CAPITULO I.

PLANTEAMIENTO DEL PROBLEMA.

1.1 ANTECEDENTES.

La seguridad es primordial en el ser humano y en la realización de cualquier proyecto o situación de la vida, como lo da entender el autor Rosales (2002, p.33) Al establecer que "La seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella"

De acuerdo con el autor anteriormente mencionado, coincidimos que la seguridad es una necesidad básica, que en el ramo científico o tecnológico que se aplique sirve para prevenir, mantener el funcionamiento y resguardar posesiones.

En todo objeto de estudio de la humanidad, se necesita estabilidad y protección de información o bienes, en informática sabemos que la herramienta principal que ayudo a su divagación en el mundo, son las computadoras, cualquiera que sea la categoría.

Es por eso que en este trabajo de investigación referente a computación e informática nos parece importante dedicarlo a la investigación de factores de protección informática, mostrando y describiendo los métodos de protección, conociendo los tipos y medios de ataque a nuestro sistema de información en una red de datos local.

Se pretende informar a los usuarios lo que deben saber para no caer fácilmente en ataques externos o virus informáticos.

1.2 PROBLEMÁTICA ACTUAL.

Las empresas tienen riesgo de perder información, esto podría detener su operación, deteniendo procesos de producción o administrativos, para ello es necesario proteger el funcionamiento de la información, existen diferentes maneras o métodos de proteger un sistema de información, todas estas partes del sistema de seguridad deben trabajar en conjunto para asegurar la informática de la empresa.

La seguridad informática existe solo si se juntan todos los elementos y métodos que la hacen posible ya que cualquier método utilizado por sí solo no puede abarcar todos los puntos vulnerables de los sistemas de información, así lo da a entender, Hallberg (2003, p.97). “La seguridad informática solo brinda áreas de oportunidad, en los sistemas informáticos y no brinda por si sola seguridad en la información de la organización, la seguridad informática, no puede por sí misma

proporcionar la protección para su información". De acuerdo con el autor, es por que pretendemos mostrar los puntos de protección en una empresa que usa una red de datos local para compartir y automatizar su información.

En este trabajo de investigación identificaremos las realidades acerca de la seguridad informática y describir recomendaciones, estrategias, errores comunes y amenazas para con la seguridad informática.

La manera en que manejamos la seguridad de la información ha evolucionado con el tiempo, a medida que nuestra sociedad y tecnología evolucionan, por ello es importante comprender esta evolución para entender como necesitamos enfocar la seguridad informática en la actualidad, ya que lo que en algún momento es seguro con el paso del tiempo ya no lo es, como lo describe Maiwald (2003, p.8) "La seguridad de las comunicaciones y de las emisiones era suficiente cuando los mensajes se enviaban por medio de teletipos, pero al cambio de tecnologías estos ya no lo eran, la mayor parte de los activos de la información de las organizaciones migraron hacia ellas en formato electrónico, cambiando por completo la idea de seguridad en la información", es por esto que pretendemos mostrar y describir los elementos y características que conforman la seguridad informática.

Las empresas hoy en día administran su información, con ayuda de la tecnología construyendo sistemas de información, para que los colaboradores de las empresas puedan acceder rápidamente a toda la información

empresarial, confiando completamente la información a los sistemas computacionales.

Cuando no se conoce el alcance que tienen los sistemas informáticos, ni lo vulnerables que pueden ser, si son expuestos a Internet por los mismos empleados de la organización, puede haber fuga de información hacia el exterior, al hablar de seguridad informática podemos hablar desde un software que restringe otros programas malignos, llamado antivirus, un software que previene que personas foráneas logren acceder, llamado firewall, hasta seguridad física, que bien podría ser un buen edificio con controles de acceso y seguridad privada que restrinjan el acceso a personas.

Para esto pretendemos describir por que las empresas cuidan la información, de qué manera lo hacen, que es la seguridad informática, conceptualizando una teoría general de la seguridad lógica, física e ingeniería social, y mediante ejemplos básicos y prácticos que hablen de seguridad lógica, es decir, como instalar un antivirus, un firewall y un sistema de actualizaciones de sistema operativo Windows, para proteger la información.

Describiremos los puntos más importantes en la seguridad informática, como ya se dijo como lo son firewall, antivirus, conductas del usuario, seguridad informática física, ingeniería social, esto para crear una idea completa de los factores que tienen que ver con la seguridad informática.

En la actualidad la seguridad informática es indispensable en un sistema de información, los sistemas de información y redes de datos deben hacerse con la seguridad informática en mente.

Las organizaciones siempre tienen sus computadoras conectadas en red, esto crea riesgos y las hace más vulnerables, como lo menciona Maiwald (2003.P.9) “Cuando las computadoras se unen en redes, surgen nuevos problemas de seguridad y los viejos problemas se comportan de diferentes formas”, estamos de acuerdo con el autor ya que las redes son el principal medio de accesos de información no autorizados, por hackers, o destrucción de información por software maligno que generalmente es propagado por red.

1.3 OBJETIVO GENERAL.

A continuación describiremos los objetivos en este trabajo de investigación, tanto los generales como los particulares, plantearemos los objetivos en base a lo que pretendemos abordar en nuestro estudio. El objetivo general de nuestra investigación es el siguiente:

“Dar a conocer y describir los métodos para proteger la información en una red de datos área local ya establecida, para protegerse de las amenazas más comunes”

1.4 OBJETIVOS PARTICULARES.

- Describir que es la seguridad física.
- Describir que es la ingeniería social informática.
- Describir teóricamente los métodos de protección indispensables de seguridad lógica.
- Ejecutar procesos básicos de instalación de programas referentes a la seguridad lógica.
- Identificar las formas que hay para proteger la información.
- Mostrar a los usuarios que la seguridad informática, puede ser ayudada por ellos mismos.

1.5 IMPORTANCIA DE SU ESTUDIO.

La seguridad informática tiende a ser motivo de descuido en las empresas, si no se describen los puntos importantes en su estudio, se ignora de los riesgos que conlleva confiar la información a los sistemas de información.

Es importante su estudio ya que así se conoce la problemática que puede traer el no conocer los aspectos que pueden evadir la seguridad informática en las empresas tanto físicas como lógicas.

Es necesario tener seguridad en la información ya que las organizaciones se apoyan de la informática para mantener la operación, producción y administración organizacional y es necesaria como lo menciona Maiwald (2003. P.10) “La seguridad informática es necesaria para proteger la información en tránsito”, Lo cierto es que ningún producto proporcionara seguridad informática total a una organización, es necesario tener muchos elementos y tipos de productos para proteger completamente los activos de información, por ello es necesario estudiar todos para saber cuál o la combinación de cuales es necesaria para proteger nuestra información.

Debemos de tomar en cuenta que a la información o a los sistemas de cómputo de una organización les pueden ocurrir cosas malas de muchas maneras, algunas de estas son hechas a propósito y otras ocurren por accidente. Sin importar como ocurran los eventos, es importante conocer y estudiar todas las formas de ataques y las maneras de proteger la información.

CAPITULO II.

FUNDAMENTOS TEORICOS.

2.1 ANTECEDENTES DE LA SEGURIDAD.

Los primeros conceptos de seguridad se encuentran en los inicios de las escritura, con los sumerios y también en la Biblia, han existido autores de obras, donde se mencionan rasgos de seguridad para gobernar o para ganar en determinada guerra, también para cuidar posesiones que los países necesitan y llegar a ser un mejor país. Incluso antes, se sabe que los humanos primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales luchando o huyendo para eliminar o evitar la causa.

Así también como cualquier otro concepto, la seguridad se ha desarrollado y ha seguido una evolución, en cuanto a aplicaciones, desde el punto de vista humano individual, hasta en una organización social o empresa.

En las empresas, el próximo paso de la seguridad fue la especialización, así nace la seguridad externa, aquella que se preocupa por amenazas de entes externos a la organización, también está la seguridad interna, aquella que se preocupa por amenazas de la misma organización como la falta de prevención.

Entonces podemos decir que la seguridad informática es parte de la seguridad interna y externa de una empresa.

La seguridad desde el punto de vista legislativo, está a cargo de políticos quienes les toca decidir en común acuerdo, su importancia y aplicación, manteniéndose la seguridad con leyes y sanciones a quien no la cumplan.

La seguridad informática es un rama de la informática que vigila y conoce las amenazas y debilidades que puede tener un sistema de información en una empresa, el termino en si fue aceptado por expertos en informática que la definen como un conjunto de métodos y herramientas destinados a proteger la información y por ende, los sistemas informáticos ante cualquier amenaza.

Las empresas forman un departamento experto en tecnologías de información que mantiene el sistema y se encarga de la seguridad informática, otra definición según el libro del escritor informático Molina (2004. P17), establece que “se divide en dos tipos una la seguridad física que es una aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”.

La seguridad informática, se creó cuando al establecer sistemas funcionales, el personal de las empresas se dieron cuenta que resulta más peligroso un robo o ataque al sistema que una falla en si del mismo, sólo basta con repasar unas pocas estadísticas. Durante 1997, el 54 por ciento de las empresas norteamericanas sufrieron ataques de Hackers en sus sistemas. Las

incursiones de los piratas informáticos, ocasionaron pérdidas totales de 137 millones de dólares en ese mismo año. El Pentágono, la CIA, UNICEF, La ONU y demás organismos mundiales han sido víctimas de intromisiones por parte de estas personas que tienen muchos conocimientos en la materia y también una gran capacidad para resolver los obstáculos que se les presentan.

A continuación listamos conceptos de algunos autores especialistas en seguridad informática:

“La informática es la disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales. También es definida como el procesamiento de información en forma automática.” Alvar (1998 p.13)

“Es la actividad relacionada con el uso de computadoras. Este término viene del francés y su equivalente en lengua inglesa es tecnología de la información que es la conjunción de computadoras, Telecomunicaciones y microprocesadores.” Estema (2004, p.15)

“Es una rama de la ingeniería que estudia el tratamiento de la información mediante el uso de máquinas automáticas.” “Es una disciplina que estudia la automatización de la información para poderla aplicar a software y hardware facilitando así la vida diaria de las personas.” Benedito (1994, p.45).

La tecnología ha evolucionado aceleradamente estos últimos años más que otras épocas, esto a permitido avances en salud, hogar, entretenimiento y

herramientas para las empresas, estas herramientas basadas en el sistema de información son las que se deben proteger mediante los métodos e información que describimos en nuestro trabajo de investigación.

La computadora es un elemento clave para la solución a muchos de nuestros problemas, desde buscar una receta de comida hasta un complicado programa diseñado con redes neuronales. La computadora ha permitido un acceso a la información en una magnitud inmensa y a velocidades nunca antes pensadas. Nosotros nos enfocaremos en una red de datos empresarial

Pero esto ha provocado que toda la organización solucione sus problemas por medio del uso de computadoras, ya que mucha entidades son más competitivas y por supuesto esto beneficia de una manera generalizada en todos sus aspectos, en ello radica la importancia de los sistemas.

Los sistemas de información en las empresas están formados por computadoras en red, pero manejado por personas así lo comentan los autores y expertos en seguridad en informática, “Un grupo ordenado de los elementos como son los componentes físicos y las personas” Kendall & Kendall, (2000, p.33). “Conjunto o arreglo de cosas conectadas o interrelacionadas entre si además interdependientes para formar una unidad compleja.” Senn, (2000, p.10).

Otros autores describen la seguridad informática como elementos que trabajan en conjunto para lograr objetivos sin mencionar conceptos actuales de seguridad informática, lo cual también es válido por que debe de haber preocupación por protección de información incluso si no existen computadoras. “Serie de elementos que forman parte de una actividad, procedimiento, plan de procesamiento que busca metas comunes mediante la manipulación de datos.” Murdick (Ross, p.27).

Un sistema es un conjunto de elementos interdependientes que interactúan para formar un todo, esto crea un conjunto de elementos los cuales se complementan unos a otros, permitiendo así que exista un buen funcionamiento y conseguir objetivos que busquen todos los componentes de este sistema.

