, a su vez, le puedan recibir todos los dispositivos conectados a sus puertos.

Dentro de este mismo punto se mencionará una definición importante:

Grupo de Trabajo (Workgroup): Conjunto de dispositivos (estaciones de trabajo, PC´s, impresoras, modems, plotters, etc.) que interactúan entre sí para un fin común. Un Grupo de Trabajo puede ser un departamento, un equipo de trabajo, etc. Todos los que forman el Grupo de Trabajo comparten software, datos y periféricos.

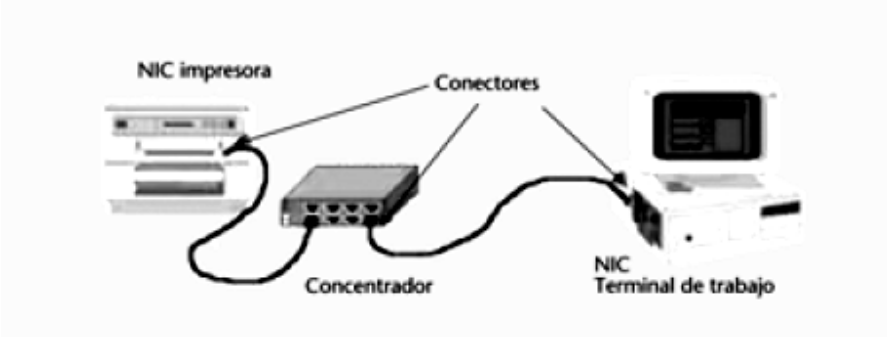


Figura 1.31 Ejemplo de configuración de un Concentrador (Hub)

1.5.12 Protocolos de red

En las redes, las computadoras deben de comunicarse entre sí e intercambiar datos con sistemas operativos y hardware muy distintos. En el nivel físico, esto se realiza a través de placas de redes, y una conexión entre las mismas. Lógicamente se debe de establecer una comunicación del mismo lenguaje, entre distintos sistemas operativos y palcas. Este lenguaje es lo que se llama protocolo.

Algunos protocolos se encargan de transportar datos, mientras que otros se encargan de la comunicación entre computadoras, y otros de convertir correctamente los datos. Así un Protocolo es el conjunto de normas (lenguaje de reglas y símbolos) que rigen cada tipo de comunicación entre dos computadoras para el intercambio de información.

Actualmente existen protocolos para cualquier tipo de comunicación; muchos de ellos han caido en el desuso y otros se encuentran en su plenitud de utilización. Esto es el producto de una sociedad cada vez más intercomunicada y relacionada, en donde lo importante es que la información llegue a su destino, pero también lo es que llegue en las mismas condiciones en que ha sido enviada y en el tiempo previsto.

Algunos de los protocolos más conocidos y difundidos son:

NETBIOS-NETBEUI-NWLINK-WINS

Network Basic Input Output System, es el protocolo más sencillo. Está compuesto por menos de 20 comandos que se ocupan del intercambio de datos. Se ha perfeccionado y ampliado recibiendo el nuevo nombre NETBEUI (Netbios Extended User Interface) pero continúa utilizando el juego de comandos NetBios y luego para hacerlo compatible con otros protocolos (como IPX/SPX) se amplio nuevamente recibiendo el nombre de NWLink (NetWare Link).

NetBios toma los puertos 137-139 en computadoras que utilizan el sistema operativo Windows de la empresa Microsoft. Está considerado el protocolo más fácilmente vulnerable de los existentes, a punto tal que cualquier especialista de seguridad recomienda no ser utilizado.

TCP/IP

En los años 80’s una gran cantidad de instituciones estaban interesadas en conectarse a una red que expandía por todo el mundo. Para esto definieron un conjunto de reglas que establecen como conectar computadoras entre sí para lograr el intercambio de información.

Actualmente TCP/IP se utiliza en la versión (IPv4) que no incluye la seguridad como, parte de su construcción. Sin embargo se encuentra en desarrollo (Ipv6 o IPSec) que dentro de sus estándares soporta autenticación, integridad y confidenciabilidad a nivel de datagramas.

Basado en las capas del modelo OSI, se definió un conjunto de protocolos de TCP/IP, que consta de 4 capas principales y que se ha convertido en un estandar a nivel mundial como ya ha sido descrito en este capitulo con anterioridad.

Modelo TCP/IP	
Capas	**Protocolos**
4) Aplicación	ICMP, FTP, HTTP, SMTP, POP, MIME, NNTP, SNMP
3) Transporte	TCP, UDP
2) Internet	IPX-SPX, IP, DNS, APPLE TALK
1) Física	ARP, SLIP
	RARP, PP

Figura 1.32 Tabla de Protocolos usados en el Modelo TCP/IP

IPX-SPX

El Internetwork Packet Exchange-Sequenced Packet Exchange es el protocolo de nivel de red de NetWare (para su sistema operativo Novell) siendo utilizados en las redes de tipo LAN.

TCP

TCP (Transmission Control Protocol), Protocolo de Control de Transmisión. Proporciona transporte de datos fiables de un nodo a otro mediante el uso de técnicas orientadas a la conexión.

El funcionamiento de TCP se basa en la filosofía de conmutación de paquetes, en la que un conjunto de información viaja por la red dividida en segmentos de información más pequeños e independientes. Cuando una aplicación de nivel superior entrega a la capa de transporte del Modelo OSI una información para enviar, éste la fragmenta en porciones de un tamaño fijo, añadiéndole a cada una las informaciones de control, entre las que se encuentra un número que define el orden en que han de volverse a unir los fragmentos para componer el mensaje original. Cada una de estas porciones de información se denomina paquete. Además, de este número de orden de los paquetes para su reordenación, cada uno necesita contener cierta información del destino y la capa de transporte correspondiente sepa a qué aplicación o servicio que corre por encima de él ha de entregarle los paquetes, esta información se proporciona colocándole a cada paquete un número de puerto que identifica la aplicación a la que va destinado. Los puertos, en el protocolo TCP, se numeran del 0 al 65.000, existiendo algunos números asignados a aplicaciones concretas, tales como el número 23, que indica aplicaciones Telnet, el número 25 aplicaciones de correo electrónico, etc.

Puerto	Aplicación	Protocolo	Descripción
20	FTP-Data	TCP/UDP	Transferencia archivos
21	FTP	TCP	Control Transferencia Archivos
23	TELNET	TCP/UDP	Servicio Remoto
25	SMTP	TCP/UDP	Envío de mails
43	Whois	TCP/UDP	
53	DNS	TCP/UDP	Servicio de Nombre de Dominios
70	Gopher	TCP/UDP	
79	Finger	TCP/UDP	
80	WWW-HTTP	TCP/UDP	World Wide Web
110	POP3 (PostOffice)	TCP/UDP	Recepción de mail
119	UseNet	TCP	Newsgropus de usuarios
137	NetBIOS	UDP	
194	IRC (Internet Relay Chat)	TCP/UDP	Chat
443	HTTPS	TCP	HTTP Seguro vía SSL
750	Kerberos	TCP/UDP	
6667	IRC (Internet Relay Chat)	TCP	Chat

Figura 1.33 Tabla de algunos puertos asignados a aplicaciones especificas.

IP

IP (Internet Protocol), Protocolo de Internet define la base de todas las comunicaciones en Internet. Es utilizado por los protocolos de nivel de transporte (como TCP) para encaminar los datos hacia su destino. IP tiene únicamente la misión de encaminar el datagrama, sin comprobar la integridad de la información que continué. Para ello se utiliza una nueva cabecera que se antepone el datagrama que se está tratando.

La cabecera IP tiene un tamaño de 160 bits y está formada por varios campos de destino significado entre los que se destaca el tipo de protocolo de transporte del datagrama, el número de paquete (para su posterior ensamble), la dirección de origen y la de destino, etc.
Cabe notar que este protocolo no garantiza la llegada de los paquetes a destino (conexión sin garantía) ni su orden; tan solo garantiza la integridad del encabezado IP. La fiabilidad de los datos deben garantizar los niveles superiores. También, se trata de una transmisión sin conexión porque cuando se envía el paquete, no se avisa al receptor para que esté preparado (no existe una conexión directa emisor-receptor). De hecho, muchas veces se mandan paquetes a un destino inexistente o que no se encuentra disponible.

El Protocolo IP identifica a cada equipo que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bits que debe de ser único para cada Host, y normalmente suele representarse como cuatro cifras de 8 bits separadas por puntos (por ejemplo 205.025.076.223).

En el nivel IP se definen los siguientes aspectos de intercambio de información:

- Un mecanismo de direcciones que permite identificar de manera unívoca al emisor y al receptor, sin considerar las ubicaciones ni las arquitecturas de las redes a las cuales pertenece cada uno. Este mecanismo permite la universalidad de la red.
- Un concepto relativo al transporte de los paquetes de los datos, para que el mismo llegue al receptor a través de los nodos de las redes involucradas. Dentro de cada red tendrá que haber al menos un receptor (Router) que esté conectado con otra computadora en otra red en el exterior. Los Routers reconocen un paquete y comprueban que no sea para alguna máquina conectada a su red y entonces lo mandan a otra, más cercana al destino. Esto se hace sucesivas veces hasta que el paquete llega al Router de la red donde se encuentra la computadora destinataria del mensaje.
- Un formato para los paquetes (cabecera). Con esto, el Router podrá identificar al destinatario del mensaje, ya que como se explicó, uno de los datos de la cabecera es el nombre del destino del mensaje.

La dirección IP se utiliza para identificar tanto a la computadora en concreto como la rede a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentren conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron cuatro clases diferentes.

Los cuales se representan mediante tres rangos de valores:

- Clase A: Son en las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar a la red, quedando los otros tres bytes disponibles para cada uno de las computadoras (Hosts) que pertenezcan a una misma red. Esto significa que podrán existir más de dieciséis millones de Hosts en cada una de las 126 redes de esta clase. Este tipo de direcciones es usado por redes muy extensas.
- Clase B: Estás direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, debiendo ser un valor entre 128.001 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos primeros bytes de la dirección constituyen el identificador de la computadora permitiendo, por consiguiente, un número máximo de 64,516 computadoras en la misma red. Este tipo de direcciones tendría que ser suficiente para la mayoría de las organizaciones grandes.
- Clase C: En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.001.001.001 hasta 223.254.254.254 De está, manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 computadoras en cada red.
- Clase D: Está clase se usa con fines de multidifusión a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.255.255.

Actualmente se planea la utilización de la clase E que comprendería el rango 240.0.0.0 hasta 247.255.255.255.

CAPÍTULO 2

TEORÍA DE SEGURIDAD

2.1 ¿Qué es seguridad?

La seguridad informática como materia académica no existe, y es considerada por los estudiosos como una herramienta dentro del ámbito en que se le estudia. Muchos sostienen que es una teoría tan amplia, compleja y abstracta. 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.

“La Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella”. Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 A.C.) o el Hammurabi (2000 A.C.). Los descubrimientos arqueológicos marcan, sin duda, las más importantes pruebas de seguridad de los antiguos: las Pirámides Egipcias, el Palacio de Saron, El Templo Karnak en el valle del Nilo; el Dios Egipcio Anubi representando una llave en su mano, etc.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo, para eliminar o evitar la causa. Así la pugna por la vida se convertía en la parte esencial y los conceptos de alertar, detectar, alarmar y reaccionar ya eran manejados por ellos.

Con todo concepto, la seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La primera evidencia de una cultura y organización en seguridad madura aparece en los documentos de la Roma Imperial y Republicana. El próximo paso de la seguridad fué la especialización, así nace la Seguridad Externa (aquella que se preocupa por la amenaza de agentes externos hacia la organización y la Seguridad Interna (aquella preocupada por las amenazas de agentes internos dentro de la organización).

Desde el siglo XVIII, los descubrimientos científicos y el conocimiento resultante de la imprenta han contribuido a la cultura de la seguridad. Los principios de probabilidad, predicción y reducción de fallos y pérdidas han traído nueva luz a los sistemas de seguridad. La seguridad moderna se originó con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época.

Con la aparición de los cerebros electrónicos se mantuvo la idea de que las medidas de seguridad serian en la parte física, no se pensaba en otra medida de seguridad, ¿Quién sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?. Hoy en día desde el punto de vista técnico, la seguridad está en manos de las organizaciones, y en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

Es en este proceso donde se aprecia que no se ha añadido ningún nuevo concepto a los ya conocidos en la antigüedad; los actuales sólo son perfeccionamientos de aquellos.

2.2 Definiciones de Seguridad

El concepto de seguridad es borroso o su definición se maneja con cierto grado de incertidumbre teniendo distinto significado para las personas que para las cosas. Esto tiene la peligrosa consecuencia de que la función de seguridad puede ser frecuentemente etiquetada como inadecuada o negligente, haciendo imposible a los responsables justificar técnicas ante reclamos basados en ambigüedades de conceptos y definiciones.

A continuación se mencionarán algunas definiciones de seguridad:

1. Seguridad: Que impide algún peligro, daño, accidente, etc. O bien lo previene.

2. Seguridad: Condición de estar libre de peligro, daño, pérdida o falla.

3. Seguridad: Sin riesgo, con certeza.

4. Seguridad: Se refiere a todo tipo de precauciones y protecciones que se llevan acabo para evitar cualquier acción que comprometa a la información.

5. Seguridad: Calidad de seguro.

6. Seguridad: La seguridad es hoy en día una profesión compleja con funciones especializadas.

7. Seguridad: Prevenir y detectar amenazas. Responder de una forma adecuada y con prontitud ante un incidente.

8. Seguridad: Proteger y mantener los sistemas funcionando.

9. Seguridad: Garantía o conjunto de ellas que se da a alguien sobre el cumplimiento de un acuerdo.

10. Seguridad: Políticas, procedimientos y técnicas para asegurar la integridad, disponibilidad y confiabilidad de datos y sistemas.

Como se dijo anteriormente hemos visto que el concepto de seguridad es algo difícil de definir por que existe un sin fin de conceptos, dependiendo del punto de vista filosófico, operacional o práctico. Pero para nuestro tema de estudio, cada vez que se mencione a la información se estará haciendo referencia a la información que es procesada por un sistema informático: definiendo a éste último como el "conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones."

2.3 Servicios de Seguridad

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y los documentos.

Existe información que debe o puede ser pública, puede ser visualizada por cualquier persona y aquella que debe de ser privada. Sólo puede ser visualizada por un grupo selecto de personas que trabajan con ella. En esta última debemos maximizar nuestros esfuerzos para preservarla reconociendo las siguientes características de la información:

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

Como los sistemas de información llegan a ser cada vez más penetrantes y esenciales, la información electrónica toma muchas de las funciones tradicionalmente interpretadas por los documentos en papel. Así que los tipos de funciones tradicionalmente asociados con los documentos de papel deben de ser interpretados como documentos existentes de forma electrónica.

Es posible poder distinguir entre un documento original y una copia fotostática. Sin embargo, un documento electrónico es simplemente una secuencia de bits; no hay diferencia alguna entre el original y algún número de copias.

En este caso si nosotros quisiéramos hacer algún tipo de prueba de manera física en un documento se podría hacer de manera más evidente, algún tipo de borrado y en sí la misma firma; pero mientras que en un documento electrónico si se alteraran los bits en una computadora de dicho documento no darían evidencia de que fue alterado.

De esta manera debemos de asegurar que el documento electrónico que ha llegado a su destino debe de ser auténtico, por lo cual debemos de garantizar su seguridad de esta manera definimos lo siguiente; como algo importante que se debe de considerar.

Un **servicio de seguridad** es aquel que mejora un sistema de información y el flujo de información de una organización. Los servicios están dirigidos a evitar ataques y utilizan uno a más mecanismos de seguridad para proveer el servicio.

2.3.1 Clasificación

Una clasificación muy utilizada en los servicios de seguridad es la siguiente:

1. Confidenciabilidad.
2. Autenticación.
3. Integridad.
4. No repudio.
5. Control de acceso.

6. Disponibilidad.

1. - Confidenciabilidad.

La confidenciabilidad es la capacidad de asegurar que sólo las personas autorizadas tengan acceso a algo. La confidenciabilidad es un aspecto primario y sumamente importante en la seguridad, significa mantener la información secreta para proteger los recursos y la información contra el descubrimiento intencional o accidental por personal no autorizado, es decir, es la protección de datos transmitidos de cualquier ataque pasivo.

La confidenciabilidad es algo que está presente en nuestra vida diaria tanto en las organizaciones como con la gente, lo que deseamos es proteger todo aquello que no queremos que llegue a manos desconocidas. Si nos imaginamos el daño que provocaría si algún individuo o individuos tuvieran información privada acerca de nosotros o que alguna persona dentro de una compañía fuera capaz de tener acceso a la información secreta de dicha compañía y éste a su vez fuera un espía de otra compañía quien es la compañía competidora, tendría acceso a lo más valioso “la información”, los daños serían incalculables.

Los servicios de Confidenciabilidad proveen protección de recursos y de la información en términos del almacenamiento y la información, para asegurar que:

- Nadie pueda leer, copiar, descubrir o modificar la información sin autorización.
- Nadie pueda interceptar las comunicaciones o los mensajes entre entidades.

Estos dos aspectos de la Confidenciabilidad son llamados **confidenciabilidad de contenido** y **confidenciabilidad de flujo de mensaje**.

- **Servicios de confidenciabilidad de contenido:** Utilizando una técnica de cifrado para prevenir el descubrimiento no autorizado del contenido de un recurso de la red como un mensaje, un archivo o un registro de datos. Las formas de este tipo de servicio pueden ser en protección a un solo mensaje o campos específicos dentro de un mensaje.

- **Servicios de confidenciabilidad de flujo de mensaje:** Son provistos a través del cifrado y una técnica de envoltura para permitir al creador del mensaje ocultar el flujo de un mensaje lo cual procura que la información sea protegida.

La criptografía es utilizada para proveer los servicios de confidenciabilidad.

2. - Autenticación.

Es verificar la entidad. Esto es que la autenticidad garantiza que quien dice ser es realmente. Es decir, se deben implementar mecanismos para verificar quien esta enviando la información.

Es muy sencillo nosotros todos los días autenticamos algo por ejemplo cuando vamos al banco lo autenticamos por medio del logo, los colores y el nombre, o cuando realizamos algún tipo de

pago con la tarjeta de crédito la manera de autenticar que la tarjeta es de quien dice portarla es por medio de su firma.

El servicio de autenticación trata de asegurar que una comunicación sea auténtica. La autenticación es utilizada para proporcionar una prueba al sistema de que en realidad es la entidad que se pretende ser. El sistema verifica la información que alguien provee contra la información que el sistema sabe sobre esa persona.

La autenticación es realizada principalmente a través de:

a) Algo que se sabe. Una contraseña o un número personal de identificación, es algo que se sabe. Cuando se le provee al sistema, este lo verifica contra la copia que esta almacenada en el mismo sistema para determinar si la autenticación es exitosa o no.

b) Algo que se tiene. Una tarjeta o un pasaporte es un ejemplo de algo que se tiene, lo cual es utilizado por el sistema para verificar la entidad.

c) Algo que es. La voz, la retina, la imagen del rostro o una huella digital pueden identificar de quien se trata y pueden ser utilizadas en el proceso de autenticación.

3. - Integridad.
Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben de considerar elementos menos obvios como respaldos, documentación, registros del sistema, tránsito en una red, etc. Esto comprende cualquier tipo de modificaciones:

- Causadas por errores de hardware y/o software.
- Causadas de forma intencional.
- Causadas de forma accidental.
- Causadas por errores humanos.

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

Existen dos tipos de servicios de integridad. Servicio de integridad del contenido y servicios de integridad de la secuencia de mensaje.

- **Servicios de integridad del contenido.** Estos proveen pruebas de que el contenido no ha sido alterado o modificado por inserción o supresión.

- **Servicios de integridad de la secuencia del mensaje.** Proporcionan pruebas de que el orden de una secuencia de mensajes ha sido mantenida durante su transmisión.

Los servicios de integridad de los datos pueden ofrecerse a través de varios mecanismos de seguridad:

- **Código de detección de modificación.** Es una suma de comprobación de los datos generada utilizando un algoritmo criptográfico.
- **Código de autenticación del mensaje.** Es una suma de comprobación cifrada de los datos generada con base en la criptografía.

- **Firma Digital.** Es una pieza de información asociada con los datos que únicamente puede ser creada por el firmante y puede ser verificada por cualquier persona.

- **Número de secuencia del mensaje**. Identifica la posición del mensaje en la secuencia. Este número es transferido con el mensaje de manera normal o de manera cifrada.

4. - No repudio.

Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa. Los servicios de no repudio suministran pruebas que puedan ser demostradas a una tercera entidad. Los siguientes servicios son los que pueden ser proporcionados.

- **No repudio de origen.** Provee pruebas del origen de datos, con ello se previene a la entidad del origen de cualquier denegación falsa al suministrar los datos.

- **No repudio de envío.** Provee pruebas del envío de datos, por lo tanto previene a quien recibe los datos de cualquier denegación falsa al recibir los datos.

- **No repudio de presentación.** Provee pruebas de presentación de los datos, con ello protege contra cualquier intento de falso de negar que los datos fueron presentados para el envío.

- **No repudio de transporte.** Provee pruebas del transporte de los datos con lo que protege contra cualquier intento de negar que los datos fueron transportados.

- **No repudio de recepción.** Provee pruebas de recepción de los datos con esto se protege al emisor de que el receptor niegue haber recibido el mensaje.

5. - Control de Acceso.

Es la habilidad para limitar y controlar el acceso a los sistemas anfitriones y las aplicaciones mediante los puentes de comunicación. Para lograr este control, cada entidad que trata de ganar acceso, debe de identificarse primero o autentificarse, así que los derechos de acceso pueden ser adoptados de manera individual.

Ejemplos de los privilegios o permisos de una entidad:

- Creación o destrucción.
- Lectura o escritura.
- Adición, supresión o modificación del contenido.

- Exportación o importación.
- Ejecución.

6. - Disponibilidad.

La información debe estar presente para ser usada cuando se requiera y tantas veces como se desee. De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por tanto, se deben de proteger los servicios de cómputo de forma que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

2.4 Criterios de Seguridad

2.4.1 Antecedentes

A principios de los años 80, se desarrollaron en Estados Unidos los criterios de seguridad recogidos bajo el nombre de Trusted Computer System Evaluation Criteria (TCSEC) y editados en el famoso “libro naranja”. Más adelante, partiendo de estas bases, se desarrolló en Europa, en 1991, los Information Technology Security Evaluation Criteria (ITSEC) con la intención de hacer dichos criterios más flexibles y adaptables a la naturaleza cambiante de las tecnologías de la información.

A lo largo de la historia se han ido definiendo diferentes criterios y métodos de evaluación, con mayor o menor aceptación, hasta llegar a un punto en que la disparidad de criterios hizo necesaria una unificación. Es por ello, por lo que se han creado una serie de criterios comunes aprobados internacionalmente bajo el nombre de Common Criteria o Criterios Comunes. En la figura 2.0 se puede apreciar la evolución de las distintas certificaciones de seguridad hasta llegar a los Common Criteria.

Se pueden distinguir cuatro tipos de certificaciones:

- Certificación de la seguridad de las Tecnologías de la Información.
- Certificación de la seguridad criptográfica.
- Certificación de la seguridad de emanaciones electromagnéticas, conocida como TEMPEST.
- Certificación de la seguridad física de los propios productos de seguridad de las Tecnologías de la Información.

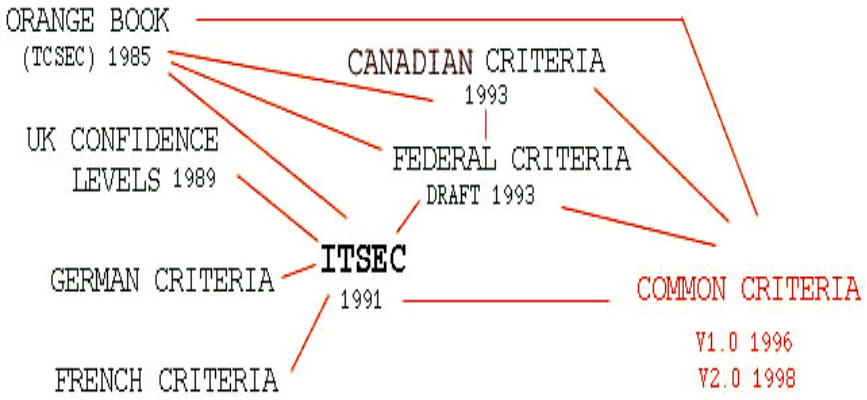


Figura 2.0 Desarrollo del COMMON CRITERIA

2.4.2 Los Criterios Comunes

Los Common Criteria (CC) nacen como resultado de grandes esfuerzos en el desarrollo de criterios de evaluación unificados. Se trata de una certificación con gran aceptación en la comunidad internacional y se ha convertido en un estándar ISO en el año 2000, concretamente, el estándar ISO-IEC 15408.

Utilizado para evaluar la seguridad (IT) de un determinado producto o sistema, total o parcialmente: Aplicaciones, redes, sistemas operativos, *chips*.

- TOE *(Target Of Evaluation)*: Parte del producto o sistema que es objeto de evaluación.

Más allá de estas consideraciones, lo que al usuario le interesa es conocer los beneficios que le puede proporcionar la adopción de los CC como estándar internacional. Estos beneficios se pueden concretar de la siguiente manera:

- Los usuarios pueden comparar sus requerimientos específicos frente a los estándares de los CC para determinar el nivel de seguridad que necesitan.
- Los usuarios pueden determinar más fácilmente cuándo un producto cumple una serie de requisitos. Igualmente, los CC exigen a los fabricantes de los productos certificados publicar una documentación exhaustiva sobre la seguridad de los productos evaluados.
- Los usuarios pueden tener plena confianza en las evaluaciones de los CC ya que no son realizadas por el propio fabricante del producto sino por laboratorios independientes.
- Debido a que los CC son un estándar internacional, proporcionan un conjunto común de estándares que los usuarios, con operaciones internacionales, pueden utilizar para escoger productos que se ajusten localmente a las necesidades de seguridad.
- Costos de soporte reducidos, ya que el producto está probado y documentado con detenimiento. Los problemas pueden ser identificados y corregidos sin necesidad de acudir, en la mayoría de los casos, al soporte técnico.

La Estructura del Common Criteria consta de tres partes diferenciadas

1. Introducción y modelo general.
2. Requisitos funcionales de seguridad:
   Definen el comportamiento de seguridad deseado del TOE ante diferentes amenazas.
3. Requisitos de aseguramiento:
   Definen las propiedades del TOE que proporcionan la confianza en su seguridad.

Los requisitos funcionales son los siguientes:

- FAU. Auditabilidad de la seguridad.
- FCO. Comunicaciones.
- FCS. Soporte criptográfico.
- FDP. Protección de datos de usuarios.
- FIA. Identificación y autenticación.
- FMT. Gestión de seguridad.
- FPR. Privacidad.
- FPT. Protección de las funciones de seguridad.
- FRU. Utilización de recursos.
- FTA. Acceso al TOE.
- FTP. Canales de comunicación cables.

Requisitos de Aseguramiento

- Gestión de configuraciones.
- Entrega y operación.
- Desarrollo de producto.
- Documentación del producto.
- Soporte durante el ciclo de vida.
- Pruebas de conformidad.
- Análisis de vulnerabilidades.

Validez de los certificados

No obstante, debemos ser cautos a la hora de evaluar si un certificado de seguridad garantiza que el producto cubre nuestras necesidades. Los certificados evalúan un producto bajo unas condiciones muy concretas y con unos requisitos muy específicos en un momento determinado. De esta manera, si los requisitos de seguridad son poco ambiciosos, quizá el producto no sea válido para nuestras necesidades. Es importante notar que, si el producto no se encuentra bajo las condiciones definidas en el certificado, es muy probable que la seguridad se vea comprometida. Éste es el caso de un sistema operativo certificado, al cual se le han instalado ciertas aplicaciones a posteriori que comprometen la seguridad del sistema y que, lógicamente, el proceso de certificación no ha podido contemplar. Puede ocurrir también que, tras un cierto periodo de tiempo, el producto deje de cumplir los requisitos de seguridad definidos, al descubrirse nuevas vulnerabilidades que comprometan la seguridad del mismo. Sin embargo,

como se comentó inicialmente, es interesante conocer el nivel de seguridad que nos garantiza un certificado.

Los Criterios Comunes proporcionan una escala de evaluación de aseguramiento formada por siete niveles EAL *(Evaluation Assurance Levels)*:

- EAL1. Funcionalmente probado.
- EAL2. Estructuralmente probado.
- EAL3. Metodológicamente probado y comprobado.
- EAL4. Metodológicamente diseñado, probado y revisado.
- EAL5. Diseñado y probado semiformalmente.
- EAL6. Diseño verificado y probado semiformalmente.
- EAL7. Diseño cerificado y probado formalmente.

Nivel – Objetivo

EAL1, Prueba funcional: Proporciona un análisis de las funciones de seguridad usando unas especificaciones funcionales y de interfaz de los Objetivos de Evaluación (TOE o Target of Evaluation), para comprender el comportamiento de seguridad. El análisis se basa en pruebas independientes de las funciones de seguridad.

EAL2, Prueba estructural: Proporciona un análisis de las funciones de seguridad usando unas especificaciones funcionales y de interfaz y un diseño de alto nivel de los componentes de los Objetivos de Evaluación. Pruebas independientes de las funciones de seguridad, con pruebas de desarrollo de “caja negra” y búsqueda de vulnerabilidades obvias.

EAL3, Prueba metodológica con chequeo: El análisis se basa en una prueba de “caja gris”, confirmación independiente del resultado de las pruebas de desarrollo y búsqueda de vulnerabilidades obvias. Son necesarios un control del entorno de desarrollo y una administración de la configuración de los Objetivos de Evaluación.

EAL4, Prueba, revisión y diseño metodológico: El análisis se basa en un diseño de bajo nivel de los módulos de los objetivos de evaluación y un subconjunto de la implementación. El test se basa en una búsqueda independiente de vulnerabilidades obvias. El control del desarrollo se basa en un modelo de ciclo de vida, identificación de las herramientas y administración automatizada de la configuración.

EAL5, Diseño y prueba semi-formal: El análisis incluye toda la implementación. La garantía está complementada por un modelo formal, una presentación semi-formal de las especificaciones funcionales, un diseño de alto nivel y una demostración semi-formal de la correspondencia. La búsqueda de vulnerabilidades debe asegurar una relativa resistencia a los ataques de penetración. Son también necesarios un análisis de canales protegidos y un diseño modular.

EAL6, Prueba y verificación de diseño semi-formal: El análisis se basa en una aproximación al diseño por capas y modular, y una presentación estructurada de la implementación. La

búsqueda independiente de vulnerabilidades debe asegurar una alta resistencia a ataques de penetración. La búsqueda de canales protegidos debe ser sistemática. El entorno de desarrollo y el control de la administración de la configuración son muy fuertes.

EAL7, Prueba y diseño formalmente verificados: El modelo formal se complementa con la presentación formal de las especificaciones funcionales y un diseño de alto nivel mostrando la correspondencia. Son necesarias una prueba de desarrollo de "caja blanca" y una completa confirmación independiente del resultado de las pruebas de desarrollo. La complejidad del diseño debe ser minimizada.

Si queremos evaluar la validez de un certificado, es indispensable que conozcamos el proceso de elaboración del mismo, desde la petición de certificación hasta la emisión del certificado por parte de un laboratorio legalmente reconocido. Antes de pedir la emisión de un certificado para un producto, debemos establecer unos objetivos de seguridad para el mismo y ajustarlo a los perfiles de seguridad del criterio seguido por la entidad certificadora. Una vez determinados los objetivos y el perfil, se deben establecer las condiciones bajo las cuales se certificará el producto y se deben determinar las especificaciones concretas del mismo. También se exige que se genere una documentación exhaustiva del producto a evaluar.

Además de los CC, existen otros estándares de certificación de seguridad muy utilizados como son los ITSEC (Information Technology Security Evaluation Criteria) y los FIPS (Federal Information Processing Standards). Ambos tienen objetivos más concretos que los CC, por lo que quizá los CC sean más útiles para evaluar un producto como un sistema operativo, amplio y difícil de ajustar a estándares determinados, y los estándares ITSEC y FIPS sean más útiles para evaluar productos más específicos, como un microcircuito que realiza un determinado cifrado, el cual debe cumplir un estándar muy concreto, etc.

Además de los laboratorios que oficialmente emiten certificados siguiendo los criterios definidos en los CC o en los ITSEC, existen otros laboratorios de prestigio y con criterios independientes. Éste es el caso de los ICSAlabs. Los ICSAlabs se han ganado el respeto y la reputación de muchos definiendo y emitiendo certificados para multitud de productos, desde soluciones antivirus, firewalls o IDS hasta los productos wireless más modernos. En la práctica, ICSAlabs probablemente sea más utilizado aún que CC, ITSEC o FIPS.

2.4.3 ISO 17799

El ISO 17799 es una norma internacional que ofrece **recomendaciones** para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización. 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 de la organización, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades del mismo.

2.4.3.1 Objetivo

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.

2.4.3.2 Historia

En 1995 el British Standard Institute pública la norma BS 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:

- Conjunto completo de controles que conforman las buenas prácticas de seguridad de la información. Aplicable por toda 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 sin apenas modificación (UNE 17799), y en 2004 se establece la norma UNE 71502, basada en BS7799-2 (no existe equivalente ISO).

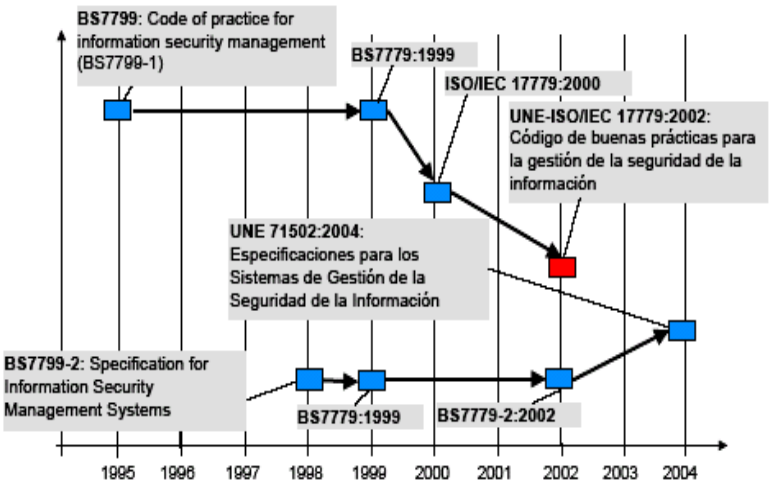


Figura 2.1 Evolución del ISO 17799.

2.4.3.3 Estructura (dominios de control)

La norma UNE-ISO/IEC 17799 establece **diez dominios de control** que cubren por completo la Gestión de la Seguridad de la Información.

Figura 2.2 Estructura.

Política de seguridad. Dirigir y dar soporte a la gestión de la seguridad de la información.

1. - Política de seguridad

Dirigir y dar soporte a la gestión de la seguridad de la información.

- La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de forma adecuada a todo el personal implicado en la seguridad de la información.
- La política se constituye en la base de todo el sistema de seguridad información.
- La alta dirección debe apoyar visiblemente la seguridad de la información en la compañía.

2. - Aspectos organizativos para la seguridad

- Gestionar 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 información de la organización que son accedidos por terceros.
- Mantener la seguridad de la información cuando la responsabilidad de su tratamiento se ha hecho externo a otra organización.

1. 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 cualquier forma.

2. Dicha estructura debe poseer un enfoque multidisciplinar: los problemas de seguridad no son exclusivamente técnicos.

3. - Clasificación y control de activos

Mantener una protección adecuada sobre los activos de la organización y asegurar un nivel de protección adecuado a los activos de información.

- Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad en la organización.

4. - Seguridad ligada al personal

Reducir los riesgos de errores humanos, robos, fraudes o el mal uso de las instalaciones y los servicios, asegurar que los usuarios son concientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están 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 la información son muy elevadas.
- Todo el personal, tanto interno como externo a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.
- Diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc.
- Procesos de notificación de incidencias claros, ágiles y conocidos por todos.

5. - Seguridad física y del entorno

Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización, evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización y prevenir las exposiciones a riesgo 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 criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, incendio...).

6. - Gestión de comunicaciones y operaciones

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 de la operación de los sistemas críticos para el negocio.

7. - Control de accesos

Controlar los accesos a la información evitar accesos no autorizados a los sistemas de información, de usuarios no autorizados. A computadoras, a la información contenida en los sistemas; detectar actividades no autorizadas, proteger los servicios de la red, así como garantizar la seguridad de la información cuando se utilizan dispositivos de informática móvil.

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

8. - Desarrollo y mantenimiento de sistemas

Asegurar que la seguridad está incluida dentro de los sistemas de información, que los proyectos de tecnología de la información y las actividades complementarias son llevadas a cabo de una forma segura; evitar las pérdidas, modificaciones o mal uso de los datos de usuarios en las aplicaciones, así como, mantener la seguridad del software y la información de la aplicación del sistema.

- Debe de 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, etc.

9. - Gestión de continuidad del negocio

Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos o desastres.

- Todas las situaciones que puedan provocar la interrupción de las actividades del negocio deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados.
- Los planes de contingencia deben de ser probados y revisados periódicamente.
- Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

10. - Conformidad con la legislación

Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad, garantizar la alineación de los sistemas con política de

seguridad de la organización y con la normativa derivada de la misma; maximizar la efectividad así como minimizar la interferencia de o desde el proceso de auditoría de sistemas.

- Se debe identificar convenientemente la legislación aplicable a los sistemas de información, integrándola en el sistema de seguridad de la información de la organización y garantizando su cumplimiento.
- Se debe definir un plan de contingencia de auditoría interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones.

2.4.3.4 Auditoría

El trabajo de **auditoría ISO 17799**: es la valoración del nivel de adecuación, implantación y gestión de cada control de la norma en la organización, proporciona **información precisa** acerca del **nivel de cumplimiento** de la norma a diferentes niveles: global, por dominios, por objetivos y por controles.
:

- Seguridad lógica.
- Seguridad física.
- Seguridad organizativa.
- Seguridad legal.

Referencia la seguridad de la información **estándar** y es aceptada internacionalmente. Una vez que conocemos el estado actual de la seguridad de la información en la organización, podemos **planificar** correctamente su mejora o su mantenimiento.

De estos diez dominios se derivan 36 objetivos 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).

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

- Nivel **mínimo aceptable**. Estado con las mínimas garantías de seguridad necesarias para trabajar con la información de la institución u organización.
- Nivel **objetivo**. Estado de seguridad de referencia para la organización, con un alto grado de cumplimiento ISO 17799.

A partir del nivel mínimo aceptable y el nivel objetivo, podemos definir un plan de trabajo para alcanzar ambos a partir del estado actual.

- 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**.

ISO 17799 **no** es una norma tecnológica. Ha sido redactada de forma flexible e independiente de cualquier solución de seguridad específica, proporciona buenas prácticas neutrales con respecto a la tecnología ya 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.
- ¿Cómo traducir especificaciones de alto nivel a soluciones concretas, para poder implantar ISO 17799?. Trabajo de consultoría, interna o externa.

La adopción de la norma ISO 17799 proporciona **diferentes ventajas** a cualquier organización:

- Aumento de la **seguridad efectiva** de los sistemas de información.
- Correcta **planificación** y gestión de la seguridad.
- Garantías de **continuidad de la organización**.
- **Mejora continua** a través del proceso de auditoría interna.
- Aumento del **valor comercial** y mejora de la **imagen** de la organización.
- Certificación.

ISO 17799 es una norma internacional que ofrece **recomendaciones** para realizar la gestión de la seguridad de la información.

- La norma se estructura en **diez dominios de control** que cubren por completo todos los aspectos relativos a la seguridad de la información.
- Implantar ISO 17799 requiere de un trabajo de **consultoría** que adapte los requerimientos de la norma a las necesidades de cada organización concreta.
- La adopción de ISO 17799 presenta diferentes **ventajas** para la organización, entre ellas el primer paso para la **certificación**.

2.5 Agujeros de Seguridad

En los inicios de la computación las computadoras no contenían circuitos integrados con millones de transistores que conocemos hoy en día. Las operaciones de cálculo se llevaban a cabo con cientos de válvulas de vacío y las funciones de memoria se realizaban en tejidos de cientos de cables, que necesitaban varias habitaciones para desplegarse. Uno de estas computadoras históricas era el Eniac.

En cierta ocasión, este gigantesco equipo comenzó a fallar y no lograba ejecutar ningún programa, este problema persistía durante tanto tiempo que los programadores decidieron revisar el sistema por completo, aunque tal misión pudiera llevarles semanas enteras de trabajo. Por fin, entre una maraña de cables, uno de ellos encontró el cadáver de una polilla que cortocircuitaba la memoria. Al retirarla todo volvió a funcionar. Desde entonces los errores de programación se conocen como bugs (bichos en inglés).

Eso fue en el origen, por lo que ahora no es necesario que se desmonte toda una computadora para encontrar que un bicho este provocando fallos. Es cierto que, a veces, los errores que se

registran tienen unas características tan especiales, que casi se podría uno imaginar que si en efecto un tipo de bicho este provocando dicho fallo en la computadora.

La explicación de estos fallos se debe a lo siguiente, todo el software que se tiene instalado en la computadora puede tener errores; al fin y al cabo, detrás de un programa informático hay un equipo de personas encargadas de desarrollarlo y éstas, en ocasiones, también se equivocan.

Cuanto mayor sea el nivel de complejidad de las tareas que ejecuta el programa, mayores son sus posibilidades de tener errores. Los bugs más preocupantes son aquellos que afectan al sistema operativo, puesto que es el elemento común a todas las actividades que realizamos con el equipo.

Un bug puede tener efectos desconcertantes, como que un archivo no pueda imprimirse, o errores graves que afecten a la seguridad de la computadora. Cuando esto es así se convierten en verdaderos agujeros por los que cualquier intruso puede colarse y provocar daños enormes que a veces no podemos ver a simple vista, sin imaginar las perdidas enormes que conlleva este tipo de prácticas.

Los agujeros de seguridad se diferencian de los bugs simples en que no se suelen detectar, ya que no están asociados a disfunciones del software. Sin embargo, son buscados de forma intensiva por muchos programadores, con el objeto de invadir ordenadores ajenos.

Hagamos una definición sencilla que podamos manejar a lo largo de este tema. Un **agujero de seguridad** es una propiedad del hardware o del software, que debido a un fallo en éstos, permiten que los usuarios sin autorización puedan acceder al sistema. Todas las plataformas tienen agujeros, de hecho, no hay nada que sea absolutamente seguro. La razón de ello es que se consolidaron como una de las vías más efectivas para realizar ataques a través de Internet.

De esta manera podemos llegar a pensar que no hay ningún sistema informático seguro y que la Red no es otra cosa que un gran agujero, estaríamos equivocados, bajo ciertas circunstancias podemos plantearnos como es posible que no haya más agujeros, sobre todo, considerando el hecho de que los usuarios no suelen preguntarse qué sucede dentro de su computadora para que trabaje. De hecho, dejando a un lado los agujeros que aparecen por una deficiente administración de un sistema, la seguridad, en general, es bastante buena. El problema real es que los piratas son también muy buenos.

Los agujeros de seguridad no son algo nuevo, pero hasta la aparición de las redes de computadoras no se les prestó demasiada atención. Su presencia va ligado a la llegada de Internet, ya que las computadoras dejan de ser máquinas aisladas para convertirse en eslabones de una inmensa cadena a través de la que se intercambian enormes volúmenes de información y por la cual millones de usuarios se conectan para tener una estrecha comunicación entre ellos desde lugares remotos

Fue en ese momento cuando los agujeros de seguridad cobraron una espectacular relevancia. Una de las primeras consecuencias fue la creación de virus los cuales eran capaces de propagarse rápidamente infectado miles de equipos. Así, dependiendo de la vulnerabilidad que se emplee, puede conseguirse que un virus se ejecute de forma automática cuando llega al

sistema, o que se introduzca a través de un puerto de comunicaciones sin necesidad de utilizar vías tradicionales como los disquetes o el correo electrónico.

Generalmente, aprovechar una vulnerabilidad no es tarea fácil, ya que son necesarios buenos conocimientos de programación para realizar los correspondientes **exploits** (son pequeños programas diseñados para utilizar una vulnerabilidad concreta). Hasta ahora y habitualmente, el propio autor del virus era quién programaba tanto el exploit como el código del virus, pero la situación se ha complicado de sobremanera por la moda reciente de publicar exploits en páginas de Internet. Debido a ello, cualquier autor de un virus que quiera incorporar un exploit no tiene más que buscarlo en la página correspondiente.

Esto ha motivado una especie de carrera contrareloj a la búsqueda de nuevas vulnerabilidades que aprovechar, en la que no importa el software de que se trate, mientras se encuentre instalado en millones de computadoras que, en un momento dado, puedan ser víctimas de un ataque.

Como ejemplo de una vulnerabilidad muy reciente podemos mencionar la denominada Exploit/MS04-028, que afecta al proceso de visualización de archivos de imagen JPEG. Este problema ha sido localizado en muchos de los productos de la compañía Microsoft, entre los que se encuentran Office XP, Office 2003 o el sistema operativo Windows XP. Concretamente, cuando un usuario abre una imagen JPEG construida para aprovechar esta vulnerabilidad se provoca un desbordamiento de buffer que permite llevar a cabo acciones tales como robo de datos confidenciales, envío masivo de mensajes de e-mail, creación de puertas traseras en la computadora, o la descarga y ejecución de todo tipo de archivos, entre otras muchas. Es muy previsible que, a partir de ahora, aparezcan amenazas que intenten hacer uso de esta vulnerabilidad.

2.5.1 Escalas de Vulnerabilidad

Existen diferentes escalas de vulnerabilidad:

- Agujeros que niegan un servicio.
- Agujeros que permiten que los usuarios con permisos limitados, los amplíen sin ningún tipo de consentimiento.
- Agujeros que permiten a usuarios ajenos al sistema, accedan a nuestra red sin autorización.

Los agujeros se pueden llegar a clasificar según el daño que se puede cometer gracias a ello. Algunos pueden llegar a ser muy importantes, tanto que incluso pueden llegar a destruir el objetivo, otros son algo menos serios, incluso sin llegar a tener importancia. A los agujeros se les dividen en tres niveles A, B y C, según su peligrosidad, y dentro de estos niveles se encuentran los distintos tipos a los que he hecho referencia antes, según podemos observar en la siguiente tabla:

Tipo	Nivel	Peligrosidad
Agujeros que permiten a usuarios ajenos al sistema, accedan a nuestra red sin autorización.	A	Muy peligrosos. Pueden dañar todo el sistema.
Agujeros que permiten que los usuarios con permisos limitados, los amplíen sin ningún tipo de consentimiento.	B	Peligrosos. Pueden llegar a conseguir el control del sistema.
Agujeros que permiten a un usuario interferir en las operaciones de un sistema. Agujeros que niegan un servicio.	C	Poco peligrosos. Pueden reiniciar un sistema.

Figura 2.3 Tabla

Agujeros que niegan un servicio: Pertenecen a la categoría C, y tienen una prioridad baja. Estos ataques se basan en los sistemas operativos dedicados a la red. Cuando se dan son los programadores creadores del sistema operativo los encargados de corregirlos y de distribuir los parches.

Para redes grandes un ataque de este tipo carece de importancia, pero en el caso de redes con un solo servidor, la cosa cambia, pues deja sin conexión a la red durante un cierto tiempo a los usuarios registrados a ella.

Agujeros que permiten que los usuarios con permisos limitados, los amplíen sin ningún tipo de consentimiento: Pertenecen a la clase B. Este tipo de agujeros son típicos de las aplicaciones o de sus plataformas, exceptuando uno muy común que son los ficheros con contraseñas no ocultas, el administrador crea una cuenta a un usuario local (usuario local se considera a alguien que tiene una cuenta en una máquina, el término local, en este caso, no se refiere a su ubicación geográfica) para que ponga su clave, mientras este usuario no ponga su clave, cualquiera puede entrar con solo el login o el nombre del usuario, y por tanto puede crear una clave y no permitirle el acceso al verdadero usuario, robándole así su cuenta. Este es un error tipo administrativo y no de sistema, imaginemos que aparte, por equivocación el administrador copia los privilegios que él tiene a esa cuenta (no es lógico ni habitual), el pirata, obtendrá pleno acceso a todos los recursos.

Un agujero típico de aplicación es el de sendmail. El Sendmail es el método más popular de transmisión de correo electrónico. Es el corazón del sistema de e-mail de Internet. Normalmente este programa se activa y se mantiene por el puerto 25, así se puede enviar los e-mails, se pude utilizar cualquiera de los distintos servidores de mails existentes en el mundo.
Los agujeros en programas como sendmail son muy peligrosos porque este tipo de utilidades está a disposición de todos los usuarios de Internet, ya que cualquier usuario dispone de los permisos necesarios para enviar un programa sendmail. Si no existiese, no se podría mandar correo electrónico. Por lo tanto, cualquier error o agujero que se encuentre dentro del programa sendmail es muy peligroso.

Lo único positivo que tiene este tipo de agujeros es que la identificación del agresor resulta muy sencilla, sobre todo si éste carece de experiencia. Si el administrador del sistema utiliza programas de registro, el atacante necesitará de una gran experiencia para que no sea detectado.

Agujeros que permiten a usuarios ajenos al sistema acceder sin autorización: Pertenecen a la clase A y son los más peligrosos de todos. Se suelen producir por errores de configuración o por la mala administración de un sistema. Un ejemplo típico de una mala administración, es almacenar en el disco duro un archivo de texto con la contraseña de todos los equipos de una red, por muy bien oculto que este dicho archivo, cuando se haga una modificación y se corrijan los datos cualquier programa de sniffer (Programa que permite almacenar en forma alternativa el tráfico de la red bajo TCP/IP identificando lo que sucede en las diversas actividades que manejan información como lo son aplicaciones internas de red los cuales pueden ser correo, navegación, FTP, chat, etc.), interceptará este archivo, y no existe nada mejor para un cracker (Es alguien que viola la seguridad de un sistema informático con fines de beneficio personal o mera diversión) que le den la lista completa de usuarios y contraseñas de una red.

Aunque parezca que este tipo de cosas no pueden ser ciertas, lo son. El ejemplo típico se puede ver en una empresa pequeña con una red y un servidor. El administrador del sistema aparte de tener esa función, por regla general suele tocar otros temas, dicho administrador no suele ser el dueño de la empresa. El mismo dueño puede exigir, que le haga un informe donde detalle un inventario de las máquinas que posee, a los usuarios que corresponden y las contraseñas que existen. Este informe se suele hacer con un procesador de texto y almacenarse en el disco duro del administrador y en papel para su superior.

El motivo principal de esta actuación, es principalmente para tener constancia en algún sitio de las contraseñas existentes en caso de que el administrador desapareciese. Incluso para mayor seguridad se guarda el documento en un sobre cerrado, esto es totalmente inseguro, cualquier empleado puede acceder a ese sobre, llevarlo a su casa y tranquilamente abrirlo, fotocopiarlo y cambiar el sobre por otro, o bien, si no dispone de otro sobre, levantar el engomado con vapor de agua.
Los agujeros de seguridad siempre estarán ahí, pero en la medida en que los programadores del software y los usuarios del hardware se percaten de la importancia de evitar estos tipos de vulnerabilidades haciendo conciencia a la hora de la realización de éste, así como de las pruebas necesarias, la seguridad para el uso y manejo adecuado tanto del hardware como del software.

2.5.2 Ataques de seguridad

En los primeros años, los ataques involucraban poca sofisticación técnica. Los empleados disconformes o personas externas con acceso a sistemas dentro de organizaciones o empresas utilizaban sus permisos para alterar archivos o registros. Las personas que atacan desde afuera de la ubicación física de la organización o empresa, ingresaban a la red simplemente averiguando un password que fuera válido.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar el control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la desaparición de aquellas organizaciones o empresas con un alto

grado de dependencia tecnológica (bancos, servicios automatizados, etc.). Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos hackers (Es una persona que está siempre en continua búsqueda de información, vive para aprender y todo para él es un reto, sólo obtiene información para su uso personal.) y sitios web, donde además encuentran todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los Ataques están a la orden del día, no existe día en el cual no lleguen noticias de nuevos ataques que son más potentes, a pesar de que la seguridad sé esta convirtiendo en un tema que va tomando fuerza y conciencia, también aquellos que pretenden perpetuarla están concientes de esto, por lo cual utilizan todo su conocimiento para usar ataques y procedimientos más sofisticados en contra de la seguridad.

2.5.3 Amenazas

Definición:

Una amenaza es una condición del entorno del sistema de información llámese (persona, máquina, suceso o idea), que dada una oportunidad, podría dar lugar a que se genere una violación de la seguridad confidencialidad, integridad, disponibilidad o uso legítimo.

Fuentes de Amenazas:

- **Humanas:** Muchas veces la amenaza surge por ignorancia en el manejo de la información, por descuido, por negligencia, por inconformidad (cuando algún empleado es despedido de alguna empresa u organización).

- **Fallas en el hardware:** Se da la amenaza por fallas físicas que presente cualquier elemento de los dispositivos que conforman a la computadora.

- **Fallas en la Red:** Esta amenaza se presenta cuando no se calcula bien el flujo de la información que va a circular por el canal de comunicación, es decir, que un atacante podría saturar el canal de comunicación provocando la no-disponibilidad de la red. Otro factor es la desconexión del canal. Por ejemplo, cuando uno o varios usuarios están conectados a la red, si el canal se llega a desconectar por cualquier razón.

- **Fallas de tipo lógico:** La amenaza se hace presente cuando un diseño bien elaborado de un mecanismo de seguridad, se implementa mal, es decir, no cumple con las especificaciones del diseño. La comunicación entre procesos puede resultar una amenaza cuando un intruso utilice una aplicación que permita enviar y recibir información, esto podría consistir en enviar contraseñas y recibir el mensaje de contraseña válida; dándole al intruso elementos para un posible ataque.

- **Factores Naturales:** Este tipo de amenaza surge de fuerzas naturales tales como las inundaciones, los terremotos, el fuego, el viento. Dichos desastres hacen surgir

amenazas directas, debido a que repercuten indiscutiblemente en el funcionamiento físico de las computadoras, redes, instalaciones, líneas de comunicación, etc.

