UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

Riesgo en el contagio de Spyware: software espía.

Seminario Taller Extracurricular
"Análisis de la Planeación"

Que para obtener el Título de:

Licenciado En Matemáticas Aplicadas y Computación

Presenta:
José Juan Escamilla

Asesor: Act. Liliana Sandoval Luna **Noviembre 2008**

A mis PADRES:

Gracias por que antes que nada me dieron la vida, y no solo física si no espiritual. Por enseñarme valores como el respeto, admiración, confianza y por sobre todo a amar de corazón.

A usted MAMÁ que nos enseño de una forma especial a leer y escribir gracias a esa enseñanza que da la vida misma y de la cual usted se graduó con honores.

A mi PAPÁ por nunca darse por vencido y luchar insaciablemente sin importar la tempestad, por ser tan responsable y ser un HOMBRE hecho y derecho. Por demostrarme que la suerte no existe, si no se busca con el trabajo día a día.

Por que estoy orgulloso de ustedes, los admiro y los respeto son el cimiento de la familia, y son un ejemplo a seguir.

Les dedico este trabajo que es de ustedes, de su esfuerzo y lucha diaria. Por que éste es el fruto de la semilla que ustedes sembraron con tanto amor y dedicación.

A mi esposa:

Por darme tres hijos hermosos fruto de nuestro amor, por este tiempo que hemos convivido y por tantos momentos felices que se quedan grabados en nuestro corazón.

Por tu apoyo brindado hacia mi persona, espero sigas siendo la mujer de la cual me enamoré, y no ocultes esa gran mujer que llevas dentro.

Para tí todo mi amor respeto y confianza.

¿Vive una rosa en tu corazón?

Vive mientras la mantengas fresca

Fresca está con el rocío de mi Amor

A mis hijos:

Por ser una parte de mí, es por tal motivo que ustedes están presentes en cada actividad que realizo.

Ustedes son el motor de mi vida, con ustedes he conocido la importancia de la risa, el ser niño nuevamente, admiro las energías que poseen pero sobre todo les agradezco el amor tan sincero que profesan. Ese amor que demuestran con una risa, una mueca, un gesto, y muchas veces hasta con una lágrima.

Porque este trabajo es para ustedes y se los dedico por que al verlos estudiar y trabajar en su escuela me enseñaron que uno es capaz de aprender y salir adelante con el simple deseo de proponérselo,

Yair, Mahetzi y Yael, espero que este libro sea un estímulo para ustedes, y un aliento para concluir sus estudios.

A mis profesores del Seminario:

Porque de ellos aprendí no solo el análisis de la planeación, si no porque aprendí que tanto el conocimiento como el saber es para trasmitirlo no para guardarse, y se propaga a través de humildad y empeño hacia el trabajo.

Al profesor Hugo por ser la parte idealista de este seminario, por poseer tanta sabiduría y ser un libro viviente.

Gracias profesora Lavín, por ser la maestra amiga, la que tiende la mano cuando uno lo necesita.

Al profesor Juan por ser el eje rector de este seminario, porque todo gira alrededor de su conocimiento y experiencia.

También al profesor Gerardo ya que posee la parte normativa que sustenta este seminario.

Y en especial a la profesora Liliana, por abrirme el panorama de lo grande que es la planeación en esa su primera entrevista para conmigo, ya estaba destinada a ser mi asesora. Por el tiempo que le dedicó a mi trabajo y corregirme los errores que en su momento tuve.

GRACIAS, les doy las mas sinceras gracias; por ser tan excelsos y tan comprometidos en su trabajo, son personas dignas de ejemplo, lucha y amor a ésta nuestra Universidad.

A la Universidad Nacional Autónoma de México:

Por ser la institución que me brindó los conocimientos necesarios para concluir una Licenciatura, por estar conmigo 7 años rodeada de conocimientos y experiencias de aprendizaje.

No por algo es la más grande Universidad de América Latina, que nos deja expresarnos libremente, por su esencia misma que ninguna otra Universidad tiene.

"Por mi raza hablará mi espíritu"

INDICE

INTRODUCCIÓN

Introducción

A lo largo del tiempo y de la historia se ha querido conocer los gustos, las preferencias, las formas de actuar, de vivir, etc. de otras personas, para obtener o sacar un beneficio personal o de interés hacia un tercero, es por es eso que se tiene la necesidad de espiar lo que realiza la persona o las personas de las cuales se tiene algún interés.

El espiar es la acción de obtener información secreta que el espiado no desea revelar dado que es personal y confidencial.

El funcionamiento y los métodos del espionaje son tan distintos así como ilimitados. Pese a la forma que le han otorgado las novelas y películas de ficción y los medios de comunicación, el espionaje generalmente esta intrínsicamente unido al engaño y muy comúnmente al fraude.