Un punto muy importante para que cualquier actividad se ejecute de manera más eficiente, pasa por una serie de procesos, este conjunto de procesos en su mayor parte están integrados dentro de un sistema. Y como sabemos hay todo tipo de sistemas como lo son los, biológicos, de negocios, políticos, financieros etc. Debido a esto la informática ha desarrollado una gran variedad de sistemas los cuales permiten aumentar el rendimiento de estas. Y como en cualquier sistema si existe una falla o algún elemento de esta resulta afectado es muy probable que empiecen a surgir errores que posteriormente crearan un colapso en el sistema.

Pero en muchas ocasiones los ambientes en los que se desenvuelven se tienen que modificar por causas ajenas a esta ya sea tanto en sistemas naturales

como en sistemas creados por el hombre y esto puede afectar a los organismos de este sistema.

El inicio de los sistemas surgió a partir de la problemática de resolver problemas de una manera más sencilla, estos permitirían automatizar muchas actividades que en estas se realizaban y en la actualidad observamos que tuvo el éxito más de lo deseado por sus creadores, esto ha permitido hacer a las organizaciones más competentes debido a su funcionamiento correcto de los sistemas implementados.

2.2 SEGURIDAD LÓGICA.

La seguridad lógica que es la que se administra directamente con computadoras y se define como: el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. La seguridad lógica involucra todas aquellas medidas establecidas por la administración, usuarios y administradores de recursos de tecnología de información- para minimizar los riesgos de seguridad asociados con sus operaciones cotidianas llevadas a cabo utilizando la tecnología de información.

En nuestra opinión en ocasiones se le da más importancia a la seguridad lógica exponiendo a veces los equipos de cómputo a robos o daños por algún desastre natural o accidente en el lugar de operación del servidor, para que la

seguridad informática sea efectiva es necesario hacer una correcta combinación de los dos tipos de seguridad.

Es decir que 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.", según Tanenbaum (2003. P.27).

En seguridad informática todo lo que no está permitido debe estar prohibido y esto es lo que debe asegurar la seguridad lógica.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizando los datos, archivos y programas correctos y con el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
7. No divulgar información no necesaria.

Un hacker puede tardar meses en vulnerar un sistema ya que son cada vez más sofisticados. Están los que interceptan códigos de tarjetas de crédito y los utilizan para beneficio propio. También están los que se entrometen en los sistemas de aeropuertos produciendo un caos en los vuelos y en los horarios de los aviones. Pero he aquí la gran diferencia en cuestión. Los crackers (crack=destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus. Esos son los crackers, personas inquietas que aprenden rápidamente este complejo oficio. Se diferencian con los Hackers porque no poseen ningún tipo de ideología cuando realizan sus "trabajos".

En cambio, el principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema. Aprovechando que en la vida diaria se maneja con sistemas de información.

Así como en otras ciencias o técnicas de la humanidad, se trata de crear y normalizar procedimientos para mejor operación entre las personas que siguen estas carreras, por ejemplo la contabilidad tiene un Colegio de Contadores, en que crea boletines aplicables a todos los contadores e instituciones de México.

En informática, aunque es un campo nuevo se han tratado de normar teorías para explicar lo que es la informática, llamándola teoría de sistemas:

La teoría de sistemas surgió con los trabajos del alemán Ludwig Von Bertalanffy, publicados entre 1950 y 1968. La teoría de sistemas no busca solucionar problemas o intentar soluciones prácticas, pero sí producir teorías y formulaciones conceptuales que pueden crear condiciones de aplicación en la realidad empírica.

La teoría de sistemas afirma que las propiedades de los sistemas, no pueden ser descritos en términos de sus elementos separados; su comprensión se presenta cuando se estudian globalmente.

La teoría de sistemas se fundamenta en tres premisas básicas:

1. Los sistemas existen dentro de sistemas: cada sistema existe dentro de otro más grande.
2. Los sistemas son abiertos: es consecuencia del anterior. Cada sistema que se examine, excepto el menor o mayor, recibe y descarga algo en los otros sistemas, generalmente en los contiguos. Los sistemas abiertos se caracterizan por un proceso de cambio infinito con su entorno, que son los otros sistemas. Cuando el intercambio cesa, el sistema se desintegra, esto es, pierde sus fuentes de energía.
3. Las funciones de un sistema dependen de su estructura.

“Para los sistemas biológicos y mecánicos esta afirmación es intuitiva. Los tejidos musculares por ejemplo, se contraen porque están constituidos por

una estructura celular que permite contracciones". (Chiavenato, 1992 p. 43)

La teoría de sistemas trajo la teoría de la decisión, donde la empresa se ve como un sistema de decisiones, ya que todos los participantes de la empresa toman decisiones dentro de conjunto de relaciones de intercambio, que caracterizan al comportamiento organizacional.

"Después de la segunda guerra mundial, a través de la teoría matemática se aplicó la investigación operacional, para la resolución de problemas grandes y complejos con muchas variables". (SCOTT, 1989 p.38).

Clasificación de los sistemas:

Los sistemas se clasifican de acuerdo con:

- El grado de interacción con otros sistemas: abiertos y cerrados. Según el nivel de influencias son sistemas abiertos o cerrados y va de abiertos a cerrados.
- La composición material y objetiva de sus elementos: abstractos y concretos. El sistema abstracto es aquel en el que todos sus elementos son conceptos, y el sistema concreto es cuando al menos 2 de sus elementos son objetos.
- La capacidad de respuesta: pasivos, activos y reactivos. Los reactivos son los que reaccionan al estímulo de otro,

- Su movilidad interna: estáticos, dinámicos, homeostáticos y probabilísticos.
- La predeterminación de su funcionamiento: determinantes y dependientes. En los dependientes existe incertidumbre sobre su futuro, y los determinantes se caracteriza por que se predice con toda certeza.
- Su grado de dependencia: independientes e interdependientes. Este es el grado de dependencia que tienen respecto de otros o del medio ambiente.

Elementos de los sistemas:

En todo sistema existen 4 elementos mínimos para su existencia.

- insumos o influjos: abastecen al sistema de los necesarios para cumplir su misión.
- proceso: transformación de los insumos de acuerdo con los métodos propios de la tecnología del sistema.
- producto: es resultado del proceso y un insumo de otros sistemas.
- retroalimentación: es la respuesta de los sistemas que han recibido como insumo el producto de un sistema previo o la respuesta de su medio ambiente, cuando este ha recibido un producto del sistema.

La seguridad informática aprovecha ciertos métodos para cumplir su objetivo a continuación describiremos los más comunes que se utilizan en las redes corporativas de datos y redes de área local.

En el mundo informático con respecto a seguridad descubrimos que estos son los métodos más utilizados para proteger los sistemas de información.

- Antivirus: sirven para capturar los virus informáticos y prevenirlos como lo menciona Tanenbaum (2003. P.43) “Los antivirus son una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos”
- Firewall: los cuales se utilizan de frontera entre el interior y exterior de la red y como lo menciona McMahon (2003, P47) “es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios”.
- Directorio Activo: Sirve para controlar los accesos a la red por entre los usuario y equipos de cómputo del sistema informático, como lo menciona Simons (2003. P.21).
- Cambio de contraseñas: la privacidad de las contraseñas son de los principales problemas a la hora de cuestionar seguridad, debido a esto es importante cambiar las contraseñas frecuentemente, una vez que esto es realizado los sistemas informáticos hacen uso de la criptología informática que como lo menciona Maiwald (2005. P117)

> “es una serie de técnicas de programación para almacenar las contraseñas de manera que no sean comprendidas por el ser humano”.

Lo más identificable para con la seguridad informática y conocido para cualquier tipo de usuario son los virus, pero existen diferentes tipos de virus, los cuales clasificaremos en este trabajo de investigación de la siguiente manera:

Los antivirus monitorean y borran diferentes tipos de virus, en este caso Symantec Corporate Edition, tiene una definición de base de datos que revisa todo el malware o virus. Existen diferentes tipos de virus, todos pueden ser englobados en los términos virus o malware.

Todos los virus tienen en común una característica, y es que crean efectos perjudiciales al sistema operativo o a alguna aplicación o programa. A continuación presentamos una clasificación de los virus informáticos, basada en el daño que causan y efectos que provocan.

Un **Caballo de Troya,** es un programa dañino que se oculta en otro programa legítimo, y que produce sus efectos perniciosos al ejecutarse este último. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

Un **Gusano** es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, se copia así mismo sucesivamente, hasta que desborda la memoria de acceso aleatorio, siendo ésta su única acción maligna.

Existen también virus que dañan un tipo de archivos específico como lo son los **Virus de macros**, es una secuencia de órdenes de teclado y Mouse asignadas a una sola tecla, símbolo o comando. Son muy útiles cuando este grupo de instrucciones se necesitan repetidamente. Los virus de macros afectan a archivos y plantillas que los contienen, haciéndose pasar por una macro y actuaran hasta que el archivo se abra o utilice.

Existen también los **Virus de Programa**, que comúnmente infectan archivos con extensiones .EXE, .COM, .OVL, .DRV, .BIN, .DLL, y .SYS., los dos primeros son atacados más frecuentemente por que se utilizan mas.

Existen otros aun más peligros y a veces irreversibles que son los **Virus de inicio**, son virus que infectan sectores de inicio de los discos duros, sistemas de archivos y el sector de arranque maestro (Master Boot Record) también pueden infectar las tablas de particiones de los discos.

Los más comunes son los **Virus Residentes,** que se colocan automáticamente en la memoria de la computadora y desde ella esperan la ejecución de algún programa o la utilización de algún archivo.

Los **Virus de enlace o directorio,** modifican las direcciones que permiten, a nivel interno, acceder a cada uno de los archivos existentes, y como consecuencia no es posible localizarlos y trabajar con ellos.

Los **Virus polimórficos,** son virus que mutan, es decir cambian ciertas partes de su código fuente haciendo uso de procesos de encriptación y de la misma tecnología que utilizan los antivirus. Debido a estas mutaciones, cada generación de virus es diferente a la versión anterior, dificultando así su detección y eliminación.

Existen también correos electrónicos **Virus falsos,** no son virus, sino cadenas de mensajes distribuidas a través del correo electrónico y las redes. Estos mensajes normalmente informan acerca de peligros de infección de virus, los cuales mayormente son falsos y cuyo único objetivo es sobrecargar el flujo de información a través de las redes y el correo electrónico de todo el mundo.

2.3 SEGURIDAD FÍSICA.

En la seguridad informática física, es muy importante ser consciente que por más que nuestra empresa sea segura desde el punto de vista de ataques externos, Hackers, virus, etc. La seguridad de la misma será nula si no se ha previsto como combatir un siniestro ya sea natural o provocado.

Además La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático, así, 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.

La seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad lógica que aseguren la información ayudándose de herramientas físicas que no forman parte de la teoría de sistemas.

Actualmente la computadora está presente en la mayoría de las actividades que realizamos desde que nos levantamos con un despertador hasta cuando dormimos, esto debido a que para el desarrollo de muchos objetos se necesita la computadora en estos tiempos, por esta razón existe una rama de la ingeniería que estudia toda su conceptualización.

Consideramos necesario explicar las clasificaciones que tiene la seguridad informática:

La *seguridad física*, es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc. (conceptos luego tratados); la seguridad de la misma será nula si no se ha previsto como combatir un incendio o un desastre natural.

Además La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación son los que prevén, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma. Así, 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.

2.4 INGENIERÍA SOCIAL.

El termino ingeniería social fue establecido por el empresario William H. Tolman en su libro “Social Engineering” y lo describe como una serie de técnicas psicológicas para persuadir o lograr resultados deseados, (William H. Tolman 1909 p.6).

En informática se aplica de la misma manera, informando los riesgos que se tienen si se da a conocer al exterior de la empresa, aun que la ingeniera social por si sola no lograría una completa seguridad informática, es limitar al máximo los riesgos. Ingeniería social también se relaciona con la modalidad que utilizan los delincuentes para robar información del usuario manipulándolo. Esto quiere decir que se utiliza más que la vulnerabilidad del sistema, la vulnerabilidad ingenua del usuario.

Un atacante al sistema de información, podría utilizar también ingeniería social para lograr sus objetivos, mediante software por ejemplo, un formulario Web, con preguntas clave, que serian de mucha ayuda, como datos de un servidor o determinada contraseña.

Una de las principales soluciones es que el usuario tome conciencia de que él es la principal vía para que ocurra y de esta manera, no ejecute cualquier archivo que llegue a través de un mail ni ingrese a enlaces que lleguen de una supuesta entidad.