2.5.4 Ataques

Definición:

Un ataque no es más que la realización de una amenaza. En pocas palabras las amenazas siempre están presentes y a la orden del día dentro de nuestro entorno informático, de esta manera cuando se presenta la oportunidad de realizar una violación, automáticamente sé esta llevando acabo un ataque.

Un ataque puede tener varios objetivos tales como el fraude, la extorsión, el robo de información, la venganza, el juego o simplemente por el placer de perpetuar un sistema. Esto puede ser realizado por atacantes externos o por gente de la misma empresa u organización, como lo pueden ser empleados con permisos de acceso, los cuales se valen de vulnerabilidades que es una debilidad que puede ser explotada para violar la seguridad para poder llevar sus objetivos acabo.

Existen otros tipos de atacantes:

Perpetradores: Un perpetrador es un individuo que se basa de cualquier medio para cometer un delito o culpa grave.

Personas Enteradas: Consideraremos a este tipo de personas como aquellas que están enteradas de toda aquella información que es valiosa para la organización o empresa, este tipo de personas siempre son aquellas que tienen permisos con accesos a la mayoría de los archivos de la empresa, gente de confianza, el éxito de este tipo de personas puede ser de un alto porcentaje por poder contar con contraseñas, ubicación y el estado actual de la información, este tipo de ataque se lleva acabo cuando algún empleado con las características antes mencionadas, ha sido despedido, marginado a otro puesto inferior, por el simple placer de perpetuar la información para uso personal o con otros fines.

Hackers: Un Hacker es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información, distribución de software sin costo y la globalización de la comunicación. El concepto de Hacker, generalmente es confundido erróneamente con los mitos que existen acerca de este tema. Un Hacker es pirata. Esto no es así ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero Hacker sólo obtiene esa información para su uso personal. Un Cracker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que el que destruye información y sistemas ajenos, no es el Hackers sino el Cracker.

Cracker: Un cracker es una palabra que proviene del inglés crack, que significa romper, es alguien que viola la seguridad de un sistema informático con fines de beneficio personal o mera diversión. También se considera como cracker a aquella persona que diseña y programa cracks

informáticos. El término fue creado alrededor de 1985 por hackers como defensa por el uso incorrecto del término hacker. Se considera que la actividad del cracker es ilegal.

Espías: Un espía, es un individuo o proceso que ha sido enviado o implantado de manera secreta, para observar, escuchar, seguir a una persona, cosa o proceso, con el único propósito de recabar información.

Código Malicioso: Se trata de cualquier software que entra en un sistema de cómputo sin ser invitado e intenta romper las reglas. Esto incluye a los caballos de troya, virus, gusanos, bombas lógicas y otros métodos de amenazas avanzadas programadas. El código malicioso explota los flujos de información en los sistemas operativos y software asociado, además explota la configuración insegura, la mayoría de los sistemas son entregados con configuración insegura y eso se debe a que es más fácil instalar y utilizar.

Existen varios tipos de códigos maliciosos y los más comunes son:

- Virus.
- Caballos de Troya.
- Gusanos.
- Spyware.
- Web Bugs.

Virus: Un virus informático es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el consentimiento o permiso de éste. Se dice que es un programa parásito por que ataca a los archivos o sector de arranque y se reproduce a sí mismo para continuar su esparcimiento. Algunos se limitan solamente a reproducirse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas.

Tienen diferentes finalidades: algunos sólo infectan, otros alteran datos, otros los eliminan y algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: propagarse.

Es importante destacar que el potencial de daño de un virus informático no depende de su complejidad sino del entorno de donde actúa.

Un virus es un programa que cumple con las siguientes pautas:

- Es muy pequeño.
- Ejecutable o potencialmente ejecutable.
- Toma el control o modifica otros programas.
- Convierte otros objetos ejecutables en clónicos víricos.
- Modifican el código ejecutable.
- Permanecen en la memoria de la computadora.
- Funcionan igual que cualquier programa.
- Es nocivo para la computadora.
- Se ocultan al usuario.

¿Cómo trabaja un virus?

Por lo general, los virus se encuentran en la parte final del programa para infectarlo; es decir, modifican su correcto funcionamiento y por supuesto, incrementan el tamaño de éste. Son pequeños pedazos de código que por sí solos no significan nada, por lo que deben de encontrar un lugar donde puedan reproducirse para así continuar su ciclo de vida. El lugar donde pueden reproducirse es; en el sector de arranque, en los programas ejecutables o en ambas partes. Otros programas considerados como virus son los macro virus los cuales infectan los archivos de información; la aparición de éstos generó alarma en los ámbitos de seguridad informática, puesto que rompían una parte del paradigma establecido en el cual los archivos que podían ser infectados por virus eran solamente ejecutables o potencialmente ejecutables como los archivos con extensiones .EXE, .COM, .BAT, .SYS, etc.

Los virus necesitan tener el control sobre sí mismos y el programa anfitrión para que puedan funcionar. Es por esta razón que se añaden en el punto de inicio de un proceso a realizarse o punto de entrada del archivo, de esta manera, antes de que se pueda ejecutar el código del programa, se ejecuta el virus.

El virus se produce cuando el ambiente es apropiado para activarse esto es: una fecha especifica, a una hora determinada, por cierta cantidad de ejecuciones, por el tamaño del archivo de información o por una combinación de teclas, estas son las condiciones necesarias para que causen daño.

En los últimos años, el área informática ha experimentado un vertiginoso crecimiento, y con esto, los programas que las compañías distribuyen alcanzan con mayor rapidez al periodo de madurez. Hace algunos años, los usuarios comienzan a grabar los programas, debido al alto precio de estos, lo que llevó a los programadores de virus a encontrar el principal modo de distribución.

Caballos de Troya: Primeramente hay que comenzar comentando en qué consiste un programa de acceso remoto o programa de administración remota. Este tipo de programas, conocidos también como RATs (Remote Administration Tool), se han desarrollado para el control remoto de un PC o un sistema, valga la redundancia. Es decir, permiten un manejo prácticamente total de un PC, que físicamente no se encuentra al alcance de nuestras manos, por medio de una conexión directa desde otro PC. El programa de acceso remoto debe estar instalado en ambos PC’s y su comunicación se produce generalmente vía Internet o vía red.

Un caballo de Troya es un programa malicioso insertado en un PC sin consentimiento de su dueño que permite el control de ese PC por parte de una persona no autorizada, pudiéndose incluso considerar un tipo de virus, ya que el PC atacado se “infecta” con él.

Sin embargo un troyano tiene unas características propias que le confieren un carácter malicioso:

- Se aprovecha frecuentemente de bugs y backdoors de los sistemas informáticos, como Back Orifice o el BackDoor.

- Sólo una de las dos partes del programa (un troyano se instala en ambos PCs) tiene capacidad de controlar (cliente del troyano) mientras que la otra sirve de conexión con el PC controlado (servidor del troyano).
- El usuario del PC que actúa como servidor (el PC controlado) no tiene conciencia o conocimiento de estar comunicado con aquel otro PC. Ni tan siquiera es consciente de haber instalado el troyano en su PC.
- El servidor del troyano se oculta intentando pasar desapercibido para actuar clandestinamente.

Definición:

Para que un troyano se instale en un PC atacado necesita de la actuación del usuario del PC en cuestión, ya que éste debe ejecutarlo personalmente. La forma habitual es la de enviar el servidor del troyano al PC que se quiere atacar, habitualmente a través de un intercambio de ficheros vía IRC, ICQ, FTP,... con la intención de que la víctima lo ejecute. Normalmente se utilizan dos formas de engañar al usuario para que ejecute el servidor del troyano en su PC.
Un caballo de troya parece ser una aplicación inocente y útil que luego se revela como maligna. No hay nada que impida que se sigan realizando las misiones benignas de la aplicación original. Lo que sucede es que alguien ha desensamblado el original y ha añadido unas instrucciones de su colección.

Gusanos: No son exactamente virus informáticos, pero se les confunde frecuentemente con ellos, incluso en algunos casos se ha llegado ha utilizar esta denominación como sinónimos de virus. Se dan en redes, de tal forma que se trasladan de una a otra terminal, se reproducen sólo si es necesario para el trabajo para el cual han sido diseñados. Viajan a través de una terminal reuniendo información; también dejan mensajes, en su mayoría burlones, antes de desaparecer. No es raro que borren toda clase de vestigio de su paso por la red para no ser detectados por los operadores del sistema.

Entre otros tipos de códigos maliciosos que se tienen y que han sido de noticias en la actualidad son los siguientes abarcando así la atención en ellos:

Spyware: Los Spywares o archivos espías son unas diminutas aplicaciones cuyo objetivo es el envío de datos del sistema donde están instalados, mediante la utilización subrepticia de la conexión a la red, a un lugar exterior, el cual por lo general resulta ser una empresa de publicidad de Internet. Estas acciones son llevadas a cabo sin el conocimiento del usuario.

Hay que aclarar que, aunque evidentemente tienen cierta similitud con los programas Troyanos, los Spyware no representan un peligro de manipulación ajena del sistema, ni de daños a nuestro equipo por parte de terceros. Sus efectos son, simple y llanamente, la violación de nuestros derechos de confidencialidad de nuestros datos, así como afectar el rendimiento del equipo.

Normalmente estos archivos vienen acompañando a programas de tipo Shareware, gratuito y sobre todo, gratuitos que incorporen publicidad. Estos programas suelen ser una oferta tentadora para multitud de usuarios, ya que algunos de ellos son verdaderos buenos programas, útiles y en ocasiones, de los mejores de su categoría. Cuando instalamos uno de estos

programas, al mismo tiempo introducimos en nuestro sistema los archivos que revelarán nuestros datos a empresas muy interesadas en ellos.

Estos programas instalan un enlace dinámico de librerías, esto es, un archivo .dll que se instala automáticamente en la carpeta System de Windows, cuando instalamos los programas que lo incorporan capturando datos.

En principio, la suposición es que esos datos capturados y emitidos son posteriormente comercializados por empresas, con motivos publicitarios.
Esos datos trasmitidos pueden ser, desde poco relevantes como:

- Número de conexiones.
- Duración de las mismas.
- Sistema operativo.

Pasando por bastante relevantes:

- Páginas visitadas.
- Tiempo de estancia en las mismas.
- Banners sobre los que se pulsa.
- Descargas de archivos efectuados.

Y llegando a ser personalmente relevantes:

- Dirección de correo electrónico.
- Número de dirección IP.
- DNS de la dirección que efectúa la conexión, es decir, ISP y área del país.
- Número de teléfono al que se realiza la conexión y contraseña de la misma, si esta última está guardada.
- Listado de todo el software instalado, extraído del registro.

Tras ver esto, está claro que con esa información se puede establecer un lucrativo comercio, cualquier empresa de publicidad estaría interesada en ellos. Pero lo cierto es que no se sabe a ciencia cierta el destino de esa información, lo que resulta mucho más preocupante. Las empresas desarrolladoras de estos Spywares alegan que la identidad del usuario se mantiene siempre a salvo, ya que ningún dato sobre esta es captado, y que si bien recogen información, esta se utiliza "únicamente" con fines de marketing y estadística.

Pero muchas de las veces no son así y las usan con otros fines, por lo que ya ha habido un seguimiento de este tipo de empresas, por lo que hoy en día los Spyware han atacado a gran escala y en pocas palabras se puede decir que es la moda en código malicioso ya que se ha valido de estos para atacar a las computadoras en el mundo, por lo que cada día nuestros equipos son infectados gracias a la cantidad enorme de personas que buscan programas o utilidades de manera gratuita sin percatarse que todo la información es transmitida a una empresa.

Web Bugs: Un Web Bug es una imagen incrustada en un documento html: Esto es, una página web o un mensaje de correo en este formato. Esta imagen resulta invisible al usuario que visite dicha página, ya que su tamaño es inapreciable, pudiendo ser este de un píxel en formato GIF y transparente. También puede presentarse en forma código de JavaScript, también de poco tamaño. Si la página es descargada, o el correo abierto, el Web Bug puede ser rastreado por la compañía emisora, lo que proporciona información sobre la actividad del usuario en la red. Las páginas web, y el formato html del correo, que provoca la ejecución del navegador, pueden así mismo introducir en nuestro sistema las conocidas cookies, estas cookies le permitirán al remitente recoger cierta información, como la dirección IP que tenemos en ese momento, el tipo de navegador que usamos, y los datos de las demás cookies almacenadas en nuestro sistema, lo que revela con exactitud los sitios Web que visitamos.

Por ahora tan sólo unas cuantas compañías, desarrollan esta técnica, aunque esto no quiere decir que sean las únicas que la utilicen. Monitorear nuestros hábitos al navegar de momento no tiene otras connotaciones perjudiciales que no sean la captura de información no autorizada por el usuario, con la violación de la privacidad que ello supone y el Spam que monitorizar mediante un Web Bug la recepción de un mensaje que lo porte, estamos develando que dicho mensaje ha llegado a una dirección real, la cual una vez confirmada será blanco seguro de multitud de mensajes no deseados.

Pero esta técnica ya supone una posible futura vía de propagación de virus, tal como apuntan algunos estudios al efecto, ya que el Bug, que requiere una conexión al servidor del remitente, posibilitaría la utilización con fines infecciosos, a la manera de los conocidos troyanos, abriendo una nueva técnica de contagios.

2.5.5 Clasificación General de Ataques

Un ataque como ya se menciono con anterioridad, no es más que la realización de una amenaza. Las cuatro categorías generales de amenazas o ataques son las siguientes:

Interrupción: Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

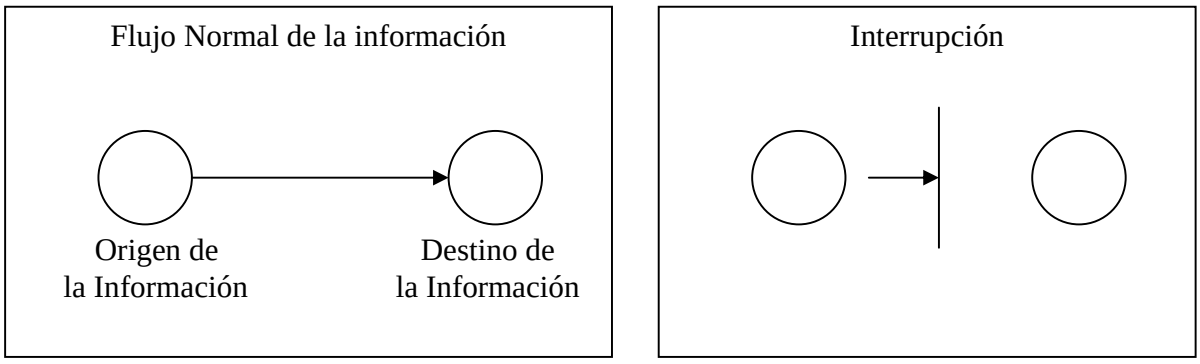


Figura 2.4 Interrupción

Como se puede observar en la Figura 2.4 muestra una representación clara de cómo debe de fluir la información de manera adecuada a lo que le podemos llamar el flujo normal de la información en el cual no debe de existir ningún tipo de obstáculos para que la información llegue a su destino.

Intercepción: Una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora. Ejemplos de este ataque son: tener acceso a una línea para hacerse de datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de los paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

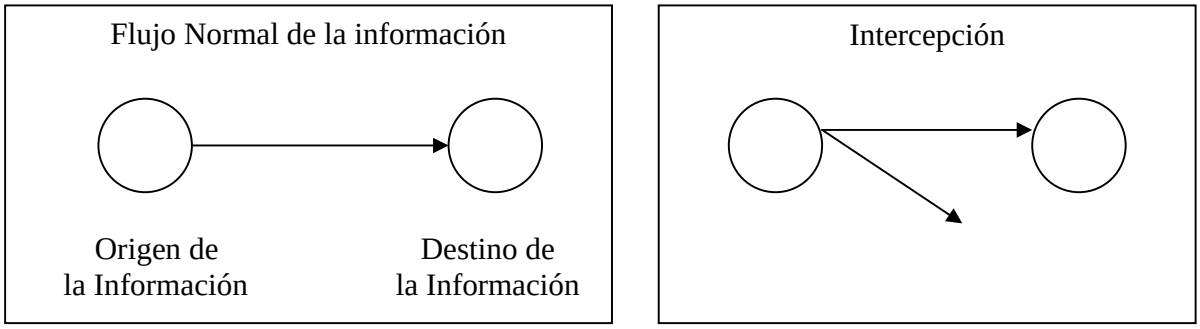


Figura 2.5 Intercepción

Modificación: Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son: el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

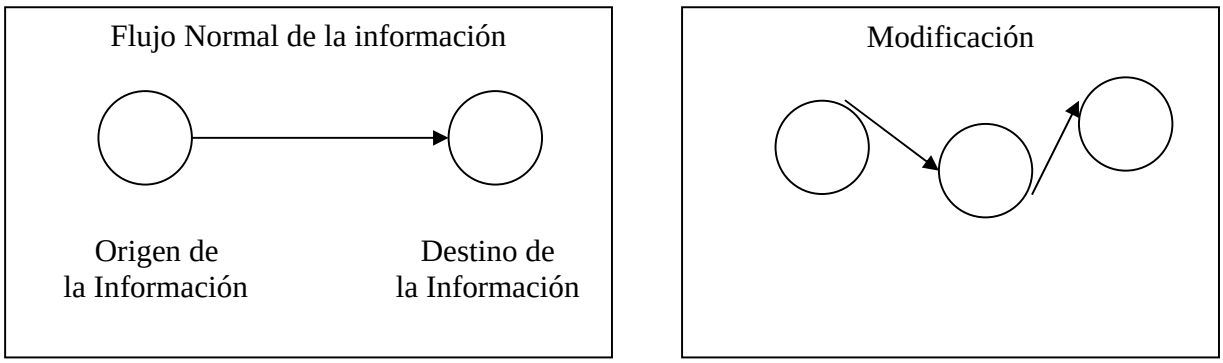


Figura 2.6 Modificación

Suplantación: Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes falsos en una red o añadir registros en un archivo, la siguiente figura nos muestra este tipo de ataque.

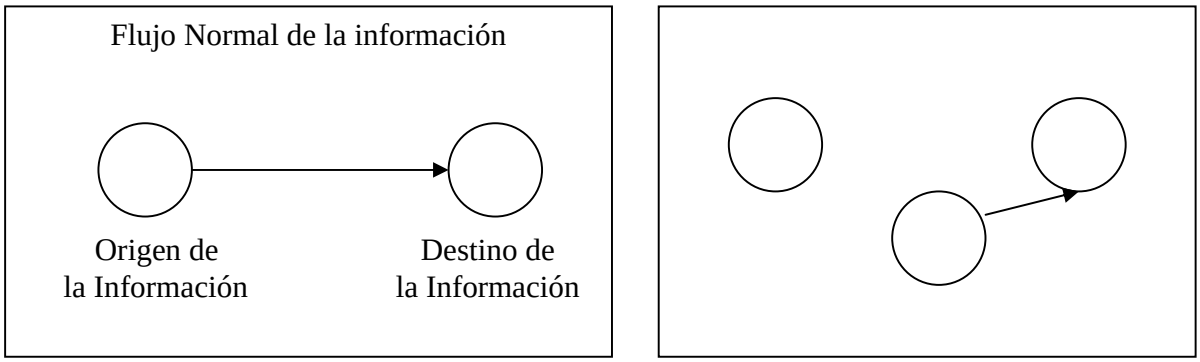


Figura 2.7 Suplantación

Otra Clasificación de los ataques es la siguiente:

1. - Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitorea, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información.

2. - Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

Suplantación de identidad: El intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

Réplica: Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

Modificación de mensajes: Una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos a la cuenta 2020" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta 4040".

Degradación fraudulenta del servicio: Impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes falsos. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

3. - Métodos de Ataque

Un ataque en un sistema de cómputo conlleva cuatro etapas:

Preparación: El método de ataque se plantea u otras preparaciones se realizan. Las formas para efectuar esta primera etapa son las siguientes:
Recolección: El fin en este punto es más que nada que el objetivo principal de cualquier atacante es la información, las personas dentro de la empresa pueden recolectarla haciendo uso de contraseñas o por medio de engaños, por el contrario, las personas externas deben ingeniárselas para obtener la información, esto puede lograrse convenciendo a la gente de hacerlo para lograr su objetivo por medio de engaños.

- Caballos de Troya: Un usuario coloca dentro de su dominio de protección, cuando el programa se ejecuta, obtienen los privilegios de dicho usuario de esta manera, se convierte en un cómplice inconsciente ya que envía y concede información a los perpetradores.

- Propagación programada: Se refiere al código malicioso que se introduce en un equipo de cómputo ya que se puede multiplicar su ámbito y daño.

- Puerta trasera: El software contiene mecanismos escondidos que permite a los diseñadores desviar los controles. Este tipo de mecanismos recibe el nombre de puerta trasera. Un ejemplo clásico de puertas traseras se refiere a un programa donde se requiera un nombre de usuario pero sin una contraseña válida.

- Enmascaramiento o engaño: Significa que se pretende ser alguien más de tal manera que se puede obtener los derechos de acceso de una persona.

- Exploración: Antes de que el enmascaramiento se realice, el atacante necesita conocer las contraseñas, números telefónicos, etc., para ello es necesario hacer uso de la exploración, es decir, es necesario enviar una secuencia de información cambiante a una computadora, para encontrar valores que muestren respuestas positivas.

- Mal uso de la autoridad: Si el atacante penetra de manera legítima al sistema, la preparación es mucho más fácil ya que está haciendo mal uso de la autoridad que posee dentro de la organización.

Activación: El ataque se activa o dispara, esta se puede realizar de diferentes maneras

Si el ámbito de preparación asume el control de una interrupción de un sistema operativo, el código de ataque es invocado cuando la interrupción se lleva acabo, si no es así, el perpetrador puede invocar directamente un programa que lleve acabo la misión.

Un ataque más sofisticado impone un retardo entre la preparación y la activación, esto ocasiona que la identificación del atacante sea mucho más difícil, el retardo puede provocar que el ataque sea más destructivo, hablando específicamente de los virus.

Una bomba de tiempo se encuentra arreglada para estallar a una hora y día determinados. Puede engancharse por si sola a programas regulares de ejecución verifica la hora designada y cuando ésta llegue, lleva acabo la misión, aunque en ocasiones la bomba puede estar planteada en un programa cíclico de funcionamiento como un proceso de fin de mes. Una bomba de tiempo es un tipo de bomba lógica, ya que ésta se acciona por cualquier combinación de condiciones.

Ejecución: La misión se lleva acabo mediante la desviación de los controles de acceso. Violación de secretos o integridad, denegación de servicio, robo de servicios, simplemente dar a conocer el ataque.

Las misiones pueden ser:

- Mal uso activo: Este afecta la integridad de la información o disponibilidad de los servicios. Los archivos pueden ser destruidos o sutilmente alterados.

- Mal uso pasivo: Cuando la confidenciabilidad es violada pero el estado del sistema no es afectado, el mal uso es pasivo pero no por eso es menos dañino, de hecho, podría resultar más letal que el activo.

2.6 Modelos de Seguridad

Se trata de una representación formal de una política de seguridad ejecutada por el sistema. El cual debe de identificar el conjunto de reglas y prácticas que regulen como un sistema: maneja, protege y distribuye información delicada.

Propósitos

- Proveer un sistema que ayude a comprender los conceptos involucrados.
- Proveer una representación de una política de seguridad formal y clara.
- Expresar la política exigida por un sistema específico.

Los modelos de seguridad pueden ser de dos tipos:

Modelo abstracto: Se ocupa de las entidades abstractas como sujetos y objetos. El modelo Bell-LaPadula es un ejemplo de este tipo.

Modelo concreto: Traduce las entidades abstractas a entidades de un sistema real como procesos y archivos.

Además los modelos sirven a tres propósitos en la segundad informática

- Proveer un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito necesitan diagramas, analogías, cartas. Un ejemplo es la matriz de acceso.
- Proveer una representación de una política general de seguridad formal y clara. Un ejemplo es el modelo Bell- LaPadula.
- Expresar la política exigida por un sistema de cómputo específico.

Criterios

Al asumir que la política de seguridad es realmente la apropiada, existen criterios que un modelo de seguridad debe seguir a medida que se va desarrollando para considerarse un buen modelo. Por lo tanto, un modelo de seguridad debe:

Representar de manera válida y precisa la política de seguridad: Los creadores del modelo deben de explicar de manera clara como el modelo corresponde a la política y deben justificar la validez de las correspondencias.

Ayudar a entender a través de expresiones enfocadas, exactas y pruebas de propiedades: un modelo ayuda a la comprensión tras aclarar conceptos y expresarlos de manera precisa, lo cual enfoca la atención sobre lo esencial. Se entiende el problema con lo que se deriva de los axiomas del modelo.
Soportar un análisis de seguridad: Un modelo debe de soportar decisiones sobre seguridad y la pregunta de sí existe algún estado del modelo en donde la propiedad especifica de seguridad no se mantiene.

Soportar la creación y verificación del sistema: Un sistema basado en un modelo debe de ser razonable para construirse y debe de trabajar de manera adecuada.

Permitir que los sistemas sean modelados en partes y después unirlas: debe de ser posible modelar sistemas complejos en partes y después unir estas partes.

2.6.1 Modelos de control de Acceso

Los modelos de control de acceso identifican las reglas necesarias para que un sistema lleve a cabo el proceso que asegura que todo acceso a los recursos sea un acceso autorizado.
Los modelos de control de accesos son:

- Modelo de la Matriz de Acceso.
- Modelo HRU.
- Modelo Take-Grant.
- Modelo Bell-LaPadula.

Modelo de la matriz de acceso

En los años 70's, se desarrollo un modelo de seguridad basado en la matriz de control de acceso, cuya primera versión fue realizada por Lampson B.W.; posteriormente fue ampliado por Denning y Graham, esto más que todo debido a su simplicidad y generalidad que a la vez permite una gran variedad de técnicas de implementación.

El modelo de matriz de acceso esta basado en la existencia de tres principales componentes:

Objetos: Representan los recursos que serán controlados como archivos o áreas de memoria.

Sujetos: Son los usuarios o los procesos ejecutados por ellos; es significativo anotar que cada sujeto es un objeto, así un sujeto puede ser manipulado por otro sujeto.

Derechos: Representan un tipo de acceso hacia el objeto como leer, escribir o ejecutar.

La matriz de acceso consta de una fila para cada sujeto s y una columna para cada objeto o, la celda (intersección creada entre una fila y columna determinada), especifica los derechos que el sujeto s tiene sobre el objeto o. Visto de otro modo, cada fila representa una lista de derechos (poseídos por cada uno de los sujetos), y cada columna representa una lista de los controles de acceso de los objetos (lista de todos los derechos de los sujetos sobre un determinado objeto).

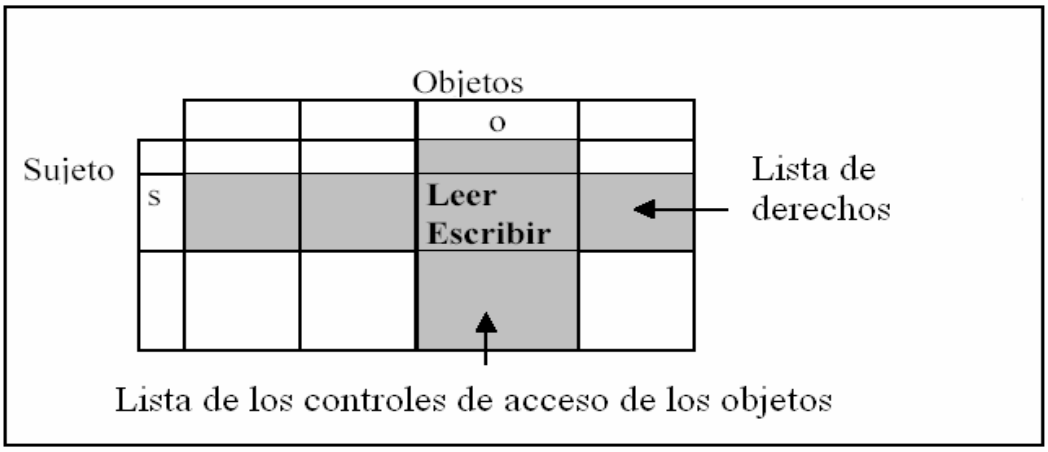


Figura 2.8 Modelo de la Matriz de acceso.

Los modos de acceso permitidos dependen del tipo de objeto y de la funcionalidad del sistema; típicamente los modos son: leer, escribir y ejecutar. Además las banderas pueden ser utilizadas para indicar propiedad sobre un objeto en particular. La matriz de acceso puede verse como el

almacenaje de los estados de protección del sistema; así ciertas operaciones invocadas por los sujetos pueden alterar estos estados.

Este modelo puede representar muchas políticas de control de acceso que aseguran la integridad y la confidenciabilidad, en este modelo se especifica quien eres y con quien estas relacionado, además de que el sistema indica que te esta permitido hacer. Para que un sistema sea más útil, la matriz de acceso no debe de ser estática, entonces los sujetos, los objetos y los derechos suelen ser cambiantes.

Modelo HRU

El modelo HRU fue creado por Harrison, Ruzzo y Ullman en 1976 al tratar de mejorar el modelo de la Matriz de Acceso, debido a que éste era débil con respecto a la seguridad ya que de manera general no toma en cuenta lo que un cambio en el modelo implica.

El modelo HRU define un sistema de protección que se encuentra constituido por dos elementos:

- **Un conjunto de derechos genéricos:** Donde ese conjunto representa los tipos de acceso del sujeto hacia el objeto como leer, escribir, borrar, modificar, ejecutar.

- **Un conjunto de comandos:** Donde un comando cuenta con una parte condicional y una principal, la condicional prueba la presencia de ciertos derechos en la matriz de acceso, si la prueba es exitosa la parte principal se ejecuta realizando una serie de operaciones primitivas que cambian la configuración de protección. Las operaciones primitivas crean y destruyen objetos y sujetos, añaden o borran derechos en la matriz de acceso.

El modelo HRU es sencillo y se encuentra diseñado para contestar preguntas fundamentales. Además, mejora la seguridad puesto que verifica si realmente se trata de un sujeto autorizado y contempla que un cambio en la matriz de acceso no permite a sujetos no autorizados obtener derechos.
El resultado importante del modelo es que no está a discusión si una configuración dada es segura para un determinado derecho. Aún cuando este resultado acerca de la matriz de acceso es fundamental, sólo aplica a un sistema de protección general y no restringido ya que para un sistema restringido monoperacional (donde cada comando se compone de una sola operación primitiva) la seguridad está a discusión pero el procedimiento de decisión es computacionalmente complejo, lo cual no es práctico.

- **Modelo Take-Grant**

Ya que un renglón de la matriz de acceso puede ser visto como una lista de capacidades especificando todos los derechos del sujeto asociado con ese renglón. Existen dos maneras principales para implementar el control de acceso:

- **Listas de control de acceso:** Una lista de control de acceso contiene todos los derechos que tiene el sujeto sobre el objeto.

- **Capacidades:** Una capacidad se define como (objeto, derechos, número aleatorio), el número asegura que no haya falsificación de capacidades.

Debido a que las capacidades no pueden ser falsificadas, pueden pasar sin la intervención de un monitor, esta propiedad de las capacidades contribuye a dar gran importancia a la flexibilidad en el diseño de sistemas, los sistemas operativos y las arquitecturas de hardware han sido diseñados con base en las capacidades.

Los modelos Take-Grant se encuentran estrechamente identificados con los sistemas de capacidad. Estos modelos representan el estado de protección mediante una gráfica dirigida, los elementos utilizados en este modelo son:

a) Vértice sólido: Representa un sujeto.
b) Vértice abierto: Representa un objeto.
c) Línea dirigida: Va de un vértice a otro y representa un derecho que el sujeto tiene sobre el objeto.
d) Vértice mixto: Representa a un sujeto o a un objeto

Un modelo Take-Grant especifica un conjunto de reglas para transformar las gráficas de protección.

Estas reglas controlan la forma en la que los derechos pueden ser pasados de un sujeto a otro. Al variar las reglas se obtienen diferentes modelos Take-Grant, por ejemplo, cuando se emplean las reglas Create (crear) y Remove (remover), el modelo indica cómo los vértices se añaden y se quitan, pero si se emplean las reglas Grant (conceder) y Take (tomar), entonces se indica cómo un sujeto concede derechos a otro o cómo adquiere los derechos de otros.

En este modelo existen dos reglas principales:

Regla Grant: Esta añade una nueva línea (b) de un vértice (y) a otro (z), esto es posible porque un primer vértice (x) concede al segundo (y) la habilidad de crear la nueva línea (b) hacia el tercer vértice (z), esto se debe a que el primer vértice (x) concede el derecho al segundo (y) porque la línea (b) está incluida en los derechos del primero (x) sobre el tercer vértice (z).

Regla Take: Añade una línea (b) del primer vértice (x) hasta el tercero (z), esto se debe a que el primer vértice (x) toma del segundo (y) el derecho de realizar la línea (b) hasta el tercero (z)
El modelo Take-Grant es más restrictivo debido a que tiene reglas particulares para transformar la gráfica de protección, lo cual logra que las decisiones de seguridad sean posibles.

Modelo Bell-LaPadula

Este modelo recibe el nombre de Bell-LaPadula ya que fue desarrollado por D. E Bell. Y L. J. LaPadula en 1976. El modelo Bell-LaPadula (BLP) formaliza la política de seguridad multinivel, la política multinivel es aquélla que clasifica la información en cuatro niveles:

- No clasificado.

- Confidencial.
- Secreto.
- Ultra secreto.

La información es descrita en términos de compartimentos los cuales representan el asunto del sujeto. El nivel de seguridad o clase de acceso de un documento es la combinación de su nivel y conjunto de compartimentos. Cualquier persona autorizada, recibe un permiso para un cierto nivel, de esta manera tanto las personas como la información, tienen niveles de seguridad o clases de acceso. La política indica que las personas pueden tener acceso a la información que se encuentra hasta su nivel autorizado y esta política tiene como objetivo controlar el flujo de la información, el modelo también ayuda en la construcción de sistemas cuya seguridad puede ser verificada.

El modelo Bell-LaPadula es un modelo de máquina de estado como muchos modelos de seguridad de computadora donde se ve a los sistemas como una tripleta (S, I, F) donde se tiene un conjunto de estados S, un conjunto de posibles entradas I y una función de transición F que transfiere al sistema de un estado a otro.

El modelo consta de los siguientes elementos:

- Sujetos.
- Objetos.
- Modos de acceso: como leer y escribir.

Niveles de seguridad

Un estado de seguridad se encuentra definido por tres propiedades que intentan expresar la política de seguridad:

- Propiedad de seguridad simple: expresa la política de autorización-clasificación.

- Propiedad estrella: representa la política del flujo de información no autorizado de un nivel alto a uno bajo.

- Propiedad de seguridad discrecional: refleja el principio de autorización y se expresa en una matriz de acceso.

Se observa que un estado del sistema satisface la propiedad de seguridad simple si para cada elemento del conjunto de acceso actual, el nivel de seguridad del sujeto domina el nivel de seguridad del objeto. La propiedad estrella se satisface si para cada acceso de escritura en el conjunto de acceso actual, el nivel del objeto es igual al nivel actual del sujeto y para cada acceso de lectura, el nivel del sujeto domina al nivel del objeto. Esta propiedad asegura que si el sujeto tiene acceso de lectura a un objeto y acceso de escritura a otro, entonces el nivel del primero se encuentra dominado por el nivel del segundo. La propiedad estrella representa la política de que un sujeto no puede copiar información de un nivel más alto a un objeto de nivel inferior.

El modelo Bell-LaPadula se ha utilizado como base para muchos sistemas concretos ya que estos modelos deben ser una interpretación válida del modelo abstracto BLP.

Algunas consideraciones del modelo son:

Restricciones de la propiedad estrella: El modelo Bell-LaPadula prohíbe el flujo de información de un alto nivel a uno inferior. La suposición es que cualquier flujo es equivalente a fusionar diversas secciones.

Sujetos confiables: El modelo muestra que no hay presiones sobre cómo los procesos confiables pueden violar la propiedad estrella, cada sistema que es desarrollado realiza sus propias reglas sobre lo que pueden realizar los sujetos confiables.

Estado incompleto del modelo: El modelo Bell-LaPadula trabaja con el conjunto de acceso actual, el cual no modela de manera explícita las lecturas y escrituras actuales, para lo cual se necesitan modelos suplementarios que aseguren que las lecturas y escrituras sean consistentes con el conjunto de acceso actual.

Canales encubiertos: El modelo no trabaja con información que es transmitida de manera indirecta, mejor conocida como canales encubiertos. Un sujeto puede transmitir información a otro a través de recursos que estén compartiendo.

Transición segura de estado: Un sistema puede ser seguro según el modelo Bell-LaPadula, pero aún muestra transiciones no seguras, este problema puede corregirse si se añaden al modelo condiciones necesarias para transiciones seguras del estado.

2.6.2 Modelos de flujo de información

Una meta de las políticas de seguridad es proteger la información. Los modelos de control de acceso se aproximan a dicha meta indirectamente, sin relacionarse con la información pero sí con objetos (tales como archivos) que contienen información.

Teoría de la información

La teoría de la información, la cual fue desarrollada por Claude Shannon para tratar con la comunicación, provee una visión sistemática de la información. La teoría de la información ha sido usada en los modelos de flujo de información y está relacionada con otros problemas y métodos de la seguridad de las computadoras.

La teoría de la información define la información en términos de incertidumbre. Al proporcionar información se elimina la incertidumbre. Por ejemplo: Una carrera entre tres competidores, con una categoría mayor, es más incierta que una carrera entre dos competidores. El concepto de la entropía captura esta idea. Los elementos que considera la teoría de la información son:

a) Entropía: Una variable aleatoria, tal como el resultado del lanzamiento de un dado, tiene un conjunto de posibles valores, tales como 1, 2, 3, 4, 5 y 6. La entropía de una variable aleatoria depende de las probabilidades de dichos valores.

b) Entropía Condicional: Un importante concepto para el modelo de flujo de información es la entropía condicional. La entropía condicional de X dado Y es una medida de la incertidumbre de X dado el conocimiento acerca de Y. Para cada valor yj de Y, existe una entropía condicional de X dado yj.

c) Canales: Un canal es una caja negra que acepta cadenas de símbolos desde alguna entrada alfabética y emite cadenas de símbolos desde alguna salida alfabética. La teoría de la información define diferentes tipos de canales.

- Un **canal discreto** puede transmitir sólo símbolos desde un número finito de entradas alfabéticas.
- En un **canal sin memoria** la salida es independiente de cualquier entrada o salida anterior.
- Un **canal discreto sin memoria** emite una cadena de la misma longitud que la cadena de entrada.

La capacidad de un canal es una medida de la habilidad del canal para transmitir información. Ésta es expresada (dependiendo del contexto) como un bit por segundo o bits por símbolo.

Un modelo enrejado del flujo de información

Una política del flujo de información define las clases de información que un sistema puede tener y cómo la información puede fluir entre esas clases. Un modelo de flujo de información desarrollado por Dorothy Denning puede expresar la política de multinivel en términos del flujo de información mejor que el control de acceso. Puede también expresar otras políticas más útiles. La política del flujo está definida por un enrejado.

Un enrejado es una estructura matemática que representa el significado de los niveles de seguridad. Un enrejado consiste de un conjunto extra, ordenado parcialmente, del menor límite superior (representado por el operador Å) y el mayor límite inferior (representado por el operador Ä). En un modelo de flujo de información, el enrejado (SC, £, Å, Ä) representa un conjunto de clases de seguridad SC y una relación con la clasificación £ sobre las clases.

Si se tienen las clases A, B y C: A £ B y B £ C implica que A £ C

Una operación causa información del flujo de X a Y si se reduce la entropía condicional de X dado Y. Esto es, la nueva información acerca de X puede obtenerse de Y. La cantidad de información que fluye es medida por la reducción en la entropía condicional H (X | Y). Un flujo potencial es un canal cuya capacidad es la máxima información que puede ser transferida por el flujo.

Una definición precisa de una restricción del flujo de información se encuentra en el concepto de no-interferencia. Un grupo de usuarios no interfiere con otro grupo si las acciones del primer grupo al utilizar ciertos comandos no tienen efecto sobre lo que el segundo grupo puede ver. La no-interferencia fue introducida por Joseph Goguen y José Meseguer entre 1982 y 1984.

Consideraciones en la seguridad del flujo de información

Debido a que la no-interferencia restringe el flujo de información, se observan varios problemas:

1. Los sistemas son modelados como máquinas de estado determinísticas aunque los sistemas frecuentemente son diseñados sin determinismo.
2. Algunos problemas prácticos no pueden ser manejados, como la política de que la información puede fluir a un nivel más bajo al pasar por un degradador confiable.
3. La no-interferencia no está permitida para la generación de datos de alto nivel desde entradas de bajo nivel.
4. La no-interferencia es un requerimiento muy fuerte y los modelos deben ser capaces de expresar una medida cuantificada de interferencia.

2.6.3 Modelos de integridad

Recordando que la integridad se refiere a que la información no sufre modificaciones si éstas no se autorizan, aunado a que es consistente internamente y con los objetos del mundo real que representa y que el sistema ejecuta correctamente, la integridad se define como toda la seguridad exceptuando la confidencialidad y la disponibilidad.

Los sistemas de integridad tienen que ver con la conducta del sistema de acuerdo a las expectativas aun cuando tengan que enfrentar ataques. La integridad de los datos incluye dos tipos de consistencia, ya que éstos deben ser internamente consistentes y consistentes con las entidades del mundo real que representan. Un concepto más amplio de la integridad de los datos es la calidad de los datos, esta calidad incluye atributos como oportunos, genealogía y entereza.

La integridad de los datos tiene las siguientes metas:

- Prevenir las modificaciones no autorizadas
- Mantener la consistencia interna y externa
- Mantener otros atributos de calidad de los datos
- Prevenir las modificaciones autorizadas pero impropias

Los modelos de integridad tienen como objetivo lograr estas metas. Existen dos tipos de modelos:

- Modelo Biba.
- Modelo Clark-Wilson.

Modelo Biba

Creado por K. J. Biba en 1977, el modelo de integridad supone un enrejado de niveles de integridad (análogo a los niveles de seguridad) con una relación ordenada menor o igual. Los objetos son asignados a clases de integridad de acuerdo al daño que sufrirían si fueran modificados de manera inapropiada. Los usuarios son asignados a clases de integridad basadas en su veracidad. Los compartimentos de integridad son interpretados como compartimentos de confidencialidad. El nivel de integridad de un sujeto está basado en el nivel de integridad del usuario que representa y en sus necesidades, de acuerdo al principio del último privilegio.
Biba presenta varios modelos, todos basados en las mismas entidades pero representando diferentes políticas de integridad. El modelo representa la política de integridad estricta el cual intenta ser un doble de la política de confidencialidad Bell-LaPadula. Las entidades del modelo son:

- S, O, I: Conjunto de sujetos, objetos y niveles de integridad.
- il: Una función que define el nivel de integridad de cada sujeto y objeto.
- leq: Relación parcial ordenada sobre los niveles de integridad, menor que o igual.
- min: Una función que regrese el límite inferior del conjunto de I especificado.
- O, m: Relaciones que definen la habilidad de un sujeto s para observar (o) o modificar (m) un objeto o
- i: Una relación que define la habilidad de un sujeto s1 para invocar a otro sujeto s2.

La política de integridad estricta se caracteriza por tres axiomas:

1. Para que un sujeto observe a un objeto, el sujeto debe tener un nivel de integridad menor o igual que el nivel de integridad del objeto.
2. Para que un sujeto modifique un objeto, el objeto debe tener un nivel de integridad menor o igual que el nivel de integridad del sujeto.
3. Para que un sujeto 1 invoque a un sujeto 2, el sujeto 2 debe tener un nivel de integridad menor o igual que el nivel de integridad del sujeto 1.

Los primeros dos axiomas indican que un sujeto no puede observar a un objeto de menor integridad y no puede modificar a un objeto de más alta integridad, el tercero establece que un sujeto no puede invocar a otro sujeto de más alta integridad, dicho axioma trata de prevenir al sujeto invocado de cualquier modificación indirecta de objetos de más alta integridad.

El modelo Biba prueba que bajo los axiomas de integridad estricta, si existe una ruta de transferencia de un objeto o1 a un objeto (on+1) entonces el nivel de integridad del objeto (on+1) es menor o igual que el nivel de integridad del objeto o1, lo cual indica que la información no se transmite a un nivel de integridad más alto. El modelo Biba no se ha utilizado mucho porque no corresponde a una política del mundo real establecida.

Modelo de Clark-Wilson

El modelo de integridad de David Clark y David Wilson desarrollado entre 1987 y 1989 comenzó una revolución en la investigación de la seguridad informática. Aunque no es un modelo altamente formal, es un armazón para describir los requerimientos de la integridad.

Clark y Wilson demostraron que para la mayoría del cómputo relacionado con las operaciones de negocios y el control de los recursos, la integridad es más importante que la confidencialidad. Ellos argumentaban que las políticas de integridad demandan modelos diferentes a los modelos de confidencialidad y diferentes mecanismos ya que se enfocan en dos controles que son centrales en el mundo comercial:

- Las transacciones bien formadas.
- Separación de la obligación.

Las entidades del modelo son:

1. Elementos de datos restringidos (CDIs): Se trata de los elementos cuya integridad debe mantenerse.

2. Procedimientos de transformación (TPs): Estos procedimientos del modelo representan las transacciones bien formadas, manipulan a los CDIs ya que transforman un conjunto de éstos de un estado válido a otro.

3. Procedimiento de verificación de integridad (IVP): Tiene el propósito de confirmar que todos los CDIs están en un estado válido, esto es, ellos reúnen los requerimientos de integridad. El IVP sirve para la consistencia interna y para la consistencia con la realidad externa de acuerdo a la visión de esa realidad. La visión particular de la realidad es llamada dominio de integridad.

4. Elementos de datos no restringidos (UDIs): Como datos de entrada son relevantes porque pueden ser transformados en CDIs.

El sistema debe asegurar que sólo los TPs pueden manipular a los CDIs. Los TPs y los IVPs deben estar certificados con respecto a una política de integridad específica. Un TP debe reunir sus especificaciones y éstas deben ser correctas.

El modelo cuenta con reglas que definen un sistema de aplicación de integridad, a continuación se mencionas estas reglas:

1. Reglas de ejecución (E): Son de aplicación independiente, son fáciles de implementar en el sistema.

2. Reglas de certificación (C): Envuelven el análisis humano y la decisión tomada hasta que alguna automatización sea posible.

Las reglas siguientes relacionan la consistencia interna y externa:

- C1: Todos los IVPs deben asegurar de manera apropiada que todos los CDIs están en un estado válido al momento de que el IVP está corriendo.

- C2: Todos los TPs deben estar certificados para ser válidos. Esto indica que transforman un CDI a un estado final válido, si el CDI está en un estado válido al inicio. Cada TP debe estar certificado para un conjunto específico de CDIs.

- EI: El sistema debe mantener una lista de las relaciones de la regla C2 y debe asegurar que cualquier manipulación de un CDI es mediante un TP y está autorizado por alguna relación.

Las reglas adicionales que se necesitan para la separación de la obligación son:

- E2: El sistema debe mantener una lista de relaciones que enlacen al usuario, al TP y los CDIs que el TP debe manipular a favor de ese usuario.
- C3: La lista de relaciones de E2 debe estar certificada para conocer la separación de la obligación requerida.

Otras cuatro reglas completan el modelo. Éstas especifican que:

- E3: Los usuarios que invocan TPs deben ser autenticados.
- C4: Todos los TPs deben certificar para que pueda tener acceso de entrada.
- C5: Los TPs que transforman UDIs a CDIs deben estar certificados.
- E4: Sólo ciertos usuarios designados deben especificar las relaciones.

Estas reglas ejecutan una política obligatoria de integridad. Este armazón para la integridad conlleva a un conjunto de requerimientos para los servicios de seguridad informática:

1. Cambio de registros y etiquetas de integridad: La autoría debe ser guardada con los datos (para soportar la política de atribución de cambio), la etiqueta de integridad registra que los datos fueron certificados por un IVP y qué dominio de integridad fue utilizado.

2. Soporte del acceso triple: Para ejecutar la política de cambio restringido, el control de acceso triple enlaza al usuario, al programa y a los datos.

3. Autenticaciones mejoradas de usuarios: Aunque la autenticación es necesaria para la confidencialidad, tiene una importancia especial para la integridad en particular con la política de separación de la obligación. Las contraseñas son inadecuadas, ya que pueden ser reveladas u observadas, permitiendo así que alguien actúe como dos personas diferentes, violando las reglas de separación de la obligación.

4. Control de los usuarios privilegiados: La separación de la obligación debe ser ejecutada por la gente que mantiene los accesos triples o quienes certifican TPs.

5. Control del programa de aplicación: Un sistema necesita herramientas automatizadas para manejar las aplicaciones de software y asegurar su integridad.

6. Separación dinámica de la obligación relacionada a los TPs: La separación de la obligación seguido requiere que los diferentes pasos en una secuencia se cumplan por

diferentes personas. Aunque una tarea estática puede reunir este requerimiento, un acercamiento más flexible es para que el sistema mantenga la pista de quién ha ejecutado cada paso y realizar la separación de la obligación a cada paso. Esto es parecido a lo que pasa en el mundo real.

CAPÍTULO 3

TIPOS DE SEGURIDAD

3.1 Seguridad Física

Cuando hablamos de Seguridad Física nos referimos a todos aquellos mecanismos, generalmente de prevención y detección, destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una disco con toda la información que hay en el sistema, pasando por el propio CPU de la máquina. Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta.

Debemos ser concientes de que la Seguridad Física es demasiado importante como para ser ignorada: un ladrón que roba una computadora para venderla, un incendio o un pirata informático que accede sin problemas a la sala de servidores nos pueden hacer más daño que un intruso que intenta conectarse remotamente con una máquina no autorizada; no importa que se utilicen los más avanzados medios de cifrado para impedir conectarse a nuestros servidores, ni que se haya definido una política extremadamente restrictiva; si no tenemos en cuenta factores físicos, estos esfuerzos para proteger la información no van a servir de nada.

Además, en el caso de organismos e instituciones con requerimientos de seguridad, las medidas de seguridad físicas ejercen un efecto disuasorio sobre la mayoría de piratas informáticos. Como casi todos los atacantes de estos entornos son casuales (esto es, no tienen interés específico sobre un equipo en particular, sino sobre cualquier equipo), si notan a través de medidas físicas que una organización e institución está preocupada por la seguridad probablemente abandonarán el ataque para lanzarlo contra otra red menos protegida.

Se debe recordar que cada sitio es diferente, y por tanto también lo son sus necesidades de seguridad; de esta forma, pueden variar desde el simple sentido común hasta medidas mucho más complejas. En entornos habituales suele ser suficiente con un poco de sentido común para conseguir una mínima seguridad física; de cualquier forma, en cada organización e institución se ha de analizar el valor de lo que se quiere proteger y la probabilidad de las amenazas potenciales, para en función de los resultados obtenidos diseñar un plan de seguridad adecuado.

3.1.1 Definición

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

El *hardware* es frecuentemente el elemento más caro de todo el entorno de nuestra red. Por tanto, las medidas encaminadas a asegurar su integridad son una parte importante de la Seguridad Física de cualquier organización e institución, se cuenta muchas veces con equipos muy caros, desde servidores con una gran potencia de cálculo hasta *routers* de última tecnología, pasando por modernos sistemas de transmisión de datos como la fibra óptica.
Son muchas las amenazas al *hardware* de una instalación informática; por lo cual habrá que hacer un estudio de estas.

3.1.2 Desastres

Un problema que no suele ser tan habitual, pero que en caso de producirse puede acarrear gravísimas consecuencias, es el derivado de los desastres naturales y su falta de prevención.

3.1.2.1 Desastres Naturales

- Terremotos

Los terremotos son el desastre natural que son muy factibles en México por su localización geográfica, pero es importante remarcar que no todos los estados son propensos a este tipo de desastre aún así por el alto índice de presencia de terremotos se debe de hacer una consideración importante, al mismo tiempo saber si la zona donde se pretende implementar una red será victima de temblores de intensidad considerable.

De cualquier forma, aunque algunas medidas contra terremotos pueden ser excesivamente caras para la mayor parte de organizaciones e instituciones y muchas veces es debido a que no se hace un estudio de la zona en particular. No cuesta nada tomar ciertas medidas de prevención; por ejemplo, es muy recomendable no situar nunca equipos delicados en superficies muy elevadas. Si lo hacemos, un pequeño temblor puede tirar desde una altura considerable un equipo de cómputo, lo que con toda probabilidad lo inutilizará; puede incluso ser conveniente y barato utilizar fijaciones para los elementos más críticos, como los CPU, los monitores o los routers. De la misma forma, tampoco es recomendable situar objetos pesados en superficies altas cercanas a los equipos, debido a que si llegaran a caer estos objetos podrían dañar severamente dichos equipos, dejándolos inutilizables para su uso.

Para evitar males mayores ante un terremoto, también es muy importante no situar equipos cerca de las ventanas, esto es debido a que si se produce un temblor pueden caer encima de los equipos, y en este caso la pérdida de datos o de hardware. Por consiguiente, situando los equipos alejados de las ventanas estamos dificultando las acciones de un potencial ladrón que se cuelgue por la fachada hasta las ventanas, ya que si el equipo estuviera cerca no tendría más que alargar el brazo para llevárselo.

Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de los equipos de cómputo, especialmente si se trata de vibraciones continúas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas. Para hacer frente a pequeñas vibraciones podemos utilizar plataformas de goma donde situar a los equipos, de forma que la plataforma absorba la mayor parte de los movimientos; incluso sin llegar a esto, una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con hardware más mecánico, como las impresoras. Estos dispositivos no paran de generar vibraciones cuando están en funcionamiento, por lo que situar una pequeña impresora encima de la CPU de una máquina es una mala idea.

- Tormentas Eléctricas

Las tormentas eléctricas generan subidas súbitas de tensión infinitamente superiores a las que pueda generar un problema en la red eléctrica. Si cae un rayo sobre la estructura metálica del edificio donde están situados los equipos es casi seguro que podemos ir pensando en comprar otros equipos; sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir nuestro hardware incluso protegido contra voltajes elevados.