El espionaje requiere y precisa de deslealtad para obtener información privilegiada. Emplea y recurre a la tecnología y algunas otras técnicas para descubrir y conseguir información secreta.

Este término de espionaje, era utilizado con mayor frecuencia en el ámbito militar, económico o político. De hecho tanto la primera como la segunda guerra mundial así como la guerra fría y ahora en la competencia de negocios necesitaron de espionaje como una estrategia para obtener información del enemigo. Hoy en día las formas y técnicas del espionaje se apoyan en las cada vez más eficientes tecnologías de la comunicación. Como ejemplo el teléfono, el cual puede ser interceptado para escuchar y espiar la información que se trasmite por este medio; o las cada vez más avanzadas cámaras de fotografía que son una herramienta para espiar aún cuando la persona se encuentre en medio de la oscuridad.

En la actualidad el espionaje utiliza a las computadoras como una herramienta principal por la gran capacidad que éstas tienen para el manejo de la información, es así como los piratas informáticos, como los hackers y crackers independientes o contratados pueden conseguir información, localizadas en computadoras; por medio de programas: software espía (Spyware), tema central de la presente investigación.

El software espía además de obtener información importante y confidencial puede ocasionar un daño muchas veces difícil de reparar o hasta en varios casos irreparable, ya que una vez infectada la máquina empieza a trabajar de una manera que en ocasiones pasa inadvertida para el usuario y que éste se da cuenta ya cuando el daño esta muy avanzado al notar que sus computadoras están muy lentas, le salen leyendas de archivos dañados o faltantes, que se reinician o apagan solas y/o en definitiva ya ni encienden o no carga el sistema operativo dejándolas inutilizables además de perder lo mas importante: la información.

La información es poder, es por ello que las organizaciones deben de valorarla mucho así como protegerla.

Además, no sólo el volumen, sino la importancia de esta información para el desarrollo económico y social, son cada vez de suma importancia. De hecho, en la actualidad, las organizaciones tienen que considerar que la información es otro bien más de sus activos y en muchos casos, prioritario sobre los restantes de la organización.

Pero gran parte de esos datos, han sido tratados sea durante su proceso, almacenamiento o transmisión, mediante las llamadas tecnologías de la información, entre las que ocupa un lugar focal la informática.

Consecuentemente, la seguridad de las tecnologías de información, y por ende de la informática, se convierte en un tema de importancia crucial para el continuo y espectacular progreso de la sociedad, e incluso para su propia supervivencia.

Este trabajo tiene como objetivo analizar los principales motivos de contagio del software espía en computadoras con sistema operativo Windows, con el propósito de proporcionar información y sus riesgos que conlleva, además de tener la intención de que sirva de guía para detectar y prevenir el Spyware, como una medida de seguridad.

Además se explicará de una forma mas detallada lo que es el software espía, sus problemas que conlleva, los riesgos de contagio, las formas de infección, así como los diferentes tipos de Spyware.

Que aunque para algunos estos conceptos sean distintos, en este trabajo se les considerará como Spyware, ya que interactúan entre sí para que el Spyware se ejecute, es decir, por ejemplo: El caballo de Troya es el medio por el cual el Spyware se introduce a la computadora de una forma oculta para no ser detectado, y se expande o distribuye por medio del spam, para reproducirse por lo general con ayuda de un virus o un malware, haciendo que la computadora se llene de adware.

La finalidad es tener una investigación que se enfoque a reducir el daño que ocasiona el Spyware y que sea útil para cualquier computadora y/o empresa, aunque en el proyecto se considerará el caso específico de usuarios de computadoras personales en un despacho contable.

El presente trabajo se divide en tres capítulos.

En el primer capítulo se hablará de lo que es el Spyware, como se instala, así como los tipos de Spyware que existen. Además de los diferente y distintos medios de

contagio para su propagación y sobrevivencia, además de la Seguridad informática, sus términos y características. Y finalmente se describirá la organización en la que se realizara el estudio que represente la problemática de los daños y riesgos el cual origina el software espía.

En la segunda parte del trabajo se explicará el diagnóstico de la problemática de la organización, así como algunas definiciones de la planeación la cual será utilizada como método y herramienta para la solución del problema. Así como su diseño para obtener el objetivo sus metas y fines. Y establecer estrategias para su logro. Además, asignar recursos y señalar responsabilidades de realizar tareas para concluir con el establecimiento de un plan así como sus mecanismos de control y seguimiento a través de sus programas.

En el último capítulo se plasmarán los resultados que se obtuvieron una vez ejecutado el plan, sus datos y su evaluación, para por último proyectar a futuro hacia donde va el Spyware a través de los escenarios, teniendo en consideración sus cuatro posibles resultados.