Para lograr defender al sistema de información es necesario cubrir dos temas determinantes: Formar y Concientizar, la primera es explicar a los usuarios como consigue un hacker engañarle y como reconocer un ataque, es decir que se limite a utilizar el sistema como herramienta de trabajo, es decir, no compartir con nadie accesos, como usuarios y contraseñas, ya que son para uso personal. Concientizar, es probarles que este tipo de ataques es cada vez

más frecuente y es por lo general el primer recurso que se utiliza cuando se quiere corromper la seguridad.

Además es necesario retroalimentar esta información y recordar periódicamente a los usuarios, esta medida es recomendada por muchos autores sobre seguridad de la información ya que respalda el trabajo previo de la ingeniería social, por eso es recomendable informar constantemente a los usuarios, (Jean-Marc Royer, 2001, p368) “La sensibilización respecto a los riesgos informáticos debe realizarse de forma recurrente, todos los años es necesario volver a formar al personal, ya que con el tiempo, no viendo ninguna alerta se instala una rutina y la atención se relaja. ”

CAPITULO III.

METODOLOGÍA Y DESARROLLO DE LOS DATOS.

3.1 METODOLOGÍA.

En esta sección de nuestro trabajo de investigación hablaremos sobre la metodología, sujetos de investigación e instrumentos que utilizaremos en nuestro trabajo de investigación, eligiendo cuales son los más apegados a nuestro estudio.

Además los instrumentos que utilizaremos ya sean entrevistas, encuestas e investigación continua acerca de las fuentes de nuestra información práctica.

En el presente trabajo de investigación estudiaremos directamente nuestro tema de investigación que es la seguridad informática, sus tipos, las personas que trabajan en estas áreas en el departamento de sistemas de información, así como los riesgos que pueden amenazar la seguridad en las redes de datos.

Debido al tipo de trabajo de investigación, la herramienta más importante es la observación dentro de la empresa, involucrando todos los sujetos, material y procedimiento que se investigaran directa o indirectamente en la investigación.

Así, también clasificaremos la investigación, por su tipo, existen cuatro, la descriptiva, la exploratoria, la correlacional y la explicativa, es muy importante la clasificación como lo menciona, Hernández (2004 p.114) “Pues el tipo de estudio, depende de la estrategia de investigación”, concordamos con esta mención debido a que al conocer el tipo de investigación es más fácil recolectar los datos y conocer nuestra investigación.

Nuestra investigación, selecciona y muestra las partes, riesgos, amenazas, estrategias, técnicas y ejercicios prácticos de la empresa investigada, para un objetivo final, asegurar la información, por eso clasificamos nuestro proyecto de investigación, como descriptivo ya que como lo menciona Hernández (2004 p.114) Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a un análisis

Desde nuestro punto de vista, es necesario, recolectar datos para este tipo de clasificación según Dankhe (1989, p.17) “Se realiza cuando el objetivo consiste en examinar un tema poco estudiado”, por ello estamos formulando una amplia investigación aprovechando todas las fuentes de información, como libros, revistas, páginas de Internet, entrevistas a expertos y no expertos y la situación en la empresa estudiada en esta investigación.

3.2 SUJETOS DE INVESTIGACIÓN.

En este apartado trataremos la descripción de los individuos que participaran y apoyaran nuestra investigación, las características de la población o universo de nuestro estudio, así como otras variables que se consideren necesarias. Ibáñez (1999, p.167).

La presente investigación se lleva a cabo gracias a la investigación de teorías y procesos ya establecidos, de la empresa en estudio y la disponibilidad de; personal de la misma para brindar la información necesaria, con la ayuda también de búsquedas y entrevistas.

En esta investigación, se trabajara con el personal de la empresa, pero mas directamente con el personal encargado de sistemas de información y por ende de la seguridad en informática de la empresa, el personal de esta área es mas capaz de brindarnos esta información ya que conoce la informática de la empresa, sus procesos, sus instalaciones, las locaciones de cada área, las áreas peligrosas y vulnerables que guardan o transportan la información.

En esta empresa llamada Teléfonos del Noroeste, en el departamento de sistemas de información existen 35, personas laborando en la gerencia de sistemas de información, para satisfacer las necesidades de información de la empresa, cuenta con un gerente de sistemas. 3 subgerentes de sistemas los cuales se dividen en, operación de sistemas, desarrollo de sistemas y soporte a la red, los que trabajan directamente con la seguridad de información, son el

área de operación de sistemas y soporte a la red ya que ellos crean los sistemas de transmisión, acceso y almacenamiento de la información, el área de desarrollo de sistemas crea programas para uso interno que le permiten al usuario no experto en sistemas visualizar la información de una manera filtrada y rápida.

A su vez cada subgerencia de sistemas de información cuenta con 1 investigador y desarrolladores o ingenieros de soporte, que forman parte del área y hacen posible la realización de las tareas, el área de desarrollo de sistemas cuenta con 9 programadores, las áreas de soporte a la red y operación de sistemas cuentan con 11 ingenieros de soporte cada subgerencia.

Los usuarios de los sistemas de información los conforma toda la empresa con acceso a una computadora asignada por la misma empresa, la empresa cuenta con alrededor de 4000 empleados activos, de los cuales alrededor de 2800 son considerados usuarios de los sistemas de información ya que se toma como referencia la computadora asignada por la empresa al usuario correspondiente.

La empresa cuenta con 1 dirección general y 12 gerencias las cuales son finanzas, atención a clientes, planta exterior, sistemas de información, mercadotecnia, ventas, compras e ingeniería, sumando entre todos aproximadamente 2000 empleados activos en la organización los cuales aproximadamente 900 son usuarios de los sistemas de información

De estos sujetos descritos anteriormente obtendremos una muestra de 40 individuos a ser entrevistados para buscar responder nuestros objetivos de investigación y una entrevista para complementar estos datos realizada al gerente del área de sistemas de información.

3.3 MATERIAL.

Esta sección es creada para describir los instrumentos y material utilizado así lo refiere Hernández (2003. P.81). así daremos descripciones generales y detalladas obtenidas a partir de nuestro trabajo de investigación.

Los instrumentos son las herramientas que nos ayudan a obtener la información necesaria como las que utilizamos en esta investigación, puede ser la observación y más concretamente las entrevistas, en este caso nos basaremos en una entrevista al gerente de sistemas de información de la empresa investigada, 40 encuestas cerradas realizadas a una muestra de 40 usuarios de sistemas de información y colaboradores del área de sistemas de información, denominados usuarios expertos, las entrevistas se crearan con base en los objetivos descritos en el primer capítulo esto para conocer los diferentes puntos de vista de cada una de las partes en lo que refiere al trabajo de sistemas de información y específicamente a la seguridad informática.

En esta sección describiremos en detalle los pasos que han de seguirse en el transcurro de el estudio y aplicación de nuestra metodología utilizada, es decir

los procedimientos de selección de la muestra y recolección de datos, es importante señalar que además del método de selección de la muestra, el exacto procedimiento de entrevista o administración del test. Ibáñez (1999. P169)

Para obtener información decidimos utilizar como instrumento de investigación una entrevista y 40 encuestas, este será nuestra muestra en la investigación, aplicaremos directamente la entrevista al gerente de sistemas de información y narraremos dicha encuesta en el apartado de resultados de nuestra investigación, debido a que este tipo de instrumentos no puede tabularse ni graficarse.

Las encuestas serán aplicadas aleatoriamente a 40 usuarios de los sistemas de información, será una encuesta cerrada eligiendo preguntas que respondan a nuestros objetivos generales y particulares y por supuesto a nuestra hipótesis, posteriormente graficaremos y realizaremos una tabulación completa de los datos obtenidos.

Las preguntas son una manera general de informarnos y alimentar la investigación para justificar la continuación de nuestro trabajo de investigación, ya que son una manera abierta de aportar a la investigación en caso de la entrevista (Anexo1) y una manera complementaria para saber que tanto los usuarios están involucrados con la manera en que se forma la seguridad de la información (Anexo2).

En este apartado describiremos el estudio de la investigación, para fundamentar el análisis y comunicar los resultados obtenidos de los instrumentos y procedimientos de la metodología. En este capítulo se comenta sobre la estructura común de un reporte cualitativo y los elementos que la integran.

Mostraremos los reportes de los resultados del proceso cualitativo con su metodología descriptiva de manera narrativa ya que eso sería el reporte cualitativo de resultados como lo menciona Merrian (2009.P 17), "El reporte cualitativo es una exposición narrativa donde se presentan los resultados con todo detalle" estamos de acuerdo con esta definición ya que es el procedimiento que seguiremos en este capítulo.

En este apartado pretendemos mostrar una interpretación clara de los resultados obtenidos, es decir "mostrar si los datos obtenidos apoyan o no las hipótesis de la investigación" Pick (1984. P17), para desarrollarlo es necesario haber procesado la información recabada, es decir, haber codificado y tabulado los datos que se recolectaron para proceder posteriormente a su análisis.

La entrevista, se aplico de manera abierta, directamente al gerente de sistemas de información de la empresa en investigación, para complementar la

información, además de las graficas y tabulaciones que presentaremos más adelante.

Los resultados obtenidos son producto de una entrevista abierta, son reales y es una muestra cualitativa de lo que para él entrevistado, es la seguridad informática en una empresa, la entrevista fue aplicada el día 29 de julio del 2010, en las instalaciones de la empresa Teléfonos del noroeste para así tener una idea de que se espera del departamento de sistemas y de la presente investigación.

Cuando al gerente se pregunto la importancia de la seguridad informática respondió: “La seguridad informática actualmente cuenta con una gran importancia en nuestros días. Tenemos la necesidad de proteger contra ataques externos como internos nuestros sistemas informáticos partiendo desde el computador que se encuentra en nuestra casa hasta aquellos sistemas de grandes empresas donde la información que es almacenada en dicho sistema es de vital importancia para el curso normal de la vida empresarial, asentimos con el ya que mostrar esto es precisamente el objetivo de nuestra investigación.

Por otra parte le pedimos que nos dijera en términos generales que es lo más importante para presumir que se tiene seguridad informática, y nos responde lo siguiente: “Para combatir dichas amenazas se han creado una serie de *Mecanismos de Seguridad Informática:*

- Preventivos.
- Detectivos.
- Correctivos.
- Software antivirus.
- Software "firewall" o cortafuegos.

Estos son de carácter informático, pero también existen unos de carácter físico:

- *Restringir el acceso a las áreas de computadoras e impresoras*
- *Instalar detectores de humo y extintores*
- *Colocar los dispositivos lejos del piso y de las ventanas.*
- *Colocar personal de seguridad.*
- *Colocar letreros restrictivos y de precaución*

Precisamente en el marco teórico indicamos que aunque la seguridad informática depende de expertos en tecnologías de la información, se deben tener en cuenta otros aspectos como la seguridad física.

3.4 RESULTADOS DE LA ENTREVISTA.

En esta sección mostraremos a manera informativa un poco de lo que arrojaron nuestras encuestas ya que las preguntas y respuestas de esta encuesta nos sirvieron para darle una dirección a este trabajo recepcional.

Encuesta a Gerente de sistemas de manera abierta y personalizada.

1.- ¿Cómo describiría la importancia de la seguridad de la información en la empresa? Es imprescindible ya que ayuda a resguardar resultados del trabajo hecho por un equipo llamado empresa.

2.- ¿Que estrategias tienen para enterarse de la problemática que tienen los usuarios al manejar la información? Se está en contacto frecuente con ellos, tenemos un correo electrónico y un centro de soporte atendido las 24 horas en el que pueden expresar sus dudas y solicitudes, además 2 veces por año formamos parte de una encuesta de clima laboral en la que el usuario expresa como se siente trabajando con nuestros sistemas de información.

3.- ¿Qué tipos de auditorías califican al área? Tenemos una auditoria de seguridad hecha por nosotros, además una vez al año personal contratado nos hace una auditoría externa en la que nos hace importantes observaciones.

4.- ¿De qué manera hace participes a los usuarios no expertos en seguridad de la información? Mediante las maneras que tenemos de contacto, cada vez que hablamos con el usuario por algún soporte, le preguntamos y recomendamos seguir las indicciones que tenemos de seguridad, además después del soporte le mandamos un correo para que exprese sus dudas, comentarios o quejas que pueda tener.