Muchas veces no tomamos en consideración el daño que pueden causarnos las tormentas eléctricas por lo que hay veces que no tomamos una medida muy fácil de implementar, la cual consiste en apagar los equipos cuando se presenta una tormenta eléctrica. Así como, dejar de suministrar energía a toda la red en concreto. Un rayo en el propio edificio, o en un lugar cercano, puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todos nuestros discos, lo que se añade a los problemas por daños en el hardware y la pérdida de toda la información de nuestros sistemas.

- Inundaciones y Humedad

Cierto grado de humedad es necesario para un correcto funcionamiento del equipo: en ambientes extremadamente secos el nivel de electricidad estática es elevado, lo que puede transformar un pequeño contacto entre una persona y un circuito, o entre diferentes componentes de una máquina, un daño irreparable tanto en el hardware como en la información. No obstante, niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una computadora.

Cuando ya no se habla de una humedad más o menos elevada sino de completas inundaciones, los problemas generados son mucho mayores. Casi cualquier medio (una máquina, una disco, un *router*...) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos. Evidentemente, contra las inundaciones las medidas más efectivas son las de prevención (frente a las de detección); podemos utilizar detectores de agua en los pisos o pisos falsos suelos de las salas de operaciones, y apagar automáticamente los sistemas en caso de que se activen. Después de apagar los sistemas podemos tener también instalado un sistema automático que corte la corriente, algo muy común es intentar sacar los equipos (previamente apagados o no) de una sala que se está empezando a inundar; esto, que a primera vista parece lo lógico, es el mayor error que se puede cometer si no se ha desconectado completamente el sistema eléctrico, ya que la mezcla de corriente y agua puede causar incluso la muerte a quien intente salvar los equipos.

Medidas de protección menos sofisticadas pueden ser la instalación de un piso falso por encima del piso real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos por los problemas que se pueden causar en caso de terremotos y vibraciones.

3.1.2.2 Desastres del entorno

Este tipo de problemas se pueden presentar de manera habitual, los cuales se encuentran alrededor del entorno en el que esta la red instalada debido muchas veces a aparatos de tipo electrónico, es por eso que son muy importantes de tomar en cuenta.

- Electricidad

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo, etc. Que a diario amenazan la integridad tanto de nuestro hardware como de los datos que almacena o que circulan por él.

El problema menos común en las instalaciones modernas son las subidas de tensión, conocidas como “picos” porque generalmente duran muy poco; durante unas fracciones de segundo el voltaje que recibe un equipo sube hasta sobrepasar el límite aceptable que dicho equipo soporta. Lo normal es que estos picos apenas afecten al hardware. Una toma de tierra sencilla puede consistir en un buen conductor conectado a los chasis de los equipos a proteger y a una barra maciza, también conductora, que se introduce en el suelo; realizando una preparación especial del área de la barra metálica el costo de la instalación es pequeño, especialmente si lo comparamos con las pérdidas que supondría un incendio que afecte a todos o a una parte de los equipos.

Otro problema en redes eléctricas modernas, son los cortes en el fluido eléctrico que llega a los equipos. Aunque un simple corte de corriente no suele afectar al *hardware*, lo más peligroso (y que sucede en muchas ocasiones) son cortes rápidos de la corriente; en esta situación, aparte de perder datos, nuestros equipos pueden sufrir daños.

La forma más efectiva de proteger nuestros equipos contra estos problemas de la corriente eléctrica es utilizar un No-break conectada al elemento que se pretende proteger. Estos dispositivos mantienen un flujo de corriente correcto y estable de corriente, protegiendo así los equipos de variaciones y cortes de voltaje; tienen capacidad para seguir alimentando las máquinas incluso en caso de no recibir suministro eléctrico durante un tiempo razonable para almacenar la información y apagar correctamente nuestro equipo, el No-break podrá solucionar la mayoría de los problemas relacionados con la red eléctrica.

- Ruido eléctrico.

Este problema no es una incidencia directa de la corriente en los equipos de cómputo, sino una incidencia relacionada con la corriente de otras computadoras que pueden afectar al funcionamiento de la máquina. El ruido eléctrico suele ser generado por motores o por maquinaria pesada, pero también puede serlo por otras computadoras o por la multitud de aparatos.

Para prevenir los problemas que el ruido eléctrico puede causar en los equipos de cómputo lo más barato es intentar no situar el *hardware* de aparatos que puedan causar dicho ruido; si no

tenemos más remedio que hacerlo, se pueden instalar filtros en las líneas de alimentación que llegan hasta las computadoras. También es recomendable mantener alejados de los equipos dispositivos emisores de ondas, como teléfonos móviles, transmisores de radio o walkie-talkies; estos elementos puede incluso dañar permanentemente al *hardware* si tienen la suficiente potencia de transmisión, o influir directamente en elementos que pueden dañarlo como detectores de incendios o cierto tipo de alarmas.

- Incendios y Humo

Una causa casi siempre relacionada con la electricidad son los incendios, y con ellos el humo; aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido. Un simple cortocircuito o un equipo que se caliente demasiado puede convertirse en la causa directa de un incendio en el edificio.

Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor. Algunos de ellos, los más antiguos, utilizaban agua para apagar las llamas, lo que provocaba que el *hardware* no llegara a sufrir los efectos del fuego si los extintores se activaban correctamente, pero si funcionaban erróneamente el equipo quedaría incompletamente inutilizable. Visto este problema, a mitad de los ochenta se comenzaron a utilizar extintores de halón; este compuesto no conduce electricidad ni deja residuos, por lo que resulta ideal para no dañar los equipos. Sin embargo, también el halón presentaba problemas; por un lado resulta excesivamente contaminante para la atmósfera, y por otro puede asfixiar a las personas, a la vez que acaba con el fuego. Por eso se han sustituido los extintores de halón (aunque se siguen utilizando mucho hoy en día) por extintores de dióxido de carbono, menos contaminante y menos perjudicial. De cualquier forma, al igual que el halón el dióxido de carbono no es precisamente sano para los humanos, por lo que antes de activar el extintor es conveniente que todo el mundo abandone la sala; si se trata de sistemas de activación automática suelen avisar antes de expulsar su compuesto mediante un sonido.

Aparte del fuego y el calor generado en un incendio existe un tercer elemento perjudicial para los equipos. El humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos. Quizás ante un incendio el daño provocado por el humo sea insignificante en comparación con el causado por el fuego y el calor.

En muchos manuales de seguridad se insiste a los usuarios, administradores, o al personal en general a intentar controlar el fuego y salvar el equipo; esto tiene, como casi todo, sus pros y sus contras. Evidentemente, algo lógico cuando estamos ante un incendio de pequeñas dimensiones es intentar utilizar un extintor para apagarlo, de forma que lo que podría haber sido una catástrofe sea un simple susto o un pequeño accidente. Sin embargo, cuando las dimensiones de las llamas son considerables lo último que debemos hacer es intentar controlar el fuego nosotros mismos, arriesgando vidas para salvar *hardware*; Lo más recomendable en estos casos es evacuar el lugar del incendio y dejar su control en manos de personal especializado.

El personal designado para usar extinguidores de fuego debe de ser entrenado en su uso, otra opción sería implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio, si este llegara a originarse en las áreas adyacentes.

- Temperaturas Extremas

Un calor excesivo o un frío intenso, perjudican gravemente a todos los equipos. Es recomendable que los equipos no deberán sobrepasar los 18 ºC y el límite de humedad no debe de superar el 65% para evitar el deterioro, aunque pequeñas variaciones en este rango tampoco han de influir en la mayoría de sistemas.

Para controlar la temperatura ambiente en el entorno de operaciones nada mejor que un aire acondicionado, aparato que también influirá positivamente en el rendimiento de los usuarios (las personas también tenemos rangos de temperaturas dentro de los cuales trabajamos más cómodamente). Otra condición básica para el correcto funcionamiento de cualquier equipo que éste se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU. La organización física del computador también es decisiva para evitar sobrecalentamientos: si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

- Cableado

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con cables instalados para evitar el tiempo y el gasto posterior, de forma que se minimice el riego de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

- **Interferencia:** Pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas, Los cables de microondas no sufren el problema de alteración (de los datos que viajan a través de el) por acción de campos eléctricos, que si sufren los cables metálicos.
- **Corte del cable:** La conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
- **Daños en el cable:** Los daños normales con el uso pueden dañar el propio cable, lo que ocasiona que las comunicaciones dejen de ser fiables.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intente acceder a los datos. Esto se puede hacer:

- **Desviando o estableciendo una conexión no autorizada en la red:** Un sistema de administración y procedimiento de identificación que puedan dar accesos adecuados hará fácil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable puede estar en peligro.

3.2 Seguridad Lógica

Existe un viejo dicho en la seguridad informática que dice lo siguiente: “Todo lo que no esta permitido debe de estar prohibido” y esto es lo que debe de asegurar la seguridad lógica. El activo más importante que se posee es la información, y por lo tanto deben de existir técnicas, más allá de la seguridad física, que lo aseguren.

3.2.1 Definición

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

Los objetivos que se deberán de plantear son los siguientes:

- La restricción al acceso de programas y archivos.
- El poder asegurar que los usuarios pueden trabajar sin una supervisión que sea muy minuciosa, así como no puedan modificar los programas ni los archivos que no correspondan.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no por otro.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

3.2.2 Controles de Acceso

Estos controles de acceso podrán ser implementados mediante un tipo de software especial en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos o en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

3.2.3 Identificación y Autenticación

Será una de las primeras defensas permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina ***Identificación*** al momento en que el usuario se da a conocer en el sistema; y ***Autenticación*** a la verificación que realiza el sistema sobre esta identificación.

Existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- **Algo que solamente el individuo conoce**: Por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- **Algo que la persona posee:** Por ejemplo una tarjeta magnética.
- **Algo que el individuo es y que lo identifica unívocamente:** Por ejemplo las huellas digitales o la voz.
- **Algo que el individuo es capaz de hacer:** Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultoso de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single login" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas. La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Esta administración abarca:

- Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior, y de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
- Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la Organización o Institución.
- Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos.
- Detección de actividades no autorizadas. Además de realizar auditorías o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.

- Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
- Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarios de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

3.2.4 Funciones

El acceso a la información también puede controlarse a través de la función del usuario que requiere dicho acceso. Algunos ejemplos de funciones serían los siguientes: programador, líder de proyecto, gerente de un área, usuario, administrador del sistema, etc.

En este caso los derechos de acceso pueden agruparse de acuerdo con el función de los usuarios así sería mucho más sencillo definir los permisos en grupo y la ubicación sería más sencilla.

3.2.5 Transacciones

En este caso sería muy eficiente el poder implementar un control a través de las transacciones, pongamos de ejemplo la transacción de un archivo, en este caso pedir una clave en especial para asegurar el procesamiento de una transacción determinada.

3.2.6 Limitaciones a los Servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

Un ejemplo podría ser que en la organización o institución se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

3.2.7 Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser de la siguiente manera, así como lo muestra la figura (3.0).

- **Lectura:** El usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- **Escritura:** Este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución:** Este acceso otorga al usuario el privilegio de ejecutar programas.
- **Borrado y Modificación:** Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- **Creación:** Permite al usuario crear nuevos archivos, registros o campos.
- **Control Total:** Este acceso permitirá todas las anteriores, para estos casos hay que considerar bien quien tendrá este tipo de privilegios.

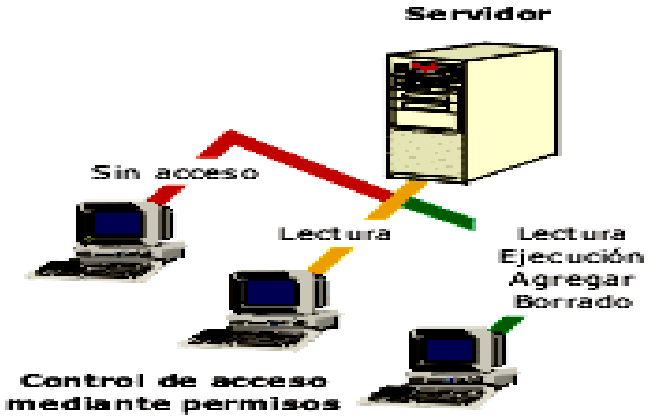


Figura 3.0 Modalidad de Acceso

3.2.8 Ubicación y Horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación tanto lógica como física de los datos o de las personas. Los horarios en cuanto se refiere a los controles que permiten controlar el acceso de los usuarios a determinadas horas del día o a determinados días de la semana.

3.2.9 Control de Acceso Interno

Cuando se quiere accesar a la computadora se hace una identificación donde se pretende identificar al usuario y de esta manera poder también proteger datos o aplicaciones que sean de suma importancia, así como asignar privilegios sobre los mismos, a continuación se desglosará los tipos de control de acceso interno.

3.2.9.1 Palabras Claves (Passwords)

Se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y

probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

- **Sincronización de passwords:** Consiste en permitir que un usuario acceda con la misma clave a diferentes sistemas interrelacionados, y su actualización automática en todos ellos en caso de ser modificada.

- **Caducidad y control:** Estos mecanismos controlan cuándo pueden y deben cambiar claves los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

3.2.9.2 Encriptación

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

3.2.9.3 Listas de Control de Accesos

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

3.2.9.4 Límites sobre la Interfase de Usuario

Estos límites generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario.

3.2.10 Control de Acceso Externo

No sólo basta con un control de acceso interno, si no también se debe de implementar un control de acceso externo esto es debido a que la red en general esta conectada también con el resto del mundo, millones de comunicaciones se llevan acabo a cada segundo, es por esta razón que se deben de filtrar y monitorear las comunicaciones, cerrando o abriendo puertos según sea el caso.

3.2.10.1 Dispositivos de Control de Puertos

Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

3.2.10.2 Firewalls o Puertas de Seguridad

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa. Los Firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización.

3.2.10.3 Accesos Públicos

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

3.2.10.4 Administración

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que desarrolla respecto a la seguridad lógica deberán guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información. Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las ***medidas de seguridad sobre la información más sensible*** o ***las aplicaciones más críticas***, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones. Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

- Administración del personal y usuarios.
- Organización del personal.

Este proceso lleva generalmente cuatro pasos:

- **Definición de puestos:** Debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
- **Determinación de la sensibilidad del puesto:** Para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.

- **Elección de la persona para cada puesto:** Requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Así mismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales.
- **Entrenamiento inicial y continuo del empleado:** Cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tareas que se asignen, deberán ser comunicadas las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo deberá conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores. Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual.

3.3 Seguridad en Redes

Introducción

En la actualidad, las organizaciones e instituciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red. A la hora de plantearse en qué elementos del sistema se deben de ubicar los servicios de seguridad podrían distinguirse dos tendencias principales:

Protección de los sistemas de transferencia o transporte: En este caso, el administrador de un servicio asume la responsabilidad de garantizar la transferencia segura al usuario final de la información de forma lo más transparente posible. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, de un servicio de mensajería con MTAs (Mail Transport Agents) seguras, o la instalación de un Firewall, que defiende el acceso a una parte protegida de una red.

Aplicaciones seguras extremo a extremo: Si pensamos, por ejemplo, en el correo electrónico, consistiría en construir un mensaje en el cual el contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío. De esta forma, el mensaje puede atravesar sistemas heterogéneos y poco fiables sin perder la validez de los servicios de seguridad provistos. Aunque el acto de asegurar el mensaje cae bajo la responsabilidad del usuario final, es razonable pensar que dicho usuario deberá usar una herramienta amigable proporcionada por el responsable de seguridad de su organización. Esta misma operación, puede usarse para

abordar el problema de la seguridad en otras aplicaciones tales como videoconferencia, acceso a bases de datos, etc.

En ambos casos, un problema de capital importancia es la gestión de claves. Este problema es inherente al uso de la criptografía y debe estar resuelto antes de que el usuario esté en condiciones de enviar un solo bit seguro.

3.3.1 Sistemas de Protección

Definición de Seguridad en Redes

Seguridad en Redes: Es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo que se pretende mantener protegido.

Para una buena seguridad en la red se deberá tomar en cuenta los siguientes puntos:

- **Sistema de Archivos:** Se debe garantizar a los usuarios autorizados que sólo ellos pueden acceder a los archivos o modificarlos.

- **Código malicioso:** Se denomina *malicioso,* al código que se inserta dentro de un programa "autorizado" y que realiza una serie de acciones desconocidas para el usuario, las cuales, además actúan normalmente en su perjuicio.

- **Autenticación de usuarios:** Proceso de verificación de la identidad de una persona en el momento de acceder a un recurso. Habitualmente, los usuarios se autentican mediante un nombre de usuario y una contraseña (existen diferentes tipos de autenticación y diferentes políticas de asignación de contraseñas, que puede determinar un administrador).

- **Criptografía:** El uso de herramientas criptográficas permite garantizar la confidencialidad de los datos que circulan por la red o que se encuentran almacenados en un sistema informático.

1. - Criptografía Simétrica por Sustitución

Es el sistema más básico. La clave consiste en una tabla de equivalencias de caracteres. Esta clave es llamada "simétrica" porque es la misma clave la que se utiliza para codificar y para decodificar.

2.- Criptografía Simétrica por Permutación

Consiste en alterar el orden de las letras siguiendo una regla determinada. Normalmente se utiliza una tabla de tamaño determinado en la que se inserta el texto original que es transformado mediante la sustitución de las columnas por las filas.

3.- Criptografía Asimétrica

La criptografía de clave asimétrica o pública fue inventada en 1976 por los matemáticos Whit Diffie y Martín Hellman y es la base de la moderna criptografía.

La criptografía asimétrica utiliza dos claves complementarias llamadas clave privada y clave pública. Lo que está codificado con una clave privada necesita su correspondiente clave pública para ser descodificado. Y viceversa, lo codificado con una clave pública sólo puede ser descodificado con su clave privada.

Firmas Digitales

La comunicación electrónica permite un sistema de firma mucho más segura. Las firmas digitales consisten en una función hash del texto codificada con nuestra clave privada. Este sistema garantiza a la vez nuestra identidad y que el texto no ha sido modificado ni en una sola coma.

Certificados Electrónicos

Un certificado electrónico es la acreditación por una entidad de que una clave pública se corresponde realmente a la identificación del usuario. El certificado va firmado digitalmente por la entidad que lo emite.

Las características de los certificados son los siguientes:

Los certificados electrónicos que siguen el estándar X.509 tienen los siguientes campos.

1.- Versión.
2.- Número de serie.
3.- Identificador del algoritmo empleado para la firma digital.
4.- Nombre del certificador.
5.- Periodo de validez.
6.- Nombre del sujeto.
7.- Clave pública del sujeto.
8.- Identificador único de certificador.
9.- Identificador único de sujeto.
10- Extensiones.
11- Firma digital de todo lo anterior generada por el certificador.

Sistemas de Encriptación

Para que lo visto anteriormente (claves simétricas, asimétricas, funciones hash, certificados digitales) tengan utilidad comercial, es necesario implementarlos en programas y sistemas orientados al usuario. Hay que tener en cuenta por tanto que los usuarios no conocen, ni les interesa, nada de criptografía.

Sistemas de Encriptación PGP

PGP es un protocolo de seguridad diseñado a comienzos de los 90 por Phill Zimmerman. La exportación del sistema fuera de los Estados Unidos le valió a su creador un largo proceso judicial, acusado de exportación de armas de valor estratégico.

En la actualidad, las versiones más avanzadas del programa PGP siguen sin poder ser exportadas legalmente de USA, pero su código fuente es considerado un artículo científico que puede ser divulgado y compilado en el exterior.

Sistemas de Encriptación SET

Es un protocolo elaborado por iniciativa de VISA y MasterCard al que se adhirieron un gran número de grandes bancos y empresas de software de todo el mundo.
La diferencia principal del sistema SET con respecto al sistema PGP es que cada clave pública va asociada a un certificado de autenticidad emitido por una autoridad de certificación (AC). Los certificados digitales y credenciales electrónicas, son documentos digitales que atestiguan la relación entre una clave pública y un individuo o entidad. Las AC asumen la responsabilidad de garantizar que los individuos o instituciones acreditadas son quienes dicen ser.

Sistemas de Encriptación SSL y SHTTP

El protocolo de seguridad SSL (Secure Sockets Layers) fue diseñado inicialmente por Marc Andreessen. Este sistema es utilizado para realizar transacciones y pagos vía Internet. Por ejemplo, la tienda virtual que acepte pagos mediante estos sistemas debe estar instalada en un servidor seguro, que disponga del software correspondiente. El vendedor, además, tiene que disponer de un par asimétrico de claves, certificadas por una autoridad.

El comprador no necesita tener ni claves, ni certificados, ni saber que existen. Cuando el usuario accede con su navegador (Internet Explorer, Netscape, Opera,...) a una tienda virtual con SSL, se inicia automáticamente una fase de saludo. El servidor envía su clave pública y certificación. El navegador cliente recibe estos datos y se prepara para la comunicación con sistema de seguridad.

3.3.2 Herramientas de seguridad

Se puede hacer uso de varias herramientas con la finalidad de comprobar y mantener la seguridad de la red. En general, podemos diferenciar las siguientes:

- Herramientas para comprobar la vulnerabilidad de las mismas máquinas.
- Herramientas que ofrecen servicios seguros.
- Herramientas que garantizan la integridad del sistema.

• **Monitorización del sistema**: Es el procedimiento mediante el cual se registran en un archivo las actividades que tienen lugar en un sistema operativo o en una aplicación. La importancia de los archivos *log* es evidente, y nos permitirá averiguar qué ha sucedido en un sistema

informático y, si es necesario, tomar las medidas adecuadas. Es muy importante plantear *qué* aplicaciones debe registrar el *log* y *cuándo* lo debe efectuar, así como cuándo se han de eliminar o enviar a un dispositivo de almacenamiento para, de este modo, tener espacio suficiente en el sistema.

• **Seguridad de las topologías y los tipos de red:** En una configuración normal de red, el Firewall suele ser un elemento fundamental de la seguridad que reúne una gran parte de las medidas de protección que evitan los ataques exteriores. En cambio, en una red sin hilos los atacantes no necesitan “pasar” por el Firewall, y pueden atacar directamente otros dispositivos de la red.

• **Seguridad del hardware de red:** En relación con la seguridad de los conmutadores, hubs, routers y concentradores es necesario tener en cuenta los siguientes aspectos:

- Activación del cifrado (en el caso de que los dispositivos lo admitan).
- En el caso de que no sea necesario, debemos desactivar el control remoto de administración.
- Cambiar las contraseñas de administración predeterminadas de estos dispositivos.

• **Seguridad de los servidores:** En un gran sistema centralizado, donde existe una gran cantidad de datos críticos y usuarios, es importante garantizar la seguridad en los servidores de amenazas accidentales o deliberadas.

La solución más sencilla sería mantener los servidores en una habitación de equipos con acceso restringido. Esto puede no resultar factible dependiendo del tamaño de la organización. No obstante, encerrar los servidores en una oficina, es factible y nos proporciona una forma de intentar garantizar la seguridad de los mismos.

▪ **Seguridad del cableado:** El medio de cobre, como puede ser el cable coaxial, al igual que una radio emite señales electrónicas que simulan la información que transporta. La información transportada en estas señales se puede monitorizar con dispositivos electrónicos de escucha.

Además, se puede intervenir el cable de cobre pudiendo robar la información que se transmite en el cable original.

Sólo el personal autorizado deberá tener acceso al cable que transporta datos sensibles. Una planificación apropiada puede garantizar que el cable sea inaccesible al personal no autorizado. Por ejemplo, el cable puede instalarse dentro de la estructura del edificio a través del techo, paredes y pisos falsos.

• **Firewall (cortafuego):** Un Firewall es cualquier sistema utilizado para separar una máquina o una subred del resto de la red para protegerla de intrusiones externas que puedan suponer una amenaza a la seguridad. La zona protegida se llama "perímetro de seguridad" y la protección se realiza separándola de una zona externa, no protegida, llamada zona de riesgo. El administrador debe instalar estos dispositivos, teniendo en cuenta la estructura de la red, y determinar los

servicios que deben quedar disponibles para los usuarios. En la práctica, las funciones del Firewall las pueden llevar a cabo diferentes dispositivos.

- Software.
- Computadoras dedicadas exclusivamente a las tareas de filtración de paquetes (servidores intermediarios, *Proxy*).

3.4 Seguridad en Internet

Entre las principales razones de la popularización y el éxito de Internet está el hecho de ser una red abierta. Como el protocolo utilizado por los ordenadores que se conectan a Internet, TCP/IP, es gratuito, cualquier red y cualquier ordenador puede conectarse sin más costo que los de la conexión. No hay ningún propietario de Internet, no hay ninguna autoridad central que pueda imponer un precio o unas condiciones diferentes de las estrictamente técnicas.

Hay cientos de millones de usuarios. El cálculo estadístico de cuántos individuos tienen acceso a Internet ha perdido ya sentido. Hay clubes, Cafés-Internet y salas de cómputo por instituciones privadas o públicas en ciudades de todo el mundo, incluyendo los países menos desarrollados, por lo que son miles de millones los individuos que pueden en cualquier momento, por un costo muy pequeño, conectarse a Internet. Esta extraordinaria facilidad de acceso y popularidad es el principal atractivo desde el punto de vista comercial pero también es la causa de que Internet esté abierto a todo tipo de gente.

Las comunicaciones comerciales realizadas por medios tradicionales, cartas o teléfono, son mucho más fáciles de interceptar que las comunicaciones a través de Internet. Realizar actividades delictivas a través de Internet requiere unos conocimientos técnicos sofisticados que no están al alcance de cualquiera.

Por otra parte, las posibilidades de protección de las comunicaciones electrónicas son mayores que las que permiten los medios tradicionales. Hay programas de computadora gratuitos y muy fáciles de usar que permiten a cualquier usuario la encriptación de sus mensajes de forma que queda plenamente garantizado que sólo el destinatario podrá entenderlos. Los certificados y firmas electrónicas garantizan la identidad de los sujetos con mucha mayor garantía que cualquier otro documento tradicional. Los sistemas de almacenamiento de datos y su protección frente a accidentes o ataques intencionados son más fáciles, baratos y seguros que las cajas fuertes o cámaras de seguridad.

Lo que ocurre es que no hay una “cultura” de la seguridad en Internet. La sociedad en que vivimos nos ha enseñado desde que éramos niños reglas básicas de protección de nuestras propiedades. El gesto de cerrar la puerta de casa, los límites que nos imponemos a la cantidad de efectivo que llevamos en el bolsillo, la forma en que reaccionamos cuando nos aborda un extraño por la calle, son comportamientos que hemos aprendido a lo largo de nuestra vida. En cambio nuestra experiencia con Internet es muy breve y ni nuestros padres ni nuestros profesores nos dijeron nunca cómo debíamos comportarnos en el ciberespacio.

La seguridad en Internet y las leyes que la protegen, están basadas principalmente en los sistemas de encriptación. Esos sistemas son los que permiten que la información que circula por Internet sea indescifrable, ininteligible, para cualquier persona que no sea aquella a la que va destinada.

Como se vio en el Capitulo 2 se mencionaron los tipos de ataque y dentro de esta clasificación mencionamos aquellos que perpetúan nuestra seguridad en Internet, muchas veces no tenemos una noción muy clara de lo que nos pueda atacar y de qué manera pero podemos seguir reglas básicas que ayudaran a tener una base de seguridad.

3.4.1 Las Reglas de Seguridad

En la protección de nuestros bienes, incluyendo la información, debemos seguir tres reglas lógicas básicas para evitar incoherencias.

- PRIMERA

La seguridad debe cubrir todos los huecos. La máxima seguridad que tenemos es la del elemento más débil del sistema.

- SEGUNDA

Los niveles de seguridad deben ser adecuados al entorno ¿Qué medidas de seguridad toman los demás? ¿Cómo se protegen los que tienen lo mismo que yo?.

Unas medidas de seguridad muy superiores a lo normal no solo serán muy costosas sino que pueden llegar a ser contraproducentes por llamar la atención.

Para evitar que te coman no es necesario correr más que el león, es suficiente con correr más que las otras gacelas.

- TERCERA

La seguridad debe ser adecuada a la necesidad de protección de lo asegurado y a los recursos disponibles.

Se trata de hacer una valoración de riesgos y de los costos de la protección de forma que en ningún momento los costos superen a los riesgos.

Para la evaluación de riesgos hay que preguntarnos lo siguiente:

- ¿Qué queremos proteger?
- ¿Cuál es su valor?
- ¿Qué riesgos existen?
- ¿Quién puede atacar?

> Los hackers valoran en mucho haber entrado en una computadora muy protegida aunque la información existente en ese ordenador no les sea de ninguna utilidad.

Estas son reglas básicas pero indispensables que se pueden adecuar a las necesidades básicas del entorno, así como de lo que queremos y pretendemos proteger.

3.5 El Derecho Informático

Hoy en día la tecnología avanza a pasos agigantados por desgracia una cultura de seguridad y respeto no ha sido muy bien planteada, creemos que el cometer delitos vía Internet no tiene repercusiones pero de igual manera es momento de abrir campo a proteger nuestros intereses.

La informática debe contar con un marco regulador y el derecho de tener un respaldo en el procesamiento de datos que proporciona la primera, de esta manera, la interrelación entre el derecho y la informática tiene dos puntos fundamentales; una primera donde el derecho utiliza a la informática como herramienta para el diseño de medios de compilación y resguardo de información que ha sido denominada Informática Jurídica; además, existe un segundo punto donde la informática se apoya en el derecho para integrar un marco regulador de sus actividades, conocido como Derecho de la Informática.

3.5 Políticas de Seguridad

La información vista como activo y los equipos informáticos son recursos vitales e importantes de una organización o institución. El valor que se le da a estos es de suma importancia al momento de tomar dicho nombre, por lo cual tenemos 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.

La información perteneciente a la organización o institución debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo se guarda la información, o cómo se procesa (PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica, etc). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Los distintos departamentos de una organización o institución están en el **Deber** y en la **Responsabilidad** de dar el tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos. Así como tener un Departamento de Seguridad donde se implemente un plan anual de revisión de políticas, así como de dar un informe de las mismas y cual ha sido el resultado de las mismas.

A todos los empleados, consultores y contratistas deberán de proporcionárseles adiestramiento, información y advertencias para que ellos puedan proteger y manejar apropiadamente los

recursos informáticos de la organización. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la organización como lo son otras áreas.

La política de seguridad debe desarrollarse como un esfuerzo conjunto entre el personal técnico, que comprenderá las implicaciones de implementar las diferentes propuestas y la directiva, la cual está capacitada para destinar los recursos necesarios y ejecutar la política en sí. Una política que no sea implementable ni ejecutable es inútil. También resulta vital lograr que todas y cada una de las personas de la organización conozca su responsabilidad en cuanto a la seguridad. La política de seguridad no puede anticipar todas las posibilidades, pero puede asegurar que para cada tipo de problema hay alguien asignado como responsable del mismo. De esta forma, pueden asignarse niveles de responsabilidad, desde el usuario, responsable de la seguridad en cuanto a acceso de su equipo de cómputo, hasta el administrador de seguridad, que responderá ante un director general. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

3.5.1 Definición

Una política de seguridad es una forma de comunicarse con los usuarios y la gente que forma parte de una organización o institución. Las políticas de seguridad establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes en la organización.
No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de lo que se desea proteger y el porque de ello.

3.5.2 Elementos de una Política de Seguridad

Una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la organización para lograr una visión conjunta de lo que se considera importante. Las políticas de seguridad deben considerar entre otros, los siguientes elementos:

Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las Políticas de Seguridad deben ofrecer explicaciones comprensibles acerca del por qué deben tomarse ciertas decisiones, así como de la importancia de ser transmitidos otros recursos o servicios.

De igual forma, las políticas de seguridad establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la organización. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la organización.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer.

Finalmente, las políticas de seguridad como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de nuevos proyectos entre otros.

3.5.3 Parámetros para el establecimiento de Políticas de Seguridad

Si bien las características de las políticas de seguridad que se han mencionado hasta el momento, nos muestran una perspectiva de las implicaciones en la formulación de estas directrices, se revisaran a continuación, algunos aspectos generales recomendados para la formulación de las mismas.

- Considerar y efectuar un ejercicio de análisis de riesgos informáticos, a través del cual se valore lo que es considerado como activos, el cual permitirá afinar las políticas de seguridad de la organización.
- El poder Involucrar a las áreas propietarias de los recursos o servicios, pues ellos poseen la experiencia y son fuente principal para establecer el alcance y las definiciones de violaciones a las políticas de seguridad.
- Comunicar a todo el personal involucrado en el desarrollo de las políticas de seguridad, los beneficios y riesgos relacionados con los recursos y bienes, así como de sus elementos de seguridad.
- Es necesario identificar quién tiene la autoridad para tomar decisiones, pues serán ellos los responsables de salvaguardar los activos críticos de la funcionalidad de ya sea un área o de la organización.
- Desarrollar un proceso de monitoreo periódico de las directrices en el hacer de la organización, que permita una actualización oportuna de las mismas.

Hay que ser explícito y concreto en los alcances, así como en las propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las políticas de seguridad trazadas.

3.5.4 Seguridad integral

Muchas veces, las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas, con relativo éxito. Según algunos estudios resulta una labor ardua convencer a los altos ejecutivos de la necesidad de buenas políticas y prácticas de seguridad informática.

Muchos de los inconvenientes se inician por los tecnicismos informáticos y por la falta de una estrategia de mercadeo de los especialistas en seguridad que, llevan a los altos directivos a pensamientos en los cuales radican que es un desperdicio de capital el invertir en algo que creen que no es de utilidad. Esta situación ha llevado a que muchas organizaciones con activos muy importantes, se encuentren expuestas a graves problemas de seguridad que, en muchos de los casos, lleva a comprometer su información sensible y por consecuencia una imagen.

Ante estos puntos expuestos, los encargados de la seguridad deben asegurarse de que las personas relevantes entiendan los asuntos importantes de la seguridad, conozcan sus alcances y estén de acuerdo con las decisiones tomadas en relación con estos asuntos. En particular, la gente debe conocer las consecuencias de sus decisiones, incluyendo lo mejor y lo peor que podría ocurrir. Una intrusión o una travesura pueden convertir a las personas que no entendieron, en blanco de las políticas o en señuelos de los verdaderos vándalos. Luego, para que las políticas de seguridad logren abrirse espacio en el interior de una organización deben integrarse a las estrategias de la organización en sí, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la organización.

De igual forma, las políticas de seguridad deben ir acompañadas de una visión que promueva actividades que involucren a las personas en su hacer diario, donde se identifiquen las necesidades y acciones que materializan las políticas. En este contexto, entender la organización, sus elementos culturales y comportamientos nos debe llevar a reconocer las pautas de seguridad necesarias y suficientes que aseguren confiabilidad en las operaciones y funcionalidad de la compañía.

A continuación, se mencionan algunas recomendaciones para concientizar sobre la seguridad informática:

- Desarrollar ejemplos organizacionales relacionados con fallas de seguridad que capten la atención de aquellos a quienes se les pretende hablar del tema.
- Asociar el punto anterior a las estrategias de la organización y a la imagen que se tiene de la organización en el desarrollo de sus actividades.
- Articular las estrategias de seguridad informática con el proceso de toma de decisiones y los principios de integridad, confidencialidad y disponibilidad de la información. Mostrar una valoración costo-beneficio, ante una falla de seguridad.
- Justificar la importancia de la seguridad informática en función de hechos y preguntas concretas, que muestren el impacto, limitaciones y beneficios sobre los activos claves de la organización.

Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas. En razón de lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos. Las políticas de seguridad constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar pro-activamente ante situaciones que comprometan su integridad. Por tanto, deben constituir un proceso continuo y retro-alimentado que observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Las políticas por sí mismas no constituyen una garantía para la seguridad de la organización. Ellas deben responder a intereses y necesidades organizacionales basadas en la visión de dicha organización, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y a reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con la organización.
La seguridad tiene varios estratos:

- El marco jurídico adecuado.
- Medidas técnico-administrativas, como la existencia de políticas y procedimientos o la creación de funciones, como administración de la seguridad o auditoría de sistemas de información interna.

Ambas funciones han de ser independientes y nunca una misma persona podrá realizar las dos, ni existir dependencia jerárquica de una función respecto de otra. En cuanto a la administración de seguridad pueden existir, además, coordinadores en las diferentes áreas funcionales y geográficas de cada entidad, especialmente si la dispersión, la complejidad organizativa o el volumen de la entidad así lo demandan.

En todo caso, debe existir una definición de funciones y una separación suficiente de tareas. No tiene sentido que una misma persona autorice una transacción, la introduzca, y revise después los resultados (un diario de operaciones, por ejemplo), porque podría planificar un fraude o encubrir cualquier anomalía; por ello deben intervenir funciones, personas diferentes y existir controles suficientes.

3.5.5 Diagrama para el análisis de un sistema de seguridad

En muchas ocasiones al momento de plantear las políticas de seguridad, así como demás mecanismos que nos permitan el poder implementar de la manera más adecuada la seguridad dentro de una organización, necesitamos de una base que contenga todo aquello que pretendemos que forme parte de un buen análisis de seguridad es por eso que se tomará este diagrama (Figura 3.0) como un diagrama base para el análisis de nuestro sistema.

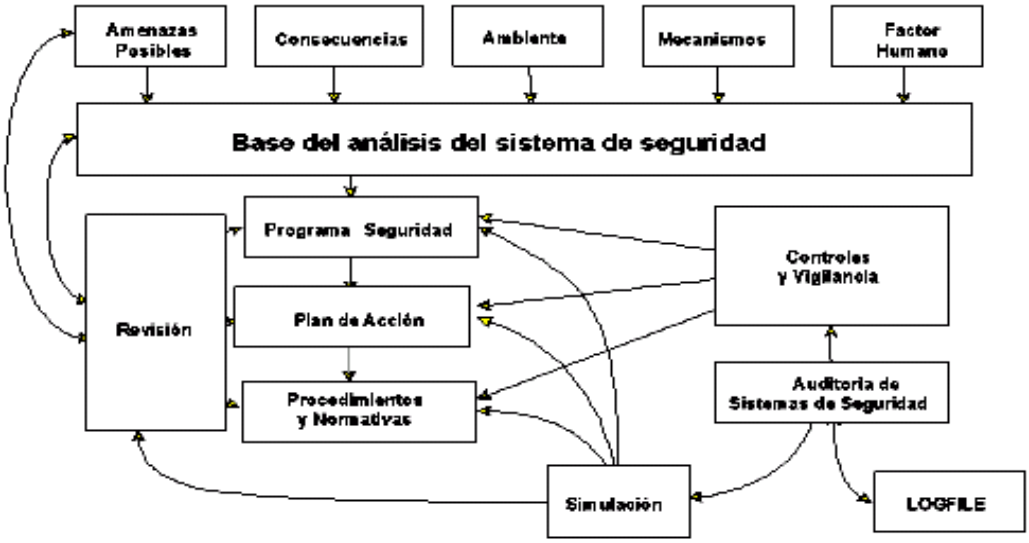


Figura 3.0 Diagrama de Análisis

Tal como puede visualizarse, en el gráfico están plasmados todos los elementos que intervienen para el estudio de una política de seguridad. Se comienza realizando una evaluación del:

- **Factor humano:** Teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad.
- **Los mecanismos:** Con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos).
- **El medio ambiente:** En que se desempeña el sistema, las consecuencias que puede traer aparejado defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las **amenazas posibles.**

Una vez evaluado todo lo anterior, se origina:

- **Programa de seguridad:** Que involucra los pasos a tomar para poder asegurar el umbral de seguridad que se desea.
- **Plan de acción:** Que es cómo se va a llevar a cabo el programa de seguridad.

Finalmente, se redactan:

- **Los procedimientos y normas,** que permiten llegar a buen destino.

Con el propósito de asegurar el cumplimiento de todo lo anterior se:

- **Realizan los controles y la vigilancia,** que aseguran el fiel cumplimiento de los tres puntos antepuestos.

Para asegurar un marco efectivo, se realizan auditorías a los controles:

- **Los archivos logísticos,** que se generen en los procesos implementados (de nada vale tener archivos logísticos si nunca se los analizan o se los analizan cuando ya ha ocurrido un problema).

Con el objeto de confirmar el buen funcionamiento de lo creado, se procede a:

- **Simular,** eventos que atenten contra la seguridad del sistema.

Como el proceso de seguridad es un proceso dinámico, es necesario realizar:

- **Revisiones,** al programa de seguridad, al plan de acción y a los procedimientos y normas. Estas revisiones, tendrán efecto sobre los puntos tratados en el primer párrafo y, de esta manera, el proceso se vuelve a repetir.

Es claro que el establecimiento de políticas de seguridad es un proceso dinámico sobre el que hay que estar actuando permanentemente, de manera tal que no quede desactualizado; que, cuando se le descubran debilidades, éstas sean subsanadas y finalmente, que su práctica por los integrantes de la organización no caiga en desuso.

CAPÍTULO 4

SOFTWARE

4.1 Clasificación del Software

4.1.1 Introducción

El software no surge con los equipos electrónicos, aunque es con ellos que adopta el nombre, está presente desde el empleo de ábacos o sumadoras mecánicas. Sin embargo, en estos casos el software no se encuentra incorporado en el equipo. Es aportado por el usuario. La máquina analítica de Charles Babbage, incidentalmente tuvo su software, y fue una amiga de éste, la legendaria lady Lovelace, quien aportó el software que no se llegó a usar, dado que la máquina nunca se completó.

Hasta este momento, no se percibía una diferencia específica entre el equipo y el control de las operaciones. El concepto de programa de control almacenado en memoria, aportación popularmente atribuida a John Von Neumann, precipitó el desarrollo de software. En éste se perfilaron dos tendencias de desarrollo: los programas de aplicación y los de servicio. Estos últimos tenían como propósito facilitar el desarrollo de programas a partir de programas.

Algunos programas de servicio fueron simples cargadores que permitieron emplear notaciones como el octal o hexadecimal más compactas que el binario. Otros como los ensambladores simplificaron más el proceso al reemplazar las notaciones numéricas con los símbolos nemónicos que aportaron para describir a cada instrucción de la máquina. El siguiente paso significativo fue la traducción de fórmulas, que permitió la descripción de los algoritmos con el empleo de expresiones algebraicas. Dicha traducción se realiza con programas que se denominan compiladores, generan programas que al ejecutarse producen los resultados.

Es importante destacar que en tanto los programas de aplicación saturaron los recursos de los equipos, imponiendo sus requerimientos en cuanto a velocidad, precisión en la aritmética y capacidad en los almacenamientos; los programas de servicio repercutieron en la evolución de la arquitectura de los equipos (hardware). Entre las aportaciones más notables, podemos citar el empleo de pilas y el reemplazo de referencias físicas por lógicas.

Con la pila (Push Down List), se da lugar al manejo recursivo de los procesos. Por ejemplo, esto ocurre en una oficina administrativa, cuando se pospone la solución de un problema para resolver otro de mayor exigencia. El problema original se suspende y se aborda nuevamente cuando el de mayor exigencia ya ha sido resuelto.

Con el reemplazo de referencias físicas por lógicas, se obtuvo un incremento más real que virtual de los recursos disponibles. Almacenamientos secundarios, registros operacionales, memoria virtual, memoria cache e hizo translapes (overlay), son algunas de las técnicas que emplean este concepto. El efecto es similar al de las operaciones bancarias nominales con que las instituciones de crédito prestan varias veces su capital.

Los programas de servicio, al interrelacionarse configuran el sistema operativo con el cual se administran los recursos disponibles en las computadoras y se establecen líneas de producción para el proceso de programas con una mínima participación del usuario. Al principio, los sistemas operativos surgen como extensiones de los lenguajes. Posteriormente, el fenómeno se

invierte de modo que los sistemas operativos configuran el ambiente en el que se desempeñan las aplicaciones y los programas de servicio.

4.1.2 Definición

El software es indispensable para el funcionamiento de la computadora. Está formado por una serie de instrucciones y datos, que permiten aprovechar todos los recursos que la computadora tiene, de manera que pueda resolver gran cantidad de problemas.

4.1.3 Funciones del Software

- Administrar los recursos de cómputo.
- Proporcionar las herramientas para optimizar estos recursos.
- Actuar como intermediario entre el usuario y la información almacenada.

4.1.4 Clasificación

El software paulatinamente adquirió mayor importancia que el hardware. En un principio, la proporción favorecía al equipo físico, pero progresivamente, el software, adquirió una mayor relevancia hasta hacerse el más importante.

4.1.4.1 Software de base o de sistema

Consistente en todo aquel software cuyo propósito es facilitar la ejecución de otro software, y se tienen las siguientes categorías:

- Sistemas Operativos.
- Compiladores.
- Sistemas gestores de bases de datos.

4.1.4.2 Software de aplicación

Consistente en aquel software que automatiza un sistema de información; Es decir, realizan una función en concreto. Tenemos las siguientes categorías.

- Procesadores de texto.
- Hojas de cálculo.
- Editores de Imágenes.
- Software de Desarrollo.

4.1.4.3 Software de usuario final

Es el software que permiten el desarrollo de algunas aplicaciones directamente por los usuarios, el software del usuario final con frecuencia tiene que trabajar a través del software de aplicación y finalmente a través del software del sistema.

4.1.4.4 Otras clasificaciones de software

- Software libre

Es el software que viene con permiso para que cualquier persona lo use, copie y distribuya, ya sea como está o con modificaciones, con o sin costo. En particular, esto significa que el código fuente debe estar disponible. Sin código fuente no es software libre. Frecuentemente el software libre es más robusto que el software no-libre.

En inglés, la palabra "free" se refiere a libertad, no a precio. En español se tiene dos palabras diferentes para cada concepto: libre y gratis. Esta libertad se refiere a la libertad del usuario para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Con mayor precisión, se refiere a cuatro tipos de libertad:

- La libertad de ejecutar el software, con cualquier propósito.
- La libertad de estudiar cómo funciona el programa, y adaptarlo a sus necesidades.
- La libertad de distribuir copias del programa, de modo que se pueda ayudar a otras personas.
- La libertad de mejorar el programa y proporcionar las mejoras al público, de modo que se beneficie a la comunidad completa.

- Software de dominio público

El software de dominio público es software sin "copyright". Es un tipo especial de software libre. La desventaja de este tipo de software es que versiones modificadas pueden no ser libres. A veces la gente usa el término "dominio público" para referirse a "disponible gratuitamente", pero "dominio público" es un término legal que significa, precisamente, sin "copyright".

- Software de Código Abierto

El término "Open Source" es de reciente creación, y es utilizado para dar más o menos el mismo sentido que el software libre. Sin embargo, no es software libre. El significado evidente para "código abierto" es (puede verse el código fuente).

Muchas compañías han abrazado esta filosofía, que para ellos se lee como "permite a los usuarios ver el código fuente y ellos arreglarán los errores", pero "el programa" sigue siendo de la compañía.

- Software semi-libre

El software semi-libre no es software libre, pero el usuario tiene permiso de usarlo, copiarlo y distribuirlo sin fines de lucro. El software semi-libre es mejor que el software propietario, pero aún así presenta problemas. El software debe ser para todos, incluyendo los negocios, no solamente para las escuelas y los aficionados.

- Software propietario

El software propietario es aquel que no es libre ni semi-libre. Su uso, redistribución o modificación están prohibidos, o requieren la solicitud de un permiso.

- Software "copylefted".

El software "copylefted" es software libre cuyos términos de distribución no permiten la adición de ninguna restricción al redistribuir o modificar el software. Esto significa que cada copia del software, aún si ha sido modificado, debe ser software libre.

Los desarrolladores de software propietario usan el derecho de copia (copyright) para quitarle libertad al usuario. De allí que la Fundación del Software Libre invierta el concepto utilizando el "copyleft", garantizando que todos los usuarios obtengan la misma libertad.

- Software comercial

El software comercial es software desarrollado por una empresa con el propósito de ganar dinero por el uso del software. El software comercial y el software propietario no son la misma cosa; casi todo el software comercial es propietario, pero hay software comercial libre, y también software no-comercial no-libre.

4.1.5 Formas de Código

El software adopta varias formas en distintos momentos de su ciclo de vida:

- Código fuente: escrito por programadores. Contiene el conjunto de instrucciones, inteligibles por el ser humano, destinadas a la computadora.
- Código objeto: resultado del uso de un compilador sobre el código fuente. Consiste en una traducción de éste último. El código objeto no es directamente inteligible por el ser humano, pero tampoco es directamente entendible por la computadora. Se trata de una representación intermedia del código fuente.
- Código ejecutable: resultado de enlazar uno o varios fragmentos de código objeto. Constituye un archivo binario con un formato tal que el sistema operativo es capaz de cargarlo en la memoria de un computadora, y proceder a su ejecución. El código ejecutable es directamente inteligible por la computadora.

4.2 Sistemas Operativos

4.2.1 Introducción

A finales de los 40's el uso de computadoras estaba restringido a aquellas empresas o instituciones que podían pagar su alto precio, y no existían los sistemas operativos. En su lugar, el programador debía tener un conocimiento y contacto profundo con el hardware, y en el infortunado caso de que su programa fallara, debía examinar los valores de los registros y paneles de luces indicadoras del estado de la computadora para determinar la causa del fallo y

poder corregir su programa, además de enfrentarse nuevamente a los procedimientos de apartar tiempo del sistema y poner a punto los compiladores, etc, para volver a correr su programa, es decir, enfrentaba el problema del procesamiento serial.

La importancia de los sistemas operativos nace históricamente desde los 50's, cuando se hizo evidente que el operar una computadora por medio de tableros enchufables en la primera generación y luego por medio del trabajo en lote en la segunda generación se podía mejorar notoriamente, esto era debido a que el operador realizaba siempre una secuencia de pasos repetitivos, lo cual es una de las características contempladas en la definición de lo que es un programa. Así, se comenzó a ver que las tareas mismas del operador podían plasmarse en un programa, el cual a través del tiempo y por su enorme complejidad se le llamó "Sistema Operativo". Por lo tanto, tenemos entre los primeros sistemas operativos al Fortran Monitor System (FMS) e IBSYS.

Posteriormente, en la tercera generación de computadoras nace uno de los primeros sistemas operativos con la filosofía de administrar una familia de computadoras: el OS/360 de IBM. Fue este un proyecto tan novedoso y ambicioso que enfrentó por primera vez una serie de problemas conflictivos debido a que anteriormente las computadoras eran creadas para dos propósitos en general: el comercial y el científico. Así, al tratar de crear un solo sistema operativo para computadoras que podían dedicarse a un propósito, al otro o ambos, puso en evidencia la problemática del trabajo en equipos de análisis, diseño e implantación de sistemas grandes. El resultado fue un sistema no funcional para el propósito planteado.

Surge también en la tercera generación de computadoras el concepto de la multiprogramación, porque debido al alto costo de las computadoras era necesario idear un esquema de trabajo que mantuviese a la unidad central de procesamiento más tiempo ocupada, así como el encolado (spooling) de trabajos para su lectura hacia los lugares libres de memoria o la escritura de resultados. Sin embargo, se puede afirmar que los sistemas durante la tercera generación siguieron siendo básicamente sistemas de lote.

En la cuarta generación la electrónica avanza hacia la integración a gran escala, pudiendo crear circuitos con miles de transistores en un centímetro cuadrado de silicón y ya es posible hablar de las computadoras personales y las estaciones de trabajo. Surgen los conceptos de interfaces amigables intentando así atraer al público en general al uso de las computadoras como herramientas cotidianas. Se hacen populares el MS-DOS y UNIX en estas máquinas. También es común encontrar clones de computadoras personales y una multitud de empresas pequeñas ensamblándolas por todo el mundo.

Para mediados de los 80's, comienza el auge de las redes de computadoras y la necesidad de sistemas operativos en red y sistemas operativos distribuidos. El Internet se va haciendo accesible a toda clase de instituciones y se comienzan a dar muchas soluciones y problemas al querer hacer convivir recursos residentes en computadoras con sistemas operativos diferentes. Para los 90's el paradigma de la programación orientada a objetos cobra auge, así como el manejo de objetos desde los sistemas operativos. Las aplicaciones intentan crearse para ser ejecutadas en una plataforma específica y poder ver sus resultados en la pantalla o monitor de otra diferente (por ejemplo, ejecutar una simulación en una máquina con UNIX y ver los

resultados en otra con MS-DOS). Los niveles de interacción se van haciendo cada vez más profundos.

4.2.2 Definición de Sistema Operativo

Definición de Sistema Operativo

Un sistema Operativo es un conjunto de programas relacionados entre sí, que permiten administrar y aprovechar los recursos de la computadora de una manera eficaz y eficiente de tal manera, que permiten la comunicación entre el usuario y la máquina.

4.2.3 Funciones de un Sistema Operativo

Los sistemas operativos desempeñan distintas funciones en una computadora, que serán mencionadas a continuación:

- Administración de los dispositivos de entrada y salida.
- Administración de la memoria.
- Administración del procesador.
- Administración del sistema de archivos.
- Administración de usuarios.
- Administración de tareas.

.

4.2.4 Clasificación de los Sistemas Operativos

Los sistemas operativos se clasifican de acuerdo a sus características. En esta sección se describirán las características que clasifican a los sistemas operativos, básicamente se mencionaran cuatro clasificaciones.

4.2.4.1 Sistemas Operativos por su estructura

Se deben observar dos tipos de requisitos cuando se construye un sistema operativo, los cuales son:

- Requisitos de usuario: Sistema fácil de usar y de aprender, seguro, rápido y adecuado al uso al que se le quiere destinar.
- Requisitos del software: Donde se engloban aspectos como el mantenimiento, forma de operación, restricciones de uso, eficiencia, tolerancia frente a los errores y flexibilidad.

A continuación se describen las distintas estructuras que presentan los actuales sistemas operativos para satisfacer las necesidades que de ellos se quieren obtener.

4.2.4.1.1 Estructura monolítica

Es la estructura de los primeros sistemas operativos constituidos fundamentalmente por un solo programa compuesto de un conjunto de rutinas entrelazadas de tal forma que cada una puede llamar a cualquier otra Las características fundamentales de este tipo de estructura son:

- Construcción del programa final a base de módulos compilados separadamente que se unen a través del ligador.
- Buena definición de parámetros de enlace entre las distintas rutinas existentes, que puede provocar mucho acoplamiento.
- Carecen de protecciones y privilegios al entrar a rutinas que manejan diferentes aspectos de los recursos de la computadora, como memoria, disco, etc.
- Generalmente están hechos a medida, por lo que son eficientes y rápidos en su ejecución y gestión, pero por lo mismo carecen de flexibilidad para soportar diferentes ambientes de trabajo o tipos de aplicaciones.