Luego entonces, los escenarios son parte fundamental para tener una visión de lo que será el futuro del software espía con base en datos tanto cuantitativos como cualitativos.

Capítulo 1
¿Qué es el Software Espía?

Capítulo 1: Comenzando

Los riesgos del Spyware (software espía) y adware (software publicitario) están aumentando a un ritmo constante, convirtiéndose en un reto de gran escala para los administradores de seguridad de redes y más aún para los usuarios de computadoras personales. El Spyware coloca a las usuarios de computadoras personales en una situación de riesgo ya que causa una disminución de la productividad, más recursos financieros solicitando ayuda hacia un tercero (llamémosle técnico y/o ingenieros en computación) pérdida de privacidad y lo peor, pérdida de información.

Ya se utilice para propósitos comerciales o con otros motivos más siniestros, el Spyware (software espía) se ha convertido recientemente en una molestia casi equiparable a los virus, si no es que superior. Y ahora la pregunta del millón. ¿Qué es un Spyware?

1.1 El Spyware

Spyware o "Software espía" es el término general que se utiliza en referencia a aplicaciones de software que llevan a cabo determinados tipos de tareas como, por ejemplo, promociones publicitarias, recopilación de información personal o modificación de la configuración de Microsoft Windows en su equipo sin su consentimiento. El software espía o las aplicaciones no deseadas pueden llegar a su sistema de varias formas: Un truco muy común es instalar el software disimuladamente durante la instalación de otro software que sí ha solicitado como, por ejemplo, un programa de archivos compartidos de música o video.[1]

El Spyware es un programa de software espía que tiene la capacidad de auto instalarse en las computadores personales de los usuarios, con objeto de conocer su identidad y monitorear el comportamiento del equipo o los hábitos de navegación en Internet.[2]

[1] "Spyware", http://www.microsoft.com/latam/athome/security/Spyware/
[2] "Spyware", http://www.seguridad.unam.mx/usuario-casero/Spyware.dsc

El Spyware puede ser instalado en el sistema a través de numerosas vías, entre las que se encuentran: troyano, que los instalan sin consentimiento del usuario; visitas a páginas Web que contienen determinados controles ActiveX o código que explota una determinada vulnerabilidad; aplicaciones con licencia de tipo shareware o freeware descargadas de Internet, etc.

El Spyware puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con recolección de datos y la forma en que son posteriormente utilizados.

Spyware es un término general que designa los programas que supervisan de forma encubierta la actividad del usuario en el equipo, y que recopilan información personal como por ejemplo nombres de usuario, contraseñas, números de cuenta, archivos e incluso el número de la licencia de conducir o de la Seguridad Social, phishing. Algunos programas de Spyware se centran en espiar el comportamiento de una persona en Internet; este tipo de Spyware efectúa, a menudo, un seguimiento de los lugares que esa persona visita y de las actividades que realiza en la red, los correos electrónicos que escribe y envía, así como sus conversaciones de mensajería instantánea. Tras recopilar toda esta información, el programa de Spyware la transmite a otro equipo por medio de correos electrónicos, spam, por lo general, con fines publicitarios. Otros más se dedican a capturar los caracteres que se escriben a través del teclado al instalar keyloggers y capturar en el momento preciso que se están digitando, mandándolos en archivos de texto o de extensión *.log.

El Spyware modifica el comportamiento de la máquina, crea nuevas carpetas, altera los registros de archivos DLL (librerías), funge como un servidor para conectarse y enviar los datos extraídos del equipo.[3]

[3] http://www.alambre.info/2007/

1.1.1 Como se instala el Spyware

El Spyware se instala de muchas formas:

Con frecuencia, el Spyware se instala involuntariamente junto con otro software que el usuario desea instalar. Por ejemplo, si se instala un servicio "gratuito" para compartir música o archivos. Por ejemplo los programas P2P, ya antes descritos, o bien si se descarga un protector de pantalla, es posible que al mismo tiempo se instale algún tipo de Spyware, o en el momento en que empieza a funcionar el protector de pantalla. También cabe la posibilidad de que algunas páginas Web intenten instalar Spyware cuando se las visite, por lo regular a través de un ActiveX o una función programada en Java, que son mostradas como ventanas emergentes. Otros Spyware se instalan al momento de jugar juegos en línea ya que abren puertos para mandar y recibir información.

Las ventanas emergentes son generalmente, ventanas muy molestas que aparecen al navegar y muestran publicidad o información que es difícil de eliminar y que aparece constantemente.

Son una forma en línea de publicidad en el World Wide Web, que aumentan el tráfico de la red o que son también usadas para capturar direcciones de e-mail. Trabaja cuando ciertos sitios abren una ventana del buscador para exhibir los anuncios. La ventana pop-up que contiene un anuncio es generada normalmente por JavaScript, pero se puede generar por otros medios también.