5.- ¿Cómo colaboran los ingenieros de soporte de sistemas a la seguridad de la información? Actualizamos en la intranet una sección de preguntas frecuentes y estamos disponibles las 24 horas para ellos, además damos una atención al problema que manifiestan y en ese momento aplicamos una revisión general a su computadora localmente y a nivel sistema.

6.- ¿Cuáles son los nombres de los programas que se encargan de la seguridad de la información? Básicamente Tenemos Websense y Symantec10.

7.- ¿Tienen documentación y licencias de estos programas?

Si, tenemos procedimientos para resolver los problemas más recurrentes y tenemos un contrato y póliza de licencia con Microsoft y Symantec, las licencias de los demás programas que utilizamos las manejamos bajo demanda.

8.- ¿Con que frecuencia se actualizan Windows?

Microsoft no tiene un plan constante para actualizar ya que es cada que ellos descubren una amenaza en sus sistemas basados en Windows, pero nosotros verificamos las actualizaciones una vez a la semana.

9.- ¿Qué recomendación daría a los usuarios de los sistemas de información? No revelar información cuando no es debido, cambiar frecuentemente sus contraseñas y reportarnos cualquier anomalía que observe en los programas a nivel sistema.

3.5 ENCUESTAS.

La primera encuesta se realizo a personas que le llamamos no expertas en tecnologías de la información y fue la siguiente:

Responda por favor como califica cada uno de los aspectos del 1 al 5 siendo 1 lo más bajo y 5 la calificación más alta, la encuesta se hizo a 20 personas.

La segunda parte de la encuesta se eligió hacer a 20 usuarios no expertos en informática que después será comparada con la segunda parte de la encuesta, teniendo como resultado un análisis entre la misma encuesta aplicada a 2 grupos diferentes dividiéndolos en usuarios y usuarios expertos.

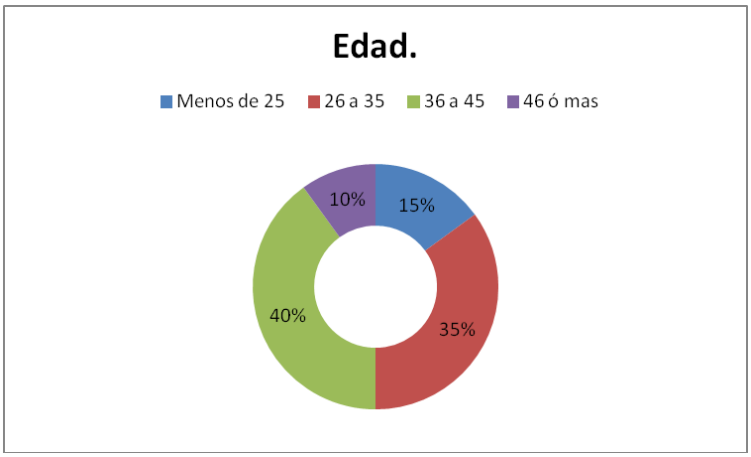
Las preguntas tratan lo que a continuación sigue:

Con la intención de tener un panorama general, se realizo la primera pregunta (anexo 2) ¿Sabe que es la seguridad informática? Y se observo que el 63%, es decir, la mayoría de los usuarios inexpertos no sabe lo que es la seguridad informática, mientras que es importante señalar que nadie considera que sabe mucho sobre seguridad informática y solo el 5% considera que sabe algo o poco sobre este tema, es necesario informar a los usuarios de equipos de computo que es la seguridad informática, por otro lado el 85% de los expertos informáticos saben con certeza que es la seguridad informática, por lo que daremos más adelante una recomendación para informar a los usuarios sobre este tema.

Para dar una idea más clara de lo que los usuarios están enterados en la empresa sobre los conceptos de seguridad obtuvimos los siguientes resultados de las encuestas aplicadas. (Fig.3.1) y obtener datos estadísticos además de las preguntas principales preguntamos otros datos como el sexo la edad y el grado universitario.

De esta manera podemos hacer un análisis comparativo e informarnos sobre lo que los usuarios de computadoras ya sean expertos o no expertos están enterados así como los hábitos que tienen sobre la confidencialidad de la información.

Como lo mencionamos para obtener un panorama más general en la entrevista les preguntamos a los usuarios datos que no estuvieran relacionados con seguridad informática, datos como Nombre, Edad, Sexo y Escolaridad.



3. 1 Que edad tienen los encuestados.

Podemos observar que en su mayoría se concentran personas o usuarios de los sistemas de información de entre 26 y 45 años, trabajando en el departamento de sistemas de información y de los que nos interesa obtener datos más generales.

Descubriendo así que en la organización, obtenemos más usuarios de mediana edad, lo cual es favorable ya que nos estuvo respondiendo personas con experiencia por su cantidad de años laborando y además en menor cantidad obtuvimos información de personas de otras edades, ya sea más grande o más chicos lo cual nos sirve para complementar y confiar más en la información obtenida.

Como ya se dijo esta segunda parte de nuestros entrevistados la manejamos para considerar un panorama más general de nuestra investigación, por eso también incluimos la escolaridad al presentarle la entrevista a nuestros sujetos de investigación. La grafica que muestra los grados de escolaridad de nuestro universo de encuestados quedo como sigue (Fig. 3.2).

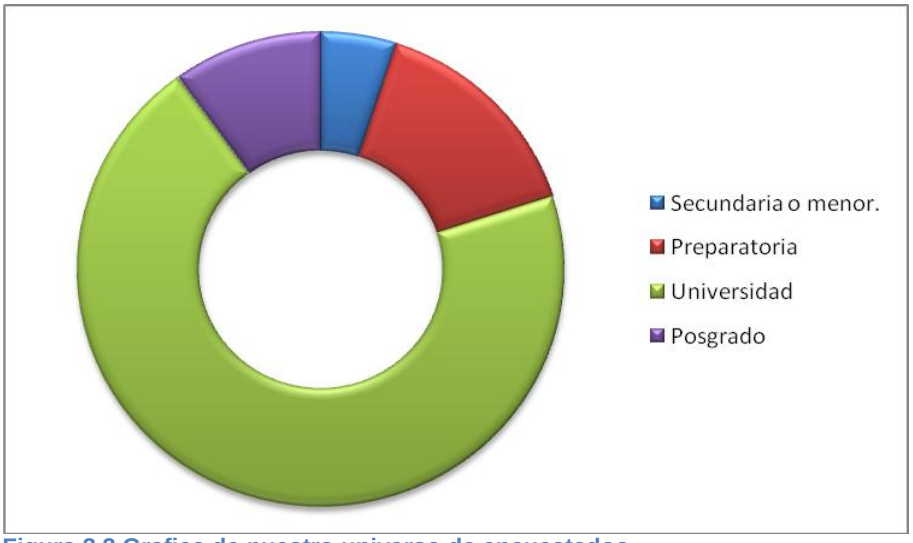


Figura 3.2 Grafica de nuestro universo de encuestados.

Las graficas anteriores nos muestran la información secundaria que decidimos obtener de nuestros entrevistados, para su visión completa mostramos a continuación una tabulación completa (Anexo 2) de los resultados obtenidos.

Respecto a nuestra primera pregunta (Fig. 3.3) podemos observar que mas de la mitad de las personas no sabe que es o cómo funciona la seguridad informática, razón por la que informaremos en este trabajo de investigación los puntos necesarios para obtener seguridad informática.

La información y resultados recabados de las encuestas será presentada de manera grafica a continuación explicando lo que para el proyecto significan y el impacto que puede tener lo que los usuarios saben acerca de seguridad informática (Anexo3).

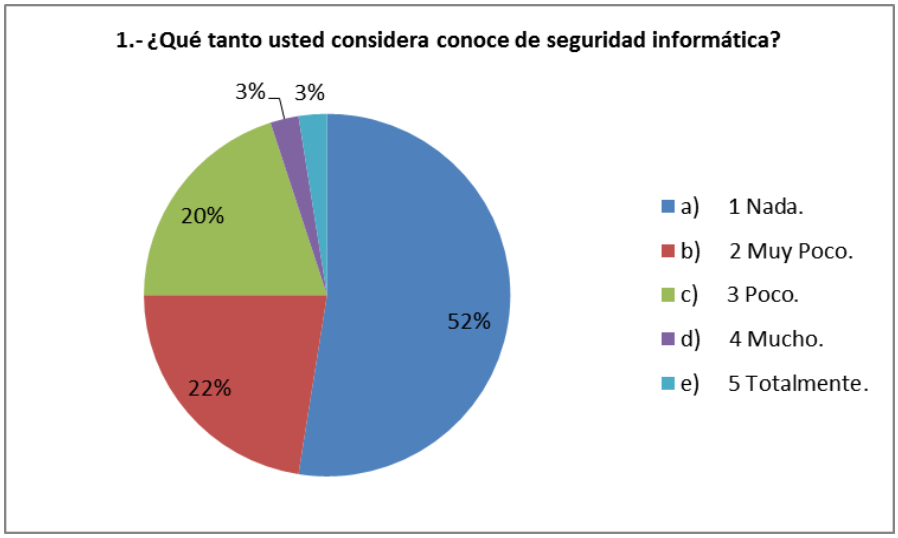


Figura 3.3 Pregunta 1.- ¿Qué tanto usted considera conoce de seguridad informática?

De una manera general pretendemos conocer como califican los usuarios la estabilidad de los sistemas de información de su empresa para poder al final de este trabajo de investigación hacer algunas recomendaciones básicas en caso de que no se cumpla una expectativa de seguridad, como podemos observar (Fig.3.4) el 30 por ciento de nuestro universo de encuestados la consideran regular o con una calificación de tres siendo el uno la más baja y el cinco la más alta.

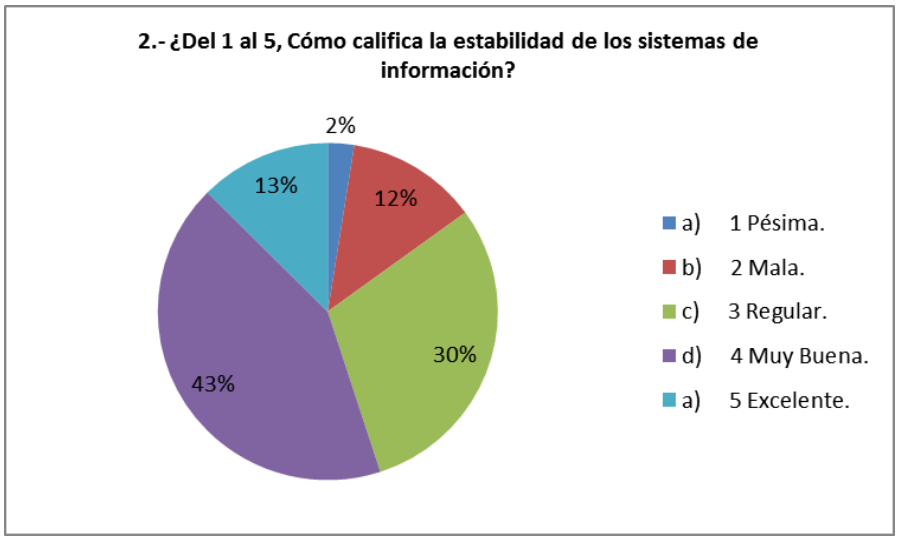


Figura 3.4 Pregunta 2.- ¿Del 1 al 5, Cómo califica la estabilidad de los sistemas de información?

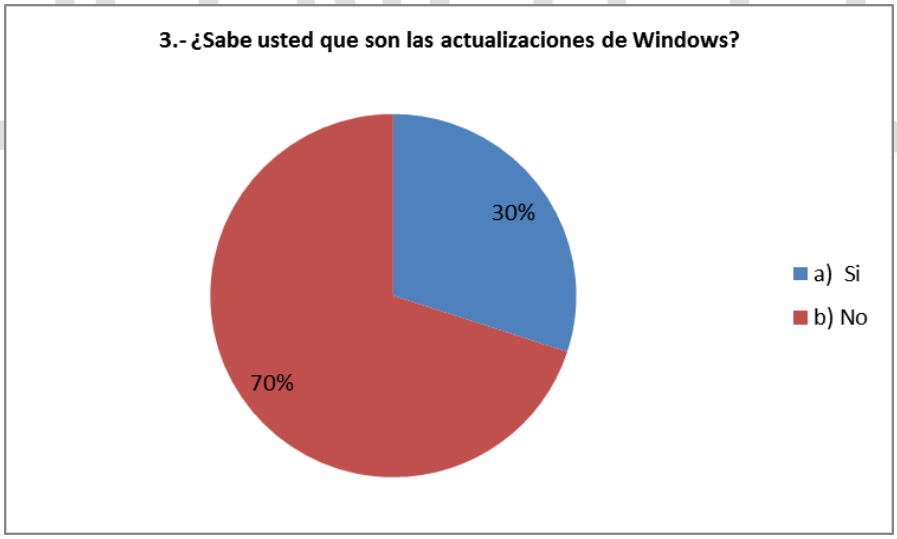


Figura 3.5 Pregunta 3.- ¿Sabe usted que son las actualizaciones de Windows?