4.2.1.2 Estructura jerárquica

A medida que fueron creciendo las necesidades de los usuarios y se perfeccionaron los sistemas, se hizo necesaria una mayor organización del software, del sistema operativo, donde una parte del sistema contenía subpartes y esto organizado en forma de niveles. Se dividió el sistema operativo en pequeñas partes, de tal forma que cada una de ellas estuviera perfectamente definida y con una clara interface con el resto de elementos. Se constituyó una estructura jerárquica o de niveles en los sistemas operativos, el primero de los cuales fue denominado THE (Technische Hogeschool, Eindhoven), de Dijkstra, que se utilizó con fines didácticos. Se puede pensar también en estos sistemas como si fueran `multicapa'. Multics y Unix caen en esa categoría.

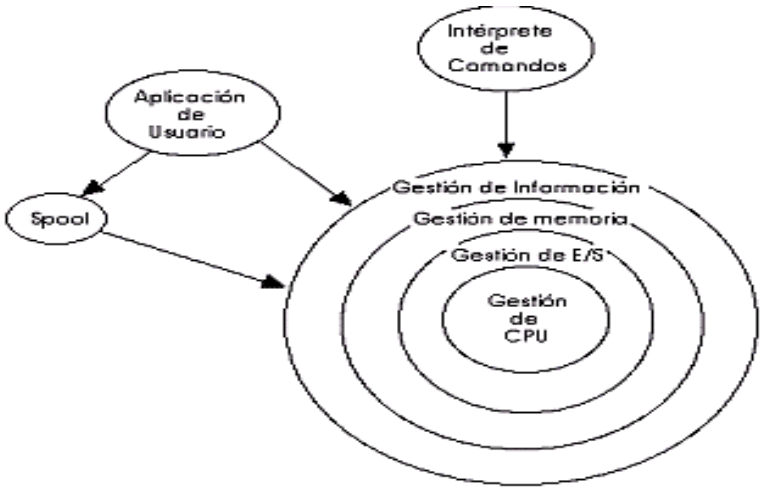


Figura 4.0 Estructura Jerárquica.

En la estructura anterior se basan prácticamente la mayoría de los sistemas operativos actuales. Otra forma de ver este tipo de sistema es la denominada de anillos concéntricos o "rings" (Figura 4.0).

En el sistema de anillos, cada uno tiene una apertura, conocida como puerta o trampa (trap), por donde pueden entrar las llamadas de las capas inferiores. De esta forma, las zonas más internas del sistema operativo o núcleo del sistema estarán más protegidas de accesos indeseados desde las capas más externas. Las capas más internas serán, por tanto, más privilegiadas que las externas.

4.2.4.1.3 Máquina Virtual

Se trata de un tipo de sistema operativo que presenta una interfaz en cada proceso, mostrando una máquina que parece idéntica a la máquina real subyacente. Estos sistemas operativos separan dos conceptos que suelen estar unidos en el resto de sistemas: la multiprogramación y la máquina extendida. El objetivo de los sistemas operativos de máquina virtual es el de integrar distintos sistemas operativos dando la sensación de ser varias máquinas diferentes.

El núcleo de estos sistemas operativos se denomina monitor virtual y tiene como misión llevar a cabo la multiprogramación, presentando a los niveles superiores tantas máquinas virtuales como se soliciten. Estas máquinas virtuales no son máquinas extendidas, sino una réplica de la máquina real, de manera que en cada una de ellas se pueda ejecutar un sistema operativo diferente, que será el que ofrezca la máquina extendida al usuario.

4.2.4.1.4 Cliente-Servidor

El tipo más reciente de sistemas operativos es el denominado Cliente / Servidor, que puede ser ejecutado en la mayoría de las computadoras, ya sean grandes o pequeñas. Este sistema sirve para toda clase de aplicaciones por tanto, es de propósito general y cumple con las mismas actividades que los sistemas operativos convencionales.

El núcleo tiene como misión establecer la comunicación entre los clientes y los servidores. Los procesos pueden ser tanto servidores como clientes. Por ejemplo, un programa de aplicación normal es un cliente que llama al servidor correspondiente para acceder a un archivo o realizar una operación de entrada/salida sobre un dispositivo en concreto. A su vez, un proceso cliente puede actuar como servidor para otro. Este paradigma ofrece gran flexibilidad en cuanto a los servicios posibles en el sistema final, ya que el núcleo provee solamente funciones muy básicas de memoria, entrada/salida, archivos y procesos, dejando a los servidores proveer la mayoría que el usuario final o programador puede usar. Estos servidores deben tener mecanismos de seguridad y protección que, a su vez, serán filtrados por el núcleo que controla el hardware.

4.2.4.2 Sistemas Operativos por Servicios

Esta clasificación es la más usada y conocida desde el punto de vista del usuario. Esta clasificación se puede observar claramente en la siguiente Figura 4.2.5.

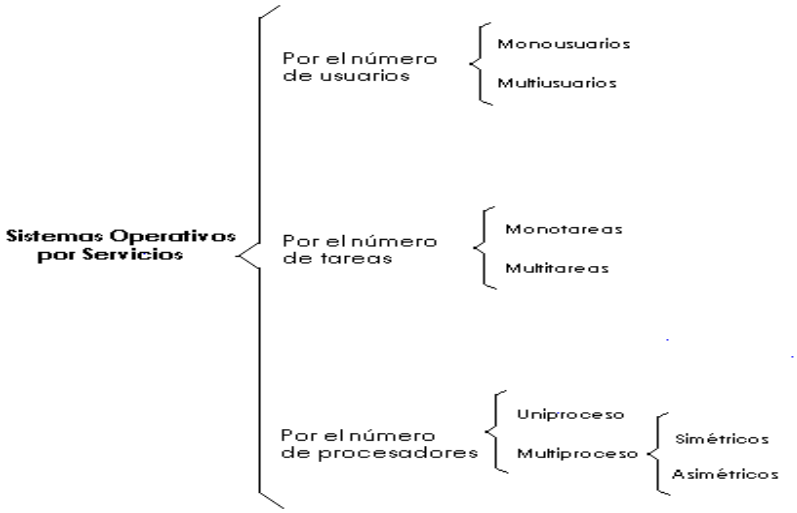


Figura 4.2.5 Sistemas Operativos por Servicios.

Por el número de usuarios:

- Monousuarios

Los sistemas operativos monousuarios son aquéllos que soportan a un usuario a la vez, sin importar el número de procesadores que tenga la computadora o el número de procesos o tareas que el usuario pueda ejecutar en un mismo instante de tiempo. Las computadoras personales típicamente se han clasificado dentro de este rango.

- Multiusuarios

Los sistemas operativos multiusuarios son capaces de dar servicio a más de un usuario a la vez, ya sea por medio de varias terminales conectadas a la computadora o por medio de sesiones remotas en una red de comunicaciones. No importa el número de procesadores en la máquina ni el número de procesos que cada usuario puede ejecutar simultáneamente.

- Monotareas

Los sistemas monotarea son aquellos que sólo permiten una tarea a la vez por usuario. Puede darse el caso de un sistema multiusuario y monotarea, en el cual se admiten varios usuarios al mismo tiempo pero cada uno de ellos puede estar haciendo solo una tarea a la vez.

- Multitareas

Un sistema operativo multitarea es aquél que le permite al usuario estar realizando varias labores al mismo tiempo. Por ejemplo, puede estar editando el código fuente de un programa durante su depuración mientras compila otro programa, a la vez que está recibiendo correo electrónico en un proceso en background. Es común encontrar en ellos interfaces gráficas

orientadas al uso de menús y el ratón, lo cual permite un rápido intercambio entre las tareas para el usuario, mejorando su productividad.

Por el número de procesadores:

- Uniproceso

Un sistema operativo uniproceso es aquél que es capaz de manejar solamente un procesador de la computadora, de manera que si la computadora tuviese más de uno le sería inútil. El ejemplo más típico de este tipo de sistemas es el MS-DOS y MacOS.

- Multiproceso

Un sistema operativo multiproceso se refiere al número de procesadores del sistema, que es más de uno y éste es capaz de usarlos todos para distribuir su carga de trabajo. Generalmente estos sistemas trabajan de dos formas: simétrica o asimétricamente. Cuando se trabaja de manera asimétrica, el sistema operativo selecciona a uno de los procesadores el cual jugará el papel de procesador maestro y servirá como pivote para distribuir la carga a los demás procesadores, que reciben el nombre de esclavos. Cuando se trabaja de manera simétrica, los procesos o partes de ellos (threads) son enviados indistintamente a cualquiera de los procesadores disponibles, teniendo, teóricamente, una mejor distribución y equilibrio en la carga de trabajo bajo este esquema.

Se dice que un **thread** es la parte activa en memoria y la ejecución de un proceso, lo cual puede consistir de un área de memoria, un conjunto de registros con valores específicos, la pila y otros valores de contexto. Un aspecto importante a considerar en estos sistemas es la forma de crear aplicaciones para aprovechar los varios procesadores. Existen aplicaciones que fueron hechas para correr en sistemas monoproceso que no toman ninguna ventaja a menos que el sistema operativo o el compilador detecte secciones de código paralelizable, los cuales son ejecutados al mismo tiempo en procesadores diferentes. Por otro lado, el programador puede modificar sus algoritmos y aprovechar por sí mismo esta facilidad, pero esta última opción las más de las veces es costosa en horas hombre y muy tediosa, obligando al programador a ocupar tanto o más tiempo a la paralelización que elaborar el algoritmo inicial.

4.2.4.3 Sistemas Operativos por la forma de ofrecer sus servicios

Esta clasificación también se refiere a una visión externa, que en este caso se refiere a la del usuario, el cómo accesa los servicios. Bajo esta clasificación se pueden detectar dos tipos principales: Sistemas operativos de red y Sistemas operativos distribuidos.

4.2.4.3.1 Sistemas Operativos de Red

Los sistemas operativos de red se definen como aquellos que tiene la capacidad de interactuar con sistemas operativos en otras computadoras por medio de un medio de transmisión con el objeto de intercambiar información, transferir archivos, ejecutar comandos remotos y un sin fin de actividades. El punto crucial de estos sistemas es que el usuario debe saber la sintaxis de un

conjunto de comandos o llamadas al sistema para ejecutar estas operaciones, además de la ubicación de los recursos a los que se deseen acceder.

4.2.4.3.2 Sistemas Operativos Distribuidos

Los sistemas operativos distribuidos abarcan los servicios de los de red, logrando integrar recursos (impresoras, unidades de respaldo, memoria, procesos, unidades centrales de proceso) en una sola máquina virtual que el usuario accesa en forma transparente. Es decir, ahora el usuario ya no necesita saber la ubicación de los recursos, sino que los conoce por nombre y simplemente los usa como si todos ellos fuesen locales a su lugar de trabajo habitual. Los avances tecnológicos en las redes de área local y la creación de microprocesadores de 32 y 64 bits lograron que computadoras mas o menos baratas tuvieran el suficiente poder en forma autónoma para desafiar en cierto grado a los mainframes, y a la vez se dio la posibilidad de intercomunicarlas, sugiriendo la oportunidad de partir procesos muy pesados en cálculo en unidades más pequeñas y distribuirlas en los varios microprocesadores para luego reunir los sub-resultados, creando así una máquina virtual en la red que exceda en poder a un mainframe.

Ventajas de los Sistemas Distribuidos

En general, los sistemas distribuidos, exhiben algunas ventajas sobre los sistemas centralizados que se describen enseguida.

- Economía: El cociente precio/desempeño de la suma del poder de los procesadores separados contra el poder de uno solo centralizado es mejor cuando están distribuidos.
- Velocidad: Relacionado con el punto anterior, la velocidad sumada es muy superior.
- Confiabilidad: Si una sola máquina falla, el sistema total sigue funcionando.
- Crecimiento: El poder total del sistema puede irse incrementando al añadir pequeños sistemas, lo cual es mucho más difícil en un sistema centralizado y costoso.
- Distribución: Algunas aplicaciones requieren de por sí una distribución física.
- Compartir datos: Un sistema distribuido permite compartir datos más fácilmente que los sistemas aislados, que tendrían que duplicarlos en cada nodo para lograrlo.
- Compartir dispositivos: Un sistema distribuido permite acceder a dispositivos desde cualquier nodo en forma transparente, lo cual es imposible con los sistemas aislados.
- Comunicaciones: La comunicación persona a persona es factible en los sistemas distribuidos, en los sistemas aislados no.
- Flexibilidad: La distribución de las cargas de trabajo es factible en el sistema distribuido, se puede incrementar el poder de cómputo.

Desventajas de los Sistemas Distribuidos

Así como los sistemas distribuidos exhiben grandes ventajas, también se pueden identificar algunas desventajas, algunas de ellas tan serias que han frenado la producción comercial de sistemas operativos en la actualidad. El problema más importante en la creación de sistemas distribuidos es el software: los problemas para compartir los datos y los recursos es tan complejo que los mecanismos de solución generan mucha sobrecarga al sistema haciéndolo ineficiente.

Otros problemas de los sistemas operativos distribuidos surgen debido a la concurrencia y al paralelismo. Tradicionalmente las aplicaciones son creadas para computadoras que ejecutan secuencialmente, de manera que el identificar secciones de código paralelizable es un trabajo arduo, pero necesario para dividir un proceso grande en sub-procesos y enviarlos a diferentes unidades de procesamiento para lograr la distribución.

4.2.5 Tendencias actuales

Con el gran auge de las redes de comunicaciones y su incremento en el ancho de banda, la proliferación de paquetes que ofrecen la compartición de archivos es común. Los esquemas más solicitados en la industria es el poder acceder a los grandes volúmenes de información que residen en grandes servidores desde las computadoras personales y desde otros servidores también.

A veces se requieren soluciones más complejas con ambientes heterogéneos: diferentes sistemas operativos y diferentes arquitecturas. Uno de los sistemas de archivos más expandidos en estaciones de trabajo es el NTFS, y prácticamente todas las versiones de UNIX traen instalado un cliente y hasta un servidor de este servicio. Lo importante aquí es observar que el mundo se va moviendo poco a poco hacia soluciones distribuidas, y hacia la estandarización.

En la siguiente tabla se muestra algunos sistemas operativos así como una breve descripción de los mismos.

Sistema Operativo	Descripción
MSDOS	MSDOS es un sistema operativo basado en comandos, fue uno de los primeros sistemas operativos utilizados en una PC, ya que por su tamaño no requiere de muchos recursos para funcionar. Aunque prácticamente este considerado como obsoleto, en la actualidad todavía se sigue utilizando como una herramienta para resolver algunos problemas.
WINDOWS 3.0 – 3.11	Es prácticamente es primer sistema operativo con ambiente gráfico, después del ofrecido por Macintosh Una versión de Windows con muchas mejoras a Windows 3.0. Incluye soporte para fuentes True Type y OLE. Esta versión fue testigo de la pérdida del modo real, lo cual significa que no corre en procesadores Intel 8086.
WINDOWS 95	Sucesor de Windows 3.11 para PC's IBM. Se le conoció cómo "Chicago" durante su desarrollo. Lanzado el 24 de Agosto de 1995. En contraste con las anteriores versiones de Windows, Win95 es un sistema operativo más que una interfaz gráfica de usuario que corre sobre DOS. Provee soporte para aplicaciones de 32 bits, multitarea con desalojo, soporte de red incorporando (TCP/IP, IPX, SLIP, PPP, y Windows Sockets). Incluye MS-DOS 7.0 como una aplicación. La interfaz gráfica, aunque similar a las previas versiones, fue significativamente mejorada.
WINDOWS NT	Fue diseñado para tomar ventaja de todo el poder que ofrecen los procesadores más avanzados de Intel, así como algunos de los procesadores RISC. Windows NT es la respuesta de Microsoft a UNIX. Windows NT ofrece los mismos servicios que UNIX, inter-opera con redes UNIX pero remplaza los comandos críticos de UNIX, su estructura de archivos ARCANE y la mezcla de GUIs con una simple y estandarizada interfaz para el usuario como lo es Windows. Además, NT tiene las características que originalmente iba a tener el OS/2: un avanzado sistema operativo de 32 bits y compatibilidad con Windows GUI, además de soportar las aplicaciones hechas en DOS pero liberándose de las limitaciones de éste.

WINDOWS 98	Este es uno de los sistemas operativos de escritorio con mayor cantidad de usuarios en el mundo, ya que se encuentra a mitad de camino (en términos de tiempo) entre la aparición de Windows 95 y de Windows 2000, entre sus principales características se encuentra el soporte real a multitarea (en Win95 era simulado).
WINDOWS MILENIUM	Este sistema está pensado para potenciar la experiencia multimedia de todos los usuarios, haciendo que mejore la red de casa, la multimedia, los CD`s de audio, el video digital y la conectividad a Internet.
WINDOWS 2000	Windows 2000 es la nueva generación del sistema operativo para redes de esta empresa (Windows NT), constituyéndose en una mejora significativa desde varias perspectivas, entre las que cabe destacar la estabilidad.
WINDOWS XP	Este sistema operativo hace uso del nuevo «motor de sistema» que Microsoft desarrollo para Windows 2000, por lo tanto integra altas prestaciones gráficas junto a características de trabajo corporativo (en redes) heredadas de Windows 2000.
WINDOWS 2000 SERVER	Es una versión del Sistema Operativo de Microsoft, Windows 2000 (anteriormente llamado Windows NT 5.0) y también es un sistema operativo de Red, creado especialmente para actuar como un servidor de red, para gestionar la red, crear cuentas de usuarios, asignar recursos, etc.
WINDOWS 2003 SERVER	Es la versión de Windows para servidores lanzada por Microsoft en el año 2003. Está basada en el núcleo de Windows XP, al que se le han añadido una serie de servicios, y se le han bloqueado algunas características (para mejorar el rendimiento, o simplemente porque no serán usadas). • Sistema de archivos NTFS. • Windows Driver Model: Implementación básica de los dispositivos más utilizados, de esa manera los fabricantes de dispositivos sólo han de programar ciertas especificaciones de su hardware. • Active Directory: Directorio de organización basado en LDAP, permite gestionar de forma centralizada la seguridad de una red corporativa a nivel local. • Autentificación Kerberos5. • DNS con registro de IP's dinámicamente. • Políticas de seguridad.
WINDOWS VISTA	Es la versión del sistema operativo Microsoft Windows que sucede a Windows XP, lanzado el 30 de noviembre de 2006 para el mundo empresarial. Dentro de las características importantes se destacan: • Ingeniería de la plataforma cliente. • Garantía de compatibilidad de las aplicaciones. • Método de implementación. • Diseño modular. • Formato de imágenes de Windows (WIM). • Equipo protegido contra virus, gusanos, spyware y otro software potencialmente no deseado. • Herramientas de seguridad mejoradas.

Sistema Operativo	Descripción
GNU/LINUX	LINUX es un sistema operativo, compatible Unix. Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente. El sistema lo forman el núcleo del sistema (kernel) mas un gran número de programas/librerías que hacen posible su utilización. Es un sistema libre desarrollado por miles de personas a través de Internet, y que es el sistema operativo de mayor crecimiento en la actualidad, y el segundo de mayor uso en el mundo, tomando como uno sólo a toda la gama de la familia Windows.
DEBIAN	Debian utiliza el núcleo Linux (el corazón del sistema operativo), pero la mayor parte de las herramientas básicas vienen del Proyecto GNU; de ahí el nombre GNU/Linux. Debian GNU/Linux ofrece más que un SO puro; viene con más de 8710 paquetes, programas precompilados distribuidos en un formato que hace más fácil la instalación en su computadora.
MANDRAKE LINUX	La nueva versión 8.2 de Mandrake Linux amplía su oferta de servicios y confirma su compromiso ofrecer el sistema operativo Linux más completo, fácil usar y de mejor adaptación a los servidores. El mantenimiento mucho mas simplificado, utilitarios completos para el escritorio y herramientas profesionales avanzadas. Utilizando estas herramientas y nuestros nuevos servicios en línea, podrá realizar un rango ilimitado de tareas de computación tanto con seguridad como con profundidad. 7 CD`s y más de 2.500 aplicaciones.
FEDORA	Fedora es el descendiente libre de Linux Red Hat. Abarcado enteramente de software abierto de la fuente, la base de Fedora es un sistema operativo Linux basado en el desarrollo conjunto de los desarrolladores de Red Hat y de la comunidad de Linux.

Sistema Operativo	Descripción
VMS	El sistema operativo VMS (Virtual Memory System) es uno de los más robustos en el mercado, aunque es propietario de la compañia Digital Equipment Corporation. Actualmente con su versión OpenVMS 5.x existe para los procesadores de las máquinas VAX (CISC) y con el Alpha-chip (RISC). Ofrece un amplio conjunto de comandos a través de su intérprete Digital Command Language (DCL), utilidades de red (DECnet), formación de 'clusters' de computadoras para compartir recursos, correo electrónico y otras facilidades. Es un sistema operativo multiusuario / multitarea monolítico.
UNIX	Unix es uno de los sistemas operativos más ampliamente usados en computadoras que varían desde las personales hasta las macro. Existen versiones para máquinas uniprocesador hasta multiprocesadores. Debido a su historia, que evoluciona en los Laboratorios Bell de AT&T con un simulador de un viaje espacial en el sistema solar, pasando por su expansión en universidades y la creación de las versiones más importantes que son la de la Universidad de Berkeley y el Sistema V de la misma AT&T.
OS/2	El sistema operativo OS/2 ha tenido una historia turbulenta en el seno de Microsoft e IBM, creciendo en algún tiempo bajo equipos de trabajo de ambas compañias y prosiguiendo finalmente con la última. Los objetivos para este sistema operativo eran: compatibilidad para ejecutar los programas existentes para DOS en las computadoras 80x86, ofrecer la multitarea, la facilidad de memoria virtual y servicios de red de área local.

Sistema Operativo	Descripción
MAC OS X	Es un sistema operativo desarrollado por Apple Computer Inc., es una reescritura prácticamente completa de su sistema operativo Macintosh, este nuevo sistema Mac está basado en el sistema Darwin. Un proyecto «Libre»), el cual utiliza características de otros sistemas UNIX como Mach, FreeBSD y otros, la idea detrás de Mac OS X y por supuesto de Darwin es crear un completo sistema operativo con la flexibilidad y robustez de un UNIX y la facilidad de uso que siempre a caracterizado a los MAC.
SISTEMA 7.5	Apple se ha propuesto desde hace mucho tiempo, convertirse en el proveedor principal de las redes de área local de las compañías basadas en Macintosh, pero sólo recientemente ha diseñado una estrategia que parece funcionar. Mediante una serie de protocolos compatibles con el modelo OSI, Apple ha proporcionado a las compañías importantes alguna seguridad de que sus redes basadas en Macintosh se podrán comunicar con cualquier LAN basada en PC de IBM.
APPLETALK	El sistema operativo de red AppleTalk está completamente integrado en el sistema operativo de cada equipo que ejecuta el Mac OS. Su primera versión, denominada LocalTalk, era lenta en comparación con los estándares de hoy en día, pero trajo consigo la interconexión de los usuarios que rápidamente hicieron uso de ella. Todavía forma parte del Apple Sistema Operativo de Red una forma de interconexión por el puerto de serie de LocalTalk.

Sistema Operativo	**Descripción**
GENTOO	Contiene las dos imágenes ISO que componen el Sistema Operativo *Gentoo 2004.3* (*Universal-CD y Packages*), la cual incluye: Linux Kernel 2.6, el ambiente de escritorio XFCE4 (además de KDE y GNOME), OpenOffice 1.1 y otras aplicaciones incluidas en esta distribución.
SLACKWARE	Contiene las dos imágenes ISO que componen el Sistema Operativo *Slackware 10*, la cual incluye: Linux Kernel 2.4.26, Mozilla 1.7, GNOME 2.6, KDE 3.2.3, GCC 3.3 y otras aplicaciones incluidas en esta distribución.
KNOPPIX	Contiene la imágen ISO que compone el Sistema Operativo *Knoppix 3.7*, la cual permite ejecutar el sistema operativo Linux directamente de un CD-ROM (*Live-CD*) sin la necesidad de realizar ninguna instalación en un disco duro, ideal para demos o sistemas de rescate, incluye: Linux Kernel 2.4 y 2.6, KDE 3.2, Open-Office y más de 900 paquetes incluidos en la distribución.
OPENBSD	La distribución ofrecida en OpenBSD.org, en lo que a su estructura se refiere, se encuentra bajo derechos exclusivos de Theo de Raadt -- el pionero de OpenBSD -- razón por la que no podemos distribuir una copia exacta. No obstante, el sistema operativo puede seguir siendo copiado libremente, la única restricción de copia se refiere a la estructura / layout del CD.

OPEN-CD	Incluye la última distribución (2.0) del Open-CD que contiene una serie de aplicaciones libres y de código abierto para ser utilizadas en ambientes Windows. Las aplicaciones libres y de código abierto que incluye el Open-CD: Oficina y Diseño: OpenOffice 1.1.3, AbiWord 2.2.1, PDFCreator 0.8, GIMP 2.0.5, Blender 2.35a, Dia 0.94, TuxPaint 0.9.14. Internet y Comunicaciones: FireFox 1.0, Thunderbird 1.0, Mozilla suite 1.7.3, Gaim 1.1.0, Filezilla 2.2.9, TightVNC 1.3dev6, WinHTTrack 3.32-2. Multimedia y Juegos: Audacity 1.2.3, Celestia 1.3.2, CDex 1.51, Sokoban 1.187, Battle for Wesnoth 0.8.8, Lbreakout 2.4.1. Utilerías y Otros: 7-zip 3.13, Notepad2 1.0.12, SciTE 1.62.
NETBSD	NetBSD es tal vez el sistema operativo más portado en el mundo, es otro descendiente de 4.4 BSD y 386 BSD, por lo cual también se distribuye bajo los términos de la licencia BSD, lo que implica que puede ser libremente distribuido en forma binaria o de código fuente. El principal objetivo de NetBSD es la portabilidad, obviamente sin descuidar seguridad y estabilidad como la mayoría de derivados UNIX.
OPENBSD	Este sistema operativo es derivado de NetBSD, sus principales metas son la seguridad, la estandarización y la portabilidad, está catalogado como el sistema operativo más seguro del mundo (aunque en términos de seguridad no se puede hablar de una verdad absoluta.
FREEBSD	FreeBSD es un sistema operativo derivado del 386 BSD, es un sistema operativo libre (y gratuito) creado por cientos de desarrolladores, es altamente usado como servidor de Internet debido a sus altas prestaciones en comunicaciones.

Symantec en su mas reciente reporte (**Internet Security Threat Report**), determinó que el sistema operativo Windows (Figura 4.2.6) es el sistema más seguro muy por arriba de Red Hat, de Mac OSX, de HP-UX y de Solaris de SUN. Los resultados de la encuesta que publica **Symantec** están basados en la cantidad de vulnerabilidades que son detectadas por los fabricantes y/o la comunidad, la criticidad de las mismas y cuantos días le toma a la compañía el liberar el parche desde que son encontradas. Cabe mencionar que las compañías dedicadas a crear sistemas operativos deberán tener una base sólida de desarrollo metódico para generar sistemas operativos más confiables.

Sistema Operativo	# de Vulnerabilidades	# de Vulnerabilidades Criticas	Días para reparar
Windows	39	12	21
RedHat Linux	208	2	58
Mac OSX	43	1	66
HP-UX	98	-	101
Sun Solaris	63	-	122

Figura 4.2.6 Tabla comparativa.

4.3 Software de Trabajo

Dentro de la organización o institución se cuenta con diferente tipo de software dependiendo del rol de cada organización, no obstante cabe mencionar que este es un punto muy importante a considerar dentro de nuestro esquema de seguridad, por lo consiguiente es necesario especificar a que se le llama software de trabajo.

El software de trabajo será aquel que es fundamental para la organización o institución para llevar acabo el objetivo principal de la misma.

Dentro de este software habría que clasificarlo por secciones de área de trabajo, por ejemplo si existe un área de recursos humanos será el software que sólo se use en esa área si se tiene un área de contabilidad será sólo el software dedicado a esa área y así sucesivamente, pero sin duda habrá software que será compartido en común un tipo de software básico, pero fuera de esto el poder tener un control de cada área y el tipo de software que se maneja será fundamental para asignar los privilegios para la obtención e instalación del mismo y así de esta manera el poder protegerlo de futuras instalaciones en los equipos de trabajo donde es necesario.

Es importante remarcar la clasificación del software de trabajo como se dijo anteriormente cuál es su utilidad ya que en muchas ocasiones se instala software que no es necesario en un área de trabajo y esto puede ocasionar que la productividad se vea afectada y así no se lleve acabo el objetivo planteado de la organización, como sabemos la gente dentro de la organización muchas veces no conoce el rol que juega dentro de la misma así como de la responsabilidad, esto a su vez provoca que realicen acciones indebidas, como se ha visto la mayor cantidad de incidentes de seguridad son generados por el desconocimiento de la gente, así como se menciono con anterioridad que la gente no ubica su posición se podría presentar el caso en donde si no se tuviera el control del software, una persona pudiera instalar algún tipo de software no permitido que podría llenar de virus, spyware o web bugs, etc. En otro caso pudiera ser el borrado del software del servidor por la falta de un buen control de acceso así como de los privilegios del mismo.

Resumiendo, el software es otro de los elementos clave en la parte de la seguridad y la productividad de la organización. Se deberá tener en cuenta la siguiente lista de comprobaciones:

- Tener el software imprescindible para el funcionamiento de la actividad, nunca menos pero tampoco nunca más. Tener controlado al personal en cuanto a la instalación de software es una medida que va implícita. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (no debería permitirse software pirata o sin garantías). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre.
- Disponer del software de seguridad adecuado. Cada actividad, forma de trabajo, métodos de conexión a Internet requieren una medida diferente de aproximación al problema. En general, las soluciones domésticas, donde únicamente hay un equipo expuesto, no son las mismas que las soluciones empresariales.

- Métodos de instalación rápidos. Para permitir la reinstalación rápida en caso de contingencia.
- Asegurar licencias. Determinado software imponen métodos de instalación de una vez, que dificultan la reinstalación rápida de la red. Dichos programas no siempre tienen alternativas pero ha de buscarse con el fabricante métodos rápidos de instalación.
- Buscar alternativas más seguras. Existe software que es famoso por la cantidad de agujeros de seguridad (Un agujero de seguridad es un fallo en un programa que permite mediante su explotación violar la seguridad de un sistema informático.) que introduce. Es imprescindible conocer si se puede encontrar una alternativa que proporcione iguales funcionalidades pero permitiendo una seguridad extra.

4.4 Software de seguridad

Muchas veces cuando se quiere proveer de seguridad a un sistema de información, una de las decisiones mas difíciles es decidir que tipo de software se tiene que adquirir, sin duda, la decisión definitiva depende de un estudio detallado y largo, según sea el tamaño de la organización a la cual se requiere proveer de seguridad. Sin embargo en muchas ocasiones tanto se carece de los recursos como del personal adecuado para poder realizar dicho estudio, en muchos casos se justifica un gasto que permita realizar satisfactoriamente todo el proceso, pero en otros muchos casos no es posible hacer ese gasto, entonces cómo proveer de seguridad a nuestra información sin caer en, casos muy lejanos de la verdadera solución.

Nuestro primer paso es identificar que tipo de problema de seguridad se tiene, y así adquirir el producto exactamente necesario y/o realizarlo uno mismo. Este análisis debe de ser muy cuidadoso ya que cualquier punto sin considerar puede ser perjudicial y este afectaría tanto en costo como en beneficio dejando así el análisis inservible para poder tomar la decisión adecuada para atacar el problema.

Algo importante, es hacer notar que en muchas ocasiones es necesario hacer una solución a la medida del problema que se tenga que resolver, sin embargo en varios casos se puede ya comprar algún dispositivo o software que este en el mercado. Claro está que en la mayoría de los mercados es muy difícil que los productos tengan especificaciones tan técnicas, sin embargo el poder hacer una mejor elección del producto necesario.

Cabe mencionar que quizá para una sola PC o un pequeño sistema si podamos evitar tal análisis, y quizá solo con un antivirus, un firewall, la buena elección de la administración de passwords y eventualmente con un certificado digital podamos contar con la seguridad óptima dependiendo de lo que realmente es necesario.

4.5 Antivirus

Los antivirus son programas cuya función es detectar y eliminar virus informáticos así como otros programas maliciosos (a veces denominados *malware*).

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos (también conocidos como firmas o vacunas) de los virus conocidos, por lo que es

importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como heurística) o la verificación contra virus en redes de computadoras.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador web (ActiveX, Java, JavaScript).

4.5.1 Antivirus (activo)

Estos programas como se ha mencionado tratan de encontrar la traza de los programas maliciosos mientras el sistema está funcionando. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

Como programa que está continuamente funcionando, el antivirus tiene un efecto adverso sobre el sistema en funcionamiento. Una parte importante de los recursos se destinan al funcionamiento del mismo. Además dado que están continuamente comprobando la memoria de la máquina, dar más memoria al sistema no mejora las prestaciones del mismo.

Otro efecto adverso son los falsos positivos, es decir al notificar al usuario de posibles incidencias en la seguridad, éste que normalmente no es un experto de seguridad se acostumbra a dar al botón de autorizar a todas las acciones que le notifica el sistema. De esta forma el antivirus funcionando da una sensación de falsa seguridad.

Los factores más importantes a la hora de valorar un antivirus son:

- **Capacidad de detección y desinfección:** Es lógico, un antivirus será mejor cuanto más virus sea capaz de detectar y eliminar. Es más peligroso pensar que no se tiene un virus que tener la duda.
- **Velocidad:** Hoy en día los discos duros son enormes, y si pensamos en intranets y redes corporativas la cantidad de datos a escanear puede ser colosal. Por lo tanto se valorará en un antivirus la capacidad de escanear rápidamente.
- **Actualización:** Cada día aparecen cientos de virus nuevos, para que un antivirus sea capaz de eliminar un virus es necesario que incluya la información del virus y su antídoto en las librerías o bases de datos víricas. La posibilidad de actualizar esas librerías (sobre todo a través de Internet) es un factor fundamental.
- **Servicio de atención:** Una infección de un virus puede dar lugar a situaciones de pánico en algunos casos. El tener un servicio técnico al cual poder recurrir es otro punto a favor.
- **Recomendación:** Hay algo que quizá sea un consejo fundamental. No se puede confiar plenamente en un antivirus.

Cada uno tiene sus limitaciones, por lo tanto, la mejor forma de evitar una infección es la prevención, y en cualquier caso tener instalados dos antivirus en vez de uno.

4.6 Auditoria

La evaluación consiste en identificar la existencia de unos controles establecidos.

Las listas de control se utilizan, como una guía de referencia, para asegurar que se han revisado todos los controles.

La naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información.

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Para hacer una adecuada planeación de la auditoría, se deberá seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

Para auditar un sistema se necesita tener una estrategia en las cuales se incluye una serie de preguntas como parte del proceso a escoger una estrategia de auditoría.

- ¿Por qué se está auditando?.
- ¿Se necesita tener requerimientos diferentes de auditoría para sistemas diferentes?.
- ¿Quién es el responsable de recoger y archivar el registro?.
- ¿Quién debería tener acceso a los registros de auditoría?.
- ¿Es aceptable la pérdida de información de auditoría?.
- ¿Cuanto tiempo hay que guardar los registros?.
- ¿Quién es el responsable de revisar los registros de la auditoría?.
- ¿Con qué frecuencia se debe revisar los registros?.
- ¿Se necesita herramientas para revisar los registros?.
- ¿Que procedimiento se debe tomar cuando se encuentra algo sospechoso?.
- ¿Es necesario una notificación inmediata cuando ocurre un incidente?.
- En caso de notificación inmediata, ¿quién va a responder y cómo?.
- ¿Necesita centralizar los registros de auditoría?.
- ¿Se necesita analizar los registros de varios sistemas a la vez?.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

La auditoría de sistemas debe abarcar tres grandes áreas:

- Auditoría de Infra-Estructura Física y Lógica.
- Auditoría de Aplicaciones y estaciones de trabajo.
- Auditoría de Sistemas y su Administración.

Este tipo de auditorías generalmente son realizadas por un equipo de expertos en diferentes ramas de la informática, con el objetivo de poder revisar a fondo el área asignada y utilizar herramientas de software que permitan obtener "Logs o Bitácoras" de que esta aconteciendo en cada área, con lo cual se podrán analizar y dictaminar el estatus de un departamento dentro de la organización.

Para hacer una planeación eficaz, lo primero que se requiere es:

- Obtener información general sobre la organización.
- Sobre el área y su función dentro de la organización.
- Investigación preliminar y algunas entrevistas previas.

Con base en esto:

Planear el programa de trabajo, el cual deberá incluir:

- Tiempo.
- Costo.
- Personal necesario.
- Documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

4.6.1 Auditoria del equipo

Generalmente las organizaciones poseen un departamento administrativo que tiene definidos los Roles, funciones, atribuciones de cada uno de los miembros de la organización, por consiguiente, el área de administración de sistemas debe tener conocimiento de que funciones tiene un miembro de la organización, para poder instalar el software necesario para el trabajo de dicho miembro. Así poder determinar que no tenga juegos o herramientas que distraigan su atención, o que solamente consuman recursos de la estación de trabajo necesarios para su trabajo cotidiano. Por ello es que la organización debe tener clara estas definiciones.
Los puntos que se tocan dentro de la auditoría de equipo son los siguientes datos:

- Que los usuarios no sean Administradores de sus equipos, para que no puedan instalar Software a su discreción.

- Revisión de poseer con las licencias de los programas instalados en la estación de trabajo.
- Hay que hacer las revisiones del caso con Software si se cuenta para el inventario de equipo.
- Que cuente con las actualizaciones.
- Que el sistema operativo sea el establecido.
- Que las políticas de seguridad estén implementadas.
- Que el software instalado sea el correcto.
- Que el software cuente con las licencias.
- Que el número del inventario del equipo coincida con el que se presenta en el inventario del documento proporcionado.
- Ubicación del equipo sea la correcta de acuerdo al inventario establecido.
- Que los puertos abiertos sean los correctos.
- Las cuentas sean las correctas.
- Las políticas de cuentas estén implementadas.
- Las políticas de usuario sean las correctas.
- Los privilegios sobre archivos.
- Los privilegios sobre impresoras.
- Si se cuenta con las bitácoras mencionados.
- Revisión si se tiene habilitado las directivas de auditoría en los equipos.
- Revisión si se tiene habilitado las directivas de auditoría en los equipos.

4.7 Escaneo de la Red

Escaneo de red: Es la utilización de una red de cómputo para obtener información sobre los sistemas conectados a dicha red y el cual puede ser usado para mantenimiento de los sistemas, evaluación de redes así como para ataques. Esto incluye el escaneo de puertos y el escaneo de vulnerabilidades.

- Escaneo de puertos: Es el proceso de enviar paquetes de datos a través de la red a números de puertos seleccionados (HTTP: 80, Telnet: 23, etc) de un equipo de red con el propósito de identificar la disponibilidad de servicios de red en ese sistema. Este proceso es de gran ayuda para encontrar problemas en los sistemas o para mejorar la seguridad. El escaneo de un puerto es un método para obtener información y cuando se efectúa por individuos desconocidos se considera el preludio de un ataque.

- Escaneo de vulnerabilidades: Es el proceso de identificación de vulnerabilidades conocidas en un sistema de red. Este proceso va más allá de la identificación de los servicios de red disponibles en un sistema de red como es el caso del “escaneo de puertos”. El escaneo de vulnerabilidades identificará las debilidades de un sistema operativo o de software de aplicación lo cual puede ser utilizado para comprometer o para hacer que falle un sistema. El escaneo de vulnerabilidades es invasivo y debe ser efectuado con cuidado ya que en ocasiones puede causar que el sistema falle o se comporte de forma errática. Estos escaneos también obtienen información de los

sistemas y cuando son efectuados por individuos desconocidos se consideran un preludio a un ataque.

Los escaneos no autorizados pueden resultar en:

1.-Revelar información sensitiva: Los escaneos de red recopilan una cantidad importante de información acerca de los dispositivos conectados a la misma. Esta información es crucial para los atacantes en su intento de comprometer los sistemas de cómputo. Si un sistema crítico es comprometido, un atacante puede tener acceso ilimitado a información confidencial.

2.-Pérdida de servicio: Los ataques a la red varían enormemente en su naturaleza. La meta de un atacante puede ser obtener el control de un sistema de cómputo o simplemente hacer que nadie mas lo puede acceder. Incluso el proceso de escaneo para verificar la vulnerabilidad de un sistema puede ocasionar que este se comporte de manera errática o que quede de fuera de servicio.

3.-Pérdida de conexión a la red y del rendimiento de la misma: Los escaneo pueden involucrar a cientos o hasta a miles de sistemas de cómputo. El abrupto volumen de tráfico puede ocasionar un tremendo esfuerzo en los recursos de los sistemas de computo y de la red, resultando en un bajo desempeño lo cual afecta directamente a los usuarios.

4.-Pérdida de reputación: Sí se permite el uso de la información indebida, o se incurre en escaneos que no son autorizados, se perjudica ampliamente a quien desea realizar tener un buen manejo de la información que despliega el escaneo a la red, por lo cual es necesario que sólo sea el personal dedicado a esa área quien pueda realizar dichos escaneos ya que se puede poner en reputación lo que se maneja con dicha información.

Dentro de las herramientas para el escaneo de las redes encontramos las siguientes:

Nmap 4.11 (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad (Figura 4.7). Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características.

La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la “tabla de puertos interesantes”. Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado. El estado puede ser `open` (abierto), `filtered` (filtrado), `closed` (cerrado), o `unfiltered` (no filtrado). Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. `Filtrado` indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra `abierto` o `cerrado`.

Los puertos `cerrados` no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como `no filtrados` son aquellos que responden a los sondeos de Nmap, pero para los que Nmap no puede determinar si se encuentran abiertos o cerrados. Nmap informa de las combinaciones de estado `open-filtered` y `closed-filtered` cuando no puede determinar en cual de los dos estados está un puerto. La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. Nmap ofrece información de los protocolos IP soportados, en vez de puertos abiertos, cuando se solicita un análisis de protocolo IP con la opción (`-sO`).

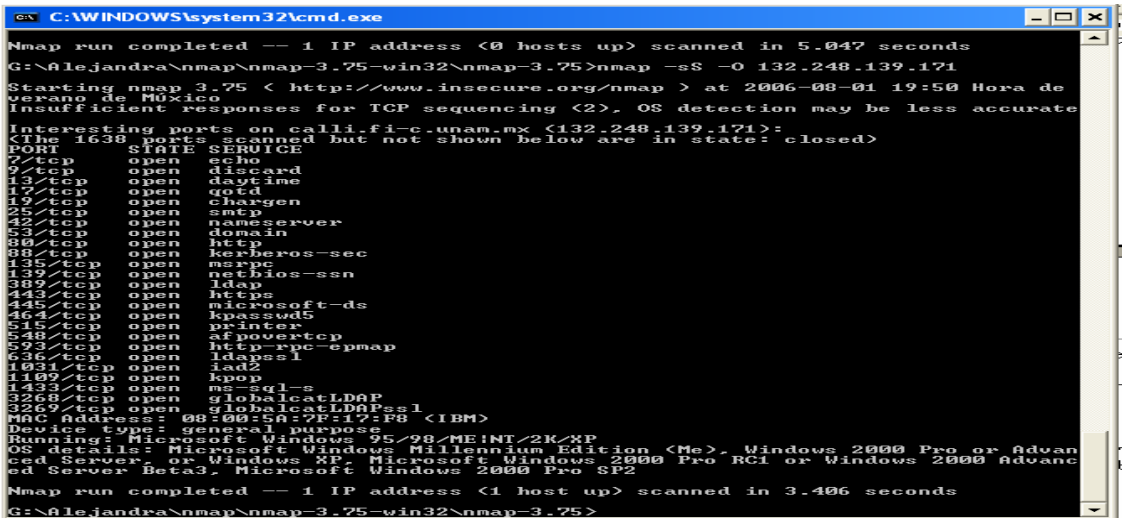


Figura 4.7 Entorno De Nmap 4.11.

Show Traffic (Figura 4.7.1) es una herramienta que permite monitorear el tráfico de la red y así poder detectar algún tráfico sospechoso que pudiera generar la privación de algún servicio. Un monitoreo constante del tráfico de la red, ya que dicha herramienta cuenta con un entorno muy amigable, además de que cuenta con opciones de filtrado de protocolos los cuales pueden ser TCP, UDP e ICMP, además proporciona la ip origen, así como la IP destino y el servicio del protocolo que muestra.

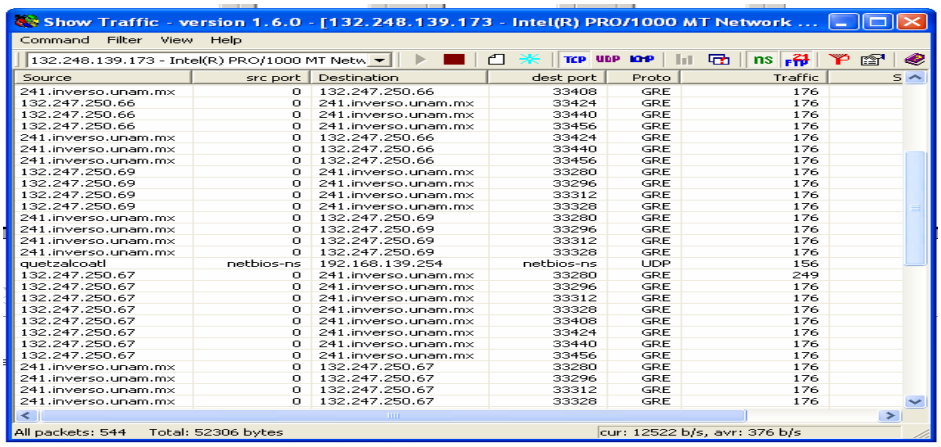


Figura 4.7.1 Entorno de Show Traffic 1.6.0.

4.8 Revisión de Bitácoras

Los sistemas de cómputo generan una gran cantidad de información, conocidas como bitácoras o archivos logs, que pueden ser de gran ayuda ante un incidente de seguridad, así como para la auditoría de los equipos. Las vulnerabilidades de los sistemas aumentan, al mismo tiempo que se hacen más complejos, el número de ataques también aumenta, por lo anterior se reconoce la importancia y utilidad de la información contenida en las bitácoras de los sistemas de cómputo.

Una bitácora puede registrar mucha información acerca de eventos relacionados con el sistema que la genera los cuales pueden ser:

- Fecha y hora.
- Direcciones IP origen y destino.
- Dirección IP que genera la bitácora.
- Usuarios.
- Errores.

La importancia de las bitácoras es la de recuperar información ante incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas y evidencia legal. En la Sala de Cómputo se llevo acabo la implementación de bitácoras como se estipulo en el capítulo 6, pero adicionalmente a prueba se llevo acabo la implementación de bitácoras externas el cual su función fue llevar un detallado respecto a la actividad de los equipos de cómputo, para el apoyo de estas bitácoras se contó con las bitácoras que generaba el mismo equipo, estas bitácoras constaron de la siguiente información

- Equipo.
- Ubicación en la sala.
- Hora y fecha.
- Suceso.
- Implementación o medidas a llevar acabo.
- Responsable.

Esto con el fin de llevar una bitácora que proporcionará todos aquellos eventos que se llevaran con los equipos, además de tener un cotejo al momento de realizar la revisión de las bitácoras internas que se generan, la implementación de esta bitácora proporciono información de cómo y cuando se llevaron acabo los ajustes a los equipos, además de proporcionar información a los miembros de la Sala de Cómputo una información completa al instante, debido a que en ocasiones anteriores se presentaba fallos sobre algún equipo o modificaciones en software y aplicaciones. Por lo cual proporcionó un seguimiento de todas las fallas y ajustes, se tuvo más conciencia actuándose con mayor rapidez y exactitud ante nuevos problemas.

4.9 Revisión periódica de los avances

Considerando como punto de partida el análisis de riesgos, estrategia de seguridad y el desarrollo de las políticas, normas, criterios y procedimientos se definieron las soluciones

tecnológicas así como las herramientas que serán requeridas para soportar la base normativa y conceptual de lo argumentado anteriormente.

Lo anterior usualmente representa un problema que debe ser tratado de forma cuidadosa en la que se tenga un buen conocimiento de las herramientas tecnológicas que se encuentran al día en el mercado siendo un factor importante en el monitoreo de la implementación de los nuevos lineamientos establecidos.

Como se ha planteado constantemente la seguridad es un proceso dinámico, y como tal es necesario llegar a las revisiones periódicas. Las revisiones se hacen sobre la estrategia de seguridad, concientización y entrenamiento, los procedimientos, normas, criterios y políticas establecidas. Estas revisiones tienen efecto sobre las amenazas, el análisis de vulnerabilidades, ambiente y consecuencias, mecanismos y el factor humano como lo muestra el diagrama base (Figura 7.13) donde recae todo el análisis e implementación.

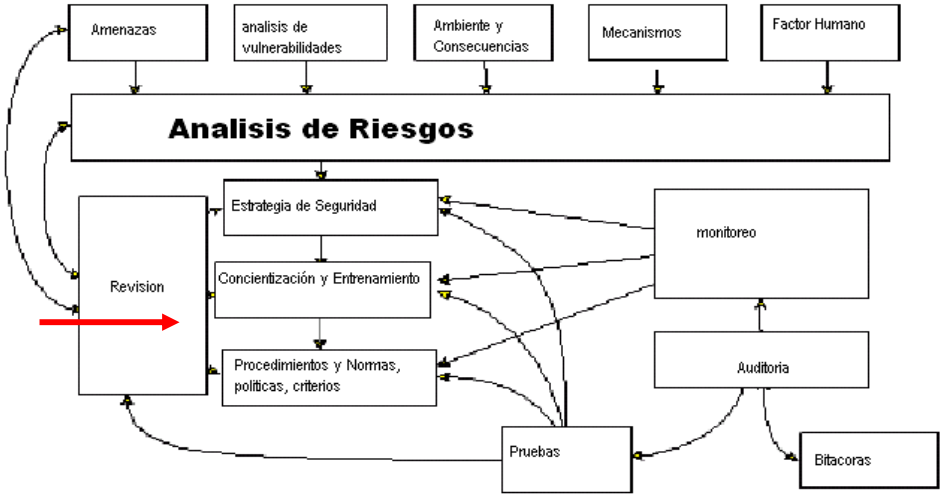


Figura 4.9 Diagrama base

Igual que las revisiones, el monitoreo juega un papel importante este se hace sobre las estrategias, procedimientos, políticas, criterios, normas, medidas, concientización y entrenamiento con el fin de asegurar el cumplimiento de las mismas y observar que funciones de acuerdo a las necesidades. La gente que lleva acabo el monitoreo debe estar capacitados para tomar acciones que vayan más de allá de hacer alguna detección apropiada una respuesta que compense una protección que no haya sido adecuada.

Es la última parte en el ciclo las revisiones, y se debe responder a:

- ¿Qué está haciendo la gente?
- ¿Cómo funcionan los procesos?
- ¿Cómo se esta usando la tecnología?

Además de

- ¿Cómo está funcionando la tecnología?
- ¿Los esquemas de trabajo satisfacen los requerimientos de operación y seguridad?
- ¿Cuáles son los puntos de mejora y las entradas para el inicio del ciclo nuevamente?
- Recolección, examinación y preservación de evidencia para delitos informáticos.

Tanto los monitoreos como las revisiones deberán ser en un periodo de cada 15 días mínimo a un mes máximo esto con la finalidad de que los elementos sobre los que recae el monitoreo y las revisiones se lleven acabo cumpliendo con los requerimientos que se piden para la solventación del análisis realizado.

4.10 Programa de concientización y capacitación

El programa de concientización y capacitación es el 50 % del éxito del diagrama (arquitectura de seguridad) implementado por lo cual es necesaria la inversión en este punto, esta es una actividad interna en donde se pretende llegar a la idea de la importancia de la seguridad en la organización. Sin el personal capacitado el software es una protección estática, la educación es vital y atender un evento como este, es una de las mejores inversiones que se puedan hacer, la gente como se sabe es uno de los factores más vulnerables dentro de la seguridad.

El poder controlar la tecnología es relativamente fácil, y en este caso se puede decir que se puede saber el comportamiento que va a seguir mas adelante, con las herramientas necesarias se puede hacer que los miembros de la organización se adecuen a los passwords seguros con las políticas que se pretende implementar, pero en lo que respecta a su comportamiento si no se tiene una buena educación con respecto a la seguridad, lo mas probable será que los passwords sean anotados en pequeños papeles pegados a la computadora o sean proporcionados a otras personas que no deben tenerlas.

CAPÍTULO 5

ANÁLISIS DE LA PROBLEMÁTICA EN PARTICULAR

5.1 Problemática en particular

Como sabemos hoy en día la seguridad no es un tema aislado en donde ya no se tienen las bases para poder proporcionar una seguridad adecuada dentro de una organización donde sus sistemas de información son computarizados, es por eso que al principio se planteo un punto de referencia, en donde los capítulos anteriores han dado las bases con un estudio fundamentado sobre seguridad, partiendo de los capítulos anteriores se empezará a plantear el esquema de lo que será el tema sobre el cual se está trabajando enfocado en un problema real, de igual manera se llegará a una especificación general para la adecuación de otros problemas reales.

La problemática a la que se enfocará el tema propuesto será en la Unidad de Servicios de Cómputo Académico (UNICA) ubicada en las instalaciones de la Facultad de Ingeniería, en la UNAM, por lo que será de suma importancia conocer parte de su historia, así como sus objetivos para empezar a plantear lo que será la metodología de seguridad adecuada con respecto a su infraestructura.

5.1.1 Esquema general

Unidad de Servicios de Cómputo Académico (UNICA).

- Historia

Surge en el año de 1994 cuando se decide seccionar el Centro de Cálculo de acuerdo a sus objetivos y funciones, con la finalidad de proporcionar una mayor eficiencia en el desempeño del personal. Con base a esto se crean dos Unidades para desempeñar el trabajo que realizaba el Centro de Cálculo. La Unidad de Servicios de Cómputo Académico (UNICA) y la Unidad de Servicios de Cálculo Administrativo (USECAD), son las dos unidades creadas para llevar a cabo las tareas Académicas y Administrativas de la Facultad de Ingeniería.