En este trabajo de investigación queremos saber si es útil explicar que son las actualizaciones de Microsoft Windows por eso preguntamos si saben lo que son

(Fig.3.5) y nos dimos cuenta que el 70 por ciento de los usuarios no sabe lo que son debido a esto, explicaremos mas adelante que son y cual es la mejor manera de administrarlas.

La siguiente pregunta es interesante ya que según las respuestas de los usuarios podemos ver (Fig.3.6) que el 77 por ciento de los encuestados no comparte información con el exterior de la empresa y el cero por cien ha compartido información alguna vez, lo cual nos ayuda con la ingeniería social que pretendemos adjuntar en la investigación.

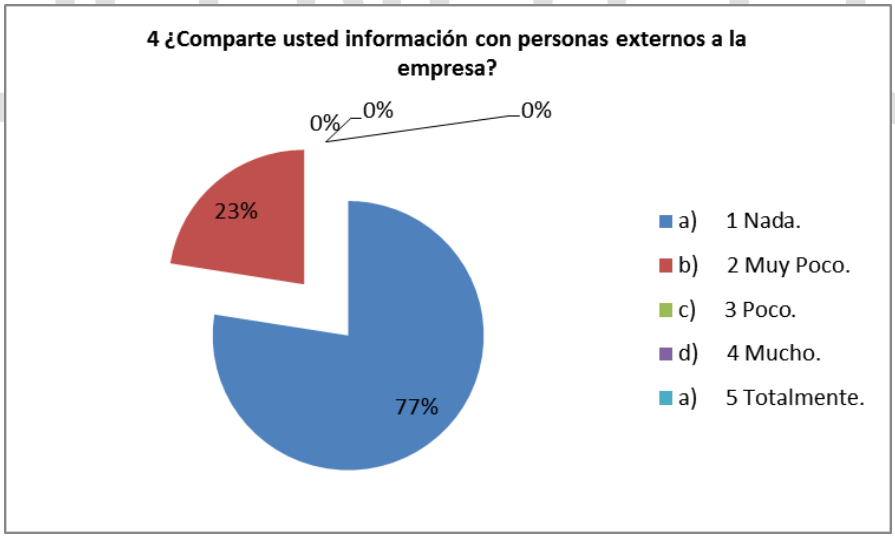


Figura 3.6 Pregunta 4.- ¿Comparte usted información con personas externas a la empresa?

Una de las estrategias claves en la implementación de seguridad y que sin duda puede ser decisiva en el éxito o el fracaso de la protección de la información es el cambio frecuente de contraseñas de los sistemas o aplicaciones utilizadas por el usuario ya sea que sean accesos a recursos en la red, algún archivo, una base de datos o un correo electrónico.

De acuerdo con esto decidimos incluir en nuestra encuesta a usuarios una pregunta para saber si cambian sus contraseñas o de una manera calculada por ellos mismos si cambian frecuentemente sus contraseñas, el resultado fue el siguiente (Fig.3.7).

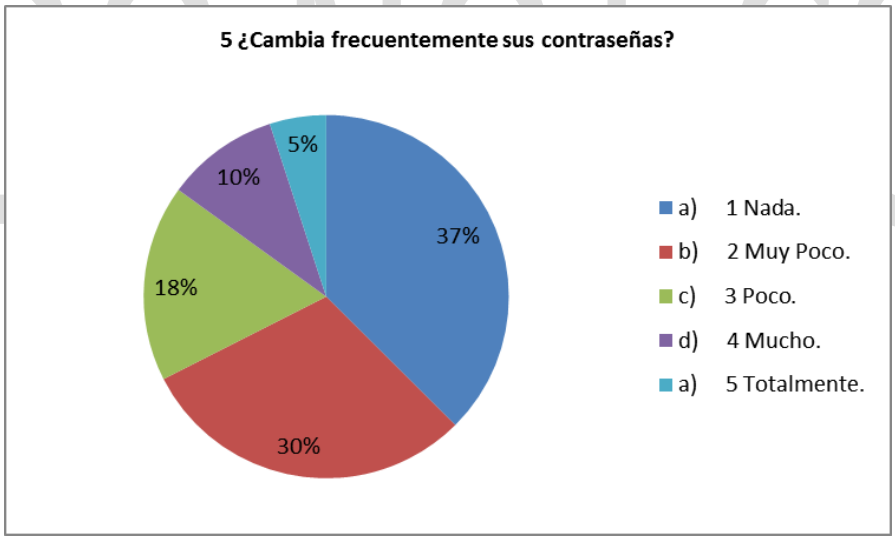


Figura 3.7 Pregunta 5.- ¿Cambia frecuentemente sus contraseñas?

Observamos que la mayoría de las personas no cambia frecuentemente sus contraseñas, como resultado más adelante explicaremos porque la importancia de cambiar las contraseñas frecuentemente.

CAPITULO IV.

ANALISIS DE LOS RESULTADOS.

4.1 INTERPRETACIÓN DE LOS RESULTADOS.

Este ultimo capitulo comprende tres partes principales las cuales mostraran, describirán en base a los resultados, para finalizar con algunas recomendaciones que se obtuvieron después de nuestra investigación y análisis de los datos, que como ya se dijo antes la cual tratara la interpretación de los resultados, conclusiones y recomendaciones.

En esta parte realizaremos una discusión de los resultados la cual traducirá e interpretara los hallazgos obtenidos en nuestra investigación y su relación con los objetivos y la hipótesis.

En base a los resultados obtenidos, observamos que en ocasiones no se cuenta con seguridad computacional, por falta de prevención, toda vez que observamos que los mismos usuarios ya sea expertos o no expertos no cambian frecuentemente sus contraseñas, esto por falta de información, además descubrimos que aunque en bajo porcentaje, existen todavía personas que no saben lo que es un antivirus o un firewall, primordiales en la seguridad informática, esto es preocupante ya que es importante y necesario un antivirus

en cualquier equipo de computo así lo refiere Maiwad (2005. P.12) en el que dice que “un software antivirus es una parte necesaria de un buen programa de seguridad informática”, así como también un bajo porcentaje de usuarios no saben lo que es un firewall (muro de fuego), que dentro de las organizaciones es tan importante como el mismo antivirus como también nos dice Maiwad (2005. P12) donde menciona que “un firewall es un dispositivo de control de acceso para la red y puede ayudar a proteger la información interna de una organización contra ataques externos”

4.2 CONCLUSIONES.

Dedicaremos esta sección para presentar las conclusiones obtenidas, las implicaciones teóricas y prácticas de los hallazgos del estudio, “las conclusiones deben analizar y evaluar los puntos principales de la investigación”, así lo refiere Ibáñez (1999. P169), de esta manera pretendemos terminar, analizar y evaluar nuestro trabajo de investigación.

La seguridad informática, tiene muchas partes y amenazas como indicamos en capítulos anteriores, debido a ello creemos que tiene que ver con todas las partes de nuestra investigación y los tres puntos que más sobresalieron en cuando a informática se refieren, como lo son, programas de seguridad informática (seguridad lógica), infraestructura de las instalaciones donde se encuentran nuestros sistemas de información (seguridad física) y la conducta

de los usuarios, como podría ser estar enterados de las implicaciones de la seguridad informática lógica y física así como también el cambio frecuente de las contraseñas, ya que observamos que la mayor parte de los accesos no autorizados a la información inicia con el usuario, cambiando frecuentemente sus contraseñas y eligiendo contraseñas complejas, para que a la hora de un intento de robo sea más difícil de identificar.

En general concluimos que si los usuarios de los sistemas de información ya sean expertos o inexpertos no están enterados de los métodos y elementos que componen la seguridad informática y los aplican en conjunto no se podrá cumplir la seguridad informática y podemos confirmar nuestra idea principal de investigación la cual menciona que: La seguridad en las tecnologías de la información se ve amenazada cuando se desconocen los métodos de seguridad informática.

Además de confirmar nuestra motivo de investigación descubrimos en el proceso de investigación que se necesita crear una cultura de protección de la información por parte de los usuarios de los sistemas, cambiando sus contraseñas frecuentemente, actualizando sus antivirus, y hasta siguiendo las medidas más básicas de la seguridad general en las instalaciones de las empresas.

¿Cómo prevenir virus y ataques externos? Si bien este trabajo de investigación es lo que trata de demostrar una de las más grandes recomendaciones que se hacen para garantizar al máximo posible la seguridad informática es hacer por

lo menos una revisión general al mes de los siguientes puntos, llevados a cabo a manera de bitácora con una lista de revisión que incluya los siguientes puntos.

- Actualización de programas de seguridad de Microsoft Update.
- Verificar que el antivirus este actualizando frecuentemente su base de definiciones de virus.
- Hacer una exploración completa del disco duro con el antivirus.
- Hacer una exploración completa de los discos extraíbles más usados.
- Depurar correo electrónico.
- Eliminar archivos temporales y cookies.
- Verificar que el firewall este activado.
- Cambiar contraseña de Windows y aplicaciones utilizadas.
- Recordar al usuario que debe hermetizar la información y no compartirla por ningún medio de comunicación, ya sean electrónicos o personales

4.3 RECOMENDACIONES.

En esta sección describiremos las recomendaciones de nuestros hallazgos en la información, en base a nuestros instrumentos de investigación y metodología utilizada en el trabajo de investigación.

En la investigación descubrimos que solo el 10% de nuestros entrevistados cambian frecuentemente sus contraseñas lo cual nos deja entre un rango de nada a poco del 90% de personas que no cambian continuamente las contraseñas de sus sistemas de información, así bien, recomendamos que los usuarios tengan un habito de cambio de contraseñas, por el lado de los expertos en tecnologías de la información recomendamos ampliamente extender sus conocimientos de seguridad informática, sobre antivirus, firewall y medidas preventivas a los usuarios que ignoren esta información ya que descubrimos que en conjunto todas estas medidas nos llevan a poder declarar que no se tiene incertidumbre o dudas sobre perdida de la información y se cuenta con seguridad informática.

Una vez contemplado en este trabajo de investigación un amplio panorama de los diferentes riesgos y según lo que encontramos en nuestro objeto de estudio, propondremos algunas maneras de proteger la información lo mas recomendable es usar todas en conjunto o usar alguna equivalente en cada recomendación.

4.3.1 INSTALACIÓN DE CONSOLA DE ANTIVIRUS.

Como se comento en capítulos anteriores la instalación de un antivirus es primordial a la hora de establecer los puntos de seguridad, este antivirus debe estar preferentemente administrado por una consola de seguridad la cual nos ayuda a manejar los clientes remotamente, como instalar el antivirus, actualizar la versión antivirus, actualizar la base de datos de protección de virus, ejecutar revisiones de disco duro de antivirus, es por ello que dedicaremos esta parte a explicar paso a paso como se instala, en este caso un Symantec Antivirus 11 Endpoint Protection Manager 11.

Se explicara con "pantallas" tomadas al mismo tiempo que fue hecha la instalación de este sistema antivirus en la empresa, se instalara el cliente de antivirus en todas las computadoras administradas por esta consola antivirus, mostraremos también la manera en que se están instalando los clientes en las computadoras de la empresa.

En la siguiente figura (Fig.4.1). Se inicia la instalación desde los archivos de instalación o fuentes, proporcionados por el proveedor en este caso Symantec.

Nos muestra una bienvenida a la instalación, avisando que el programa esta protegido por los derechos de autor, damos clic en “Next”.