La Unidad de Servicios de Cómputo Académico, se esfuerza siempre para estar a la vanguardia de la tecnología en el área de cómputo.

Las funciones que desempeña la Unidad de Servicios de Cómputo Académico:

- Mantener el liderazgo en cuanto a tópicos en cómputo.
- Continuar proporcionando recursos de cómputo de calidad a la comunidad de la Facultad.
- Impulsar a nivel de la Facultad la creación de una política de cómputo definida.
- Lograr la capacitación cada vez más completa y actualizada para la formación de recursos humanos.
- Aplicar todos los conocimientos y las herramientas de cómputo con los que cuenta la Unidad para realizar las actividades de forma más eficiente y segura.

La excelencia de UNICA se debe a que una de las principales actividades de la Unidad es brindar el mejor servicio a los usuarios para ayudar en su formación como futuros

profesionistas. El hecho de ser parte de UNICA nos ha brindado una visión de la problemática que enfrenta el profesionista en el campo profesional.

- Política de Calidad

En UNICA nuestro objetivo principal es cumplir con los requerimientos de nuestros clientes en el área de cómputo, teniendo como meta elevar la calidad de nuestros productos y servicios, para ello nos comprometemos en un proceso de mejora continua.

- Misión

La misión de La Unidad de Servicios de Cómputo Académico es la de proporcionar eficaz y eficientemente en el ámbito institucional, los servicios de cómputo y el apoyo en actividades relacionadas que conlleven al proceso integral de formación académica en la Facultad de Ingeniería.

- Visión

La proyección de la Unidad de Servicios de Cómputo Académico al año 2010 es continuar siendo una unidad líder en la prestación de servicios de cómputo de vanguardia a la Facultad de Ingeniería, al entorno universitario y a la sociedad en general.

- Contando con la organización, administración y recursos adecuados.
- Siendo lideres en la formación, capacitación y difusión de la cultura informática.
- Contando con las herramientas y convenios adecuados para el desarrollo y la investigación informática.
- Contando con una infraestructura de red de cómputo moderna y tecnología de punta, brindando servicios de calidad y alta disponibilidad en tecnologías de la información y comunicación.
- Contando con los servicios y procesos de atención sistematizados actuales, en apoyo a los eventos de seguridad informática.
- Contando con la infraestructura adecuada y mecanismos para la actualización continúa del equipo de cómputo.
- Valores.

El ambiente de trabajo de los integrantes de UNICA se basa en un clima de cordialidad, respeto, honestidad, responsabilidad, ética y compromiso.

5.2 Análisis de las Técnicas y Políticas a utilizar

5.2.1 Metodología

Definición de método

Método: Modo ordenado y sistemático de proceder para llegar a un resultado o fin determinado.

- Procedimiento que se sigue para conseguir algo.
- Procedimiento que se sigue en las ciencias para aumentar el conocimiento y enseñarlo: método sintético; el parcelamiento de los objetos de estudio, regla básica del método analítico desde Descartes, es una de las claves del cientifismo.
- Conjunto de reglas y ejercicios destinados a enseñar una actividad, un arte o una ciencia:

Metodología: Parte de la lógica que estudia los métodos. Conjunto de métodos que se siguen en una investigación científica, un estudio o una exposición doctrinal: metodología de la enseñanza; metodología del trabajo, etc.

Objetivos de una metodología

- El tiempo es finito y además cada minuto que pasa cuesta, es necesario maximizarlo.
- Identificar de manera rápida, metódica y estratégica las vulnerabilidades y/o debilidades de los sistemas objetivo.
- Identificar las posibles vías de ataque.
- Optimizar recursos.
- Trabajar de manera estructurada.
- Análisis.
- Encontrar los puntos más débiles.

Fases

- Identificación y Valuación.
- Análisis.
- Arquitectura.
- Planeación.
  - Bases.
  - Estrategia.
  - Procedimientos.
  - Control.
- Auditoría.
- Monitoreo.
- Revisión.
- Modificación.

Una buena metodología nos llevará hacer una buena utilización de los recursos con los que contamos, de igual manera nos proporcionará una base sólida para poder aplicar de manera eficaz las técnicas necesarias para poder implementar una buena seguridad.

En el capítulo 3 sección (3.5.5, Diagrama para el análisis de un sistema de seguridad) se explicó un diagrama el cual se retomará de nuevo al llegar a este punto, dicho diagrama nos permitirá tener un estudio mas detallado para implementar políticas de seguridad sustentada en una metodología.

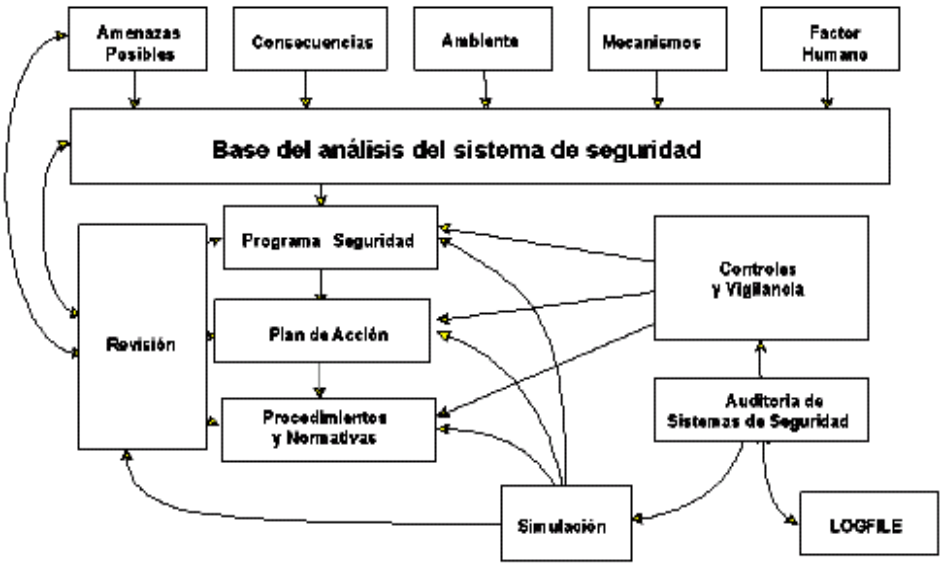


Figura 5.0 Diagrama de análisis.

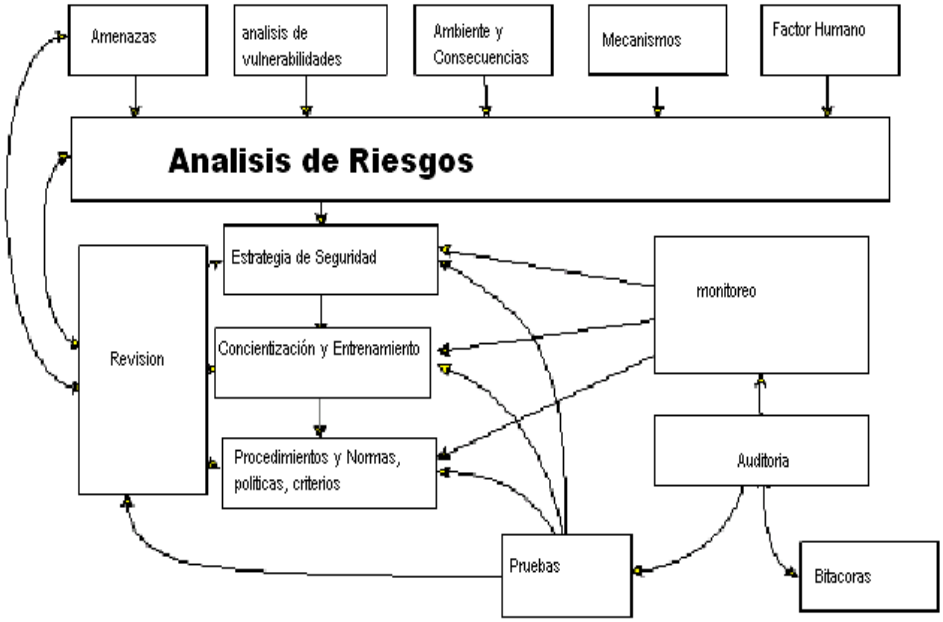


Figura 5.1 Diagrama modificado.

Como se puede observar el diagrama fue modificado para poder hacer una compatibilidad de lo que se pretende, un enfoque estructurado, con nuevos conceptos que serán implementados realizando mejor control de la seguridad a la que se pretende llegar.

Haciendo un análisis de los cambios hechos al diagrama base se puede observar los nuevos puntos a tratar:

- Análisis de Vulnerabilidades: Proceso que nos permitirá identificar, evaluar y reducir los riesgos.
- Análisis de Riesgos: Tomará el análisis de vulnerabilidades y las amenazas para poder tomar criterios de control y estrategias.
- Estrategia de Seguridad: Definir prioridades y proyectos de seguridad.
- Concientización y Entrenamiento: La gente es el punto más vulnerable y de ella dependerá la implementación.
- Procedimientos, Normas, Políticas y Criterios: Determinar lineamientos, herramientas, soluciones estratégicas, fundamentales para un buen programa de seguridad.
- Bitácoras: Archivos que nos permitirán analizar posibles procesos activos.
- Pruebas: Permitirán observar que las herramientas utilizadas serán aquellas que nos ayuden a implementar lo anterior mencionado así como elementos que pueden estar en peligro.

Estos son los conceptos que serán tratados en cada punto de avance de acuerdo al diagrama establecido.

5.2.2 Análisis de las técnicas a utilizar

Dentro de nuestra metodología haremos un análisis de lo que será la base para poder crear una arquitectura completa de seguridad por lo cual en este punto se hará una pausa para comenzar.

El análisis además de ser una base; definirá relaciones con otros puntos importantes que deberán ser tratados, por lo cual nos llevará a realizar los siguientes puntos:

- Es la base para una buena metodología.
- Define requerimientos importantes para la organización.
- Nos llevará a realizar una buena campaña planeación.
- Conocer cuánto se va invertir en implementar ciertas medidas.

Para poder tener dichos elementos es muy importante realizar acciones de manera que sean ordenadas y concretas, que nos conduzcan a resultados precisos por lo cual dentro de estas acciones estarán los análisis, la valoración, identificaciones, procedimientos y monitoreos.

Dentro de las técnicas a utilizar se ha efectuado un listado completo de los análisis a dentro de este marco de metodología que son los siguientes:

- Análisis valuativo.
- Análisis del hardware.
- Análisis de la red física.

- Análisis del software.
- Análisis de vulnerabilidades.

En donde cada análisis se verá en forma detallada, dando un esquema en particular así como un general; las técnicas serán básicas para un buen desarrollo de una metodología.

5.2.3 Análisis de evaluativo

El poder realizar una evaluación, se encuentra dentro de los procesos dentro de la organización, proporcionando así los medios necesarios para poder llevar acabo otro de los análisis que se tocaran más adelante, el cual es el análisis de riesgo llevando acabo un acotamiento de la información y procesos críticos de la información.

Es en este punto donde se han de hacer las siguientes preguntas:

- ¿Cuál es el objetivo principal de la organización?
- ¿Cuál es su misión?
- ¿Cuál es su perspectiva a futuro?
- ¿Qué es lo que se va a proteger?
- ¿Cuánto vale aquello que se quiere proteger?
- ¿A que nivel de seguridad se quiere llegar?

En este punto cabe recordar que al inicio de este capítulo se dio una breve introducción con respecto a la problemática en particular, por lo cual al momento de poder hacer el análisis valuativo, considerando que se tienen las preguntas generales, se empezará a especificar esta parte

¿Cuál es el objetivo principal de la organización?

Dar servicio de cómputo a los alumnos en la Facultad de Ingeniería.

La Unidad de Servicios de Cómputo Académico (UNICA) se esfuerza siempre por estar a la vanguardia de la tecnología en el área de cómputo el poder mantener, continuar, impulsar, capacitar y lograr la innovación en la tecnología de cómputo, de manera completa, eficiente y segura; proporcionando recursos de cómputo de alta calidad.

En UNICA el objetivo principal es cumplir con los requerimientos de nuestros clientes en el área de cómputo, teniendo como meta elevar la calidad de sus productos y servicios, para ello se comprometen en un proceso de mejora continua.

¿Cuál es su misión?

La misión de La Unidad de Servicios de Cómputo Académico es la de proporcionar eficaz y eficientemente en el ámbito institucional, los servicios de cómputo y el apoyo en actividades relacionadas que conlleven al proceso integral de formación académica de los alumnos en la Facultad de Ingeniería.

¿Cuál es su perspectiva a futuro?

El ser una unidad líder en la presentación de servicios de cómputo de vanguardia para la facultad de Ingeniería, el entorno y la comunidad. Con una organización, administración y recursos, que sean los adecuados para el desarrollo, investigación, infraestructura, y procesos en calidad de servicios de cómputo.

¿Qué es lo que se va a proteger?

Los servicios de cómputo de la comunidad estudiantil de la Facultad de Ingeniería.
¿Cuánto vale aquello que se quiere proteger?

El brindar el servicio de manera adecuada a la comunidad estudiantil de la Facultad de Ingenieria, cumpliendo con los objetivos planteados.

¿A que nivel de seguridad se quiere llegar?

La seguridad real no existe la óptima para poder brindar los servicios de la organización sería la adecuada a llegar.

- Estar alineados a las necesidades de la organización.
- Este basada en el análisis de vulnerabilidades y riesgos.
- La seguridad implementada deberá de operar de manera adecuada para mantener los principios de seguridad: integridad, confidenciabilidad y disponibilidad.

5.3 Análisis del Hardware existente.

El hardware como se ha visto en capítulos anteriores se le ha dado un seguimiento con respecto a la seguridad que este debe de tener, por lo cual es necesario empezar a hacer un análisis completo del hardware con el que cuenta la organización.

Uno de los activos importantes es el hardware, sin el en este caso no se llevarían acabo los objetivos vistos al principio, UNICA (Unidad de Servicios de Cómputo Académico) brinda en sus instalaciones el uso de computadoras a los alumnos de la Facultad de Ingeniería, de igual manera se imparten cursos, cuenta con un Plan de Becarios, con el fin de formar alumnos que apoyen a la unidad brindando servicios a los usuarios con el apoye de cursos y proyectos, entre otros servicios. Pero el fin de retomar este punto es llegar que el punto clave de esto es el poder brindar un servicio de cómputo de alta calidad a los alumnos de la Facultad, esto nos con lleva a percatarnos que el uso del hardware esta al día dentro de las instalaciones de UNICA por lo cual se empezará hacer el análisis de dicho.

Sala 2 –Ubicada a espaldas del Auditorio Sotero Prieto en el Edificio Sur.

Ubicación	Nombre	Cantidad	Descripción
Aula A	Tlamemes	2	Pentium IV Dell
		3	Pentium III Hp Vectra
		10	Pentium 100 Acer P100
Aula B	Águilas	12	Pentium III Hp Vectra
Aula C	Príncipes	21	Pentium 100 Acer 100
Aula D	Tigres	10	Pentium IV Dell
Usuarios (Comunidad Estudiantil)			
Total de Computadoras en Salas A, B, C y D		**58**	

Tabla 5.0 Hardware Sala 2 Área Aulas.

La Sala 2 –Auditorio Sotero Prieto se encuentra dividida en cuatro aulas, un cuarto de servidor así como el entorno de Administración donde también se encuentran computadoras, la relación es la siguiente:

Ubicación	Nombre	Cantidad	Descripción
Servidores	Bonampak	1	Pentium II HP Brio
	Xel-Ha	1	Pentium III HPE200
	NAT-Anexo	1	Pentium III HP E200
	SCOSU	1	Pentium IV Dell
"Seguridad"	**Firewall 1 y 2**	**2**	**Pentium IV Dell**
Total de Computadoras Servidores		**4**	
Administradores	Quetzalcoatl	1	Pentium IV Dell
	Miztli	1	Pentium IV Armada
	Kukulcan	1	Pentium III HP Vectra
	Tochtli	1	Pentium III HP Vectra
Control de usuarios	Coatl	1	Pentium III HP Vectra
Total de Computadoras Administración		**5**	
			Sistema Operativo Windows 2000 Server, NT **Linux**
		Total De Computadoras En Sala 2	**67**

Tabla 5.1 Hardware sala 2 Área Administración.

Sala 3 –Planta Baja Torre de Ingeniería

La Sala 3 – Planta Baja Torre de Ingeniería cuenta con 4 Aulas de cómputo, una sala de administración y cuarto de servidores, de igual manera tienen a su disposición computadoras para otros usos, la relación es la siguiente:

Ubicación	Nombre	Cantidad	Descripción
Aula E	Sócrates	40	Pentium III HP Vectra
Aula F	Aristóteles	40	Pentium II HP Brio
Aula G	Platón	30	Pentium III HP Vectra
Aula H	Linux	8	Pentium IV Dell
		8	Pentium III HP Vectra.
	Total Computadoras Linux	**16**	
	Pitágoras	17	Pentium Acer 100
		1	Pentium Armada
		2	Pentium Acer Altos
Uso (Comunidad Estudiantil)	**Total Computadoras Windows**	**20**	
Total de Computadoras en Salas E, F, G y H		**146**	

Tabla 5.2 Hardware Sala 3 Área Aulas.

Ubicación	Nombre	Cantidad	Descripción
Servidores	Zeus	1	Pentium III HP E200
	Hades	1	Pentium III HP E200
	Medusa	1	Pentium III HP E200
	Linux	1	Pentium III HP Vectra
Total de computadoras Servidores		**4**	
Impresión	Impresión	1	Pentium III HP Vectra
	Impresión	1	Pentium III HP Vectra
	Impresión	1	Pentium III HP Vectra
Total de Computadoras Impresión		**3**	
Administradores	Vulcano	1	Pentium III HP Vectra
	Tritón	1	Pentium III HP Vectra
	Linda	1	Pentium III HP Vectra
	Quetzalli	1	Pentium III HP Vectra
	Apolo	1	Pentium II HP Brio
	Pitágoras	1	Acer Altos
	Apocalipsis	1	Pentium II HP Brio
	Hermes	1	Pentium II HP Brio
Total de Computadoras Servidoras		**8**	
Total de Computadoras en Sala 3		**161**	

Tabla 5.3 Hardware Sala 3 Área Administración

En la Siguiente tabla se muestra los años de utilidad de los equipos, cual es su función dentro de la unidad, así como la carga y tiempo a la que son expuestos.

Descripción	Años de utilidad	Uso	Funcionamiento
Pentium Acer P100	9 años	El quipo lo utiliza el alumnado de la Facultad de Ingeniería	Por el tiempo de vida que llevan trabajando, se puede decir que este tipo de equipo, necesita mantenimiento a nivel preventivo y correctivo, es un equipo que presenta más fallas a nivel hardware, los procesos son lentos, así como la paquetería debe ser la menor instalada para tener un desempeño mejor.
Pentium II HP Brio	6 años		En este tipo de equipos por la cantidad de años que lleva presenta de igual manera fallas a nivel hardware, no tan continuo como con el caso anterior. Dando como resultado un mantenimiento correctivo frecuente, de igual manera los procesos empiezan a ser lentos,

Tabla 5.4 Función de los equipos de cómputo

Descripción	Años de Utilidad	Uso	Funcionamiento
Pentium III HP Vectra	4 años	Dentro de este punto hay que remarcar que se tienen servidores que funcionan las 24 horas del día.	El tiempo de vida de estos equipos es menor que en los anteriores, El tipo de mantenimiento aplicado en este tipo de equipos es el preventivo y de esta manera evitar posibles fallas a nivel de hardware, los procesos son rápidos a pesar de la cantidad de paquetería instalada en las máquinas.
Pentium IV Dell	3 años		El tiempo de vida de este equipo no ha sido tan largo por lo que se puede decir que los procesos son rápidos, el mantenimiento preventivo se les da para evitar algún tipo de falla a corto o largo plazo

Tabla 5.5 Uso de los equipos de cómputo

Al hacer el análisis en un cuadro comparativo nos dará mayor información acerca del tipo de hardware con el que contamos, así como el tiempo de trabajo de dicho equipo contemplando la carga y tiempo de vida por lo tanto se propone este formato para tener una mayor control del hardware existente.

Se puede observar que dependiendo del sistema operativo que se tenga es como vamos a proteger el equipo con ciertas restricciones o políticas.

5.4 Análisis de la Red Física instalada.

Cada una de las salas es una Red LAN, ya que cuenta con los requerimientos básicos de una red, como servidores, estaciones de trabajo, elementos de conexión, una topología Ethernet, arquitectura de red de modelo OSI, provee una comunicación de 10-100 Mbps, dispositivos de red en este caso ruteadores, concentradores, entre otros elementos.

En la siguiente figura se puede observar como esta distribuida la red física en general, para el caso de la Sala 2 "Ubicada a espaldas del Auditorio Sotero Prieto" se encuentra dividida por cuatro aulas de cómputo las cuales cuentan con equipo que el cual cuenta con un nodo conectado por medio de un cable de par trenzado, cada uno de los equipos esta dentro de un dominio, cada uno de ellos cuenta con una clave de red para poder acceder al dominio. Los equipos están divididos por medio de escritorios individuales, los cables de cada equipo se encuentran sujetos, se cuentan con canaletas para poder tener un mejor control de los cables de conexión, cada uno de los nodos tienen un número asignado para un mejor control de los mismos, de igual manera cada aula cuenta con aire condicionado debido a las altas temperaturas que se llegan a presentar, por lo cual se cuenta con la ventilación adecuada, el acceso a las salas es restringido sólo por alumnado de la Facultad de Ingeniería, el acceso al área administrativa es restringido sólo por personal autorizado, el cuarto de servidores se encuentra cerrado bajo llave y candado, por lo tanto únicamente el administrador de la sala de cómputo cuenta con las llaves necesarias para poder ingresar al cuarto de servidores se encuentran, de igual manera este cuarto cuenta con aire acondicionado, así como, nobreaks por si existe algún fallo en el suministro de corriente y no se presente un daño grave en los servidores, estos cuentan con un nodo y conexión vía cable de par trenzado. En el cuarto de control de red es donde se encuentran los concentradores, fibra óptica, routers y cableado, el cual llega hacia las salas por medio de cableado estructurado, es por esta razón que está zona es de las más cuidadas, sólo gente capacitada puede acceder a está zona.

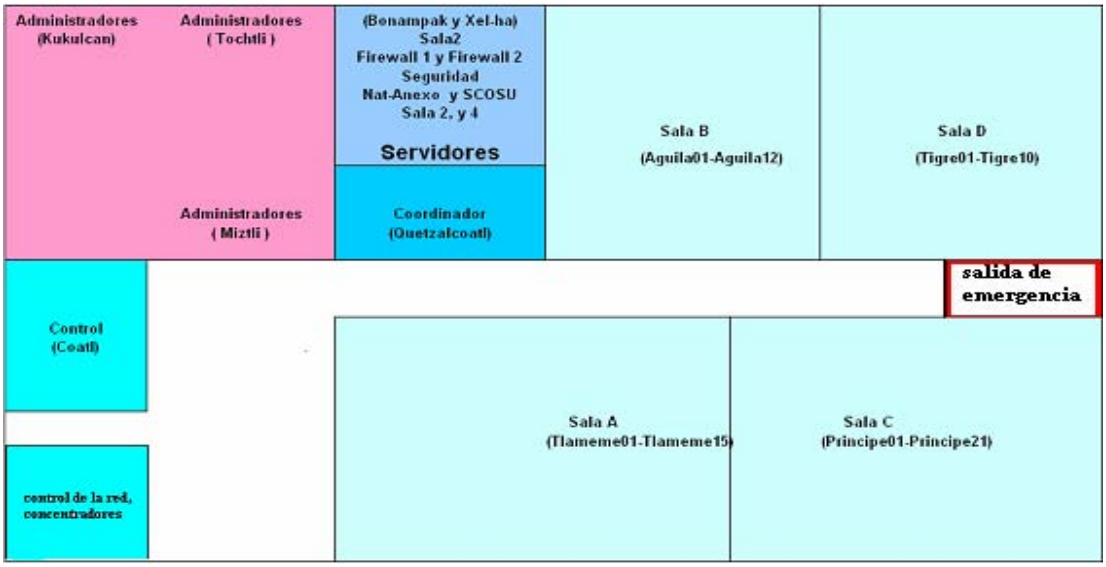


Figura 5.3 Diagrama de Distribución de Clientes (Red)

La sala 3 “Torre de Ingeniería” se encuentra dividida en cuatro aulas las cuales cuentan con equipo de cómputo como anteriormente se mencionó, estos equipos están divididos por escritorios individuales, los cables de los equipos junto con el de conexión de red se encuentran sujetos, cada uno de los equipos tienen asignado un nodo y la conexión está hecho por medio de un cable de par trenzado, cada una de las aulas cuentan con aire acondicionado por lo anterior mencionado se necesita de una ventilación adecuada por las altas temperaturas que se llegarán a presentar dentro de la sala de cómputo; en el área de administración se encuentran los equipos asignados para los administradores de las salas, cada uno cuenta con un equipo, la oficina de administración cuenta de igual manera con aire acondicionado, el cuarto de control cuenta con aire acondicionado y nobreaks para seguridad de los equipos de comunicación (concentradores y switch’s).

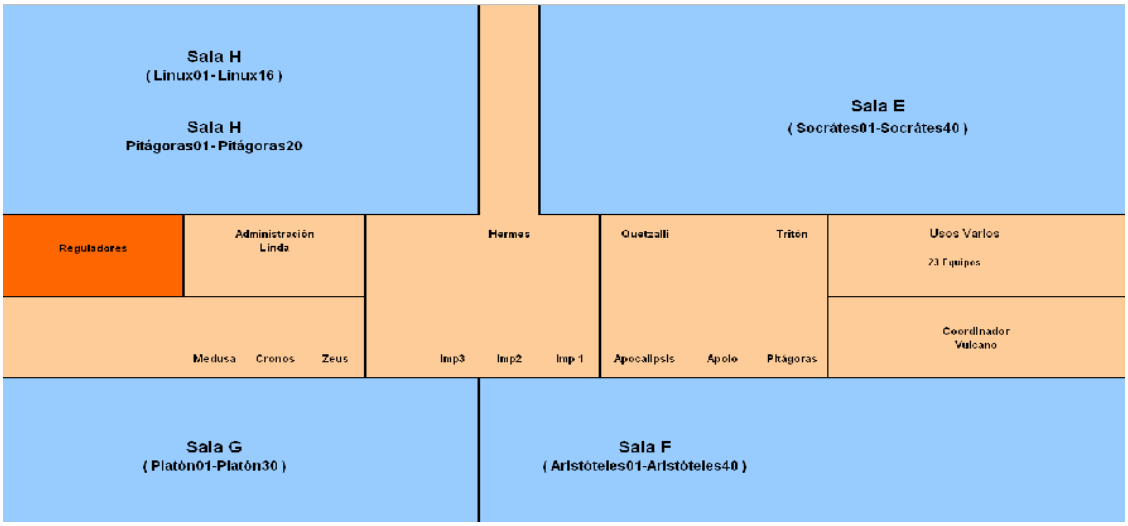


Figura 5.3 Diagrama de Distribución de Clientes (Red)

5.5 Análisis del Software existente.

En el capítulo anterior se hizo énfasis en la parte de software dando como resultado la clasificación del mismo así como la división que debe de haber para tener un mejor control de este dentro de la organización, como se sabe hoy en día existe un infinidad de software "libre" en la Internet que puede llegar a nuestros equipos pero este tipo de software puede ser inestable, en el cual se debe de tener cuidado debido a que puede generar resulta un agujero de seguridad. Dentro del software hay que buscar muchas alternativas con respecto a la funcionalidad del mismo para evitar caer en la tentación de instalar software que sea de dudosa procedencia, un software sin licencia no tendrá la misma funcionalidad ni proporcionará todos los elementos necesarios para su buen funcionamiento.

El tener un buen control del software instalado nos permitirá saber ¿Quién?, ¿Cómo?, ¿Porqué? y ¿Cuándo? tuvo que ser instalado para futuras revisiones e instalaciones de emergencia, así como de recuperación. El especificar el software de trabajo es base para poder llevar acabo el objetivo de la unidad, el demás software será de control administrativo, de servicio y para otras actividades propias de UNICA, pero no hay que olvidar el software de seguridad nos permitirá mantener a nuestro equipo de cómputo protegido contra malware.

En este caso se sabe que el servicio que se proporciona es el uso de equipo de cómputo para los alumnos, al hacer el análisis de la red instalada, la primera sala esta dividida en pequeñas aulas donde están situados los equipos por lo consiguiente, en estos está el software instalado que es requerido por ellos, en los equipos se encuentra instalado 3 tipos de software los cuales son los siguientes:

- Software de Base: Este software comprende, el que es usado por los alumnos como recurso para sus materias, que es de uso educacional.
- Software Administrativo: Este software es el instalado por los administradores de salas el cual es para control del software de base, el sistema operativo o el equipo de cómputo en general.
- Software de Seguridad: Este software es para la protección del equipo de cómputo de posible malware que se pudiera presentar, así como de posible instalación de software malicioso al equipo.

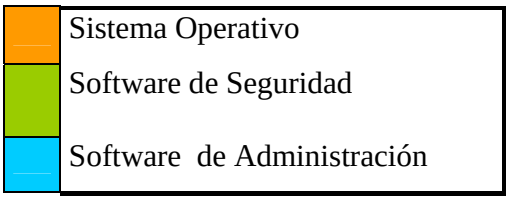
Por sala tenemos la siguiente distribución de software

Sala 2 "Auditorio Sotero Prieto"

Aula A	
Equipo **Software 1 - 5**	**Equipo** **Software 6 -15**
Windows 2000 Profesional 5.0 Service Pack 4	Windows 98 2A. Edición Antivirus AVG 7.0 Free AD-AWARE SE PERSONAL 1.06
Antivirus AVG 7.0 Free AD-AWARE SE PERSONAL 1.06	TweakUI Deep Freezer Win Off Fast RAM 2.6 Cleaner 1.0
Acrobat Readear 7.0.5	Microsoft Office 2000
Microsoft Office 2003	Secure Shell 3.0
Secure Shell 3.0	WinZip 9.0 o Win RAR 3.41
WinZip 9.0 o Win RAR 3.41	Win2PDF
Win2PDF	Java 1.2.4
Java 1.2.4	Navegador Mozilla Fire Fox 1.0.7
Navegador Mozilla Fire Fox 1.0.7	Acrobat Readear 7.0.5
Cleaner 1.0	Start UP
Start UP	Turbo C
Macromedia Flash MX	**Borland C++**
Macromedia Dreamwaever MX	
Macromedia FreeHands MX	
Macromedia FireWorks Visual Basic 6.0	

Tabla 5.6 Distribución de Software

Al hacer un análisis se puede observar que las celdas de color rojo nos muestran el sistema operativo que se tiene instalado en los equipos, las celadas de color verde muestran el software de seguridad, mientras las celdas de color azul muestran el software de administración para los equipos. Las celdas no coloreadas son en este caso el software base o en su defecto el software de trabajo.



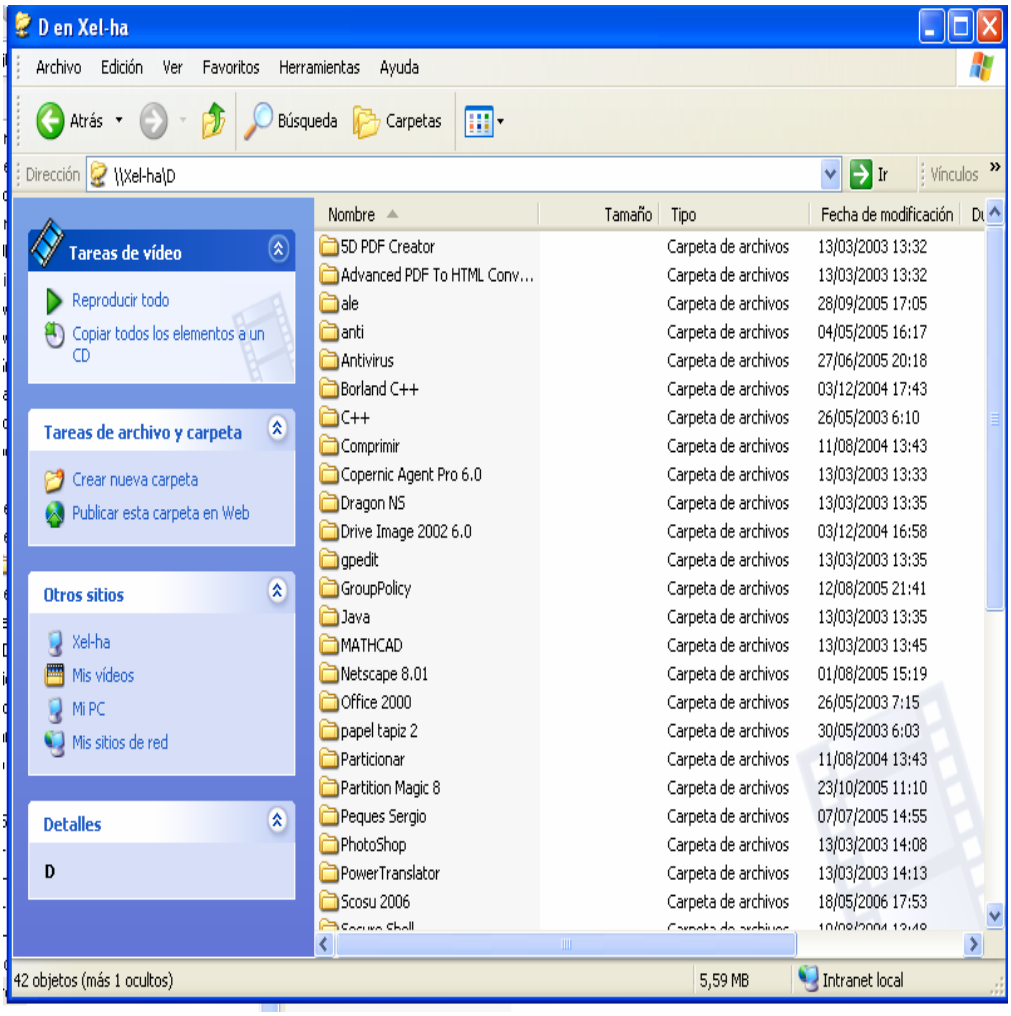
Aula B	Aula C	Aula D
Software	**Software**	**Software**
Windows 2000 Profesional 5.0	Windows 98 2A. Edición	Windows XP Profesional
Service Pack 2		Service Pack 2
Antivirus AVG 7.0 Free AD-AWARE SE PERSONAL 1.06	Antivirus AVG 7.0 Free AD-AWARE SE PERSONAL 1.06	Antivirus AVG 7.0 Free AD-AWARE SE PERSONAL 1.06
Cleaner 1.0 Win Off Deep Freezer Fast RAM 2.6 TweakUI	TweakUI Cleaner 1.0 Deep Freezer Win Off Fast RAM 2.6	Win Off Cleaner 1.0 Fast RAM 2.6 Deep Freezer TweakUI
Microsoft Office 2003	Acrobat Readear 7.0.5	Microsoft Office 2003
Secure Shell 3.0	Microsoft Office 2000	Secure Shell 3.0 WinZip 9.0 o Win RAR 3.41
WinZip 9.0 o Win RAR 3.41	Secure Shell 3.0 WinZip 9.0 o Win RAR 3.41	Win2PDF
Win2PDF	Win2PDF	Java 1.2.4 Navegador Mozilla Fire Fox 1.0.7
Java 1.2.4 Navegador Mozilla Fire Fox 1.0.7	Java 1.2.4 Navegador Internet Explorer 6.0	Acrobat Readear 7.0.5
Start UP	Start UP	Start UP
Acrobat Readear 7.0.5	Turbo C	Visual .NET
Macromedia Flash MX Macromedia Dreamwaever MX	Borland C++	Maple 7.0
Macromedia FreeHands MX		Matlab 5.0
Macromedia FireWorks		Mathematica 4.0
Visual Basic 6.0		Fortran 2000
Ayudas de Visual 5.0		Autocad 2004
		PhotoShop
		SAP 2000

Tabla 5.7 Distribución de Software.

Para el caso de la Sala 2, al hacer un análisis del software en este caso para el área de servidores se puede ver en las siguientes tablas expuestas que cuentan con el software de servidores pero además tienen paquetería que no deben tener, debido a que estos son 2 servidores que solo se encargan del almacenamiento de software y del control de la sala para el mejor manejo de las aulas de la sala 2. Con respecto a los siguientes servidores como se especifico en el análisis de hardware y de red física, su función son de firewalls y de servicios que brinda la sala pera el control de la misma manejadas por el Departamento de Seguridad en Cómputo que existe dentro de la Facultad.

Sala de Servidores (Servidor A) Servidores de control de cuentas y de software	**Sala de Servidores (Servidor B)** Servidores de control de cuentas y de software
Software	**Software**
Windows NT 4.0	Windows 2000 Server 3.0
Service Pack 4	Service Pack 4
Symantec Client Security	Symantec Client Security Avg Antivirus for Server
Oracle	Nero
Hp cd creador	SQL Server 7.0
WinZip 9.0	

Tabla 5.7 Software en servidores



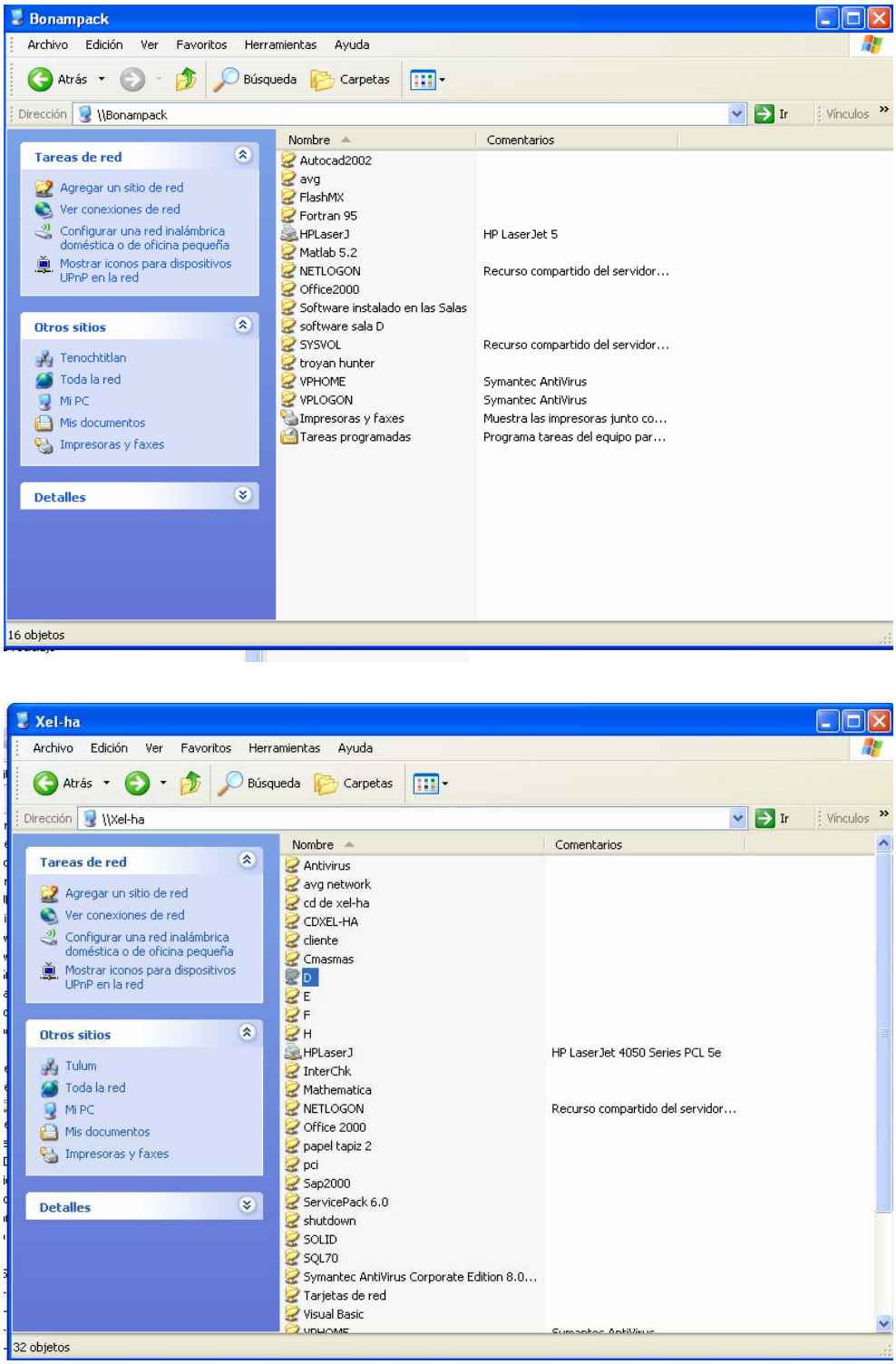


Figura 5.4 Clasificación de software en servidores.

Sala 3 “Planta Baja de la Torre de Ingeniería”

Aula E
Software
Windows 2000 Profesional 5.0
Service Pack 4
Antivirus AVG 7.0 Free
Acrobat Readear 7.0.5
Microsoft Office 2003
Secure Shell 3.0 WinZip 9.0 o Win RAR 3.41
Win2PDF
Java 1.2.4
Autocad 2004
MatLab 6.5

Aula F
Software
Windows 2000 Profesional 5.0
Service Pack 4
Antivirus AVG 7.0 Free
Acrobat Readear 7.0.5
Microsoft Office 2003
Secure Shell 3.0 WinZip 9.0 o Win RAR 3.41
Win2PDF
Java 1.2.4
Macromedia Flash MX Macromedia Dreamweaver MX
Macromedia Freehand 10
Macromedia FireWorks
Visual Basic 6.0
Ayudas de Visual 5.0
Multisim 6.0

Aula G
Software
Windows 2000 Profesional 5.0
Service Pack
Antivirus AVG 7.0 Free
Acrobat Readear 7.0.5
Microsoft Office 2003
Secure Shell 3.0 WinZip 9.0 o Win RAR 3.41
Win2PDF
Java 1.2.4
Autocad 2004
MatLab 6.5

Aula H
Software
Linux Ubuntu
Linux Fedora 4.0
OpenOffice
KWrite
GCC Compilador
Bison Compilador
Mozilla FireFox
TAR
GZip
SecureShell
Windows 98 2A. Edición
Antivirus AVG 7.0 Free AD-AWARE SE PERSONAL 1.06
Cleaner 1.0 Deep Freezer Fast RAM 2.6 Win Off
Microsoft Office 2000
Secure Shell 3.0 WinZip 9.0 o Win RAR 3.41
Win2PDF
Java 1.2.4 Navegador Mozilla Fire Fox 1.0.7
Acrobat Readear 7.0.5
Turbo C
Borland C++

Tabla 5.8 Distribución de Software Sala 3.

Sala de Servidores Servidores de control de cuentas y de software Software
Windows 2003 server 3.0
Service Pack
Symantec Client Security
Nero

Sala de Servidores Servidores de control de cuentas y de software Software
Windows 2003 server 3.0
Service Pack
Symantec Client Security
Nero

Tabla 5.9 Distribución de Software Servidores Sala 3.

La última actualización del archivo de software instalado en las salas es de febrero de 2006, al hacer este tipo de análisis se pudo observar la paquetería que contienen los servidores.

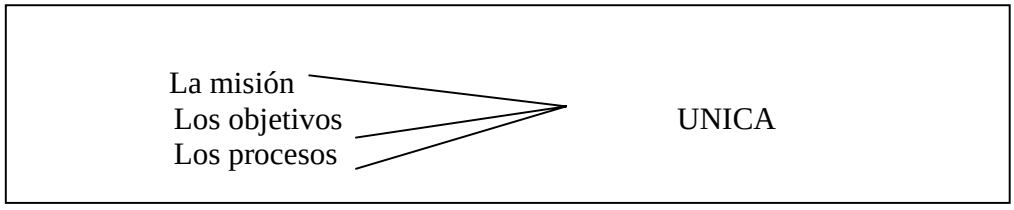
Con respecto a los servidores que en ambos casos para las dos salas, presentan parte de las bases principales de seguridad, cuentan con un antivirus y actualizaciones, pero los permisos sobre carpetas hacia paquetería son muy abiertos a exponerse ante un ataque. Pero este tema será tocado en el siguiente punto con mayor profundidad.

5.6 Definir claramente las vulnerabilidades de la red, software y hardware

Para poder hacer una definición correcta y clara de las vulnerabilidades, debemos conocer antes conceptos importantes que conllevarán a nuestro punto de análisis.

Vulnerabilidad: Debilidad o falla de seguridad.
Indica que el activo es susceptible a recibir un daño a través del aparejamiento con una amenaza.

Riesgo: Probabilidad, posibilidad de que un evento desfavorable ocurra. Tiene un impacto negativo si este se materializa, dicho impacto puede ser sobre:



Una amenaza es una condición del entorno del sistema de información llámese (persona, máquina, suceso o idea), que dada una oportunidad, podría dar lugar a que se genere una violación de la seguridad confidencialidad, integridad, disponibilidad o uso legítimo.

Impacto: Es la materialización de un riesgo.

Control: Es una medida o mecanismo para mitigar un riesgo.
Es un mecanismo establecido para prevenir, detectar y reaccionar ante un evento de seguridad.

Una vulnerabilidad por una amenaza conlleva a un riesgo resumiendo los anteriores conceptos mencionados.

Muy poca gente esta disponible y no se encuentra especializada en el tema, al menos con las bases necesarias para poder hacerle frente a algún problema relacionado con la seguridad. La gente dedicada al rol de la seguridad en la organización o institución debe de estar prevenida ante cualquier ataque, debido a que cualquier atacante sólo necesita una vulnerabilidad para poder explotarla.

El proceso de corrección de vulnerabilidades debe de ser muy restrictivo:

- Disponibilidad de la gente y de los usuarios.
- El tiempo de corrección no sea excesivo.

Un **análisis de vulnerabilidades** será un proceso que nos permitirá identificar, evaluar y reducir los riesgos a un nivel que nos permita implementar un control correcto para mantener ese nivel de riesgo aceptable. Un **análisis de riesgos** tomará el análisis de vulnerabilidades y las amenazas se valdrá de herramientas para poder identificar y evaluar las vulnerabilidades así como las amenazas posibles que conlleven a dichos riesgos para justificar la implementación de dicho control.

Un análisis de riesgos nos dará la base para:

- Estrategia de Seguridad.
- Definir los requerimientos de seguridad y la importancia para la organización o institución.
- Para realizar una campaña de concientización efectiva en seguridad.
- Conocer la inversión requerida para mitigar los riesgos.

Para poder administrar los riesgos se pueden tomar varias alternativas:

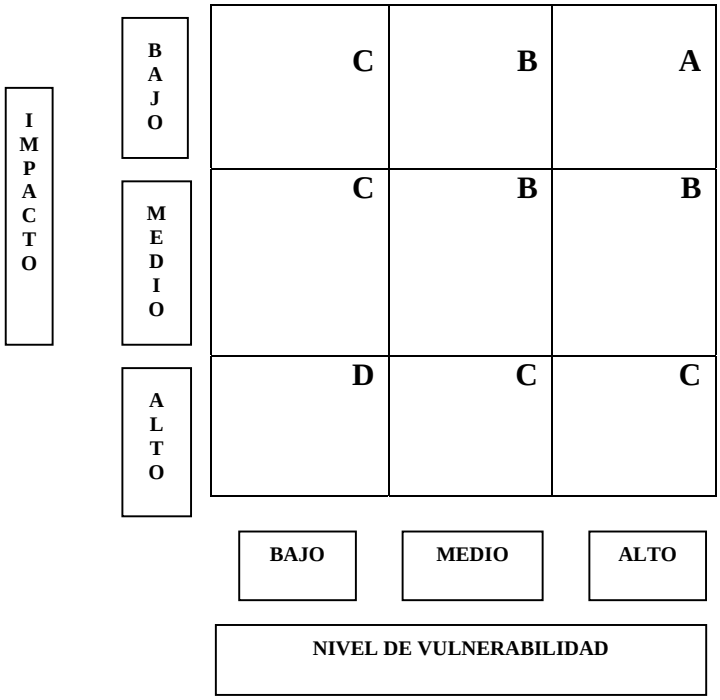
- Tolerarlo.
- Transferirlo.
- Mitigarlo.

Y en algunos casos

- Evitarlo.

Al obtener las vulnerabilidades existentes se tomará un mapa guía que nos proporcionará de manera gráfica el grado de impacto de dichas vulnerabilidades sobre la organización o

institución, esto será el análisis de riesgos que nos proporcionara los siguientes puntos de nuestro diagrama de análisis.



Dentro de este mapa gráfico contamos con secciones definidas por letras las cuales definen las acciones o correcciones a las vulnerabilidades dependiendo del grado de impacto.

Secc.	Estrategia / Acción
A	Deberán ser atendidos de inmediato con acciones correctivas. Deberán ser mitigados de manera preventiva con controles y herramientas.
B	Deberán ser atendidos a la brevedad con acciones correctivas. Deberán ser mitigados de manera preventiva con controles y/o herramientas.
C	Requieren monitoreo Deberán ser mitigados de manera detectiva con controles.
D	No requieren acciones.

Al encontrar las vulnerabilidades deberán ser colocadas dentro de nuestro mapa para poder encontrar las acciones necesarias para mitigarlas de manera adecuada.

Los análisis de vulnerabilidades que se realizaron fueron a la red, software y hardware que en este caso son parte fundamental de nuestro estudio, para poder realizar dichos análisis se buscaron herramientas para poder analizar la red de tal manera que nos pudiera arrojar la información necesaria para poder obtener las vulnerabilidades existentes, las herramientas utilizadas fueron las siguientes:

- Microsoft Baseline Security Analyzer 2.0

Microsoft Baseline Security Analyzer 2.0 (MBSA 2.0) es una herramienta fácil de utilizar que ayuda a las pequeñas y medianas empresas a determinar el estado de la seguridad de la empresa en función de las recomendaciones de seguridad de Microsoft (Figura 5.5), el cual cuenta con guías para corregir los fallos. MBSA permite descubrir errores comunes en la configuración de la seguridad y actualizaciones de seguridad no instaladas en los sistemas.

Funciona bajo plataformas Windows 2000/XP/2003 Server, la instalación es muy sencilla y el entorno es demasiado sencillo, se pueden escanear desde una computadora hasta la red completa, por lo cual resulta demasiado accesible, conociendo con anterioridad el análisis que se realizó a la red se puede observar que el sistema operativo con el que cuenta las computadoras es Windows en sus diferentes versiones, por lo cual es una herramienta muy útil que permitió encontrar los datos necesarios para el análisis de vulnerabilidades.

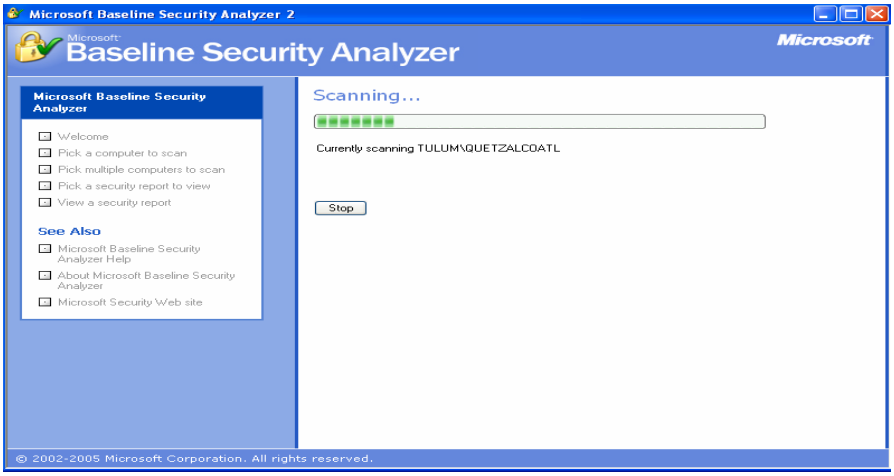


Figura 5.5 Entorno de Microsoft Baseline Security Analyzer 2.0.

- Belarc Advisor 7.1

Genera un completo informe sobre hardware y software. Belarc Advisor (Figura 5.6) es una utilidad que, nada más al instalarse, realiza un análisis a fondo de la computadora, detectando todos los elementos de hardware conectados y las aplicaciones instaladas.

El programa genera un detallado informe con todos estos datos, entre los cuales se encuentra información sobre el sistema operativo, procesador, memoria RAM, unidades de disco locales y en red, impresoras instaladas, placa base, puertos, tarjeta gráfica y todo el software que tiene instalado, de igual manera cuenta con una pequeña sección de seguridad, donde proporciona una amplia información sobre vulnerabilidades que se tenga en dicha computadora. Es una herramienta sencilla de instalar, funciona bajo sistemas Windows2000/XP/2003 Server, el entorno es demasiado sencillo.

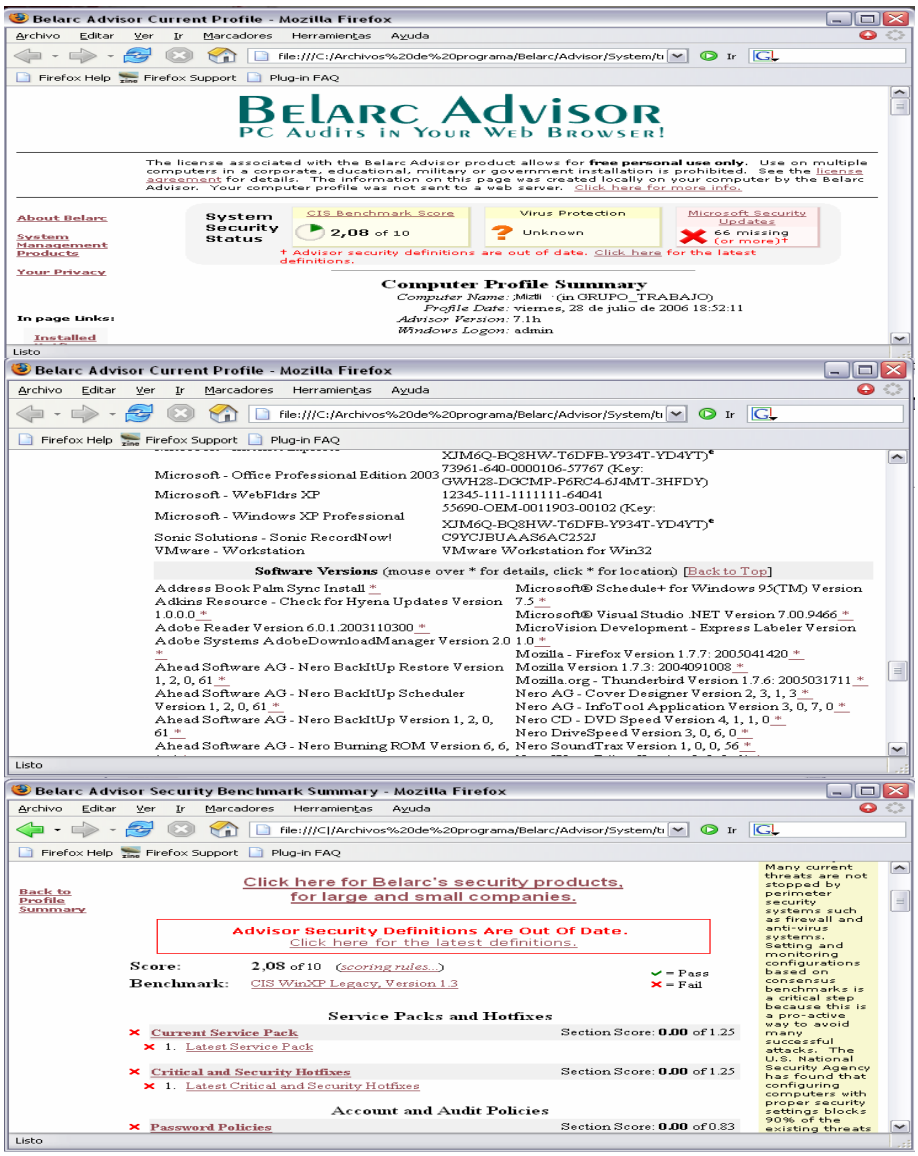


Figura 5.6 Entorno de Belarc Advisor.

- GFI LANguard Network Scanner 7.0

GFI LANguard Network Security Scanner (N.S.S.) analiza la red mediante los métodos potenciales que un hacker podría utilizar para atacarla (Figura 5.7). Mediante el análisis del sistema operativo y de las aplicaciones que se están ejecutando sobre los equipos de red, GFI LANguard N.S.S. identifica todas los posibles brechas de seguridad. En otras palabras, alerta al administrador de las debilidades antes de que un hacker pueda encontrarlas, permitiendo que la organización se ocupe de estos casos antes de que un hacker pueda aprovecharlos.

Esta herramienta es muy sencilla en su instalación además cuenta con una herramienta mas dentro del kit para generar reportes gráficos (GFI LANguard N.S.S. ReportPack) durante el análisis de seguridad. Funciona en plataformas Windows 2000/XP/2003 Server.

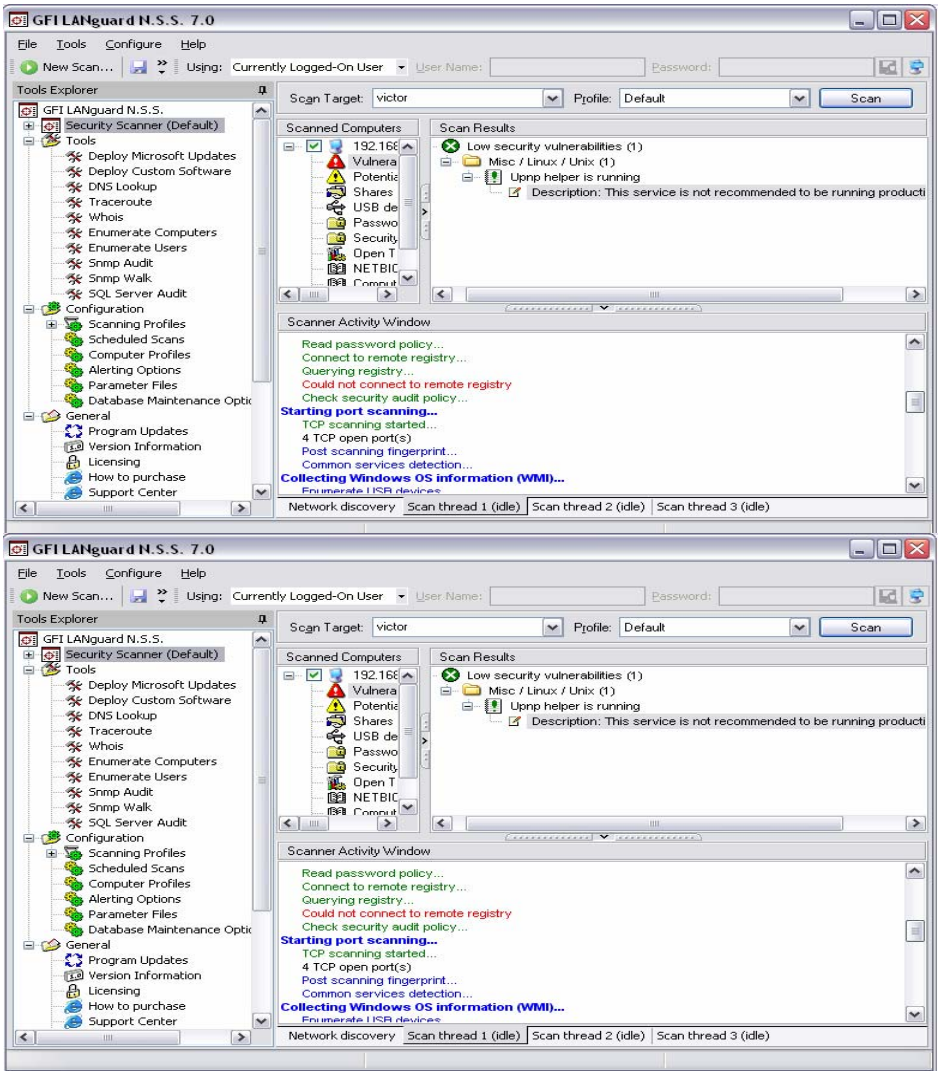


Figura 5.7 Entorno de GFI LANguard Network Scanner 7.0.

Las herramientas se utilizaron en toda la red por lo cual se revisó minuciosamente cada una de las computadoras que la forman haciendo un recuento de todos los resultados que se arrojaron se encontraron las siguientes vulnerabilidades:

5.6.1 Vulnerabilidades de red

Haciendo un resumen general de los resultados que arrojaron las herramientas de seguridad que se emplearon para el análisis de vulnerabilidades se tiene un recuento de las mismas:

1.- Carpetas y archivos compartidos sin permisos seguros sobre grupos o usuarios de la red.
2.- No existen grupos específicos para las cuentas de usuario por cada una de las sub-salas de las dos salas de cómputo.
3.-Existen grupos de cuentas de usuarios que no son utilizados.
4.-Políticas de passwords inexistentes
5.-Malos passwords.
6.-Usuarios con privilegios que pueden perjudicar la integridad del sistema.
7.-Existen cuentas de usuarios sin passwords.
8.-Existen cuentas de usuarios que no son utilizadas y por consiguiente se encuentran habilitadas.
9.-Cuentas de usuarios que ya no se encuentran como personal de la organización activas y no se han dado de baja.
10.-Permisos NTFS no aplicados.
11.-Servicios innecesarios.
12.-Las Actualizaciones en algunas aplicaciones no se encuentran al día.
13.-Existen demasiados puertos abiertos que no son necesarios.
14.-Autologeado de cuentas.
15.- Sin Auditorías establecidas por el sistema operativo
16.-Firewall no activado y en algunos casos no contemplado en el caso de Windows XP el cual cuenta con su mismo firewall.
17.-Protocolos inseguros
18.-Anti-Spyware no instalado en todas las computadoras.
19.-No existe un plan de contingencia.
20.-Instalación del sistema operativo no es segura.
21.-El equipo que se encuentra dedicado al manejo de control de acceso a las salas no cuenta con un manejo apropiado del software, debido a que este cuenta con software que puede provocar una falla de integridad del sistema de acceso, de igual manera el manejo de usuarios y passwords es inseguro.
22.-Existe software instalado que no esta dentro de la relación de software que debe de estar instalado en las salas.
23.-No existe un Programa de Capacitación en Seguridad.

Para el caso de Servidores con los que se cuenta dentro de las salas de cómputo:

1.-No existen todas las actualizaciones necesarias.
2.-Protocolos inseguros establecidos.
3.- Existen cuentas de usuarios que no son utilizadas y por consiguiente se encuentran habilitadas.
4.-Políticas de passwords inexistentes.
5.- No existen grupos específicos para las cuentas de usuario.
6.-Permisos mal estructurados.
7.-Archivos compartidos sin los permisos adecuados de seguridad.
8.-Permisos de usuarios con mayor privilegio contradiciendo el tipo de trabajo que representan.
9.-Antivirus no el más adecuado para dichos servidores.
10.-Servicios innecesarios.
11.-Puertos abiertos.
12.-Unidades de almacenamiento sin los permisos correspondientes.

13-Ninguno de los servidores cuenta con servidores de respaldo.
14.-Las bitácoras no se encuentran al día.
15.-Existen software instalado que es innecesario para el fin del servidor.
16.-Sin firewall.
17.-No existen procedimientos de control, administración segura, implementación, resguardo, instalación y configuración de los servidores.
20.-Instalación del sistema operativo no es segura.

5.6.2 Vulnerabilidades de software

Al hacer el análisis de software existente y al utilizar las herramientas se pudieron encontrar estas vulnerabilidades:

1.-No existe un control del software con el que cuenta las salas de cómputo.
2.-El software almacenado en los servidores no tiene una clasificación correcta.
3.-El software en salas cuenta con permisos para usuarios y grupos inseguros por lo cual un usuario con mínimos privilegios puede acceder a el.
4.-El software con el que se cuenta no tiene un control de administración adecuada.
5.-Las licencias del software que se maneja no se encuentran en su totalidad recopilada y resguardada de manera segura.
6.-No existe un procedimiento de control de instalación de software.
7.-No existe respaldo del software.
8.-El software que se tiene de manera física no se encuentra en un resguardo seguro.

5.6.3 Vulnerabilidades de Hardware

Al realizar un análisis de hardware se encontraron las siguientes vulnerabilidades:

1.-El equipo de cómputo no cuenta con un mantenimiento adecuado.
2.-Existe equipo que requiere de reparación urgente.
3.-El cableado de red no es el adecuado esto puede causar varios accidentes.
4.-El aire acondicionado debe de ser regulado para que trabaje de manera adecuada.
5.-No se tiene un control adecuado de inventariado de equipo.
6.-Existe equipo que se encuentra fuera del lugar de asignación.
7.-No existe una planeación de recuperación de desastres

5.6.4 Estrategia de Seguridad

Si colocamos estas vulnerabilidades encontradas dentro de nuestro mapa realizaríamos la estrategia de seguridad correspondiente al análisis previo, por lo cual se tiene lo siguiente:

Proyectos	Medidas
Politicas de Seguridad Mejor estructuradas	De Inmediato
Politicas de Antivirus	De Inmediato
Politicas de Permisos	De Inmediato
Politicas a Grupos de Usuarios	De Inmediato
Procedimiento de alta de cuentas de usuarios	De Inmediato
Procedimiento para determinar passwords seguros	De inmediato
Procedimiento de baja de cuenta de usuarios	De Inmediato
Procedimiento de verificación de acceso	Corto plazo
Programa de Capacitación en seguridad	Corto Plazo
Administración y control de activos	Mediano Plazo
Procedimiento de instalación, administración y configuración del sistema operativo	Corto Plazo
Administración de Servidores	Corto Plazo
Seguridad organizacional	Corto Plazo
Cumplimiento y verificación de acceso físico y lógico	Corto Plazo
Procedimiento para el análisis de tráfico en la red	Mediano Plazo
Procedimiento de modificación de archivos	Corto Plazo
Procedimiento para el resguardo de copias de seguridad	Corto Plazo
Procedimiento para la verificación de las máquinas de usuarios	Corto Plazo
Procedimiento para el monitoreo de puertos en la red	Mediano Plazo
Procedimiento para dar publicidad a las nuevas normas de seguridad	Corto Plazo
Procedimiento para la determinación de identificación de usuario y grupo de pertenencia por defecto	Corto Plazo
Procedimiento para recuperar información	Corto Plazo
Procedimiento para la Implementación de Actualizaciones	Corto Plazo
Procedimiento de control de instalación de Software	Corto Plazo
Procedimiento para la recuperación en caso de desastres	Largo Plazo

En al tabla anterior se puede observar que la estrategia es llevar acabo los proyectos anteriores que han sido generados a partir del análisis realizado, esto nos da la base para poder realizar las medidas necesarias.

5.7 Definir los Criterios, las Políticas y las Normas de Seguridad a implementar

¿Qué son las políticas, estándares, guías y procedimientos?

- Solucionan el problema de la seguridad de forma estratégica.
- Constituyen la parte fundamental de cualquier programa de seguridad.
- Proveen los lineamientos a los cuales debe apegarse la tecnología, la gente y los procesos actuales y futuros en materia de seguridad.
- Es una fuente de conocimiento para determinar qué herramientas tecnológicas necesitan ser adquiridas para solucionar el problema de la seguridad de forma operativa.

5.7.1 Criterios

Al asumir que la política de seguridad es realmente la apropiada, existen criterios que una metodología de seguridad debe de seguir a medida que se va desarrollando para considerarse en este caso una buena metodología. Por lo tanto, una metodología de seguridad debe:

- **Representar de manera válida y precisa la política de seguridad:** El creador de dicha metodología deberá explicar de manera clara como la metodología corresponde a la política de seguridad y deberá justificar la validez de las correspondencias.
- **Ayudar a entender a través de expresiones enfocadas, exactas y pruebas de propiedades:** Una metodología ayuda a la comprensión tras aclarar conceptos y expresarlos de manera precisa, lo cual enfoca la atención sobre lo esencial.
- **Soportar un análisis de seguridad:** Una metodología debe soportar decisiones sobre seguridad y la pregunta de si existe algún estado de la metodología en donde una propiedad específica de seguridad no se mantiene. Desafortunadamente existe una tensión entre la seguridad y la precisión, si la metodología está restringida de manera que la seguridad puede decidirse, no se representará una política de seguridad demasiado precisa.
- **Soportar la creación y verificación del sistema:** Un sistema basado en una metodología debe ser razonable para constituirse y debe trabajar de manera adecuada.
- **Permitir que los sistemas sean modelados en partes y después unirlas:** Debe ser posible modelar sistemas complejos en partes y después unir estas partes, de esta manera cada parte será más clara y su verificación simple y correcta

5.7.2 Procedimientos

Los procedimientos son manuales escritos que deben ser llevados acabo al pie de la letra, si se desea llegar a una certificación es indispensable tenerlos a la mano en resguardo seguro.

Procedimiento de alta de cuenta de usuarios

Cuando un elemento de la organización requiere una cuenta de operación en el sistema, debe llenar un formulario que contenga, al menos los siguientes datos:

- Nombre y Apellido.
- Actividad dentro de la organización.
- Jefe inmediato superior.
- Descripción de los trabajos que debe realizar en la organización.
- Consentimiento de que sus actividades son susceptibles de ser auditadas en cualquier momento y de que conoce las normas de uso de los recursos, se le proporcionara una copia de las normas establecidas.
- Explicaciones breves, pero claras de cómo elegir su password.

Asimismo, este formulario debe tener otros elementos que conciernen a la parte de ejecución del área encargada de dar de alta la cuenta, datos como:

- Tipo de cuenta.
- Grupo de usuarios al que pertenece.
- Fecha de caducidad.
- Fecha de expiración.
- Datos referentes a los permisos de acceso (por ejemplo, tipos de permisos a los diferentes directorios y/o archivos).
- Si tiene o no restricciones horarias para el uso de algunos recursos y/o para el ingreso al sistema.

Procedimiento de baja de cuenta de usuario

Este procedimiento es el que se lleva a cabo cuando se aleja un elemento de la organización o cuando alguien deja de trabajar por un determinado tiempo. En base a la explicación anterior hay, entonces, dos tipos de alejamientos: permanente y parcial. Aquí, es necesario definir un circuito administrativo a seguir, y que como todos los componentes de la política de seguridad, debe estar fuertemente apoyado por la parte administración de la organización.

Un ejemplo de este circuito, podría ser: ante el alejamiento se debe informar en un formulario de “Alejamiento de personal”:

- Todos los datos del individuo que ha dejado la organización
- Posición que éste ocupaba.
- El tipo de alejamiento (permanente o no).

Una vez llegada la información al departamento encargado de la administración de sistemas, se utiliza para dar de baja o inhabilitar la cuenta del usuario.

La definición de si se da de baja o se inhabilita es algo importante debido a que, si se da de baja:

- Se deberían eliminar los archivos del usuario.
- Eliminar directorios del usuario.

Mientras que si sólo se inhabilita:

- Sólo se guardan.

Si el alejamiento del individuo no era permanente, al volver a la organización, la sección que había informado anteriormente de la ausencia, debe comunicar su regreso, por medio de un formulario dando cuenta de tal hecho para volver a habilitar la cuenta al individuo.

Procedimiento para determinar passwords seguros

Aunque no lo parezca, la verificación de palabras claves efectivas no es algo frecuente en casi ninguna organización. El procedimiento debe explicar las normas para elegir una password:

Se debe explicitar

- La cantidad de caracteres mínimo que debe tener.
- No tiene que tener relación directa con las características del usuario(nombre, fecha de cumpleaños o evento de índole sentimental).
- Debe constar de caracteres alfanuméricos, mayúsculas, minúsculas, números y símbolos de puntuación.
- Determinar, si es posible, el seguimiento de las palabras claves (llevar registros de las palabras claves anteriores elegidas por el usuario).

Una vez que el usuario ha elegido su password, se le debe correr un “programa crackeador” para tener idea de cuán segura es, en base al tiempo que tarda en romper la palabra.

Procedimientos de verificación de accesos

Debe explicar la forma de realizar las auditorías de los archivos logísticos de ingresos a fin de detectar actividades anómalas. También debe detectar el tiempo entre la auditoría y cómo actuar en caso de detectar desviaciones.

Normalmente, este trabajo es realizado por programas a los que se les dan normativas de qué y cómo comparar. Escanean archivos de “.log” con diferentes fechas tomando en cuenta las reglas que se le han dado. Ante la detección de un desvío, generan reportes informando el mismo. En el procedimiento debe quedar perfectamente indicado quién es el responsable del mantenimiento de estos programas y cómo se actúa cuando se generan alarmas.

Procedimiento para el análisis de tráfico en la red

Permite conocer el comportamiento del tráfico en la red, al detectar variaciones que pueden ser síntoma de mal uso de la misma. El procedimiento debe indicar el/los programas que se ejecuten, con qué intervalos, con qué reglas de trabajo, quién se encarga de procesar y/o monitorear los datos generados por ellos y cómo se actúa en consecuencia.

Procedimiento de modificación de archivos

Este procedimiento sirve para detectar la modificación no autorizada y la integridad de los archivos, en muchos casos, permite la traza de las modificaciones realizadas. Al igual que en los casos anteriores, debe estar bien determinada la responsabilidad de quién es el encargado del seguimiento y de actuar en caso de alarmas.

Procedimientos para el resguardo de copias de seguridad

Este procedimiento debe indicar claramente dónde se deben guardar las copias de seguridad y los pasos a seguir en caso de problemas. Para lograr esto, deben estar identificados los roles de las personas que interactúan con el área, a fin de que cada uno sepa qué hacer ante la aparición de problemas.

Procedimientos para la verificación de las máquinas de los usuarios

Este procedimiento permitirá encontrar programas que no deberían estar en las máquinas de los usuarios y que, por su carácter, pueden traer problemas de licencias y fuente potencial de virus. El procedimiento debe explicitar los métodos que se van a utilizar para la verificación, las acciones ante los desvíos y quién/quiénes lo llevarán a cabo.

Procedimientos para el monitoreo de los puertos en la red

Este procedimiento permite saber qué puertos están habilitados en la red, y, en algunos casos, chequear la seguridad de los mismos. El procedimiento deberá describir qué programas se deben ejecutar, con qué reglas, quién estará a cargo de llevarlo a cabo y qué hacer ante las desviaciones detectadas.

Procedimientos para dar publicidad a las nuevas normas de seguridad

Este tipo de procedimiento no siempre es tenido en cuenta. Sin embargo, en una organización es muy importante conocer las últimas modificaciones realizadas a los procedimientos, de tal manera que nadie pueda poner cómo excusa “que no conocía las modificaciones”. En él, debe describirse la forma de realizar la publicidad de las modificaciones: puede ser mediante un mailing, por exposición en transparencias, por notificación expresa, etc.; quién estará a cargo de la tarea y las atribuciones que tiene. Es fundamental tener en cuenta este último punto ya que un porcentaje de los problemas de seguridad, según está demostrado en estudios de mercado, proviene del desconocimiento de las normas y/o modificaciones a ellas por parte de los usuarios.

Procedimientos para la determinación de identificación de usuario y grupo de pertenencia por defecto

Este procedimiento determina la forma de establecer las identificaciones y los grupos a los que pertenecerán los usuarios por defecto en el momento de darlos de alta. En él deben explicarse, concisamente, los pasos a seguir para cambiar los derechos y las identificaciones de los usuarios dados de alta y la manera de documentar los mismos, así también como quién será responsable de la tarea.

Procedimientos para recuperar información

Este procedimiento sirve para reconstruir todo el sistema o parte de él, a partir de las copias de seguridad. En él, deben explicarse todos los pasos a seguir para rearmar el sistema a partir de los back-up existentes, así como cada cuánto tiempo habría que llevarlos a cabo y quiénes son los responsables de dicha tarea.

Procedimiento de instalación, administración y configuración del sistema operativo

Este procedimiento consta para realizar una instalación segura desde el momento en que se inserta el disco de instalación, los pasos que conllevarán a este, así como la administración que debe ser llevada por algún responsable, la configuración del mismo tomando en cuenta las normas previamente establecidas.

Procedimiento para la recuperación en caso de desastres

Este procedimiento es uno de los que debe de llevar un mayor cuidado y tiempo debido a que hablamos del después de que exista algún desastre se debe tener en cuenta a todos los miembros de la organización, planes de continuidad, adiestramiento en caso de contingencia, capacitación para el uso de extintores y otros elementos, etc.

5.7.3 Políticas

Una **política de seguridad** es una forma de comunicarse con los usuarios y la gente que forma parte de una organización o institución. Las políticas de seguridad establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes en la organización

La política de seguridad debe reflejar fielmente el mundo real, significa que debe de ser especificada sin ambigüedades, las politicas seleccionadas deben de ser hechas sobre la situación actual en la que se encuentra la red. Una política de seguridad debe de estar especificada en un documento especial para tal propósito redactada en un lenguaje natural, claramente y sin ambigüedades posibles. El documento deberá especificar que propiedades de seguridad se pretenden cubrir con la aplicación de las políticas y la manera de usarlas.

Estas politicas deberán estar contenidas dentro de un documento el cual deberá tener un formato estricto, el cual será proporcionado por el jefe inmediato, los elementos mínimos deberán tener en la portada, el titulo, referencia a, fecha de creación, persona o personas que intervinieron en

la realización, nombre de los jefes inmediatos encargado de dicha área, entre otros elementos que la directiva considere.

Políticas de alta de cuentas de usuarios

1.-Las políticas sobre cuentas serán realizadas y especificadas por el área encargada de la seguridad.
2.-El encargado del área deberá informar sobre las políticas implementadas al jefe inmediato.
3.- Sólo el administrador del servidor dará de alta las cuentas de usuario tanto en el servidor, como en los equipos de cómputo que sean para la administración de las Salas de Cómputo.
4.-Al dar de alta una cuenta se deberá contar con el siguiente formato:

- Nombre y Apellidos.
- Actividad dentro de la organización.
- Jefe inmediato superior.
- Descripción de los trabajos que debe realizar en la Sala de Cómputo.

5.-Informar a los usuarios cuales son sus actividades son susceptibles de ser auditadas en cualquier momento y de que conoce las normas de uso de los recursos, se le deberá de proporcionar una copia de las normas establecidas.
6.- Explicar a los usuarios de manera breve, pero claras de cómo elegir su password.
7.- Al dar de alta la cuenta se especificaran, datos como:

- Tipo de cuenta.
- Grupo de usuarios al que pertenece.
- Fecha de caducidad.
- Fecha de expiración.
- Datos referentes a los permisos de acceso (por ejemplo, tipos de permisos a los diferentes directorios y/o archivos).
- Si tiene o no restricciones horarias para el uso de algunos recursos y/o para el ingreso al sistema.

8.- Los usuarios deberán respetar las políticas, en dado caso de no cumplirlas, se les aplicará una sanción administrativa.

Políticas de Passwords

A nivel local, grupo y dominio:

1.-La longitud mínima para un password será de 8 caracteres.
2.-El password no deberá tener relación directa con las características del usuario (nombre, fecha de cumpleaños o evento de índole sentimental).
3.-Debe constar de caracteres alfanuméricos, mayúsculas, minúsculas, números y símbolos de puntuación.
4.-El periodo mínimo de vigencia adecuada será de 7 días.
5.-El periodo máximo de vigencia adecuada será de 30 días.

6.-Se habilitara la Directiva de Contraseñas de la Configuración de seguridad local (Figura 5.9) para cada uno de los equipos de cómputo a nivel local y grupo, configurando los siguientes puntos:

- Forzar el historial de contraseñas a 6 contraseñas a almacenar.
- Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio deshabilitada.
- La contraseña debe de cumplir los requerimientos de complejidad habilitada.
- Longitud mínima de la contraseña 8 caracteres.
- Vigencia mínima de la contraseña 7 días.
- Vigencia máxima de la contraseña 42 días.

7.-El password es confidencial por lo cual el usuario no deberá proporcionarlo, ni deberá tenerlo a la vista.
8.-En caso de violación a lo antes establecido se aplicará una sanción de falta administrativa.

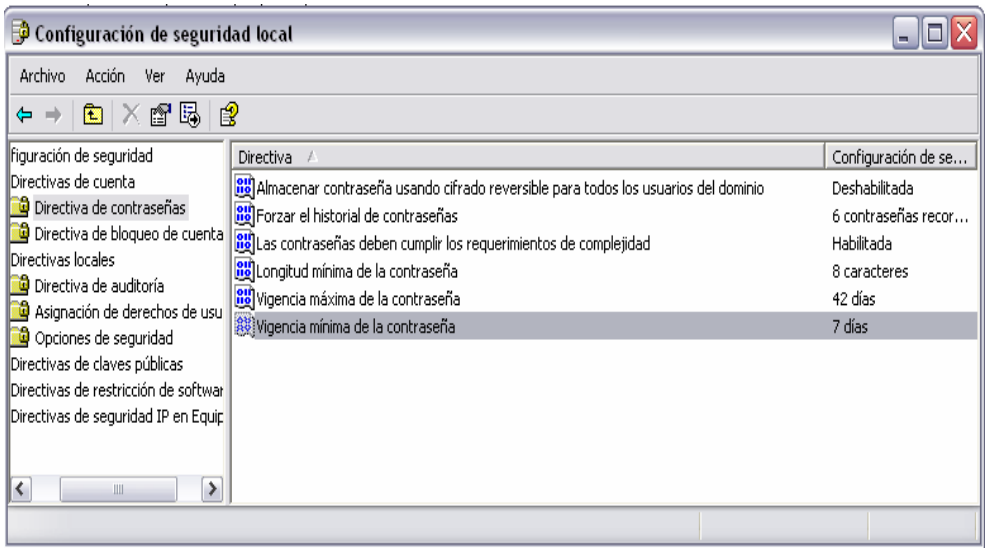


Figura 5.9 Configuración de seguridad local

Sobre servidores, a nivel dominio, local y grupo:

9.-Las políticas antes mencionadas excepto la política 6, y agregando la política 10.
10.-Se habilitará la Directiva de Contraseñas de la Configuración de seguridad local (Figura 5.10) para cada uno de los servidores a nivel local, grupo y dominio, configurando los siguientes puntos:

- Forzar el historial de contraseñas a 24 contraseñas a almacenar.
- Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio deshabilitada.
- La contraseña debe de cumplir los requerimientos de complejidad habilitada.
- Longitud mínima de la contraseña 8 caracteres.

- Vigencia mínima de la contraseña 2 días.
- Vigencia máxima de la contraseña 42 días.

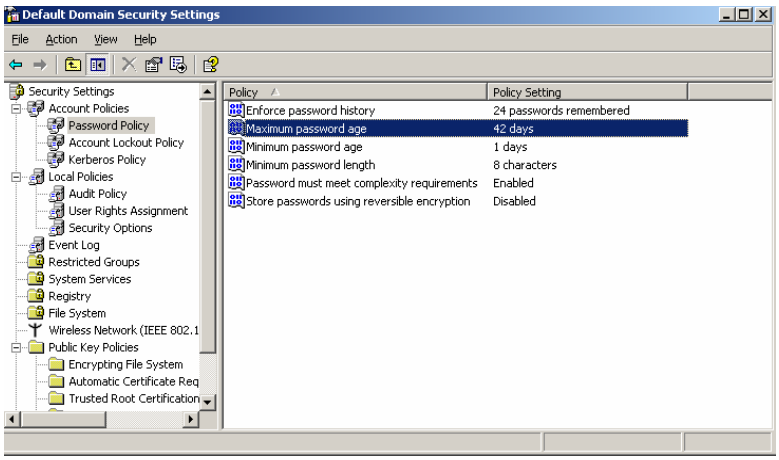


Figura 5.10 Directiva de políticas de password.

Políticas Bloqueo de Cuentas

A nivel local y dominio:

1.-La duración de bloqueo de cuentas será de 15 minutos.
2.-El umbral de bloqueo de cuentas será de 10 intentos.
3.-Restablecer el contador del bloqueo de las cuentas después de 15 minutos a nivel local y en servidores a nivel dominio dejar la situación hasta que el administrador lo desbloquee.

Políticas Auditoría

A nivel local y dominio:

1.- Configuración de políticas de auditoría (Figura 5.11) en los equipos de cómputo y servidores con las siguientes políticas.
2.-Auditar los sucesos de inicio de sesión de cuenta éxito y falla.
3.-Administración de la cuenta de auditoría éxito y falla.
4.-Auditar el acceso al servicio de directorio éxito y falla.
5.-Auditar sucesos de inicio de sesión.
6.-Auditar el acceso a objetos.
7.-Auditar el cambio de políticas éxito.
8.-Auditar el uso de privilegios éxito y falla.
9.-Auditar el seguimiento de los procesos sin auditoría.
10-Auditar los sucesos del sistema éxito.

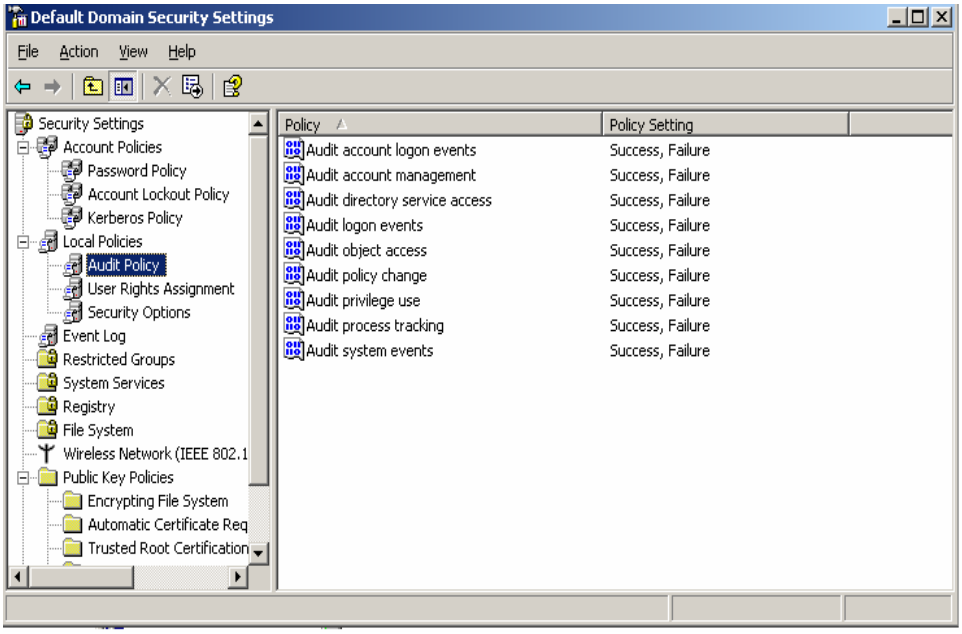


Figura 5.11 Políticas de Auditoría.

Políticas sobre cuentas de usuarios en los equipos de las Aulas de las Salas de Cómputo 2 y 3

1.-Implementar las políticas sobre alta de cuenta.
2.-Implementar las políticas sobre passwords.
3.-Implementar las políticas sobre bloqueos.
4.-Implementar las políticas sobre auditoría.
5.-Los equipos solo deberán contar con 4 cuentas de usuarios locales:

- Cuenta de Administrador: La cual no deberá tener por defecto este nombre.
- Cuenta de Usuario: Nombre del Equipo.
- Cuenta de Usuario: Servicio Social y Alumnos Cursos.
- Cuenta de Usuario: De Seguridad.

6.-Será deshabilitada la cuenta del Administrador y creada otra, la cual tendrá por defecto un nombre distinto, por seguridad.
7.-Serán deshabilitadas las demás cuentas de usuarios locales de los equipos de cómputo.

Políticas sobre grupos de usuarios en los equipos de las Aulas de las Salas de Cómputo 2 y 3

1.-Sólo serán 5 grupos locales:

- Administradores.

- Usuarios Avanzados.
- Usuarios.
- Operadores de Configuración de Red.
- Operadores de Copia.

2.- En el grupo de Administradores estarán:

- Usuario Administrador del equipo.
- Usuario de Seguridad.

3. En el grupo de Usuarios avanzados

- Usuario Servicio Social y Alumnos de cursos.

4.-En el grupo de Usuarios

- Usuario Nombre del Equipo.

5.-En el grupo de Operadores de Copia y Configuración de Red

- Usuario Administrador del equipo.

6.- Los demás grupos deberán ser eliminados.

Políticas sobre permisos de usuarios y grupos en los equipos de las Aulas de las Salas de Cómputo 2 y 3

1.-Permisos sobre grupos:

- Administradores: Control total.
- Usuarios Avanzados: Lectura, ejecución y escritura sobre archivos específicos, este último contenido en permisos especiales.
- Usuarios: Lectura y ejecución de cierto software permitido.
- Operadores de Configuración de Red: Lectura y ejecución a nivel configuración red.
- Operadores de Copía: Lectura y ejecución a nivel copias de seguridad.

2.- Permisos sobre usuarios, los cuales serán según lo estipulado bajo los grupos y controles antes establecidos:

- Cuenta de Administrador: La cual no deberá tener por defecto este nombre, es el encargado de la administración de los recursos del equipo de cómputo.
- Cuenta de Usuario Nombre del Equipo: Es el usuario alumno.
- Cuenta de Usuario Servicio Social y Alumnos Cursos: Como lo indica usuario servicio social y alumnos de cursos.
- Cuenta de Usuario de Seguridad: Implementador de las políticas, medidas, software y seguridad sobre equipos de cómputo.

Políticas sobre cuentas de usuarios en los equipos del Área de Administración de la Sala de Cómputo 2 y 3

1.-Implementar las políticas sobre alta de cuenta.
2.-Implementar las políticas sobre passwords.
3.-Implementar las políticas sobre bloqueos.
4.-Implementar las políticas sobre auditoría.
5.-Los equipos solo deberán contar con 3 cuentas de usuarios locales:

- Cuenta de Administrador: La cual no deberá tener por defecto este nombre, este usuario es el usuario Administrador de Aula de las Salas de Cómputo.
- Cuenta de Usuario Servicio Social.
- Cuenta de Usuario de Seguridad.

6.-Para el caso Coordinadores de la Sala sólo estará 1 cuenta.

- Cuenta de Administrador: La cual no deberá tener por defecto este nombre.

7.-Será deshabilitada la cuenta del Administrador y creada otra la cual tendrá por defecto un nombre distinto, por seguridad.
8.-Serán deshabilitadas las demás cuentas de usuarios locales del equipo de Computó.

Políticas sobre grupos de usuarios en los equipos del Área de Administración de las Salas de Cómputo 2 y 3

1.-Sólo serán 4 grupos locales:

- Administradores.
- Usuarios Avanzados.
- Operadores de Configuración de Red.
- Operadores de Copía.

2.- En el grupo de Administradores estarán:

- Usuario Administrador del equipo.
- Usuario de Seguridad.

3. En el grupo de Usuarios avanzados

- Usuario Servicio Social.

5.-En el grupo de Operadores de Copia y Configuración de Red

- Usuario de Seguridad.

6.- Los demás grupos deberán ser eliminados.

Políticas sobre permisos de usuarios y grupos en los equipos del Área de la Administración Salas de Cómputo 2 y 3

1.-Permisos sobre grupos:

- Administradores: Control total.
- Usuarios Avanzados: Lectura, ejecución y escritura sobre archivos específicos, este ultimo contenido en permisos especiales.
- Operadores de Configuración de Red: Lectura y ejecución a nivel configuración red.
- Operadores de Copía: Lectura y ejecución a nivel copias de seguridad.

2.- Permisos sobre usuarios, los cuales serán según lo estipulado bajo los grupos y controles antes establecidos:

- Cuenta de Administrador.
- Cuenta de Usuario Servicio Social: Como lo indica usuario servicio social.
- Cuenta de Usuario de Seguridad: Implementador de las políticas, medidas, software y seguridad sobre equipos de cómputo.

Políticas sobre cuentas de usuarios en los Servidores del Área de Administración de la Sala de Cómputo 2 y 3

1.-Implementar las políticas sobre alta de cuenta.
2.-Implementar las políticas sobre passwords.
3.-Implementar las políticas sobre bloqueos.
4.-Implementar las políticas sobre auditoría.
5.-El servidor solo deberá contar con las siguientes cuentas de usuarios locales:

- Cuenta de Administrador: La cual no deberá tener por defecto este nombre, este usuario es el usuario Administrador del servidor.
- Cuenta de Usuario de Seguridad.
- Cuenta Coordinador de Sala de Cómputo.

6.-El servidor solo deberá contar con las siguientes cuentas de usuarios de Dominio:

- Cuentas de Equipos de Cómputo.
- Cuentas de Nombres de Equipo de Cómputo.
- Cuentas de Administrador Aula Sala de Cómputo.
- Cuentas de Servicio Social.

7.-Será deshabilitada la cuenta del Administrador y creada otra cuenta.
8.-Serán deshabilitadas las demás cuentas de usuarios locales del equipo de Computó.

Políticas sobre grupos de usuarios en los Servidores del Área de Administración de las Salas de Cómputo 2 y 3

1.-Serán los grupos estipulados en el Active directory a nivel local (Figura 5.12).

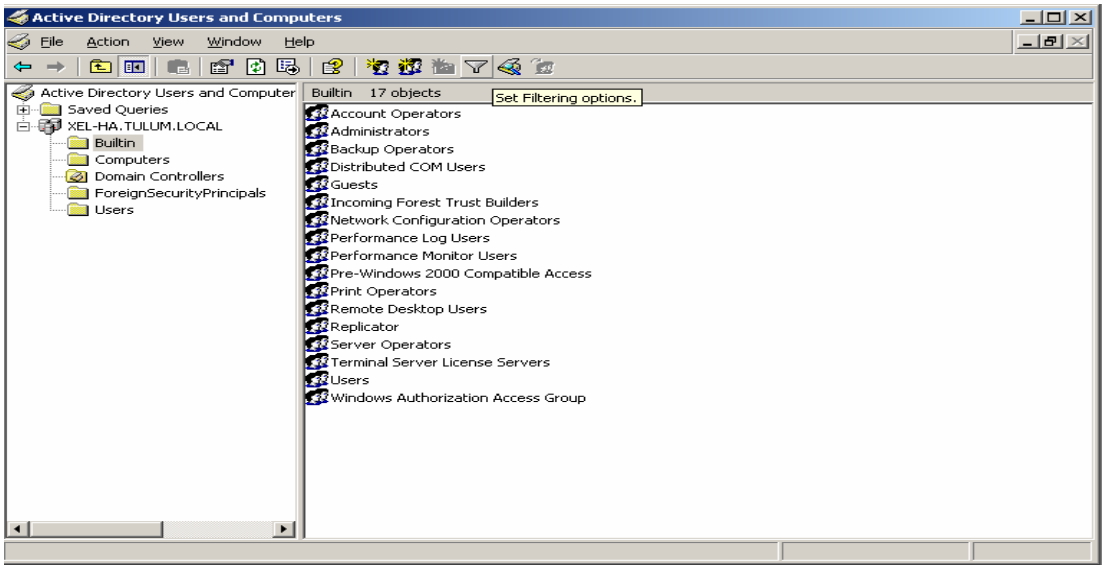


Figura 5.12 Grupos Locales del Servidor.

2.- Los usuarios locales deberán estar contenidos en todos los grupos:
3.-Los grupos de Dominio serán:

- Administradores: Contenidos los usuarios locales.
- Administradores de Dominio: Solo el administrador del servidor.
- Administrador de DNS: Solo administrador del servidor.
- Computadora de Dominio: Todos los equipos de cómputo.
- Controladores de Dominio: Solo administrador del servidor.
- Usuarios de Dominio: Servicio social, computadoras y cuentas de nombres de computadoras.
- Administradores de Aulas de la Sala de Cómputo: Solo Administradores de Aulas.
- Grupo Aula Nombre: En este estarán contenidos los equipos de cómputo y los nombres de los mismos de cada una de las aulas.

Políticas sobre permisos de usuarios y grupos en los Servidores del Área de la Administración Salas de Cómputo 2 y 3

1.-Permisos sobre grupos de dominio:

- Administradores: Control total.
- Administradores de Dominio: Control total.
- Administrador de DNS: Control Total.
- Computadora de Dominio: Lectura y ejecución.

- Controladores de Dominio: Control Total.
- Usuarios de Dominio: Lectura y ejecución en el caso de los equipos dentro del área de administración de Salas de Cómputo.
- Administradores de Aulas de la Sala de Cómputo: Lectura, ejecución y escritura en ciertas carpetas y archivos, permisos especiales.
- Grupo Aula Nombre: Lectura y ejecución.

2.- Permisos sobre usuarios, los cuales serán según lo estipulado bajo los grupos y controles antes establecidos.
3.- Permisos sobre Usuarios Locales control total.

Políticas sobre permisos ejecución de software en los Servidores del Área de la Administración Salas de Cómputo 2 y 3

1.- El software será implementado de acuerdo a las necesidades de la sala.
2.-Los permisos serán de acuerdo a las políticas de usuarios y grupo en los servidores.
3.-Se deberá contar con un formato donde se especificará lo siguiente:

- Nombre del software.
- Tipo de Software.
- Quien lo solicita.
- Fecha de permiso.
- Nombre del jefe inmediato que autorizó.
- Fecha de la instalación.

4.-El software será dividido en cuatro grupos:

- Software de Trabajo: Los grupos contenidos serán:

    - Administradores: Control total.
    - Administradores de Dominio: Control total.
    - Administrador de DNS: Control Total.
    - Computadora de Dominio: Lectura y ejecución.
    - Controladores de Dominio: Control Total.
    - Usuarios de Dominio: Lectura y ejecución en el caso de los equipos dentro del área de administración de Salas de Cómputo.
    - Administradores de Aulas de la Sala de Cómputo: Lectura, ejecución y escritura en ciertas carpetas y archivos, permisos especiales.
    - Grupo Aula Nombre: Lectura y ejecución.

- Software Administración: Los grupos contenidos serán:

    - Administradores: Control total.
    - Administradores de Dominio: Control total.

- Administradores de Aulas de la Sala de Cómputo: Lectura, ejecución y escritura en ciertas carpetas y archivos, permisos especiales.

- Software para uso del personal que labora en las salas de cómputo:

  - Administradores: Control total.
  - Administradores de Dominio: Control total.
  - Administrador de DNS: Control Total.
  - Computadora de Dominio: Lectura y ejecución.
  - Controladores de Dominio: Control Total.
  - Usuarios de Dominio: En el caso de los equipos dentro del área de administración de Salas de Cómputo.
  - Administradores de Aulas de la Sala de Cómputo: Lectura, ejecución y escritura en ciertas carpetas y archivos, permisos especiales.

- Software aplicativo.

  - Administradores: Control total.

5.- Al llegar un software nuevo deberá ser inventariado.

Políticas de Acceso

1.-Los Miembros de la Sala de Cómputo deberán portar su gafete.
2.-El personal que pertenezca a la UNICA podrá ingresar al área administrativa.
3.-Los administradores de los servidores y administradores de seguridad podrán ingresar al área de servidores.
4.-Los administradores de los servidores y administradores de seguridad podrán utilizar los servidores.
5.-El equipo que se encuentra en el área administrativa será usado por el personal asignado a cada uno de los equipos.
6.-El uso de equipo de cómputo para los alumnos cuenta con su propio reglamento establecido, este deberá ser llevado acabo.
7.-Las faltas a cualquiera de los puntos establecidos conllevara a una falta administrativa.

CAPÍTULO 6

IMPLEMENTACIÓN DE LA SEGURIDAD

6.1 Administración de servidores

La administración de servidores es un punto importante dentro de la seguridad informática, debido a que estos nos brindaran aplicaciones y servicios por lo cual deben proporcionar la confiabilidad de que los servicios estarán disponibles aunque se produzca un error en el sistema o independientemente del tamaño de las aplicaciones que se lleven acabo, deben estar disponibles en el momento que se les requiera, de esta manera se puede observar que son elementos de alta vulnerabilidad si no se tiene una adecuada administración. La administración de servidores es un tema que abarcaría un seguimiento completo y muy detallado, dentro de nuestro tema implementado el punto el cual abarcaremos será en el aspecto de seguridad, sin dejar por un lado toda la parte que engloba la administración.

Dentro de la administración de un servidor se le debe de dar un seguimiento fundamentalmente a la seguridad del mismo, como se menciono con anterioridad dentro de la administración se hizo un enfoque directo a la administración segura de un servidor tema que se ha estado desarrollando.

Para la administración de un servidor se deben de considerar los siguientes puntos:

1. -Elección adecuado del sistema operativo.
2. -Documentación acerca del sistema operativo seleccionado.
3. -Verificación del sistema operativo que se desea implementar.

    ¿Es el adecuado?
    ¿Cumple con lo que requiere la organización?
    ¿Se cuenta con los elementos necesarios para la implementación del mismo, así como de la administración?
    ¿Ventajas y Desventajas del mismo?
    ¿El costo?
    ¿Las Licencias?

4. -Requisitos necesarios para su implementación.
5. -Generar el procedimiento para su instalación.

    - Instalación segura desde el inicio: Creación de un cd booteable o srranque del Sistema que cuente con el Service Pack màs actualizado para dicho sistema operativo.
    - Contar con una copia de seguridad del mismo.

6. -Realizar una bitácora de la instalación.
7. -Implementar las actualizaciones necesarias, previamente deberán ser obtenidas con anterioridad.
8. -Implementar el antivirus adecuado y de igual manera realizar las configuraciones pertinentes.
9. -Implementación del Firewall adecuado con las configuraciones pertinentes.
10. -Configuración del servidor: En este punto es preguntar qué función va ha realizar cuáles son los servicios que va a ofrecer.

- Servidor DHCP
- Servidor como controlador de Dominio
- O ambos.

11. -Realizar un procedimiento detallado de cómo se llevará acabo la configuración del servidor.
12. -Generación de bitácora de configuración del servidor.
13. -Implementación del Active Directory.
14. -Realizar un procedimiento detallado de la implementación del Active Directory.
El cual deberá de llevar los siguientes puntos:

- Creación de unidades organizativas y grupos.
- Equipos.
- Dominios y confianzas.
- Sitios y servicios.
- Consola de administración de directivas de grupo (GPMC).

15.-Dentro de este mismo procedimiento se deberán llevar los siguientes puntos acabo:

- Políticas de dominio.
- Políticas de cuenta.
- Políticas de contraseña.
- Política de bloqueo de cuentas.
- Asignación de permisos.
- Políticas de auditoría.

16.-Implementación de los servicios que vá a proporcionar el servidor.
17.-Para cada servicio se llevará acabo un procedimiento.
18.-Fortalecimiento de los distintos servicios, implementando la seguridad adecuada.
19.-Bitácora de los servicios implementados.
20.-Administración de discos duros.
21.-Administración de almacenamiento de datos.
22.-Administración de software.
23.-Administración de recuperación.
24.-Política de auditoría.
25.-Implementación de herramientas de seguridad.
26.-Escaneo y bloqueo de puertos.
27.-Escaneo del servidor.
28.-Políticas de respaldo.
29.-Modificaciones y configuraciones adicionales.

Para nuestro caso se tomarán a consideración los puntos para administrar servidores Windows, por lo cual la parte de seguridad se enfoco en este punto exactamente; por lo cual al realizar el análisis se optó por tener un servidor Windows 2003 Server en su versión Enterprise Edition, así, se dará una explicación de por qué esta versión.

De acuerdo al análisis para la implementación de medidas de seguridad, y después de analizar los requerimientos y necesidades de la Sala de Cómputo de UNICA (Problemática a resolver en cuestión de seguridad), se decidió utilizar Windows 2003 Server Enterprise Edition, ya que debido a los servicios que presta a la comunidad de la Facultad de Ingeniería, y sus funciones operativas internas, es el más adecuado dado que se tienen experiencia en el manejo administrativo con Windows Server en versiones anteriores, de igual manera proporciona estabilidad y las herramientas necesarias, para su manejo.

Esto no quiere decir que los otros sistemas operativos no se adecuen a las necesidades que se requieren, siendo así que se cuenta con dos servidores Linux Open BSD para reforzar algunos servicios.

Además los equipos con los que se cuenta soportan sin problema este tipo de sistema operativo (Windows 2003 Server Enterprise Edition). Y contestando de manera general a las preguntas realizadas anteriormente con respecto a la elección del sistema operativo se tiene lo siguiente:

- La instalación es fácil y sencilla y se puede realizar de manera segura desde el principio.
- Se cuenta con las actualizaciones en línea o CD.
- Permite ejecutar aplicaciones tales como sistemas de red, de mensajería, de inventario y de servicio de atención al cliente, bases de datos, sitios Web de comercio electrónico y servidores de archivos e impresión.
- Confiabilidad y escalabilidad.
- Protege las redes ante un posible código malintencionado.
- Seguridad funcional.
- Realización de bitácoras de manera sencilla.
- Herramientas importantes de administración automática, incluyendo los servicios de actualización de software (WSUS) de Microsoft Windows y los asistentes de configuración de servidores para facilitar la automatización de la implementación.
- Permite la instalación y configuración de Firewall de una manera sencilla.
- En cualquier punto de la instalación o funcionamiento se pueden agregar servicios o funciones.
- Active Directory es más rápido y robusto.
- La administración de directivas de grupo es más sencilla con la nueva Consola de administración de directivas de grupo (GPMC), permite una mejor utilización del Active Directory dando como función un ahorro de costos mayores. Además, las herramientas de línea de comandos permiten que los administradores realicen la mayoría de las tareas desde la consola de comandos.

De acuerdo al análisis realizado, y tomando en cuenta las funciones que realizará el servidor, será un servidor de dominio el cual contemplará:

- Una instalación segura del sistema operativo con el service pack más reciente.
- La implementación de actualizaciones para Windows 2003 Server previamente bajadas a un CD para su instalación.
- El Antivirus con las especificaciones del procedimiento establecido.
- La Configuración de Servidor como controlador de dominio.

- DNS (Sistema de nombres de dominio).
- Active Directory (servicio de directorio que almacena información acerca de los objetos de una red y la pone a disposición de los usuarios y administradores de la red).

- Implementación y Administración del Active Directory basados en los puntos establecidos por el procedimiento, para lo anterior se contemplaron los siguientes puntos:

  - Creación unidades organizativas y grupos.
  - Creación de cuentas de usuario.
  - Equipos.
  - Dominios y confianzas
  - Sitios y servicios.

- Se usará la Consola de Administración de Directivas de grupo (GPMC) para poder utilizar objetos de directiva de grupo en un entorno de Active Directory, contando con el procedimiento para la implementación del GPMC en el cual se tocaron los siguientes puntos.

  - Instalación y configuración GPMC.
  - Administración de objetos de Directiva de grupo.
  - Hacer una copia de seguridad, restaurar, copiar e importar objetos de Directiva de grupo.
  - Creación de modelos de objetos de Directiva de grupo.

- Se manejará una administración de discos duros con la herramienta que nos proporciona Windows 2003 Server Enterprise Edition de acuerdo a las necesidades de la Sala de Cómputo.
- Las herramientas de seguridad que deberán estar implementadas serán:

  - Nmap 4.11.
  - GFI LANguard Network Security Scanner 7.0.
  - Fport1.2.
  - Belarc Advisor 7.1
  - Process Explorer 10.06.
  - ShowTraf 1.6.0.
  - Microsoft Baseline Security Analyzer 2.0 (MBSA 2.0).

- Se implementará la automatización de actualizaciones empleando el Microsoft Windows Server Update Services (WSUS), tanto para las estaciones de trabajo como para servidores.
- Los escaneos de puertos se harán 3 veces al día con Nmap 4.11 en los equipos desde el servidor.

- El escaneo de puertos al servidor se hará con Fport 1.2 y con GFI LANguard Network Security Scanner 7.0
- Las auditorías sobre el servidor y equipos se deberán llevar al cabo una vez al semestre tomando en cuenta los puntos establecidos.
- Los respaldos sobre archivos. Log generados por los escaneos, análisis de tráfico, análisis de red, de sucesos y del mismo servidor, deberán ser llevados a cabo diariamente y almacenados en una unidad de disco estipulada para dicho respaldo; sobre software e inventario dos veces por mes.
- Se realizará la administración de software que se utiliza en las salas de cómputo de manera que siempre este disponible para su implementación vía red. Tomando en cuenta la siguiente clasificación:

  - **Software de Trabajo:** Este software se encuentra instalado en los equipos en las dos Salas de Cómputo para el uso de los alumnos de la facultad de Ingeniería.