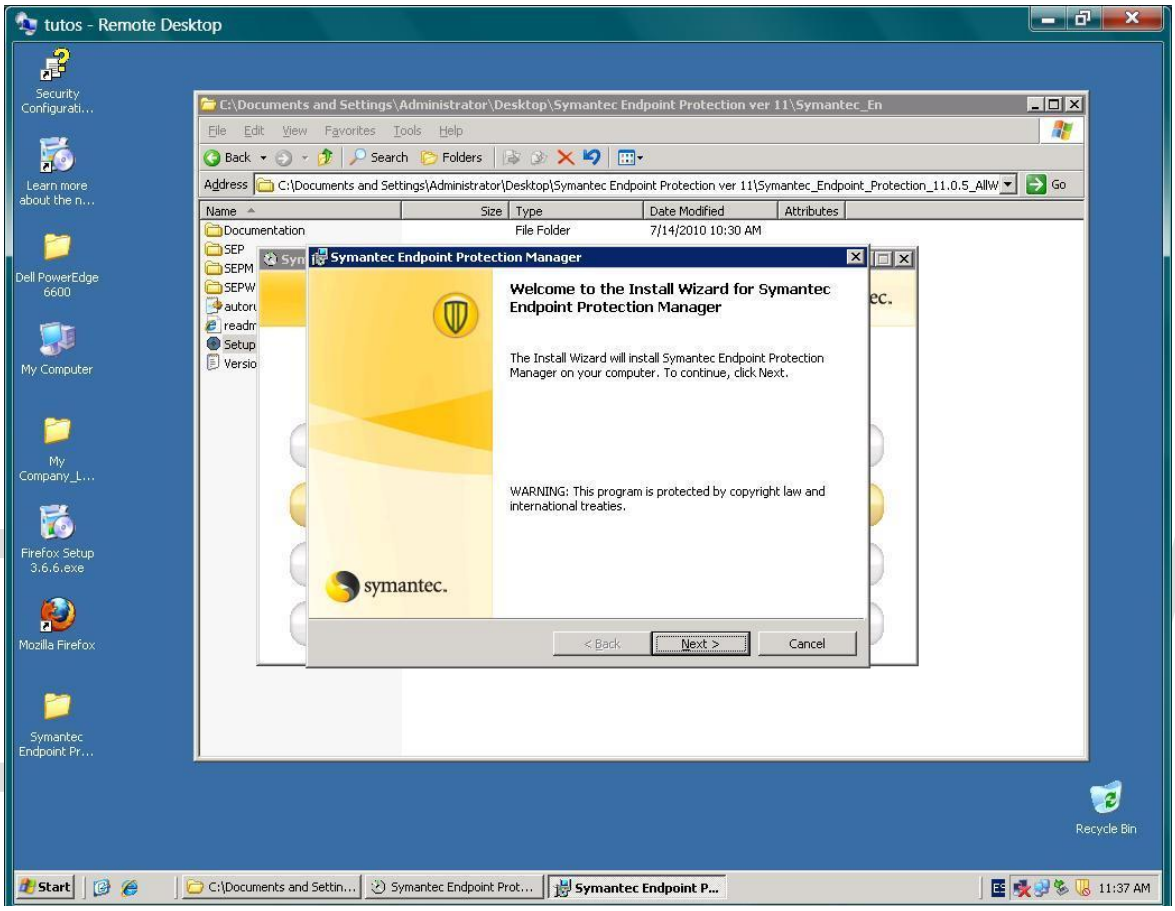


Fig.4.1. Bienvenida al asistente de instalación de Symantec Endpoint Protection Manager.

En la siguiente figura (Fig.4.2). Se muestran los términos de uso, o acuerdo de licencia, se recomienda imprimir o leer esta información ya que es necesario saber lo que el proveedor da a conocer y puede o no ofrecer o garantizar con la instalación de este producto, así como también los alcances legales de no cumplir con él acuerdo.

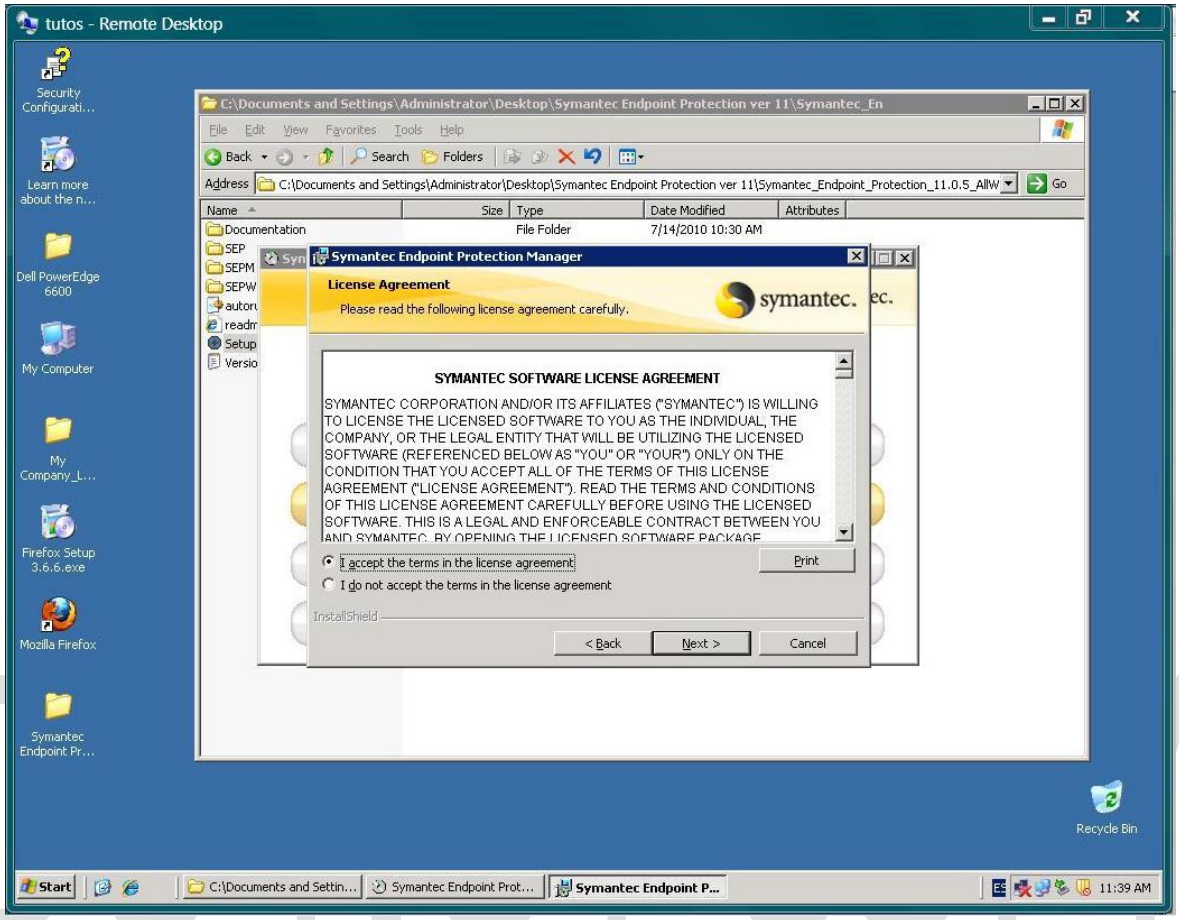


Fig.4.2. Acuerdo de licenciamiento.

Ahora es necesario dar clic en “Install” (Fig.4.3).

Fig.4.3. Listo para iniciar la instalación.

Después de unos minutos la instalación termina y se da clic en “Finish”. (Fig.4.4).

Fig.4.4. Instalación completa.

Una vez que tenemos instalada la consola antivirus accedemos desde el icono de antivirus nos muestra dos opciones para configurar elegimos “Advanced Mode” (Fig.4.5). Configuración recomendada para más de 100 clientes.

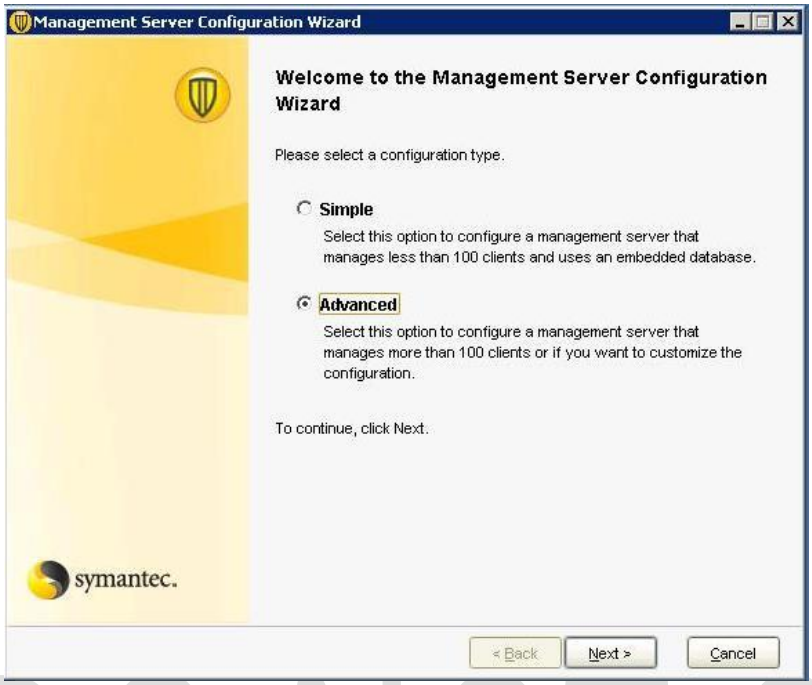


Fig.4.5. Modo avanzado para configurar más de 100 clientes de antivirus.

Como se pretende configurar un nuevo servidor de manejo, seleccionamos la opción “Install an aditional site” (Fig.4.6).

Fig.4.6 Elegir instalar un sitio adicional.

En la siguiente parte de la configuración (Fig.4.7). Debemos capturar el nombre del servidor (Server name), el puerto de comunicación (Server port), y puerto Web de administración (Web console port) y la ruta de un folder donde se guardaran los datos de configuración.

Una vez llenados los datos de “Server Name”, “Server Port”, “Web Console Port”, y “Server Data Folder” que corresponden a Nombre del servidor Puerto del servidor, consola web y carpeta de datos, respectivamente hacemos clic en “Next” para continuar con la instalación.

Fig.4.7 Información de acceso a servidor.

A continuación capturamos el nombre del sitio, “site name” (Fig.4.8). Se recomienda también elegir el mismo que se uso como nombre del servidor para evitar errores a la hora de reconocer el servidor.

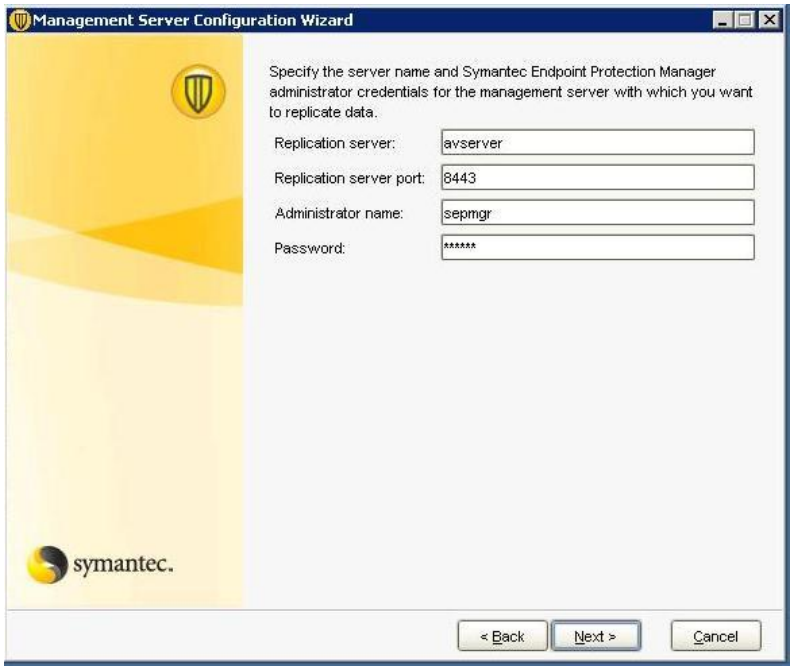


Fig.4.8 Nombre del Sitio.

Cuando se termina con estos pasos una advertencia de seguridad nos pregunta si queremos confiar en el certificado de seguridad entre Windows y el fabricante del sistema de seguridad, como nosotros mismos lo estamos instalando no hay problema hacemos clic en “Yes” (Fig.4.9).

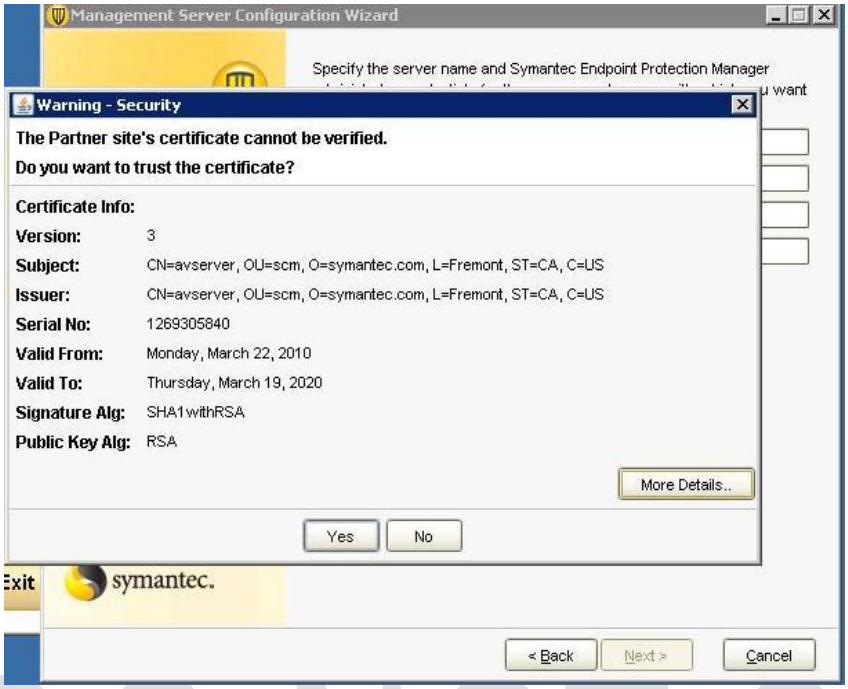


Fig.4.9 Advertencia de seguridad.

Seleccionamos “Embedded database” debido a que es más estable y de más rápido acceso (Fig.4.10).

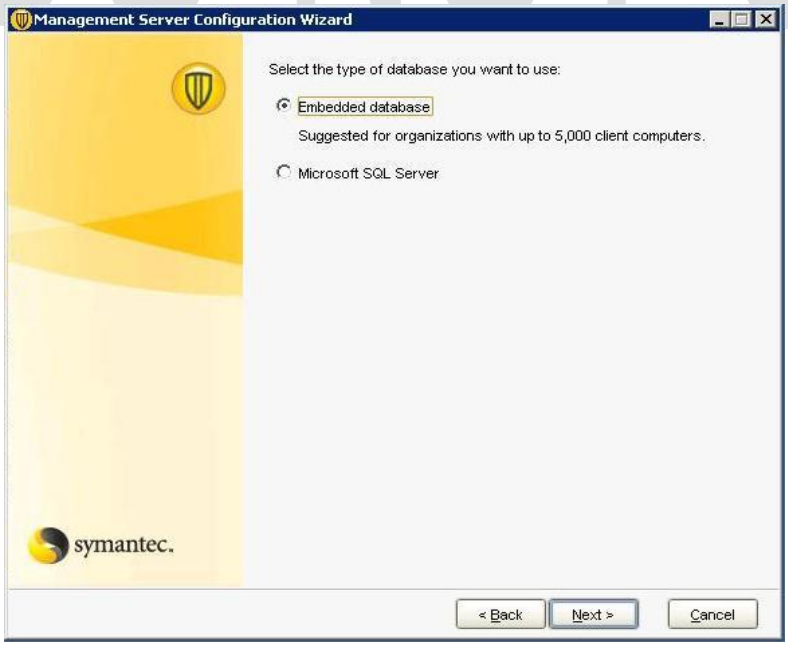


Fig.4.10 Selección del tipo de base de datos.

A continuación se configura la parte de la base de datos, en este caso la base de datos estará localmente, es decir, en el mismo servidor (nombrado como localhost) donde está instalada la consola de manejo del servidor, y en la cual para mayor seguridad es necesaria también asignar un usuario y password, así como también un puerto de comunicación.

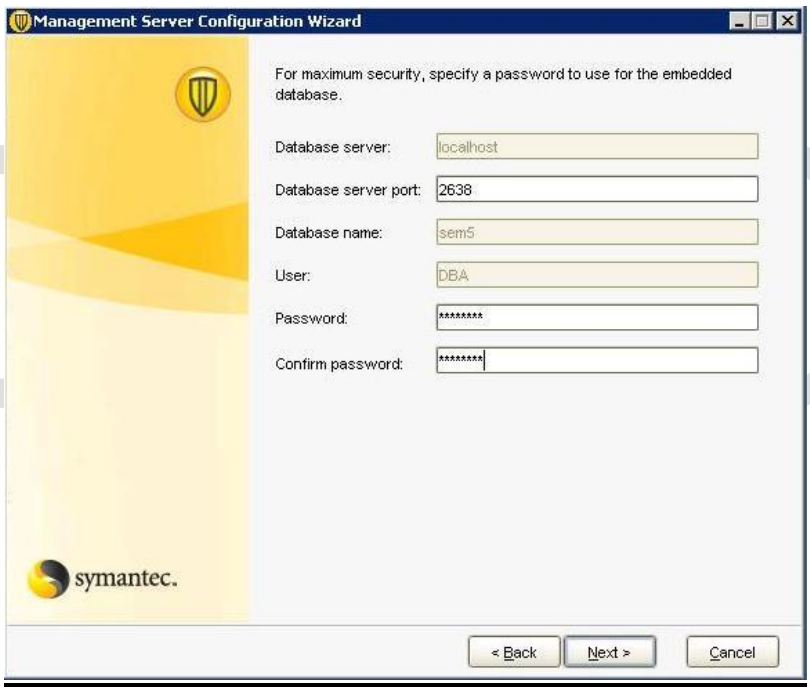


Fig.4.11 Seguridad de la base de datos.

Después de llenados los campos necesarios que brindaran mayor seguridad a la base de datos de equipo de la consola de seguridad, damos clic en siguiente (Fig.4.11). Este proceso inicia la creación de la base de datos, en la cual tarda

unos cuantos minutos para mandarnos a la siguiente parte del proceso en donde nos avisa que ha terminado (Fig.4.12) y dar clic en “Finish”.

Fig.4.12 Final de la configuración de la consola y base de datos.

A continuación seguimos con el acceso a la consola del servidor antivirus en la cual accedemos con el usuario y contraseña que hayamos asignado anteriormente iniciando una pantalla como esta (Fig.4.13).

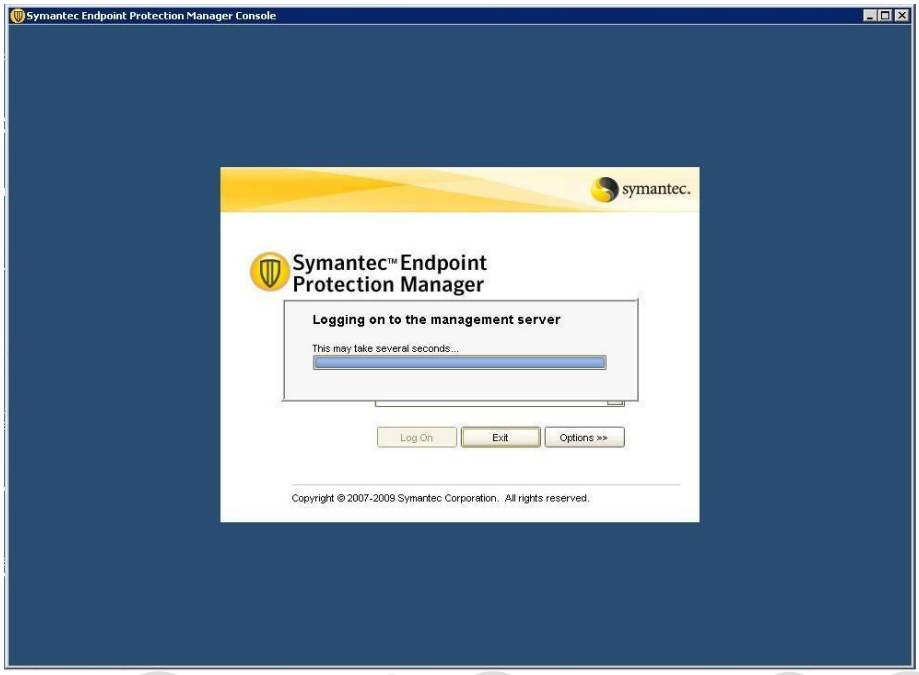


Fig.4.13 Acceso inicial a la consola de Symantec.

Inmediatamente podemos ver la consola de configuración de Symantec la cual aparece de la siguiente manera (Fig.4.14).

En ocasiones puede tardar el acceso inicial, esto depende de la velocidad de la red y las características del equipo de cómputo o servidor en el que se está instalando la consola de administración, para ello es importante cumplir y si es posible exceder los requerimientos mínimos de los programas que se usaran para crear el sistema de seguridad.

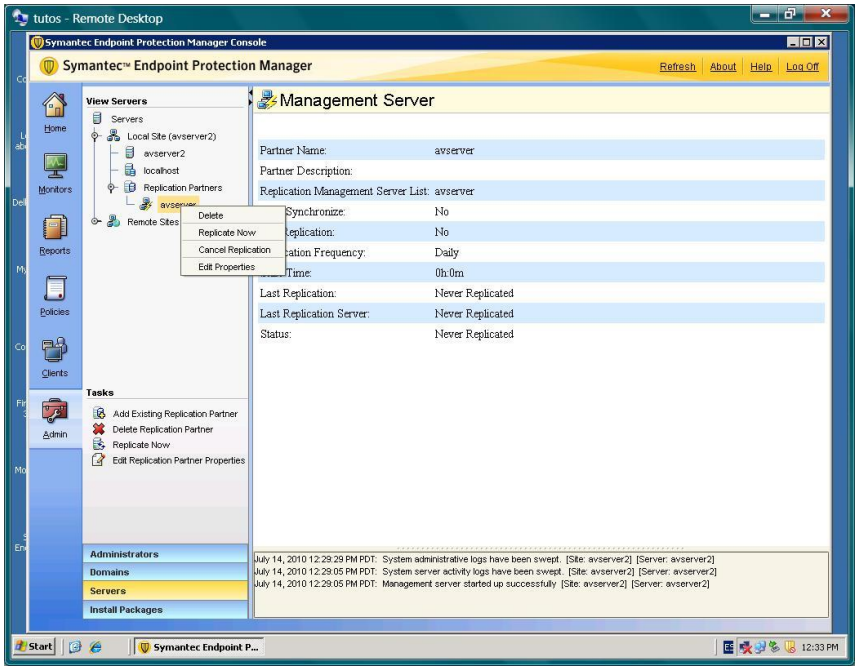


Fig.4.14 Opciones de la consola de administración de Symantec.

En la vista anterior tenemos las siguientes opciones. Home, información general de la consola, “Monitors”, en la cual podemos agregar computadoras cliente y monitorear si hay un virus o tiene las actualizaciones, “Reports”, podemos crear reglas que nos reporten el monitoreo hecho a alguna computadora cliente, “Polices”, en ella podemos editar permisos y políticas asignadas a cada computadora cliente, como si puede o no actualizar la definición de virus el mismo usuario o esta manejada por el servidor, si puede desinstalar el antivirus, en “Admin”, se pueden editar los usuarios que pueden acceder o usuario y contraseña de los administradores de la base de datos y el servidor.

4.3.2 ACERCA DEL FIREWALL O CORTAFUEGOS.

Un firewall o cortafuegos, como lo describimos en capítulos anteriores, es un programa que se encarga de permitir o bloquear el acceso a puntos en la red no permitidos, así también puede administrar el acceso desde y hacia el exterior de la red corporativa de datos.