  - **Software de Administración:** Este software lo utilizan los administradores de las salas para realizar la administración de los equipos tal como apagado automático de equipo, antivirus, actualizadores, etc.

  - **Software para uso del personal que labora en las salas de cómputo:** Este software es aquel que utiliza el personal de las Salas de Cómputo para su uso personal, además para realizar las funciones dentro de las Salas de Cómputo.

  - **Software Aplicativo:** Este software es aquel que no está instalado en los equipos pero puede ser usado a futuro para nuevas necesidades o software que se tiene de respaldo.

- Las políticas sobre creación de cuentas, passwords, usuarios, grupos y privilegios serán los estipulados en el capítulo 5.

Independientemente de las políticas y acciones antes mencionadas, se tiene previsto modificar algunas herramientas que no se encuentren funcionando de acuerdo a las necesidades por parte de la sala de cómputo de UNICA (Unidad de Servicios de Cómputo Académico).

6.2 Políticas de Respaldo

El respaldo de la información de la organización es vital, por ello se debe tomar como una actividad diaria y de prioridad alta. Para ello se deben definir políticas de respaldo que permitan tener copias de seguridad incrementales y totales de la información tanto del servidor como aquellos servicios que son de alta disponibilidad para la organización, bitácoras, registros de seguridad, etc. Para que al momento de un problema de tipo físico o lógico se pueda restaurar la información en un tiempo prudente. Por lo cual se debe de tener en cuenta que tipo de copia se debe realizar:

- Copia total: Consiste en una copia completa de todos los datos principales. Requiere mayor espacio de almacenamiento.
- Copia Diaria: Hace una copia de seguridad de los archivos que se han creado o modificado el día de hoy.
- Copia diferencial: Consiste en copiar únicamente aquellos datos que hayan sido modificados respecto a una copia total anterior. Requiere menor espacio de almacenamiento. Para restaurar una copia diferencial es necesario restaurar previamente la copia total en la que se basa. Por tanto, requiere mayor tiempo de restauración. Una copia diferencial puede sustituir a otra copia diferencial más antigua sobre la misma copia total.
- Copia incremental: Hace una copia de seguridad de los archivos seleccionados sólo si no se han creado o modificado desde la copia de seguridad anterior. Para restaurar una copia incremental es necesario restaurar la copia total y todas las copias incrementales por orden cronológico que estén implicadas. Si se pierde una de las copias incrementales, no es posible restaurar una copia exacta de los datos originales.

1.- La recomendación sería utilizar herramientas de copias de seguridad (backup), útiles y de fácil manejo. Como por ejemplo: Norton Ghost 10.0, BackUp 1.0, Copias de Seguridad 4.1d, Simply Safe Backup, BackRex Expert Backup 2.5, Norton Save & Restore, Acronis True Image Home.

O bien.

2.- Las políticas se deben de fijar en función de nivel crítico de los datos, y del volumen. La frecuencia como mínimo debe ser diaria y como máxima mensual. Para el caso de la Sala de Cómputo se recomienda una vez al mes en software de aplicación y para bitácoras de forma diaria, en información se recomienda como mínimo cada 15 días o bien diaria si así lo requiere.

3.- Adicionalmente cada DVD o CD de información debe ser almacenado en un lugar seguro y debidamente etiquetado, con el objetivo de poder ser ubicados correctamente.

4. - Se deberá hacer respaldo sobre:

- Los Servidores (archivos de información de los administradores, correspondencia importante, notas y documentos de trabajo).
- Los equipos (archivos de información de los usuarios, correspondencia importante, notas y documentos de trabajo).
- Los archivos .log.
- Los archivos generados sobre los ingresos desde el exterior a la red.
- Los archivos generados por las conexiones externas realizadas desde la red al exterior.
- Los archivos generados al realizar los análisis a la red.
- Los archivos generados al realizar el tráfico de red.
- Los archivos generados al realizar escaneo de puertos.
- Los archivos generados sobre el visor de sucesos.
- Sobre el inventario del hardware y software.

- Bitácoras.
- Sobre los archivos de mantenimiento.
- Sobre informes del firewall.
- Los archivos generados sobre la información que genera el análisis del o los antivirus instalados, así como del anti-spyware.
- Auditoría de seguridad (Equipos).

5. -Los respaldos a servidores, archivos .log, de ingresos, de conexiones de la red y visor de sucesos deberá de ser diario, análisis de red, al tráfico de la red, informes de Firewall, informes de antivirus, escaneos serán de manera incremental.

6.-Los respaldos sobre inventario de hardware y software, archivos de mantenimiento deberán ser de manera diferencial.

7.-Los respaldos hacia equipos deberán ser generados por cada uno de los usuarios o personal de la Sala de Cómputo, especificando la carpeta o unidad de disco asignado para este punto.

8.-Los respaldos deberán de ser generados por los administradores de la Sala de Cómputo asignados por cada punto expuesto.

9. -Los respaldos deberán ser guardados en un espacio de unidad de disco duró protegido con sólo acceso a quien lo realizó y una copia de seguridad como se especifico en el punto 3.

10.-Cada responsable de las áreas deberá llevar un control de quien realiza los respaldos diarios, dependiendo del área asignada y de su función.

Las últimas versiones de los sistemas operativos de Microsoft incluyen por defecto herramientas de backup bastante sencillas de utilizar, msbackup.exe en Windows 98 y ME y ntbackup.exe en Windows XP Profesional (Figura 6.0).

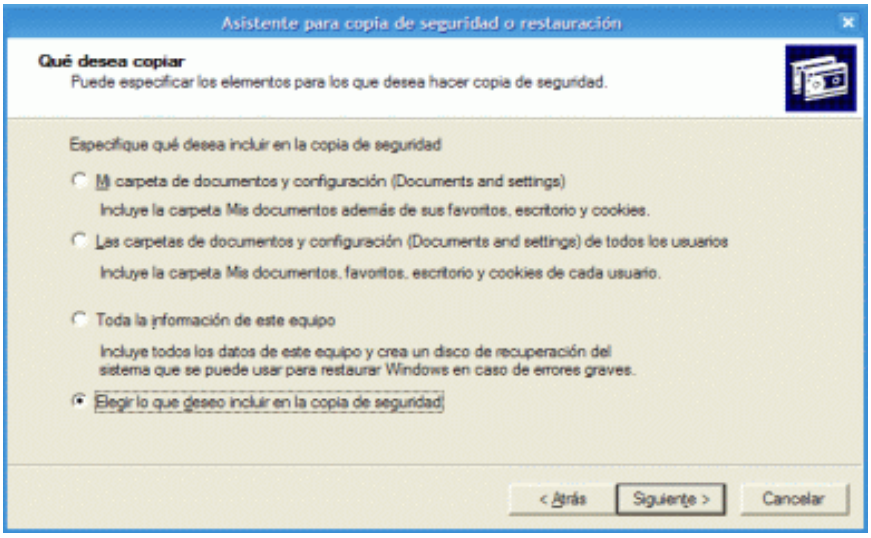


Figura 6.0 Copia de seguridad de Windows.

Por defecto ntbackup comienza en modo asistente. Aunque el modo avanzado no es nada complicado de utilizar tampoco ofrece ninguna opción extra interesante. La primera opción que se nos dará en este asistente es, evidentemente, si queremos realizar una copia de seguridad o bien restaurar una copia de seguridad creada anteriormente.

La herramienta preguntará entonces por los distintos archivos a incluir en la copia de respaldo. Las opciones predeterminadas son: los documentos y configuración del usuario actual, documentos y configuración de todos los usuarios o una copia de todos los archivos del sistema. Opción que provocará que la copia de seguridad ocupe varios gigas. Sin mencionar el hecho de que no es esta la herramienta adecuada, siendo más útil en el caso de que se quiera clonar una instalación de Windows con el uso de programas del tipo Norton Ghost, aunque también se nos da la opción de que seamos nosotros los que seleccionemos los archivos a incluir.

Si se escoge esta última opción el asistente nos mostrará un árbol del sistema de archivos para seleccionar. Por último se nos preguntará por el nombre de la copia de seguridad y el lugar donde almacenarla. Una vez en este paso bastará pulsar el botón Finalizar para llevar a cabo la copia de seguridad. Pero este proceso, si no está automatizado, no tiene mucho sentido. Por lo cual en este caso se tendía que utilizar las tareas programadas de Windows, esta seria una buena recomendación para las estaciones de trabajo.

6.3 Mantenimiento Físico y Lógico del equipo

Como se sabe existen muchos factores de índole ambiental y humano que hacen que el equipo de cómputo sufra daños de manera física por lo cual hay que tener en cuenta que dentro de la seguridad será evitar que este tipo de factores perjudique el equipo de cómputo, el poder realizar un mantenimiento preventivo y correctivo nos permitirá aumentar el tiempo de vida de estos para lo cual hay que hacer un breve espacio para efectuar este tipo de mantenimiento.

Por otro lado el mantenimiento lógico de los equipos nos permitirá tener un mayor rendimiento al usar nuestro equipo, no disminuirá su rendimiento al iniciar aplicaciones para su uso, y así tener un control total de los archivos que contiene nuestro equipo haciendo la eliminación de ciertos archivos que se albergan en los equipos ocupando espacio en disco, afecta directamente en el rendimiento del mismo.

En la mayoría de las organizaciones utilizan al personal con el que se cuenta en el área de sistemas para la realización de este tipo de mantenimientos. Por ello se recomienda que se contraten servicios externos para este tipo de actividades, pero si hablamos de seguridad deberá de ser muy confiable, porque hablamos de activos que si en vez de brindarles un mantenimiento acaban con causarle daños estaríamos provocando desde aquí una denegación de servicio, por lo que se tendrá en la sala de cómputo un área de soporte técnico, la cual deberá contar con personal capacitado para realizar dicho mantenimiento por lo que sus funciones serán las siguientes:

1. El mantenimiento físico se recomienda que se haga de forma semestral a las estaciones de trabajo de las salas de cómputo (UNICA). Se deberá incluir las Computadoras e impresoras de

la sala de cómputo (UNICA) que estén a cargo de la administración. Esta área cuenta con personal capacitado para proporcionar mantenimiento a estaciones de trabajo e impresoras.

2. Esta área de soporte técnico es capaz de brindar mantenimiento a los servidores de la organización, se tiene personal calificado, para dicha actividad. El ciclo de mantenimiento es semestral para este equipo.

3. Contratación de un servicio de mantenimiento correctivo para equipo de UNICA, con el fin de contar con un plan de contingencia ante desastres y de igual manera para solucionar problemas de equipo con daño severo que requiere de reparación inmediata, por una empresa con personal certificado en este tipo de equipo.

4.-El responsable del área de sistemas deberá tener un formato el cual especificará los siguientes datos:

- Nombre de la organización.
- Equipo.
- Modelo.
- Ubicación.
- Número de Inventario.
- Número de Serie.
- Nombre del responsable que llevó a cabo el mantenimiento.
- Reporte del mantenimiento que se realizó.
- Fecha de realización del mantenimiento.
- Jefe Inmediato.
- Quién autorizó dicho mantenimiento.
- Fecha del próximo mantenimiento, en caso de ser preventivo.

Se debe tener de igual manera un control en cuestión del equipo que se daña y el formato deberá contener los siguientes datos:

- Equipo.
- Modelo.
- Número de Inventario.
- Fecha del reporte.
- Reporte del daño presenta.
- ¿Quién reporta?.
- Jefe de Inmediato.
- Fecha del día que se lleva a reparación y por qué empresa.

Al terminar el servicio por parte de la empresa de mantenimiento correctivo (reparación), se debe de tener un formato donde se especifiquen los siguientes puntos, de igual manera archivar las facturas y reportes que presente la empresa contratada:

- Nombre de la Empresa.
- Equipo reparado.
- Número de Serie.
- Número de Inventario.
- Número de Factura.
- Fecha de salida del equipo
- Fecha de entrega.
- Reportar el estado en el que regresa el equipo
- ¿Quién recibió el equipo?
- Número de reporte.

Al hablar de un mantenimiento lógico para el equipo, los puntos que se deben tocar son los siguientes:

1.- El mantenimiento lógico del equipo se deberá hacer mensualmente.

2.- Se deberá hacer un borrado de archivos temporales, cookies, archivos de Internet, papelera de reciclaje, etc.

3.- Se deberá dar un mantenimiento lógico sobre aquel tipo de software instalado que requiera de actualizaciones ya sea semanal o mensualmente.

4.- Se deberá de programar las aulas de la sala de cómputo (UNICA) en los días y horas que se pretende hacer el mantenimiento lógico y sobre que archivos, software o carpetas se pretende realizar.

5.- Se deberá tener un control con el siguiente formato:

- Responsable o responsables del mantenimiento lógico.
- Fecha y hora en que se realizó el mantenimiento.
- Sobre que elementos se realizó el mantenimiento.
- Reporte de que se llevo acabo.
- Nombre del Jefe Inmediato.

Un adecuado mantenimiento tanto físico como lógico nos llevará a no tener problema sobre el equipo, así como en las aplicaciones que sean utilizadas, al ser preventivo y correctivo nos evitará tener equipo dañado y ampliará la vida útil del mismo y por lo tanto un mejor servicio a la comunidad estudiantil de la Facultad de Ingeniería.

6.4 Automatización de actualizaciones para Sistema Operativo

Una **actualización (update)** es el término que se utiliza para identificar los diferentes tipos de paquetes que pueden hacer que un sistema esté al día, incluyendo hotfixes, paquete acumulativo de revisiones, Service Packs, entre otros. Las actualizaciones se caracterizan por la severidad del tema que tratan. Algunas actualizaciones son críticas mientras que otras son recomendadas.

Una **actualización** (**upgrade)** es un paquete de software que reemplaza una versión instalada de un producto con una versión más nueva del mismo producto. Típicamente, el proceso de actualización deja intacta la información existente del cliente y sus preferencias mientras que reemplaza el software existente con una nueva versión.

- **Service Pack**: Es un paquete acumulativo de revisiones 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.

- **Hotfix**: Es un paquete sencillo acumulativo compuesto por uno o más archivos utilizados para corregir un defecto en el producto. También conocido como QFE, revisión y actualización.

De igual manera se realizan las actualizaciones para software en los dos tipos update y upgrade, por lo cual es importante contar con las actualizaciones para que tanto como el sistema operativo como el software con que se este utilizando no presente fallas o brechas que permitan introducción de virus o software malicioso, como se sabe en las organizaciones se cuenta con sistemas que deben de estar al día y software que es requerido, por lo cual una aplicación que permita implementar todas estas actualizaciones nos dará mayor seguridad, además de un mejor control de actualizaciones que se encuentren instaladas en los equipos, en las fechas y horarios programados. El contar con un servidor que nos permita realizar esto debe tener la siguiente aplicación.

Microsoft Windows Server Update Services (WSUS) constituye una solución completa para administrar las actualizaciones en la red. Se realizó un procedimiento para la instalación y administración con los siguientes puntos contenidos.

1.-Requisitos de la instalación de WSUS.

- Requisitos de Actualizaciones automáticas.
- Requisitos de software.
- Requisitos y recomendaciones para el disco.

2.- Instalar WSUS en un servidor.
3.-Configurar la conexión de red.
4.-Sincronizar el servidor.
5.-Actualizar y configurar actualizaciones automáticas.
6.-Crear un grupo de equipos(para Sistemas operativos y software implementado).
7.-Aprobar e implementar actualizaciones.

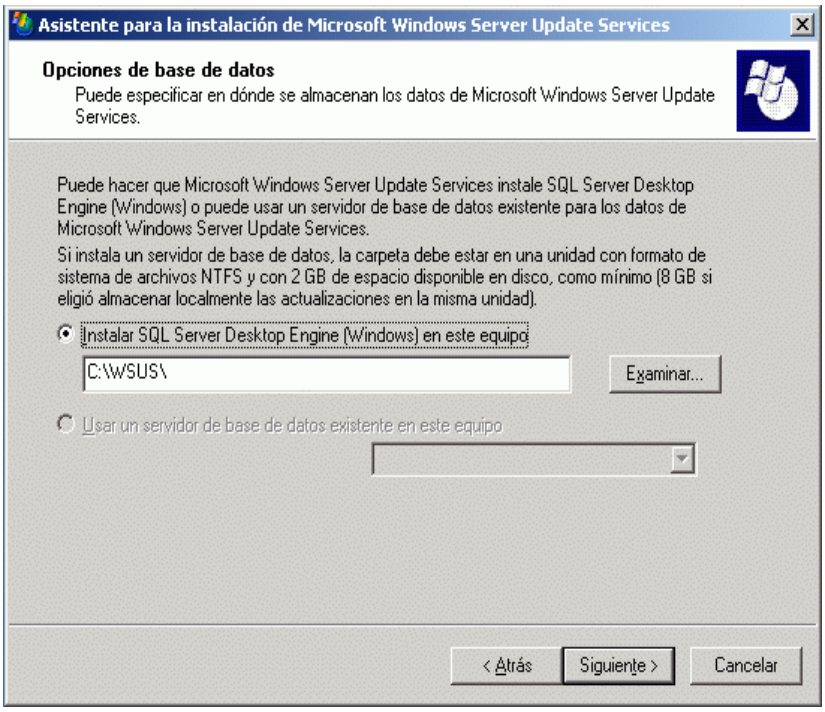


Figura 6.1 Instalación de WSUS

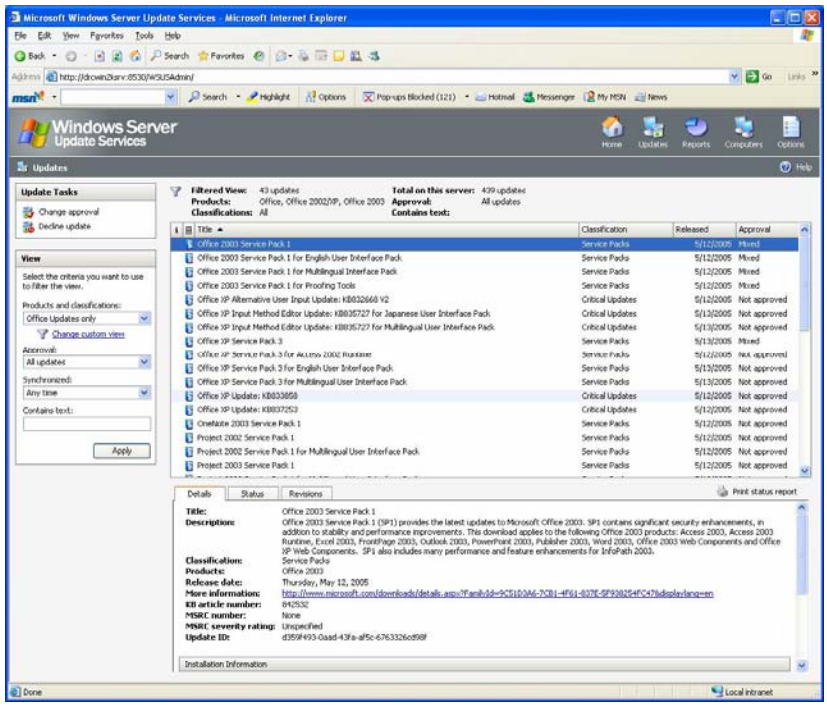


Figura 6.2 Implementación de WSUS

De lo anterior se recomienda tener en los servidores de las Salas de Cómputo de UNICA la instalación e implementación correcta de WSUS, para realizar una buena administración sobre

las actualizaciones para la automatización y optimización de recursos para las Salas de Cómputo.

6.5 Automatización de Antivirus

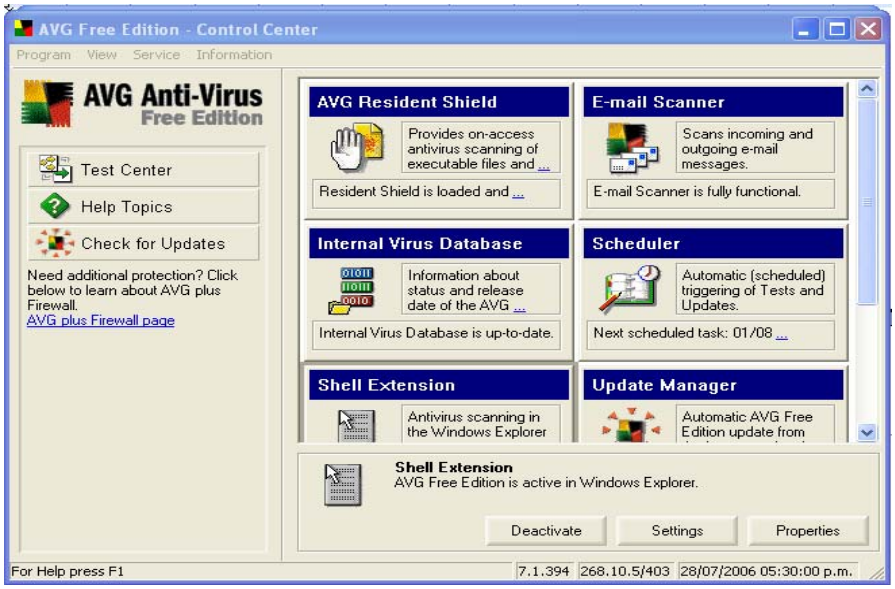
En este caso el antivirus implementado el es AVG Free 7.1.385 el cual cuenta con las características mencionadas, potente antivirus, además de contar con su versión gratuita realiza un escaneo exhaustivo y confiable.

Esta versión incluye:

- AVG Resident Protection: Monitorización constante del sistema.
- AVG Email Scanner: Escanea el correo electrónico.
- AVG On-Demand Scanner: Analiza por secciones especificadas.
- Escaneos preprogramados por fechas u horas.
- Actualización gratuita de la base de datos de virus.
- Función de actualización automática.
- Desinfección automática de archivos infectados.
- AVG Virus Vault: Sistema para manejar de forma segura ficheros infectados.

Todo esto a través de un sistema ágil y sencillo de usar. Se realizó un procedimiento donde se especificó en este caso los siguientes puntos:

1. Instalación.
2. Configuración.
3. Manejo del centro de control.
4. Configuración de las actualizaciones automáticas.
5. Configuración personalizada.



6.3 Configuración del Antivirus

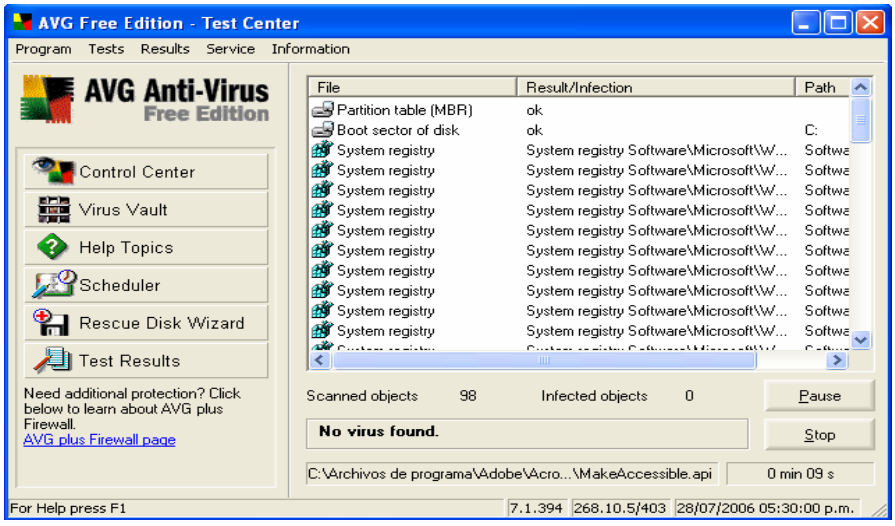


Figura 6.4 Automatización de Antivirus.

6.6 Implementación de Firewalls

En este punto se considero que los sistemas operativos que se manejan en las salas son los siguientes como se vio en los análisis realizados en el capitulo anterior:

- Sistema Operativo Windows XP.

Cuenta integrado con su propio firewall, en este caso se ha habilitado para protección del sistema, nos permite configurar dependiendo de las aplicaciones que queramos asignar cuales admitimos y cuales no.

- Sistema Operativo Windows 2000.
  No cuenta con firewall integrado.
- Sistema Operativo Windows 98.
  No cuenta con firewall integrado.
- Sistema Operativo Windows 2000 Server.
  No cuenta con firewall integrado.
- Sistema Operativo Windows NT Server.
  No cuenta con firewall integrado.

Dentro del análisis que se realizó se observó que se tiene el uso del sistema operativo Linux esos equipos son administrados por otra área de la organización por disposición de la misma, también se cuenta con firewall universal administrado estratégicamente por el Departamento de Seguridad con el que cuenta la Facultad.

Aún así se debe de utilizar y actualizar el Firewall de equipo si se cuenta con él, hacer la habilitación del mismo, realizando la configuración correcta. Se pudo observar que sólo el sistema operativo Windows XP cuenta con su propio firewall personal, el cual se configurará de la manera pertinente para que realice su función.

Como sabemos se cuenta con servidores los cuales deben de contar con firewall, por lo cual se ha decidido utilizar el siguiente:

ZoneAlarm ha sido seleccionado por millones de usuarios como una solución para contar con una conexión segura a Internet. Este servidor de seguridad personal (firewall) ampliamente utilizado, bloquea automáticamente las amenazas procedentes de Internet, conocidas o desconocidas, para proteger el equipo de intrusos y código malicioso.

ZoneAlarm proporciona seguridad básica a aquellos usuarios que necesiten protección para el equipo y mantiene la confidencialidad de la información.

La versión gratuita sólo proporciona ciertas características:

- Protección de seguridad sólida para el equipo conectado a Internet.
- Aprobación segura para programas que necesitan acceso a Internet.
- Evita que intrusos accedan a su equipo.
- Hace al equipo invisible a los intrusos.
- Proporciona controles de seguridad precisos.
- Bloqueo de todas las categorías de contenido Web ofensivo e inapropiado.
- Cifra mensajes instantáneos para que no puedan ser monitoreados; protección universal para los servicios de mensajería instantánea más populares como AOL, ICQ, Yahoo Messenger, y Trillian.
- Previene buffers overflow, URL'S ejecutables y otros ataques.

Para poder hacer la instalación y la ejecución del firewall se generó un procedimiento el cual contó con lo siguiente:

1.- Instalación de ZoneAlarm.
2.-Opciones del Centro de control.

- Centro de control.
- Consola.

3.- Descripción y configuración de los paneles de ZoneAlarm.

- Panel de información general.
- Panel Servidor de seguridad.
- Panel Control de programas.
- Panel Control de antivirus.
- Panel Control de correo.
- Panel de Alertas y registros.
- Altas.

4.-Conclusiones.
5.-Revisión.

Se realizaron pruebas bajo los sistemas Windows 2000. Windows 2003 Server.

Figura 6.5 Firewall.

CAPÍTULO 7

PRUEBAS Y RESULTADOS

7.1 Auditoría del equipo

El término de Auditoría se ha empleado incorrectamente ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase "Tiene Auditoría" como sinónimo de que, en dicha entidad, antes de realizarse la auditoría, ya se habían detectado fallas.

El concepto de auditoría es mucho más que esto. **Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.**

El auditor debe revisar o auditar los controles con la ayuda de una lista de control (checklist) que consta de una serie de preguntas o cuestiones a verificar.

En el caso de nuestra problemática en particular, la auditoría que se realizó en las Salas de Cómputo de la Unidad de Servicios de Cómputo Académico (UNICA) con respecto a la auditoría de equipo se tomó los siguientes puntos a consideración, además se tomo en cuenta lo anterior mencionado, debido a que la sala ya contaba con sus políticas, normas y procedimientos de seguridad para su equipo por lo cual al realizar la prueba de auditoría y teniendo a la mano los elementos de los puntos que se tomarían a consideración, se proporciono los documentos para poder realizar la auditoría de los equipos.

Para realizar la auditoría y cotejar con la documentación que fue proporcionada para dicho estudio se utilizaron herramientas para realizar las verificaciones, las cuales fueron las siguientes:

GFI LANguard Network Security Scanner 7.0: Es un analizador de red (Figura 7.0)

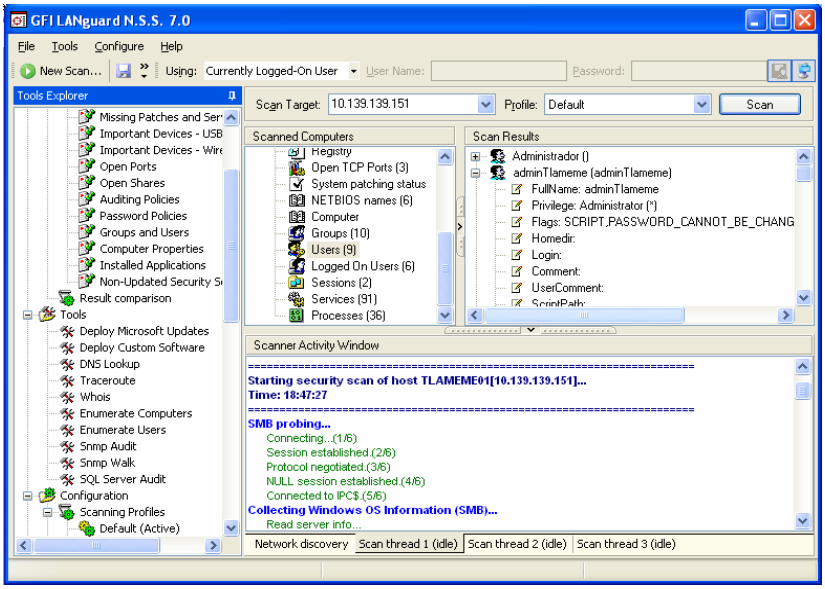


Figura 7.0 Interfaz GFI LANguard Network Security Scanner 7.0.

Belarc Advisor 7.1: Generador de informe de hardware y de software (Figura 7.1).

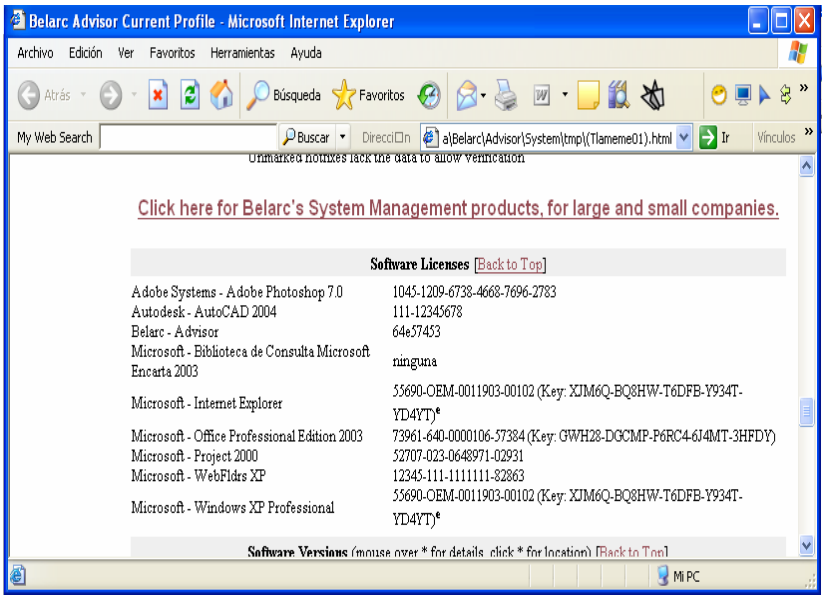


Figura 7.1 Interfaz Belarc Advisor 7.1.

Microsoft Baseline Security Analyzer 2.0 (MBSA 2.0): Nos permite analizar el estado de seguridad según las recomendaciones de Microsoft (Figura 7.2).

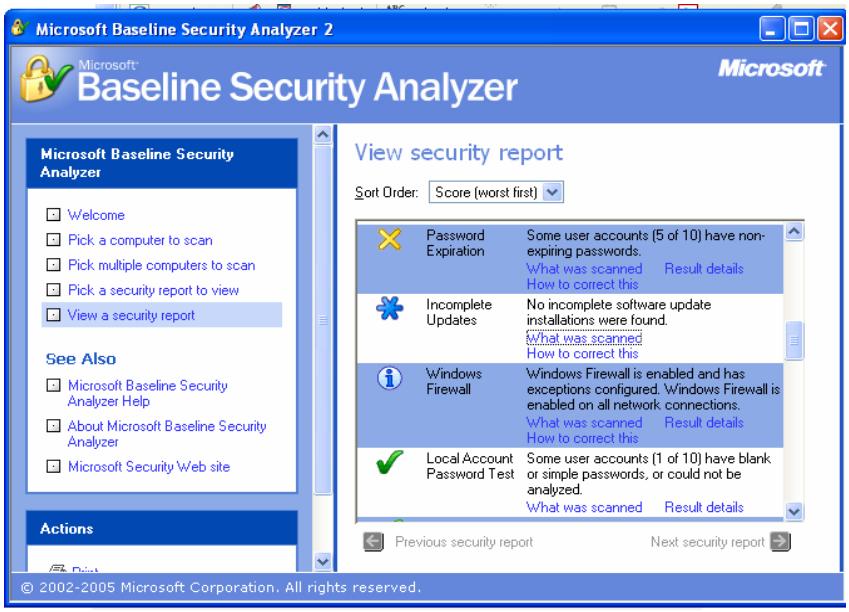


Figura 7.2 Interfaz Microsoft Baseline Security Analyzer 2.0 (MBSA 2.0).

Se pudo evaluar que no es muy eficaz el método, procedimiento y políticas con las que contaba las Salas de Cómputo de UNICA (Figura 7.3), encontrándose así que existe una gran brecha entre lo establecido y lo real.

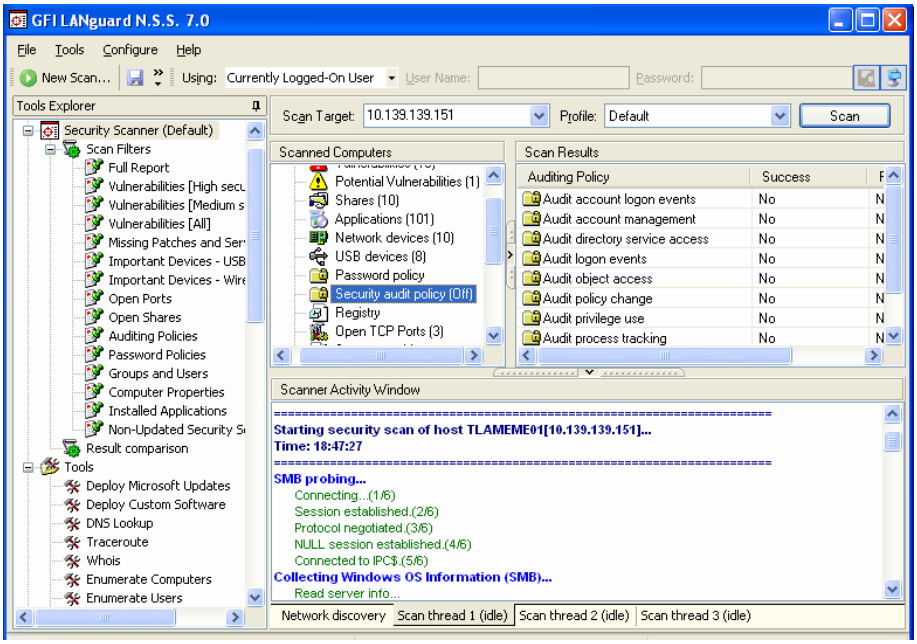


Figura 7.3 Auditoría de equipo antes de implementación de nuevos procedimientos.

Se realizó una auditoría de equipo posterior a la implementación de nuevas políticas, normas y procedimientos estipulados en el capítulo 5, esto permitió observar que tan sólidas estaban estipulados estos lineamientos, se volvieron a ocupar las herramientas.

Los resultados obtenidos fueron muy satisfactorios, se encontró:

- Que las políticas sobre usuarios y grupos estaban implementadas correctamente y el seguimiento de estas estaban correctas.
- Las actualizaciones en un 98% se encontraban instaladas.
- Los puertos en un 80% correcto.
- El inventario en un 90% correcto.
- Se contaba con las auditorías de seguridad local implementadas.
- Antivirus y Anti-Spyware instalado.
- Software instalado, correcto, inventariado, con licencia y controlado en un 80%.
- Privilegios sobre archivos, carpetas o directorios en un 90%.
- Bitácoras de sucesos en un 90% con respaldo.

En esta auditoría que se realizó al equipo de las Salas de Cómputo 2 y 3 de UNICA se vio que las políticas, normas y procedimientos se estaban realizando de manera eficaz.

Pero no podemos esperar un 100% debido a que como se ha mencionado la seguridad es dinámica, pero si se puede reducir al mínimo todo aquello que pueda provocar un riesgo.

7.2 Escaneo de la red

Para llevar acabo el escaneo a la red en las salas de cómputo 2 y 3 de UNICA, se tomaron en cuenta los puntos anteriores para tener los resultados esperados, se realizó el escaneo de red de puertos y el de vulnerabilidades, utilizando las siguientes herramientas:

1.-**GFI LANguard Network Scanner 7.0: GFI LANguard Network Security Scanner (N.S.S.)** analiza la red mediante los métodos potenciales que un hacker podría utilizar para atacarla. Mediante el análisis del sistema operativo y de las aplicaciones que se están ejecutando sobre los equipos de red, GFI LANguard N.S.S. identifica todas las posibles brechas de seguridad.

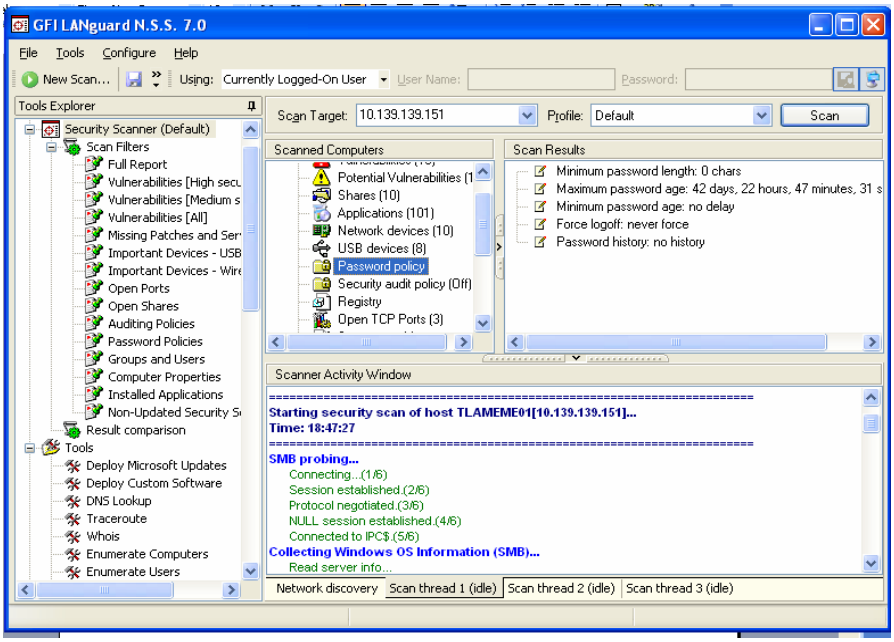


Figura 7.4 GFI LANguard Network Scanner 7.0: GFI LANguard Network Security Scanner (N.S.S.).

Se realizaron escaneos tanto equipo por equipo, rango de equipo y por dominio en UNICA como lo muestra la siguiente figura (7.6), toda la información que arrojó este escaneo se utilizó para el análisis general, pero después de la implementación de nuevas políticas, procedimientos y normas, se realizó un nuevo escaneo para comprobar los nuevos lineamientos establecidos, debido a que la misma herramienta proporciona todas las vulnerabilidades que encuentra por todos los rangos especificados, además proporcionó todas aquellas que estaban como futuras vulnerabilidades para poder tomarlas y evitarlas, la mejora sobre el escaneo de la red fue considerable, ya que redujo en un 90% las vulnerabilidades que se presentaron durante el primer escaneo y durante el segundo que se realizó ya con la implementación se logro observar nuevos puntos que no se habían implementado de manera adecuada como lo fueron:

- Privilegios.
- Puertos.
- Cuentas.

Lo cual permitió rectificar los lineamientos establecidos, se realizó un escaneo contaste sobre la red semana por semana, para observar como se comportaban los lineamientos establecidos y los nuevos brotes posibles de riesgo.

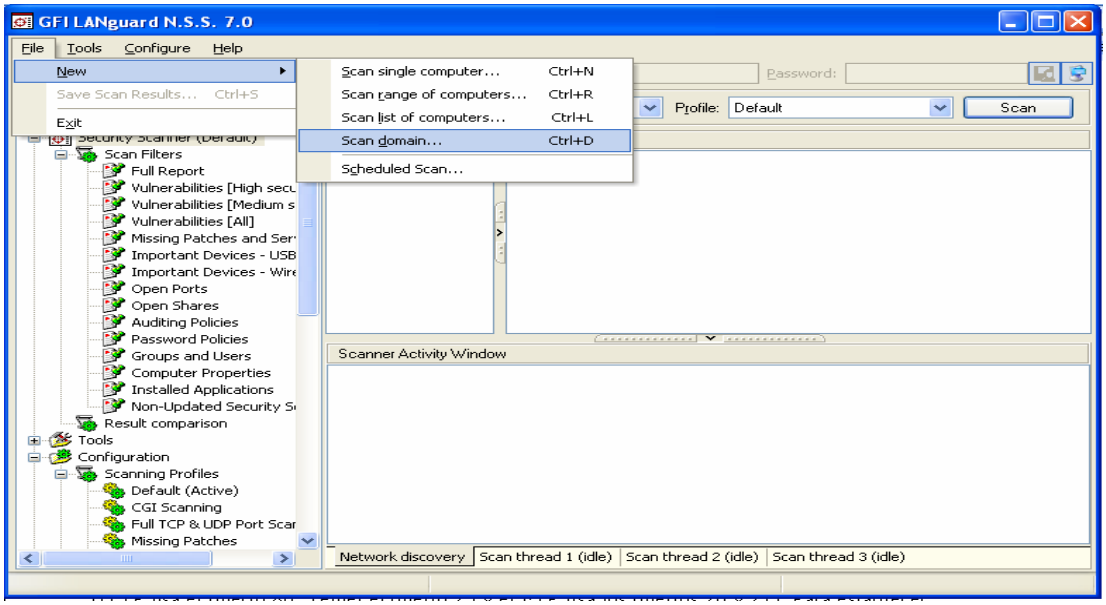


Figura 7.6 Rango de Escaneos.

2.- **Nmap** esta orientado a la identificación de puertos abiertos en una computadora, determinando que servicios se están ejecutando, e intenta determinar que sistema operativo utiliza.

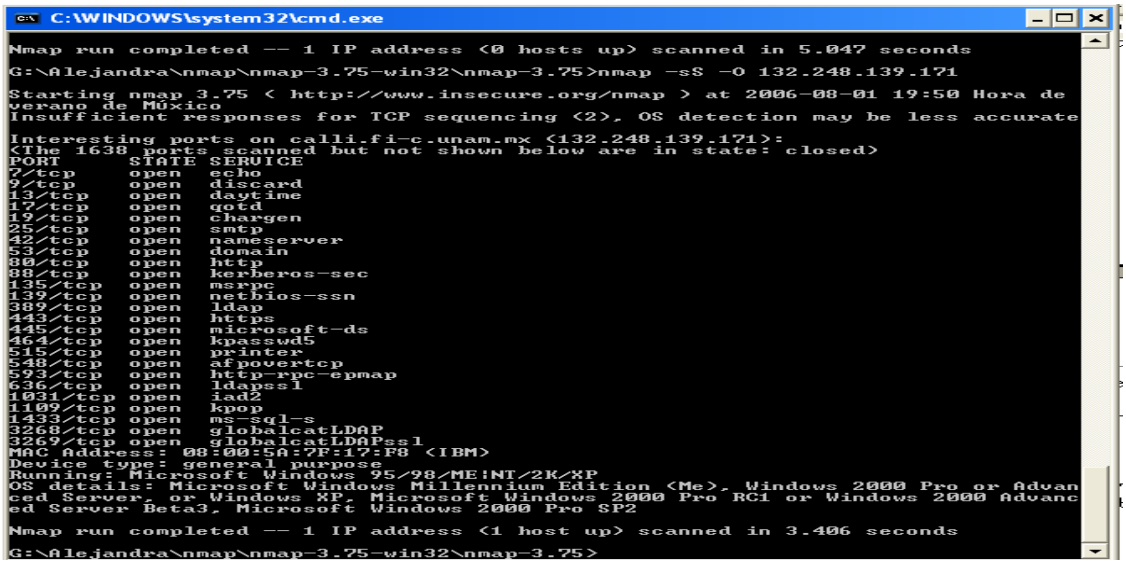


Figura 7.7 Entorno de Nmap 4.11.

Esta herramienta ha sido de gran utilidad debido a la información que arroja, como se mencionó anteriormente la lista de puertos se emplearon para observar el tipo de puerto abierto, protocolo y servicios que ofrece para la especificación de puertos abiertos que deben de tener los equipos de UNICA, además de verificar ciertas aplicaciones que no deban tenerse, se realizó un sondeo por toda la red que proporcionó todos aquellos puertos abiertos y que tendrían una brecha de seguridad estos fueron los puertos que presentó la herramienta Nmap (Figura 7.8), tanto en protocolo TCP como en protocolo UDP, aquí cabe mencionar lo siguiente no todos los puertos son necesarios y en el caso de los equipos de UNICA se tienen que cerrar todos aquellos puertos que presentan alta peligrosidad como lo son: echo (7), discard (9), systat (11), daytime (13), netstat (15), chargen (19), ftp-data (20), ftp (21), telnet (23), smnp (25), bootp (67), tftp (69), finger (79), http (80), pop-2 (109), uucp (117), upnp (5000).

Ahora en UNICA lo que se propone es evitar el uso en este caso del protocolo Netbios, los sistemas operativos de Microsoft utilizan este protocolo para comunicarse entre sí.

Para deshabilitar el Netbios sobre TCP/IP, en el panel de control, en conexiones de red, en propiedades se deshabilitó el Netbios para el caso de Windows 98, para el caso de Windows 2000 y Windows XP en el panel de control, en conexiones de red y propiedades se eligió el Protocolo TCP/IP en la opción de avanzadas dentro de la pestaña de WINS en la opción de deshabilitar la opción de Netbios sobre TCP/IP (Figura 7.9).

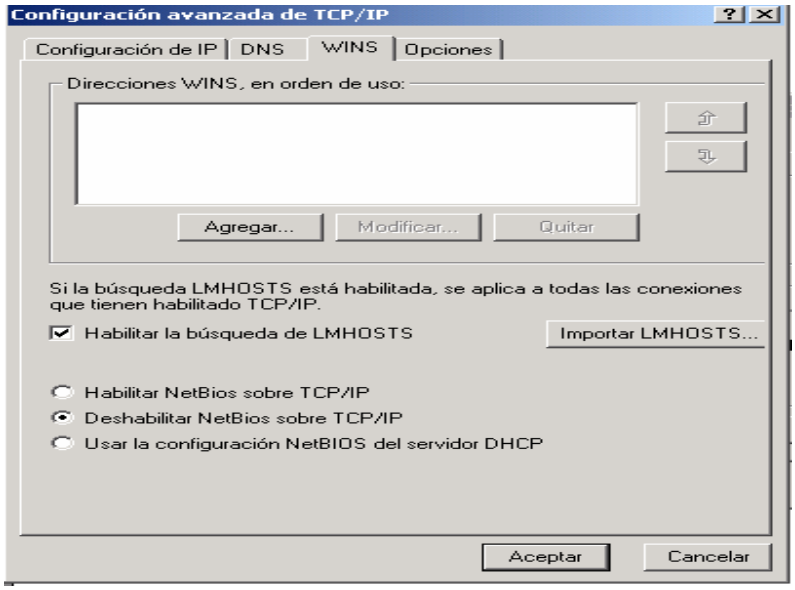


Figura 7.9 Deshabilitación del Netbios sobre TCP/IP.

Para realizar el cerrado de puertos sobre los equipos en el caso de Windows 2000 en conexiones de red, en propiedades se selecciono el protocolo TCP/IP y en la pestaña de avanzadas se selecciono opciones, donde se encuentra la opción de filtrado de TCP/IP (Figura 7.10).

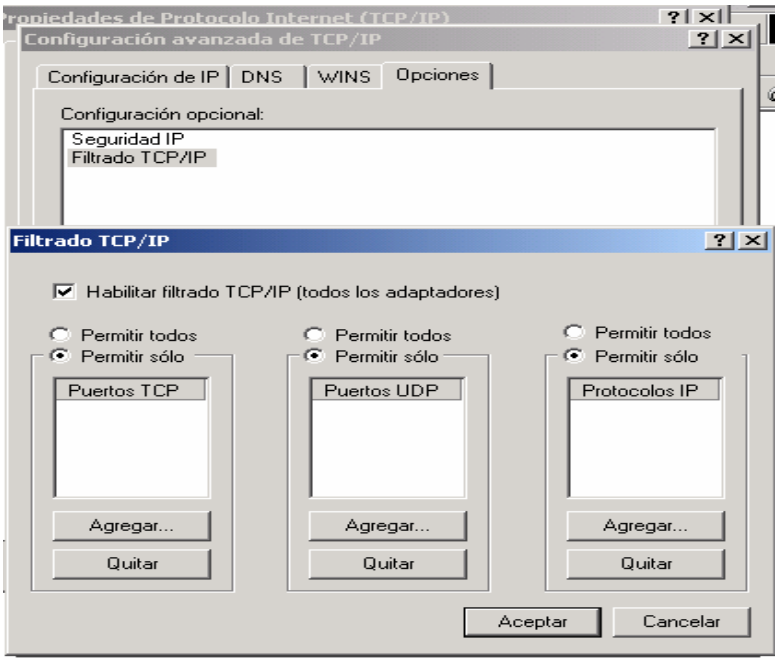


Figura 7.10 Filtrado de Protocolos.

7.3 Escaneo de puertos a servidores críticos

El escaneo de los servidores de UNICA se realizó con el objeto de determinar los puertos que se encontraban abiertos (Figura 7.12), los resultados que arrojo este escaneo de puertos a los servidores con la herramienta Nmap 4.11, fueron los puertos críticos ftp, telnet y http.

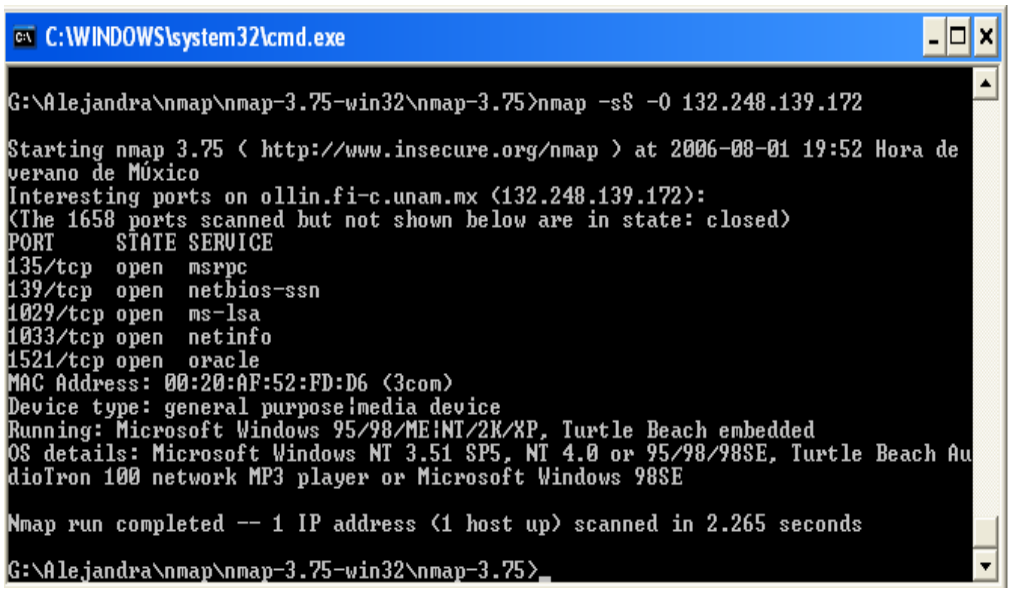


Figura 7.12 Escaneo a servidores críticos.

Únicamente deben estar abiertos los puertos que sean imprescindibles para el funcionamiento del servidor, para el caso de UNICA un servidor seguro no debe tener los puertos abiertos de telnet (23), ftp (20 y 21) y http (80), así como los puertos estipulados en el punto anterior de este capítulo, por tanto se tendrán que cerrar con el Firewall y la manera de cerrar puertos especificada en el punto anterior de este capítulo.

7.4 Revisión de Bitácoras

Se generaron bitácoras de instalación de sistema operativo y software de equipos, clonación de imágenes, instalación de servidores, dichas bitácoras proporcionaron información adecuada en caso de que algún equipo necesitará alguna aplicación o nueva instalación del sistema operativo y de esta manera se realizará adecuadamente. Las bitácoras contienen información crítica es por ello que deben ser analizadas, ya que están teniendo mucha relevancia, como evidencia en aspectos legales. Por lo cual se especifica revisar en este caso las bitácoras que generan los servidores en las Salas de Cómputo (UNICA) de la siguiente manera:

Diariamente

- Sobre las bitácoras de IIS para el servidor que contenga el servicio de WSUS.
- Escaneos de red.
- Sucesos.
- Bitácoras externas con respecto a los equipos de cómputo.

Semanalmente

- Sobre entradas y salidas de conexiones de red.
- Sobre la información que genera el antivirus.
- Sobre la que genera el Firewall.

Mensualmente

- Sobre los generados en los equipos de cómputo.

Es importante registrar todas las bitácoras necesarias de todos los sistemas de cómputo para mantener un control de las mismas, esto permitirá que en caso de fallo o sirviendo como medio legal se cuente con las que se necesiten.

7.5 Revisión periódica de los avances

En el caso de UNICA se efectuaron aproximadamente cada 15 días y las mas prolongadas fueron hasta un mes arrojando información acerca de las herramientas implementadas y si estas cumplían con lo establecido, de igual manera la revisión de los procedimientos, políticas y estrategias arrojaron ciertas brechas que se no se estaban controlando por lo cual se requiere de nuevo regresar al principio del diagrama para solventar estas fallas, llevando a realizar modificaciones y ajustes necesarios.