Existen diferentes programas firewall, que ofrecen este servicio, algunos solo administran el trafico de los nodos de la red hacia Internet, otros bloquean accesos externos y otros hacen ambas partes, para esto utilizaremos dos programas en conjunto, uno es Check Point FireWall-1 de la empresa Check Point Software Technologies Ltd. Con un aditamento llamado “SurfControl Web Filter Product Support for Check Point Firewall-1”, el cual usaremos para ejemplificar como funciona un firewall.

Firewall-1 utiliza una tecnología propia para la protección de los dispositivos en la red así lo asegura en su pagina Web “Firewall-1 es líder en la industria firewall, ofreciendo la línea mas segura de protección. Usando INSPECT, la tecnología de inspección mas adaptable e inteligente, integra protección a la capas de red, protocolos y aplicación” (http://www.checkpoint.com/products/firewall-1/, Consultado, el 20 de febrero 2011), así como también lo expresa Welch-Abernaty (2005. PP.8) “Chekpoint Firewall-1 advierte, protege e inspecciona, complejamente la red de datos de una manera rápida”.

4.3.3 UTILIZACIÓN DE WSUS (WINDOWS SERVER UPDATE SERVICES).

Cuando una versión de Windows sale al mercado aun no se conocen los riesgos o agujeros de seguridad que el sistema operativo pueda tener, es por esto que microsoft.com libera periódicamente actualizaciones de sus sistemas operativos para garantizar la seguridad antes de que posibles hackers descubran los errores de seguridad que pueda tener el sistema operativo.

Para uso domestico es normal actualizar a un horario predefinido por el usuario una revisión de actualizaciones e instalarlas o bien lo puede hacer manualmente, esto podría hacerse también en una empresa, sin embargo no es recomendable que todas las computadoras hagan esto ya que generaría demasiado tráfico en la red y las computadoras tendrían un puerto mas abierto expuesto a Internet, esto sin mencionar que el usuario podría olvidar hacer este procedimiento.

La empresa tecnológica, Microsoft ofrece un servicio de actualizaciones automáticas en el que una sola computadora esta revisando las actualizaciones para distribuirlas en una red local Fig. 4.15, este servicio es llamado: Windows Server Update Services.

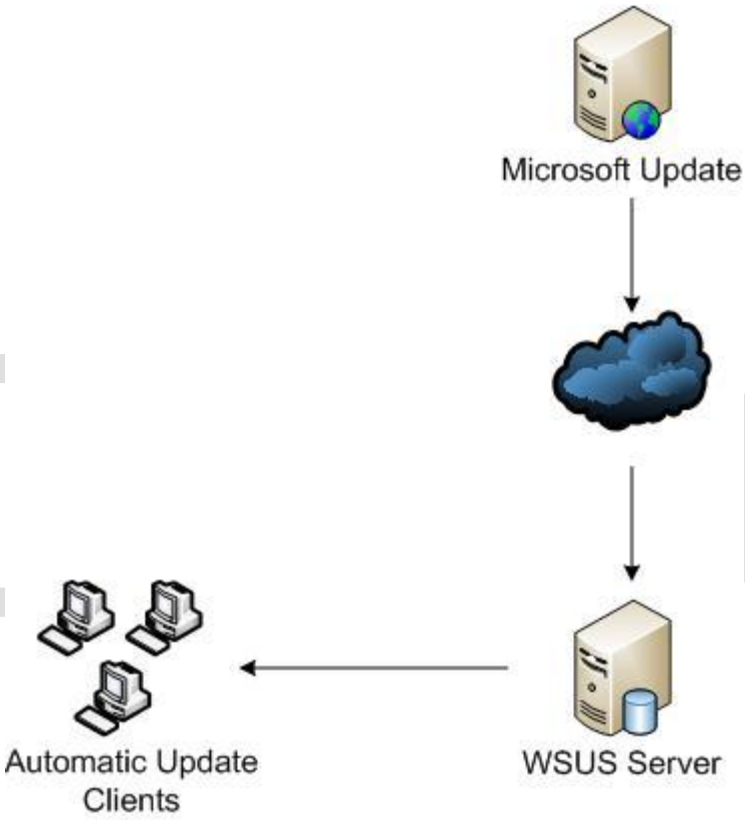


Figura 4.15 Funcionamiento de Windows Server Update Services.

Para instalar es necesario tener los archivos de instalación, explicarlos también como se instala de una manera rápida, para pasar a la consola de administración de Windows Server Update Services.

El archivo es bajado de la siguiente página: http://go.microsoft.com/fwlink/?LinkId=88321 (Consultado el 28 de Febrero 2011).

1. Hacemos doble clic en archivo, generalmente nombrado como "WSUSSetup.exe".
2. Clic en "NEXT" y seleccionamos "Administration Console Only", clic en "NEXT".
3. Leemos y aceptamos los términos del contrato de licenciamiento.
4. Hacemos clic en "Required Components to use Administration UI" esto para una interfaz de usuario grafica, clic en "NEXT".
5. Clic en "Finish".
6. Para actualizar e iniciar la consola de administración por primera vez hacemos clic en los siguientes iconos, clic en "Star", clic en "All Programs", "Administrative Tools", y al final en "Microsoft Windows Server Update Services". Ahora veremos la consola de administración de MS WSUS, Fig.4.16.

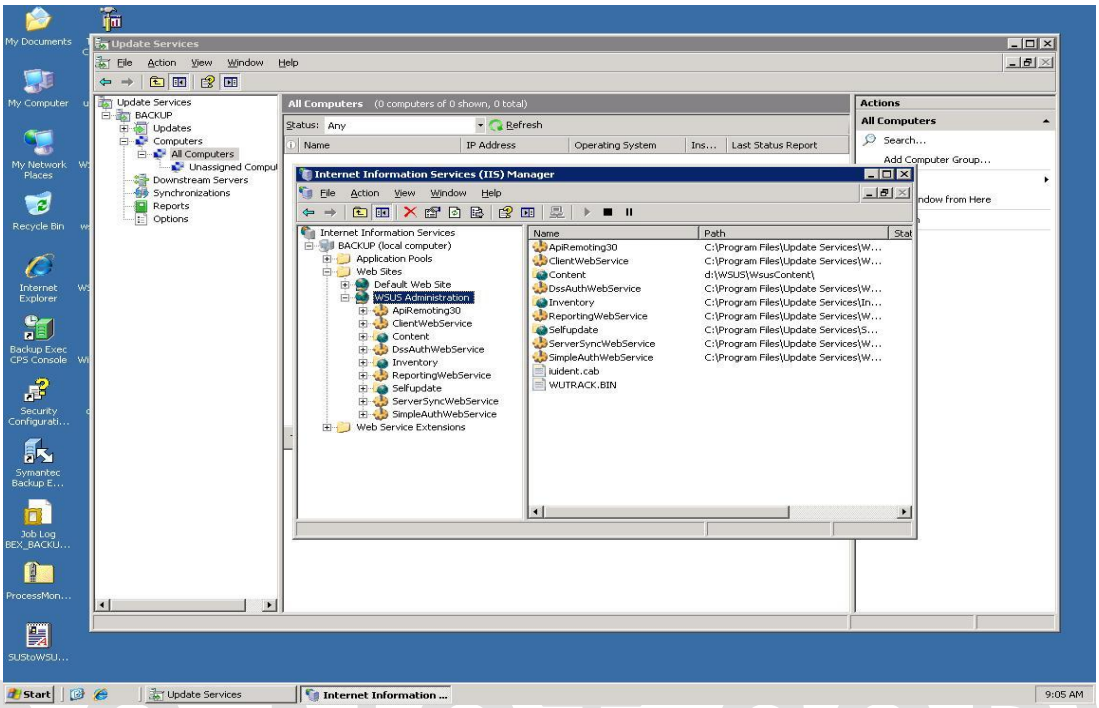


Figura 4.16 Pantalla general de WSUS.

4.3.4 ARCHIVOS DE NAVEGACIÓN.

Los archivos de navegación son archivos completos, fragmentados o encriptados que son almacenados en una ruta predefinida en el disco duro, por páginas Web mediante el navegador utilizado, se clasifican en archivos temporales y complementos.

La información de almacenamiento, puede ser vista en las opciones o preferencias del navegador, clasificadas generalmente en la sección de seguridad. Es recomendable borrar estos archivos frecuentemente por que pueden almacenar información, del usuario en la computadora como correos electrónicos y datos capturados por el usuario en algún formulario Web.

Las cookies no representan un alto riesgo, pero pueden ayudar a deducir información investigada o monitoreada por un usuario espía de tu computadora. Con esto concordamos con el autor Gorley, (2002, p.275) “Las cookies por si solas no representan un riesgo de seguridad, porque pueden ser deshabilitadas o borradas y se usan directamente en un modelo cliente-servidor”, si bien, las cookies pueden o no ser peligrosas y debe ser a criterio del usuario la decisión de cuando borrarlas. Las cookies son archivos de texto, hechas en los mismos lenguajes de programación basada en scripts que las páginas Web,

Las cookies, por ejemplo, se utilizan para: dar una bienvenida personalizada en una página Web, esto es si le das tu nombre a una página, se guarda una cookie y la siguiente vez la pagina te puede recibir con un “Hola: tú nombre”, también puede utilizarse para saber cuándo fue la última vez que se ingreso una página, o si se personalizo la pagina con algún color, o bien guardar tus datos generales como nombre, edad, sexo, etc.

Por otro lado tenemos los archivos temporales de Internet, son un apartado o carpeta en nuestro disco duro, que guarda archivos de paginas navegadas, a diferencia de las cookies, las paginas pueden crear subcarpetas en las que guardan diferentes archivos, que no tengan que ser descargados cada vez que se visita la pagina y así agilizar la velocidad al momento de recargar o acceder a la pagina.

El riesgo en los archivos temporales de Internet persiste en que las paginas con programas malignos, pueden aprovechar este acceso para guardar archivos

ejecutables o scripts (guiones automatizados) que se ejecuten en un momento determinado, por ejemplo, al reiniciar el sistema operativo y con esto causar un daño en el sistema operativo o instalar un programa como lo son los Ad-Ware.

4.4 CONCLUSIONES FINALES.

Como al principio del presente trabajo recepcional de investigación se comento que existen diferentes partes que te ayudan a garantizar el máximo nivel de seguridad informática, descubrimos finalmente que solo se lograría si se encuentran en perfecto funcionamiento y constante mantenimiento todas las partes encontradas, como lo son la seguridad física y la seguridad lógica como programas informáticos ya sea antivirus, cortafuegos un programa que restringa Internet, estar al pendiente de la ingeniería social informática.

Es así como descubrimos y recomendamos que se abarquen todos los puntos visibles y no visibles de amenazas a nuestra entidad de red para dejar menos accesos vulnerables de información y así obtener como resultado una sana seguridad informática.

REFERENCIAS BIBLIOGRAFICAS.

- Hallberg Bruce A, “Fundamentos de redes”, Editorial McGraw-Hill, 2003, primera edición. México DF.
- Hernández Sampieri Roberto, “Metodología de la investigación”, Editorial McGraw-Hill, 2003, tercera edición. México DF.
- Ibáñez Bramvila Bereneci, “Manual para la elaboración de tesis”, Editorial Trillas, 1999, segunda edición. México DF.
- Kendall Kenneth E, “Análisis y diseño de sistemas”, Editorial Pearson, 2005, sexta edición.
- Maiwald Eric, “Fundamentos de seguridad en redes”, Editorial McGraw-Hill, 2005, primera edición. México DF.
- Maxwell Steve, “Red Hat Linux” Editorial McGrawHill, 2001, primera edición. México DF.
- McMahon Richard A, “Introducción a las redes”, Editorial Anaya, 2003, primera edición. México DF.
- Molina Francisco J, “Redes de área local”, Editorial Alfaomega, 2004, primer edición. México DF.
- Rosales Uriona Guido “Estrategias para la seguridad de la información Editorial Yanapti, 2002, Primer edición, La paz Bolivia.
- Simmons Curt, “Redes con windows xp”, Editorial McGrawHill, 2003, primera edición. México DF.
- Tanenbaum Andrew S, “Redes de computadoras”, Editorial Pearson, 2003, cuarta Edición. México DF.
- http://www.symantec.com -Consultada en febrero 2011.
- http://www.microsoft.com -Consultada en febrero 2011.
- http://www.checkpoint.com -Consultada en febrero 2011.