7.6 Modificaciones y ajustes necesarios a la seguridad

Al realizar las revisiones pertinentes como se menciono en el punto anterior se realizan las siguientes modificaciones y ajustes necesarios a la seguridad para la problemática en particular, esto quiere decir que para UNICA, se plantean las siguientes modificaciones y ajustes en cuanto a la seguridad se refiere seguridad.

7.6.1 Programa Concientización y Capacitación

Si se pretende que las medidas tengan éxito se debe de empezar por hacer conciencia de hay que comenzar por todos los miembros de la organización, en este caso dentro de los ajustes que se llevaron acabo y se seguirán llevando acabo dentro de UNICA es el programa de concientización y capacitación, a lo que se pretende llegar como su nombre lo dice es dar conciencia que la seguridad es un factor sumamente importante, además de dar capacitación a su personal en esta área, por lo cual este programa deberá contener lo siguiente:

1.-El Coordinador de las Salas de Cómputo deberá ser el primero en llevar a cabo las nuevas medidas de seguridad y fomentarla hacia el personal de las Salas de Cómputo.

2.-Todos los miembros de la sala deberán capacitarse en el área de la educación y concientización en seguridad.

.

3.-El personal que estará encargado del área de seguridad deberá capacitarse constantemente dentro de las áreas de seguridad:

- Seguridad Física.
- Seguridad Lógica.
- Soluciones Tecnológicas.
- Administración y Protección de los activos.
- Monitoreo.
- Auditorías y Bitácoras.
- Investigación.
- Arquitecturas.
- Análisis.
- Implementación.

4.- Fomentar el uso correcto de los activos que maneja el personal.

5.-Deberá haber una participación activa de todos los miembros empezando, en este caso por el Coordinador General.

6.- Fomentar el rol de cada uno de los miembros de la organización para una adecuada funcionalidad de la seguridad.

Esto es con el fin de que todo lo establecido pueda ser funcional, es decir como se mencionó de nada sirve tener tanta tecnología invertida si no se puede concientizar la parte mas vulnerable que es la gente.

7.6.2 Personal dedicado al rol de la seguridad

Por lo tanto, dentro de los ajustes de seguridad para las Salas de Cómputo de UNICA se determinar implementar un nuevo concepto de la administración de la seguridad.

Este personal dedicado al rol de la seguridad deberá tener un administrador principal el cual será el encargado de dar los reportes pertinentes al coordinador, además de fomentar la seguridad entre todos los miembros de la Sala de Cómputo (UNICA).

7.6.3 Planes de continuidad

Dentro de los ajustes se contemplara un plan de continuidad para las Salas de Cómputo (UNICA), este plan debe describir el proceso de planeación para asegurar que las Salas de Computó puedan sobrevivir ante un evento que cause la interrupción del proceso normal de su servicio.

7.6.4 Herramientas complementarias

Haciendo algunas modificaciones, se integraron cinco nuevas herramientas que serán de utilidad en las Salas de Cómputo, fueron puestas a prueba durante un semestre.

Fast Ram 2.6: Es un liberador de memoria siendo este una aplicación sencilla que libera la memoria de el sistema cuando este se encuentra sobrecargado. Además, cuenta con una opción de actuar de forma automática, liberando la memoria cuando baje de cierto límite que se le haya indicado previamente (Figura 7.15).

Figura 7.15 Ambiente Fast Ram.

Wind off 3.0: Es un automatizador para apagar equipos de cómputo a una hora determinada o transcurrido cierto tiempo, con posibilidad de activar capturas de pantalla y alarmas. Se puede programar para que realice tres funciones diferentes (o cualquier combinación de ellas), pero siempre a una hora determinada o pasado cierto tiempo (Figura 7.16).

Figura 7.16 Ambiente Wind off.

Tweauik (2.10 para Windows XP y 1.33 para Windows 98 y 2000): Permite modificar características ocultas del interfaz de Windows. Muestra una cantidad variable de elementos que clasifican las distintas funciones ocultas de la versión de Windows que se tenga instalada. Todas estas características se pueden modificar manualmente desde el registro de Windows (REGEDIT). Sin embargo, la modificación incorrecta del registro puede ocasionar daños irreparables a Windows. Es aquí donde Tweak UI se destaca por su sencillo manejo mediante cuadros de diálogo evita correr riesgos (Figura 7.17)

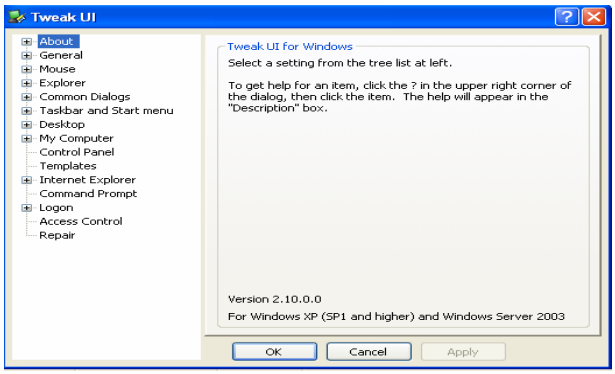


Figura 7.17 Ambiente de Tweauik.

Bodies Cleaner 1.0.2: Aplicación que permite eliminar del disco duro los ficheros temporales, haber reciclado vacío, historiales, cookies, direcciones, archivos usados recientemente, historiales. Y de esta manera evitar archivos inutilizables (Figura 7.18).

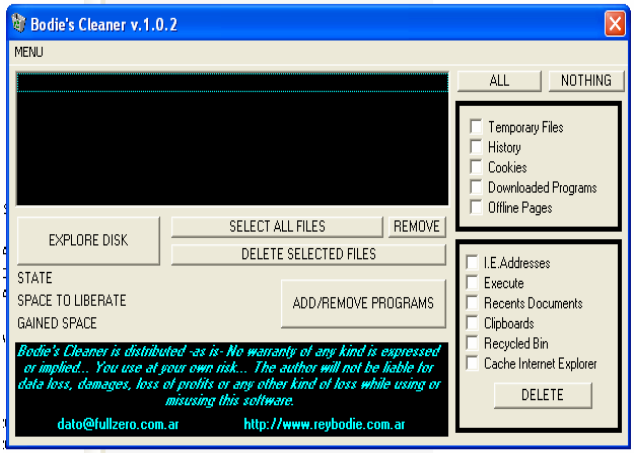


Figura 7.18 Ambiente de Bodies Cleaner.

Process Explorer 10.06: Es una utilidad que con una interfaz muy similar a la del Explorador de Windows, muestra todos los procesos y tareas activas que se están ejecutando en un momento dado. La interfaz muestra las aplicaciones que se están ejecutando y las librerías que cada una de ellas ha abierto. El programa incorpora un potente motor de búsqueda que puede localizar qué proceso tiene cierta librería en concreto.

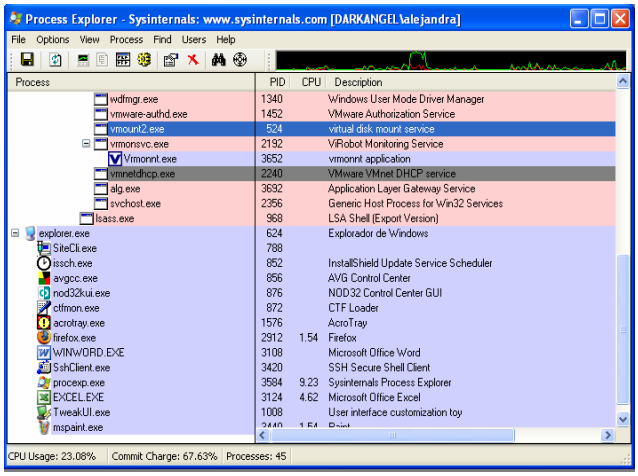


Figura 7.19 Ambiente Process Explorer

Las modificaciones y ajustes de la Seguridad serán realizas a la brevedad posible, por lo cual se pide tomar las consideraciones antes mencionadas, existen ajustes que requerirán ser implementadas a corto y otras a largo plazo, así, se requiere paciencia e inversión.

Los objetivos de las pruebas realizadas fueron valorar y detectar las vulnerabilidades que existían en la red y en general en equipos cliente, así como Servidores de aplicaciones.

Por otra parte es necesario fortalecer y actualizar las medidas y procedimientos aquí utilizados ya que el continuo avance tecnológico tanto en Hardware como en Software podría llegar a rebasar ampliamente los esfuerzos realizados en este trabajo.

CONCLUSIONES

Para la realización de este tema con llevo a encontrar toda una serie de información, lo importante aquí fue documentar la apropiada para sustentar este trabajo, por lo cual muchos de los conceptos teóricos debían estar bien fundamentados con el fin de aportar los conocimientos para la realización propia del tema.

Por lo tanto para estar al día con la tecnología así como las nuevas visiones tuve que tomar diferentes cursos que solventaran el conocimiento de ciertas herramientas que eran factibles de utilizar, además de ir a congresos de seguridad para fundamentar los conceptos propuestos en esta tesis, llevándome a tener un panorama mas amplio y actual, esto debido a que como se menciono con anterioridad la seguridad es relativa y dinámica, con la finalidad conocer más enfoques llevo a encontrar nuevas posibilidades de implementación.

Se realizó un análisis de las arquitecturas de seguridad que manejaban empresas en el conocimiento de seguridad, modelos, planes, protocolos, consistencia de políticas, bitácoras, auditorías y tanto en aspectos legales que engloban a la seguridad, me proporcionaron así nuevos lineamientos con base a nuevas preguntas y elementos necesarios para desarrollar una arquitectura bajo una base sólida.

A su vez tomando como base una arquitectura se rediseño para adaptarla a lo que había sido el planteamiento de mi problemática, dando pauta a un diagrama que proporcionara en general una base para ser implementada en demás casos.

Uno de los retos a los que me tuve que enfrentar es a las nuevas pruebas que se realizaban sobre las herramientas tecnológicas que aportaba el mercado muchas veces por falta de licencias o solo se podía contar con una versión de prueba de ellas, por lo cual en ocasiones fue complicado la documentación acerca de su funcionamiento.

En momentos se presentaban nuevas tecnologías o nuevas amenazas que tenían que ser replanteadas debido al dinamismo que presenta la seguridad, uno de los problemas que fueron de los mas difíciles de solventar y que aun en día presenta dificultad es el llevar la concientización de el rol de cada uno de los miembros de la organización, por la cual el llevar acabo un plan de tal magnitud seguirá llevando tiempo, pero en este punto se llego a la conclusión de que una concientización y entrenamiento adecuado equivale más del 50% del éxito al implementar las medidas u otros aspectos en la seguridad, esto es debido a que la gente es el factor mas vulnerable en todo este entorno

El análisis que con llevo a tener un problema en particular, me permitió tener una base teórica fundamentada en conceptos que permitieran llevar lo documentado a un problema real, por lo cual al realizar el análisis se tomaron en cuenta derivaciones de la misma para tener un mejor control del análisis global, se definió claramente cual era en este caso el objetivo primordial de la organización, para dar un análisis valuativo de todos los activos considerados. Tanto los análisis de hardware, software y de la red física en conjunto con herramientas que se utilizaron para realizar dichos análisis; arrojaron la información suficiente para llevar acabo una definición más exacta de las vulnerabilidades que se presentaron, pero todo este análisis me permitieron especificar punto por punto que pasos debían ser tomados, el diagrama mencionado en el capítulo 3, se tomo como base para realizar las modificaciones pertinentes adecuándose a las necesidades establecidas, pero además adecuarlo a ser utilizado de manera base para otros

casos. Utilicé la estrategia, criterios, procedimientos y políticas ha ser implementadas, tomando lo anterior mencionado, por lo que se puede decir que la parte teórica como la parte de herramientas (Software) me permitieron llegar hasta este punto. Concluyendo una buena arquitectura o diagrama será la base para tomar todos los elementos del entorno llevarlos hacia un análisis de riesgos, el cual proporcionará las estrategias, procedimientos, políticas, medidas, criterios que fundamentaran el construir una seguridad a la medida que responda a las necesidades.

Al realizar todo el análisis me permitió llevar acabo las medidas y procedimientos, para realizar la implementación, definir los procedimientos de seguridad, las políticas de respaldo que deberían ser tomadas en cuenta, los mantenimientos tanto físico como lógico del equipo. Además de poder implementar una herramienta que permitiera automatizar actualizaciones por lo cual documente tanto el procedimiento como las características de la herramienta a utilizar. Uno de los puntos importantes fue implementar un firewall y adecuar la configuración a las necesidades que se establecieron en el análisis.

Esté trabajo me permitió realizar las pruebas tanto en el análisis para evaluar las herramientas que estaba utilizando, así como, después de implementar todos las medidas necesarias que se habían encontrado, por lo cual los escaneos tanto a la red, como a servidores y puertos arrojaron información valiosa del comportamiento que tenia la misma, por lo cual se observo que ciertas herramientas no eran muy funcionales y se tenían que descartar, buscando nuevas herramientas que cubrieran de manera funcional lo que se pretendía implementar. Realice modificaciones y revisiones constantes llevando a una auditoría, revisando bitácoras que sirvieron para encontrar nuevos fallos que se habían pasado por alto, en esta etapa fue una en donde el tiempo invertido fue mayor que en las demás, debido al cuidado en la utilización y funcionalidad de los criterios, procedimientos, medidas, políticas y herramientas implementadas. Concluyendo las pruebas y resultados arrojaron las herramientas de seguridad, procedimientos, estrategias, políticas, etc; solventan de manera adecuada la seguridad que se requiere ante las necesidades de la organización. Las revisiones darán la pauta a iniciar el ciclo de nuevo y encontrar las posibles fallas de la implementación.

Finalmente, se puede establecer que el objetivo fundamental de este proyecto de proporcionar medidas de seguridad un centro de cómputo que ofrece los servicios de una red local, así como servicios de Internet. Obtendrá una mejoría considerable en la seguridad del equipo de cómputo ya que las vulnerabilidades más importantes han sido protegidas. Además se nos facilitará el manejo y administración del mismo ya que tendremos un mayor control del ámbito de la red y los equipos.

Empleando herramientas, técnicas, metodologías y políticas de seguridad obtendremos muchos beneficios, y así resolver la problemática de seguridad que se presenta en toda Sala de cómputo que proporciona servicio. En nuestro caso particular se fortaleció la seguridad en todos los aspectos en la Unidad de Servicios de Cómputo Académico (UNICA), no obstante la Facultad de Ingeniería ha creado una área de seguridad que ofrece sus servicios a todas las Divisiones que la conforman, capacitando a su personal y preocupándose por mejorar cada día para mejorar en todos los aspectos.

La enseñanza que obtuve de manera personal es que la carrera de Ingeniería en Computación tiene un campo muy amplio de trabajo y requiere de capacitación continua en aspectos de administración de servidores, manejo de herramientas para el desarrollo de aplicaciones, seguridad en informática y en general capacitar y concienciar a la gente que utiliza una computadora. Además de proporcionar la satisfacción de ser mejor un mejor profesional y persona cada día.

APÉNDICE

Apéndice I

DNS (Sistema de Nombres de Dominio)

DNS es una abreviatura para sistema de nombres de dominio (Domain Name System), un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP.

Por ejemplo, la mayoría de los usuarios prefieren un nombre descriptivo, fácil de utilizar, como *ejemplo.microsoft.com* para localizar un equipo (como un servidor Web o de correo electrónico) en la red. Un nombre descriptivo resulta más fácil de aprender y recordar. Sin embargo, los equipos se comunican a través de una red mediante direcciones numéricas. Para facilitar el uso de los recursos de red, los sistemas de nombres como DNS proporcionan una forma de asignar estos nombres descriptivos de los equipos o servicios a sus direcciones numéricas.

La siguiente figura muestra un uso básico de DNS, consistente en la búsqueda de la dirección IP de un equipo basada en su nombre.

Figura 1 Uso básico de DNS

En este ejemplo, un equipo cliente consulta a un servidor DNS, preguntando la dirección IP de un equipo configurado para utilizar host-a.ejemplo.microsoft.com como nombre de dominio. Como el servidor puede utilizar la base de datos local para responder la consulta, contesta con una respuesta que contiene la información solicitada, un registro de recursos de host (A) que contiene la información de dirección IP para host-a.ejemplo.microsoft.com.

Herramientas de DNS

Existe una serie de programas para administrar, supervisar y solucionar los problemas de los clientes y los servidores DNS. Entre estos programas se cuentan:

- La consola DNS, que forma parte de las Herramientas administrativas.
- Programas de la línea de comandos, como Nslookup, que se pueden utilizar para solucionar problemas de DNS.
- Características de registro, como el registro del servidor DNS, que se pueden ver mediante la consola DNS o el Visor de sucesos. Los registros basados en archivos se pueden usar también temporalmente como una opción de depuración avanzada para registrar y hacer un seguimiento de los sucesos de servicio seleccionados.
- Programas de supervisión del rendimiento, como los contadores de estadísticas para medir y supervisar la actividad del servidor DNS con el monitor del sistema.
- Instrumental de administración de Windows (WMI), una tecnología estándar para obtener acceso a información de administración en un entorno empresarial.
- El kit de desarrollo de software (SDK) de la plataforma.

Nombres de dominio DNS

El sistema de nombres de dominio (DNS) se definió originalmente en los RFC 1034 y 1035. Estos documentos especifican elementos comunes a todas las implementaciones de software relacionadas con DNS, entre los que se incluyen:

- Un espacio de nombres de dominio DNS, que especifica una jerarquía estructurada de dominios utilizados para organizar nombres.
- Los registros de recursos, que asignan nombres de dominio DNS a un tipo específico de información de recurso para su uso cuando se registra o se resuelve el nombre en el espacio de nombres.
- Los servidores DNS, que almacenan y responden a las consultas de nombres para los registros de recursos.
- Los clientes DNS, también llamados solucionadores, que consultan a los servidores para buscar y resolver nombres de un tipo de registro de recursos especificado en la consulta.

Descripción del espacio de nombres de dominio DNS

El espacio de nombres de dominio DNS, como se muestra en la ilustración siguiente, se basa en el concepto de un árbol de dominios con nombre. Cada nivel del árbol puede representar una rama o una hoja del mismo. Una rama es un nivel donde se utiliza más de un nombre para identificar un grupo de recursos con nombre. Una hoja representa un nombre único que se utiliza una vez en ese nivel para indicar un recurso específico.

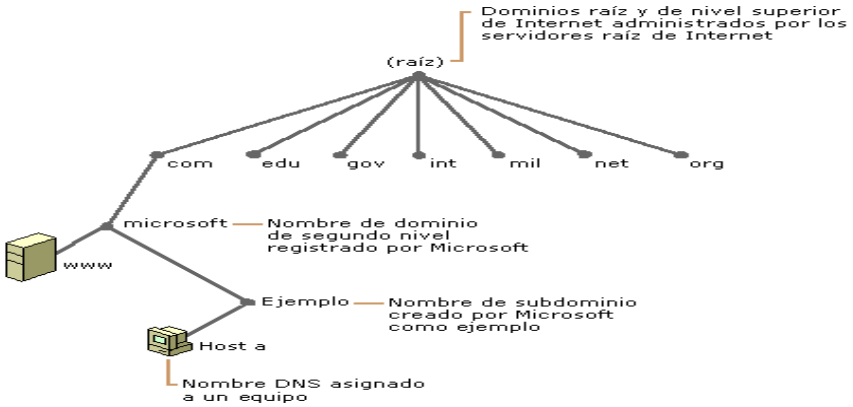


Figura 2 Descripción de espacio de nombres

En este ejemplo muestra cómo Microsoft es la autoridad asignada por los servidores raíz de Internet para su propia parte del árbol del espacio de nombres de dominio DNS en Internet. Los clientes y servidores DNS usan las consultas como método fundamental para resolver los nombres del árbol como información específica de los tipos de recurso. Los servidores DNS proporcionan esta información a los clientes DNS en las respuestas a las consultas, quienes, a continuación, extraen la información y la pasan al programa que la solicita para resolver el nombre consultado.

En el proceso de resolución de un nombre, tenga en cuenta que los servidores DNS funcionan a menudo como clientes DNS, es decir, consultan a otros servidores para resolver completamente un nombre consultado.

Diseño del espacio de nombres para DNS

Antes de empezar a utilizar DNS en la red, se debe hacer un plan para el espacio de nombres del dominio DNS. Realizar un plan para el espacio de nombres implica tomar algunas decisiones relativas a cómo pretende utilizar los nombres DNS y cuáles son sus objetivos al utilizar DNS. Algunas de las preguntas que le pueden surgir en esta fase son las siguientes:

- ¿Se ha elegido y registrado un nombre de dominio DNS para el uso de Internet?
- ¿Se van a configurar servidores DNS en una red privada o en Internet?
- ¿Se va a utilizar DNS como ayuda para utilizar Active Directory?
- ¿Cuáles son los requisitos de nombres necesarios al elegir los nombres de dominio DNS de los equipos?

Planeamiento de los servidores para DNS

Cuando se realice planes para los servidores DNS, es importante que se tenga en cuenta lo siguiente:

- Realizar un plan de capacidad y revisar los requisitos de hardware del servidor.
- Determinar cuántos servidores DNS se necesitan y su función en la red.

- Cuando se decida el número de servidores DNS que se va a utilizar, se debe considerar qué servidores alojarán las copias principal y secundaria de las zonas. Además, si se utiliza Active Directory, determinar si el equipo del servidor funcionará como controlador de dominio o como servidor miembro del dominio.
- Decidir dónde se va a situar los servidores DNS en la red para las cargas de tráfico, la duplicación y la tolerancia a errores.
- Decidir si se va a utilizar sólo servidores DNS que ejecuten Windows Server 2003 para todos los servidores DNS o si va a trabajar con una combinación de Windows y otras implementaciones de servidor DNS.

Plan de la capacidad del servidor

El plan y la distribución de los servidores DNS en la red con lleva el examen de varios aspectos de la red y de los requisitos de capacidad de cualquier servidor DNS que vaya a utilizar en ella. Algunas de las preguntas que debe considerar cuando realice el plan son las siguientes:

- ¿Cuántas zonas se espera que cargue y aloje el servidor DNS?
- ¿Qué tamaño debe tener cada zona que cargue el servidor para el servicio? (Según el tamaño del archivo de la zona o en el número de registros de recursos utilizados en dicha zona).
- En un servidor DNS de hosts múltiples, ¿cuántas interfaces se van a habilitar para escuchar y servir a los clientes DNS en cada una de las subredes conectadas al servidor?
- ¿Cuántas peticiones de consulta DNS globales o totales de todos los clientes se espera que reciba y sirva un servidor DNS?

Migrar servidores

La migración DNS puede ocurrir de alguna de las maneras siguientes:

- Al actualizar un equipo que ejecute la versión de DNS incluida en Windows NT Server 4.0 o Windows 2000 a un servidor que ejecute Windows Server 2003.
- Al mover archivos de zona de un servidor DNS existente que ejecuta otra implementación del servidor DNS, como un servidor que ejecuta una versión del software Dominio de nombres Internet de Berkeley (BIND, Berkeley Internet Name Domain).
- Al migrar zonas con una transferencia de zonas principal-secundaria de servidores BIND a servidores DNS que ejecutan Windows Server 2003.

Administración de DNS

Se deberán tomar los siguientes elementos dentro de la administración:

- Administrar servidores DNS.
- Administrar clientes.
- Administrar zonas.
- Supervisar y optimizar servidores

Recursos de DNS

Se deberán tomar los siguientes elementos dentro de recursos de DNS:

- Referencia de los registros de recursos.
- Referencia de registros del servidor DNS.
- Archivos relacionados con DNS.
- Información técnica actualizada de DNS.
- RFC de DNS.
- Dominios de Nivel superior.

Apéndice II

Active Directory

Introducción

Un directorio es una estructura jerárquica que almacena información acerca de los objetos existentes en la red. Un servicio de directorio, como Active Directory, proporciona métodos para almacenar los datos del directorio y ponerlos a disposición de los administradores así como de los usuarios de la red. Por ejemplo, Active Directory almacena información acerca de las cuentas de usuario (nombres, contraseñas, números de teléfono, etc.) y permite que otros usuarios autorizados de la misma red tengan acceso a esa información.

El servicio de directorio de Active Directory se puede instalar en servidores que ejecuten Microsoft Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition y Windows Server 2003, Datacenter Edition. Active Directory almacena información sobre los objetos de la red y facilita la búsqueda, así como su utilización de esta información para los usuarios y administradores. Active Directory utiliza un almacén de datos estructurado como base para una organización lógica y jerárquica de la información del directorio.

La seguridad está integrada en Active Directory mediante la autenticación del inicio de sesión y el control de acceso a los objetos del directorio. Con un único inicio de sesión en la red, los administradores pueden administrar datos del directorio y de la organización en cualquier punto de la red, y los usuarios autorizados de la red pueden tener acceso a recursos en cualquier lugar de la red. La administración basada en directivas facilita la tarea del administrador incluso en las redes más complejas.

Active Directory también incluye:

- Un conjunto de reglas, el esquema, que define las clases de objetos y los atributos que contiene el directorio, así como las restricciones y los límites en las instancias de estos objetos y el formato de sus nombres.
- Un catálogo global que contiene información acerca de cada uno de los objetos del directorio. Esto permite a los usuarios y administradores encontrar información del

directorio con independencia de cuál sea el dominio del directorio que realmente contiene los datos.
- Un sistema de índices y consultas, para que los usuarios o las aplicaciones de red puedan publicar y encontrar los objetos y sus propiedades.
- Un servicio de replicación que distribuye los datos del directorio por toda la red. Todos los controladores de un dominio participan en la replicación y contienen una copia completa de toda la información del directorio para su dominio. Cualquier cambio en los datos del directorio se replica en todos los controladores del dominio.
- Compatibilidad con el software de cliente de Active Directory, lo que permite que muchas de las características de Microsoft Windows 2000 Professional o Windows XP Professional también estén disponibles en los equipos que ejecutan Windows 95, Windows 98 y NT Server 4.0. En los equipos que no ejecutan el software de cliente de Active Directory, el directorio tendrá el mismo aspecto que un directorio de Windows NT.

Descripción de Active Directory

Active Directory es una implementación de los protocolos de nombres y directorios estándar de Internet. Utiliza un motor de bases de datos para procesar las transacciones y es compatible con diversos estándares de interfaces de programación de aplicaciones.

En este punto se trataran los siguientes elementos:

- Protección de Active Directory.
- Control de acceso en Active Directory.
- Uso de nombres en Active Directory.
- Almacén de datos del directorio.
- Protocolo de acceso al directorio.
- Cuentas de usuarios y equipos.
- Nombres de objeto.
- Unidades organizativas.
- Funciones de servidor de Active Directory.
- Clientes de Active Directory.
- Descripción de dominios y bosques.
- Descripción de los grupos.
- Descripción de las confianzas.
- Descripción de los sitios y la replicación.
- Descripción del catálogo global.
- Intercalar con DNS y Directiva de grupo.
- Descripción del esquema.

Implementación de Active Directory

En este punto de la implementación se toman en cuenta los siguientes elementos:

- Recursos de implementación.
- Utilizar el Asistente para instalación de Active Directory.
- Crear un controlador de dominio adicional.
- Crear un nuevo árbol de dominios.
- Crear un nuevo dominio secundario.
- Crear un nuevo bosque.
- Actualización.

Administrar Active Directory

En este punto de administración se toman en cuenta los siguientes elementos:

- Utilizar Ejecutar como.
- Utilizar consultas guardadas.
- Administrar Active Directory desde la consola de administración.
- Administrar Active Directory desde la línea de comandos.
- Buscar información del directorio.
- Administrar otros dominios.
- Delegar la administración.
- Publicar recursos.
- Administrar particiones COM+ en Active Directory.
- Administrar conjuntos de particiones COM+ en Active Directory.

Recursos de Active Directory

En este punto de recursos se toman los siguientes elementos:

- Recursos Web.
- Herramientas de soporte de Active Directory.
- Interfaces de programación.

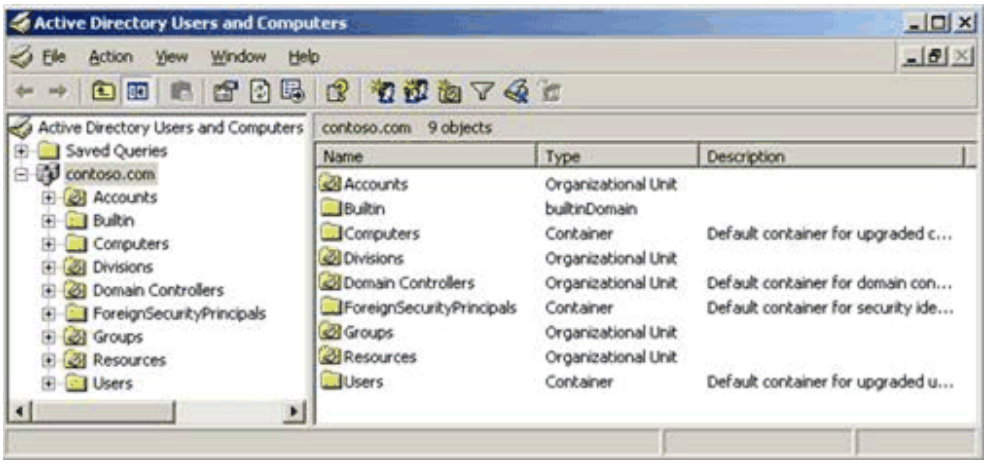


Figura 1 usuarios y grupos del Active Director.

Apéndice III

Instalación de DNS (Sistema de Nombres de Dominio) y Active Directory

1. Se hace clic en el botón Inicio y en Ejecutar, se escribe DCPROMO y, a continuación, se hace clic en Aceptar.
2. Cuando aparezca el Asistente para instalación de Active Directory, se hace clic en Siguiente para iniciar la instalación.
3. Después de revisar la información de Compatibilidad de sistema operativo, se hace clic en Siguiente.
4. Se selecciona la opción de Controlador de dominio para un dominio nuevo (opción predeterminada si así se desea, ó alguna de las opciones que aparecen en la misma pantalla) y, a continuación, se hace clic en Siguiente.
5. Se selecciona Dominio en un nuevo bosque (opción predeterminada o dependiendo de lo que requiera la organización) y, a continuación, se hace clic en Siguiente.
6. Para Nombre DNS completo, se escribe como en el siguiente ejemplo (nuevo.com) y, después, se hace clic en Siguiente. (Esta opción representa un nombre completo.).
7. Se hace clic en Siguiente para aceptar la opción predeterminada Nombre NetBIOS del dominio de ejemplo (NUEVO). (El nombre NetBIOS proporciona compatibilidad de bajo nivel.)
8. En la pantalla Carpetas de la base de datos y del registro, se establece la Carpeta de registro de Active Directory de forma que apunte a la carpeta en donde se quiera tener la base de datos y del registro como lo muestra el ejemplo (C:\Windows\NTDS) y, a continuación, se hace clic en Siguiente para continuar.
9. Se deja la ubicación de la carpeta predeterminada para Volumen del sistema compartido y, después, se hace clic en Siguiente.
10. En la pantalla de Diagnósticos de registro de DNS, se hace clic en Instalar y configurar el servidor DNS en este equipo. Se hace clic en Siguiente para continuar.
11. Se selecciona Permisos compatibles sólo con sistemas operativos de servidor Windows 2000 o Windows Server 2003 (opción predeterminada o si en el caso en que se tenga sistemas operativos inferiores se selecciona la otra opción) y, a continuación, se hace clic en Siguiente.
12.Se escribe la contraseña para Contraseña de modo de restauración y Confirmar contraseña y, después, se hace clic en Siguiente para continuar.
13. En la siguiente pantalla representa un resumen de las opciones de instalación de Active Directory. Se hace clic en Siguiente para iniciar la instalación de Active Directory. Si se indica, insertar el CD de instalación de Windows Server 2003.
14. Se hace clic en Aceptar para confirmar la advertencia de que se va a asignar una dirección IP de forma dinámica a un servidor DNS o en su defecto ya haber sido asignado una dirección IP configurada previamente en Conexiones de Red.
18. Se hace clic en Finalizar cuando termine el Asistente para instalación de Active Directory.
19. Se hace clic en Reiniciar ahora para reiniciar el equipo.

Apéndice IV

Zona Directa y Zona Inversa del DNS (Sistema de Nombre de Dominios)

1. Se abre el servidor DNS, para lo cual se accede al "Panel de Control", se hace doble clic sobre el icono "Herramientas Administrativas" y una vez allí haremos doble clic sobre el icono "DNS", mostrándose la siguiente ventana:

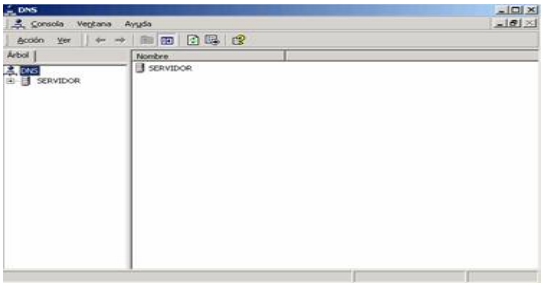


Figura 1

2. A continuación se va a definir una nueva zona de búsqueda directa, para lo cual se dará clic sobre el botón derecho del ratón en dicha carpeta y se seleccionará la opción "Crear una zona nueva".

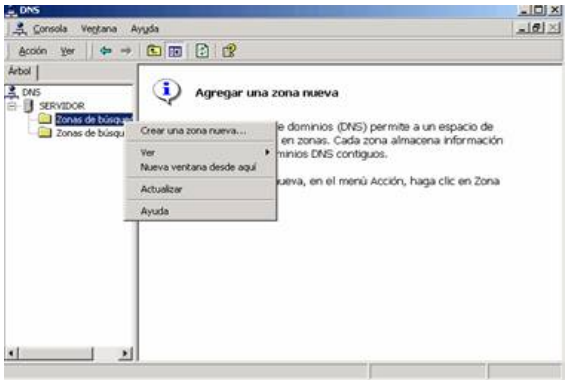


Figura 2

3. La primera pantalla que se muestra es la del asistente de creación de nueva zona; se da clic sobre el botón "Siguiente" para continuar con la definición de la nueva zona directa.

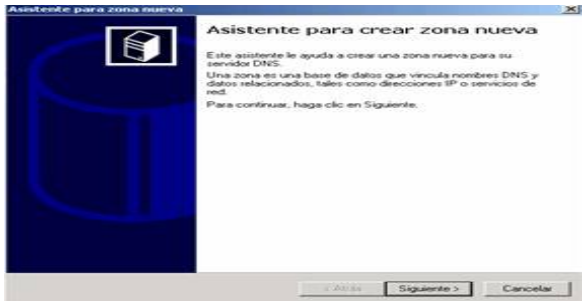


Figura 3

4. En la siguiente pantalla de instalación, se deberá seleccionar el tipo de zona que desea crear; se activara la primera de ellas para que la nueva zona a definir quede integrada en el Directorio Activo (Active Directory).

Figura 4

5. A continuación se debe indicar el nombre que se va a asignar a la nueva zona definida; dado que el servidor DNS va a resolver el nombre de dominio, indicamos éste como nombre de la zona a gestionar.

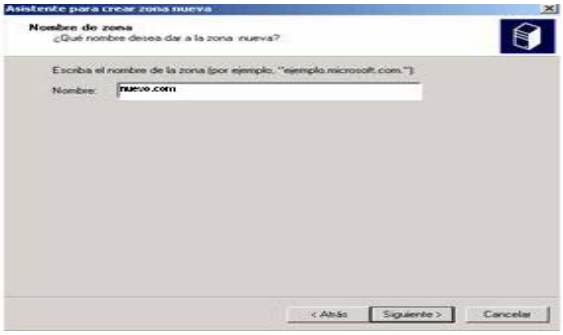


Figura 5

6. Para concluir la definición de la nueva zona creada, se hace clic sobre el botón "Finalizar".

Figura 6

De esta manera se puede observar que la nueva zona de búsqueda directa ya ha sido creada en el servidor DNS.

1. Posteriormente se definirá una nueva zona de búsqueda inversa haciendo clic con el botón derecho del ratón sobre la carpeta correspondiente y seleccionando la opción "crear una zona nueva".

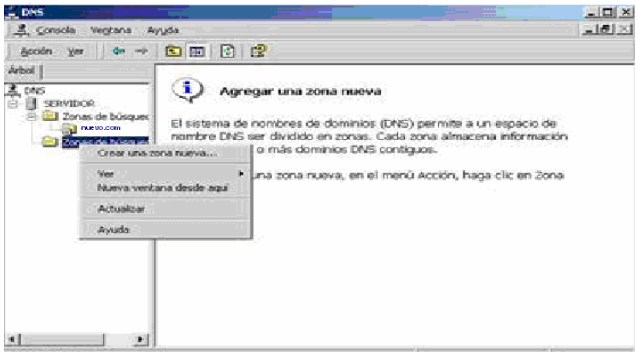


Figura 7

2. De nuevo saldrá la pantalla del asistente de creación de zona nueva; se hace clic sobre la opción "Siguiente".

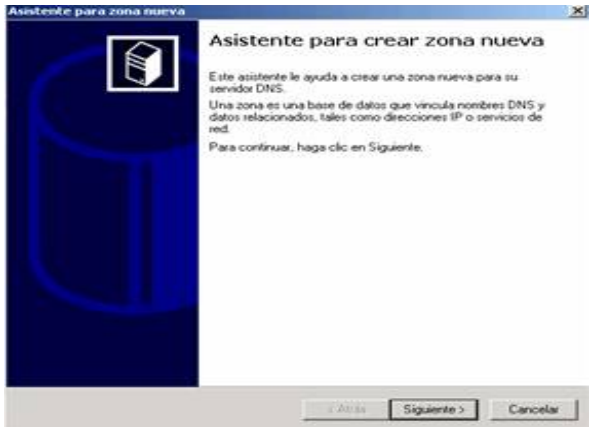


Figura 8

3. En la siguiente pantalla, de nuevo se seleccionará la opción "Active Directory integrado".

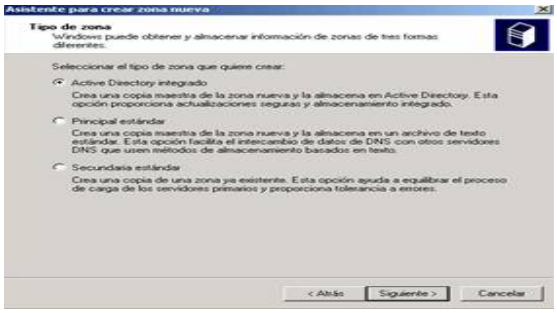


Figura 9

4. A continuación debemos especificar la zona de búsqueda inversa que deberá resolver el servidor DNS; se indica el identificativo de red para ejemplo "192.168.0", para que el servidor DNS haga resolución inversa de cualquier dirección I.P. "192.168.0.x"; cuando se complete dicha "id de red", se observa que en "Nombre de la zona de búsqueda inversa" se mostrará el nombre "0.168.192.in-addr.arpa".

Figura 10

5. Finalmente se muestra la pantalla resumen de creación de la nueva zona de búsqueda inversa; pulsaremos sobre el botón "Finalizar" para completar la creación de dicha zona.

Figura 11

Tras completarse la instalación de la nueva zona de búsqueda inversa, se observa en la ventana de administración del servidor DNS, que la nueva zona ya ha sido creada correctamente. Así mismo, en dicha ventana se observa que ya existe una entrada que ha sido incluida automáticamente en el servidor DNS, en la zona de búsqueda directa para ejemplo seria “nuevo.com", que apunta a 192.168.0.220; esta resolución es la correspondiente al nombre que se le ha asignado al servidor.

6. Para finalizar la configuración del servidor DNS, se deberá indicar que cuando las estaciones de trabajo intenten resolver URLs que no pertenezcan a la red local (y que por tanto no sea capaz a resolver el servidor DNS), reenvíe dichas peticiones a otros servidores DNS (que estén en Internet) que sí puedan resolverlas. Para ello se habrá que ubicar sobre el nombre del servidor DNS, se hace clic con el botón derecho del ratón, y se selecciona la opción "Propiedades".

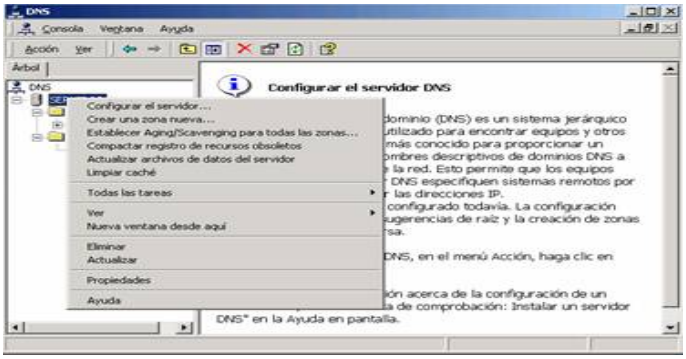


Figura 12

7. En la ventana que aparece a continuación, se selecciona la pestaña "Reenviadores", y una vez allí se activa la casilla "Habilitar reenviador(es)", y posteriormente se agrega las direcciones IP como ejemplo ("195.55.30.16" y "194.179.1.101") pertenecientes a servidores DNS públicos, tal y como se muestra en la siguiente figura.

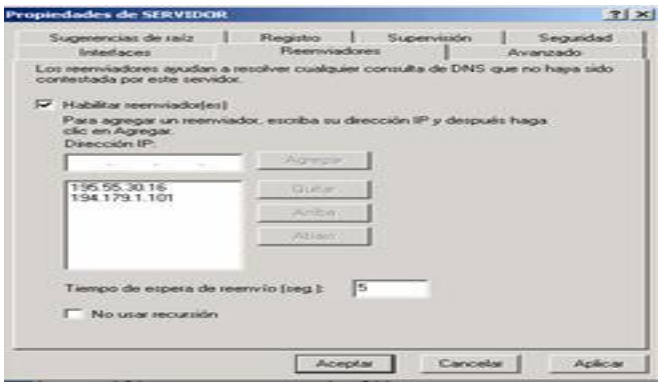


Figura 13

8. A partir de este momento ya se tiene configurado el servidor DNS.

GLOSARIO

Glosario

Active Directory: Es una estructura jerárquica que almacena información acerca de los objetos existentes en la red. Un servicio de directorio, como Active Directory, proporciona métodos para almacenar los datos del directorio y ponerlos a disposición de los administradores así como de los usuarios de la red.

Bitnet: Antigua red internacional de computadoras de centros docentes y de investigación que ofrecía servicios interactivos de correo electrónico, así como de transferencia de ficheros utilizando un protocolo de almacenaje y envío basado en los protocolos Network Job Entry de IBM. Se conectaba a Internet a través de una pasarela de correo electrónico.

Intranet: Es una red de computadoras privada basada en los estándares de Internet. Las Intranets utilizan tecnologías de Internet para enlazar los recursos informativos de una organización, desde documentos de texto a documentos multimedia, desde bases de datos legales a sistemas de gestión de documentos. Las Intranets pueden incluir sistemas de seguridad para la red, tablones de anuncios y motores de búsqueda. Una Intranet puede extenderse a través de Internet. Esto se hace generalmente usando una **red privada virtual (VPN)**.

Extranet: Es una red privada virtual resultante de la interconexión de dos o más intranets que utiliza Internet como medio de transporte de la información entre sus nodos.

DNS (Sistema de Nombres de Dominio): Un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos. Cuando un usuario escriba un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP.

Dominio: Conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios.

Firewall: Un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los Firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente Intranets. Todos los mensajes que dejan o entran a la red pasan a través del Firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad.

FTP (File Transfer Protocol): Protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos.

Funciones Hash

La criptografía asimétrica permite identificar al emisor y al receptor del mensaje. Para identificar el mensaje propiamente dicho se utilizan las llamadas funciones *Hash*. El resultado

de aplicar una función Hash a un texto es un número grande, el número hash, que tiene las siguientes características:

Características:

- Todos los números hash generados con un mismo método tienen el mismo tamaño sea cual sea el texto utilizado como base.
- Dado un texto base, es fácil y rápido calcular su número hash.
- Es imposible reconstruir el texto base a partir del número hash.
- Es imposible que dos textos base diferentes tengan el mismo número hash.

Geteway: Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red.

Host (Sistema Central): Computadora que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP.

HTTP Protocolo de Transferencia de Hipertextos (Hiper-Text Transfer Protocol): Es el protocolo usado por el Word Wide Web para transmitir páginas HTML.

IMAP: Protocolo de Acceso a Mensajes de Internet (Internet Message Access Protocol). Protocolo diseñado para permitir la manipulación de mailboxes remotos como si fueran locales. IMAP requiere de un servidor que haga las funciones de oficina de correos pero en lugar de leer todo el mailbox y borrarlo, solicita sólo los encabezados de cada mensaje. Se pueden marcar mensajes como borrados sin suprimirlos completamente, pues estos permanecen en el mailbox hasta que el usuario confirma su eliminación.

MEILBOX: Área de un servidor de correo electrónico en la cual un usuario puede dejar o recoger sus mensajes.

Malware (software malicioso): Es un software que tiene como objetivo infiltrarse en o dañar una computadora sin el conocimiento de su dueño.

Existen muchísimos tipos de malware, aunque algunos de los más comunes son los virus informáticos, los gusanos, los troyanos, los programas de spyware/adware o incluso los bots. Dos tipos comunes de malware son los *virus* y los *gusanos* informáticos, este tipo de programas tienen en común la capacidad para auto replicarse, es decir, pueden contaminar con copias de sí mismo que en algunas ocasiones ya han mutado, la diferencia entre un gusano y un virus informático radica en que el gusano opera de forma más o menos independiente a otros archivos, mientras que el virus depende de un portador para poderse replicar.

POP Protocolo de Oficina de Correos (Post Office Protocol): Programa cliente que se comunica con el servidor, identifica la presencia de nuevos mensajes.

Puente (Bridge). Conecta entre sí dos segmentos de red que pueden ser diferentes. A diferencia del repetidor, el puente resulta bastante “inteligente” para filtrar el tráfico de información entre los segmentos.

Ruteador (Router). Dispositivos que gestionan el tráfico de paquetes que proviene del exterior de la red y se dirige al interior (y al revés). Un Ruteador (Router) ayuda a la unión de dos redes a nivel capa 3, pueden ser dispositivos muy sofisticados y capaces de actuar en calidad de cortafuego (Firewall).

SMTP (Simple Mail Transfer Protocol) Protocolo de Transferencia Simple de correo: Es el protocolo usado para transportar el correo a través de Internet.

TCP (Transmission Control Protocol) Protocolo de control de Transmisión: Uno de los protocolos más usados en Internet. Es un protocolo de capa de transporte.

TCP/IP (Transmission Control Protocol/Internet Protocol): Arquitectura de red desarrollada por la "Defense Advanced Research Projects Agency" en USA, es el conjunto de protocolos básicos de Internet o de una Intranet.

Telnet: Telnet es el protocolo estándar de Internet para realizar un servicio de conexión desde una terminal remota. Está definido en STD 8, RFC 854 y tiene opciones adicionales descritas en muchos otros RFC’s.

UDP Protocolo de Datagramas de usuario (User Datagram Protocol): Protocolo que no pide confirmación de la validez de los paquetes enviados por la computadora emisora. Este protocolo es actualmente usado para la transmisión de sonido y vídeo a través de Internet. El UDP está diseñado para satisfacer necesidades concretas de ancho de banda, como no reenvía los datos perdidos, es ideal para el tráfico de voz digitalizada, ya que es un paquete perdido que no afecta la calidad del sonido.

URL Localizador Uniforme de recursos (Uniform Resource Locator): Sistema de direccionamiento estándar para archivos y funciones de Internet, especialmente en el Word Wide Web.

BIBLIOGRAFÍA Y MESOGRAFÍA

Bibliografía

TANENBAUM, Andrew S.
Redes de Computadoras
4ª. Edición, México; Pearson Educación, 2003

STALLINGS, William
Comunicaciones y Redes de Computadoras
6ª. Edición, España; Prentice Hall, 2000

LEÓN-GARCÍA, Alberto; WIDJAJA, Indra
Redes de Comunicación. Conceptos Fundamentales y Arquitecturas Básicas
España; McGraw-Hill, 2002

COMER, Douglas E.
Internetworking with TCP/IP Client server Programing and applications, Windows Socket Version Vol. III
3th edition, U.S.A.; Prentice Hall, 1997

GRAHAM, Buck
TCP/IP Addressing. Designing and Optimizing your IP addressing scheme
2nd edition, USA; Morgan Kaufmann, 2001

FINE, Leonard H.
Seguridad en Centros de Cómputo. Políticas y fundamentos
2a. edición, México; Trillas, 1997

LUTHAN S, Fred
Organizational Behavior
8th edition, U.S.A.; McGraw – Hill, 1998

CHESWICK, William R.; BELLOVIN, Steven M.
Firewall and Internet Security
U.S.A.; Addison-Wesley, 1994

HUNT, Craig
TCP/IP Network Administration
3th edition, U.S.A.; O'Reilly & Associates Inc., 2002

FOGIE, Seth; PEIK ARI, Cyrus
Maximum Wireless Security
U.S.A.; Sams Publishing, 2002

FACCIN, Stefano
IP in Wireless Networks
U.S.A.; Prentice Hall, 2003

SUMMERS, Rita
Secure Computing, Threats and Safeguards
U.S.A.; McGraw Hill, 1997

LOPEZ, Jaquelina; QUEZADA, Cintia
Apuntes de Seguridad Informátic*a*
México; Facultad de Ingeniería – UNAM, 2005

BELLOVIN, Steven, et al.
Firewalls and Internet Security: Repelling the Wily Hacker
2th edition, U.S.A.; Addison Wesley, 2003

MAIWALD, Eric
Fundamentos de Seguridad en Redes
México; Mc Graw-Hill, 2004

MCNAB, Chris
Seguridad de Redes
México; Anaya multimedia, 2004

Mesografía

http://www.saulo.net/

http://www.iec.uia.mx/proy/titulacion/proy14/seguridad.htm

http://webs.ono.com/usr016/Agika/4diccionario/diccionario.htm

http://www.mailxmail.com/curso/informatica/delitosinformaticos/capitulo21.htm

http://www.ulfix.com/index.php?option=com_content&task=view&id=472

http://www.us-cert.gov

http://www.cert.org/stats/cert_stats.html

http://webs.ono.com/usr016/Agika/3internet/seg_internet.htm

http://seguridad.uach.mx/noticias/n05072004-03.html

http://club.telepolis.com/morenocerecero/seguridad.html

http://www.unam-cert.unam.mx

http://www.infoal.com/portal/continguts/opinions/SEGURIDAD.htm

http://www.eumed.net/cursecon/ecoinet/seguridad/

http://www.eumed.net/cursecon/ecoinet/seguridad/cortafuegos.htm

http://www.eumed.net/cursecon/ecoinet/seguridad/reglas.htm

http://webs.ono.com/usr016/Agika/3internet/seg_internet.htm

http://webs.ono.com/usr026/Agika2/3internet/ataques.htm

http://webs.ono.com/usr026/Agika2/3internet/puertos.htm

http://www.consumer.es/web/es/economia_domestica/tus_derechos/comercio_electronico/2002/04/04/40763.php

http://www.unap.cl/index.pl?iid=3442

http://www.unap.cl/index.pl?iid=3442

http://www.interclan.net/fenasem/LEXMATIC/Articul.htm

http://www.segu-info.com.ar/logica/accesoexterno.htm

http://www.microsoft.com/spain/technet/seguridad/recursos/masinfo/criteria.mspx
http://www.telser.com.pe/assen/pc.htm

http://delta.cs.cinvestav.mx/~mcintosh/comun/historiaw/node26.html

http://www.cosaslibres.com/software.html

http://www.monografias.com/trabajos6/hiso/hiso.shtml#que

http://www.tau.org.ar/base/lara.pue.udlap.mx/sistoper/capitulo2.html

http://www.tau.org.ar/base/lara.pue.udlap.mx/sistoper/index.html

http://webdia.cem.itesm.mx/ac/rogomez/histoSistOper.html

http://mx.geocities.com/fundamentosdeseguridad/SEMINARIO/TEMA_6.htm

http://www.germinus.com/sala_prensa/articulos/certificacion_prod_seguridad.pdf

http://www.insecure.org/tools.html

http://www.kriptopolis.com

http://sistemas.dgsca.unam.mx/publica/pdf/orangebook.PDF#search=%22libro%20naranja%22

http://www.softdownload.com.ar/antihackers.htm

http://es.wikipedia.org/wiki/Modelo_OSI

http://www.dynamoo.com/orange/summary.htm

http://webstore.ansi.org/ansidocstore/product.asp?sku=ISO%2FIEC+17799%3A2005&source=google&adgroup=17799&keyword=iso%2017799&gclid=CP_ahefy84YCFRuoLAodk1l3Xw

http://andercheran.upv.es/~toni/personal/ISO17799.pdf#search=%22iso%2017799%22

http://www.dynamoo.com/orange

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/a9d684f0-90b1-4c67-8dca-7ebf803a003d.mspx?mfr=true

http://www.microsoft.com/latam/windowsserver2003/evaluation/overview/enterprise.mspx

http://msmvps.com/blogs/quilez/archive/2005/06/08/51039.aspx

http://www.microsoft.com/spain/technet/seguridad/herramientas/wsus.mspx

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/WSUS/WSUSStepbyStepTC/f593532c-e92e-47f3-914a-38a6c2519e94.mspx?mfr=true

http://www.microsoft.com/spain/servidores/windowsserver2003/technologies/webapp/**iis**.mspx

http://www.belarc.com.mx/products.html

http://www.lavasoftusa.com/software/adaware/

http://www.zonelabs.com/store/content/home.jsp

http://www.microsoft.com/technet/security/tools/mbsahome.mspx

http://www.gfi.com/languard/

http://insecure.org/nmap/

http://sectools.org/

http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htm

http://demosten.com/showtraf/

http://www.microsoft.com

http://www.dgsca.unam.mx/

http://www.cert.org.mx/

http://www.fi-b.unam.mx/index2.html

http://www.microsoft.com/latam/technet/seguridad/articulos/ddmmyy_guia_seguridad_windows_server_2003.asp

http://sauce.pntic.mec.es/crer0052/dns/configur.htm

https://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/928fbc3d-d940-4a71-8aa3-a770fbafd924.mspx?mfr=true