Una variante en las ventanas pop-up es hacer aparecer el anuncio debajo de la ventana activa o en direcciones fuera del área visual, normalmente en la parte inferior derecha, y suelen aparecer como intentos de abrir una página nueva durante unos milisegundos, hasta cargarse y cumplir su cometido, cerrándose inmediatamente, con lo cual el usuario no se percata cuando surge, sino hasta que cierra su navegación, con lo que difícilmente puede identificar junto a que página surgió, sobre todo en aquellas sesiones en que se tienen varios documentos abiertos.

Pero una de las maneras mas comunes de adquirir Spyware es al visitar páginas pornográficas, unas tan solo con visitarlas es suficiente para infectarse del Spyware, y otras más después de realizar un recorrido supuestamente gratis, se les pide que instalen un programa adicional para ver miles de imágenes más, solo que el usuario no sabe que ese programa adicional es el Spyware, es decir, es el mismo usuario que con su consentimiento pero con ignorancia lo instala.

De igual modo, si una persona desea supervisar sus actividades en Internet, puede instalar Spyware de forma manual. En función de cómo se haya realizado la instalación, puede tratarse de la supervisión aceptable de una persona o de una acción poco grata o incluso ilegal considerada como una invasión de la privacidad.

Para que el Spyware se instale, claro esta en forma oculta y sin que el usuario se de cuenta, llama la atención con temas actuales o información que el usuario quiere conocer, por ejemplo en la época navideña, alienta en instalar software con alusión a la fecha, o mandar postales para amigos que no son más que software oculto, es decir caballos de Troya, que una vez que el usuario lo ejecuta esta ejecutando al mismo tiempo el Spyware, otro ejemplo es “bajar” canciones o videos que están de moda de una forma gratuita y que por lo regular viene supuestamente compreso, ya que supuestamente el archivo es el nombre de la canción con extensión zip o rar, de hecho el archivo si viene compreso pero no incluye la melodía o la canción si no un archivo ejecutable, que es el programa o software espía, y es aquí donde el usuario se da cuenta que pudo haber cometido un error, aun sin estar seguro, aunque lo que si sea seguro es que su computadora ha sido contagiada de Spyware.

Se introduce en las computadoras sin que se tenga conocimiento aunque si muchas veces con consentimiento, efectúa las operaciones de una forma más lenta de lo normal, muestra anuncios no deseados (adware) y espía los hábitos de navegación por Internet; dada su creciente presencia, el software espía últimamente se ha convertido en una amenaza casi tan o más importante que los virus. Se presenta bajo

diversas formas y, en ocasiones, se asocia con caballos de Troya o con técnicas relacionadas con el robo de identidad. El software espía intenta robar contraseñas o espía las pulsaciones de teclas con objeto de acceder a información confidencial, es posible que esto sólo constituya un pequeño porcentaje en comparación con otras categorías de Spyware , pero, sin lugar a dudas, se trata de una cifra nada despreciable que debería ser motivo suficiente para proteger la computadora.

1.1.2 Tipos de Spyware

A continuación encontrará la descripción de las diferentes formas que adopta el Spyware.

Adware

Adware es una palabra inglesa que nace de la contracción de las palabras Advertising Software, es decir, programas que muestran anuncios. Se denomina adware al software que muestra publicidad, empleando cualquier tipo de medio: ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc. La publicidad está asociada a productos y/o servicios ofrecidos por los propios creadores o por terceros.

El adware puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así. Lo mismo ocurre con el conocimiento o falta del mismo acerca de sus funciones.

Adware: esos molestos anuncios constituyen quizá el tipo de Spyware más irritante, pero no necesariamente el más peligroso; el adware es el software espía que muestra anuncios no deseados cuando se conecta a Internet. No sólo obstaculizan la navegación por Internet, sino que también la ralentizan considerablemente, y algunos anuncios dirigidos a adultos pueden mostrar, en algunos casos, contenidos desagradables. El adware puede infiltrarse en las computadoras cuando se instala software gratuito que contiene adware (como software para el uso compartido de

archivos musicales) o bien cuando visita páginas Web plagadas de Spyware. En teoría, su objetivo consiste en mostrar publicidad, preferiblemente relacionada con los intereses del usuario de Internet.

Malware

Malware malicious software, también (del inglés llamado badware o software malicioso) es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas ya que en esta categoría se encuentran desde un troyano hasta un Spyware.[4]

Malware o software de actividades ilegales es una categoría de código malicioso que incluye virus, gusanos y caballos de Troya. El malware destructivo utiliza herramientas de comunicación conocidas para distribuir gusanos que se envían por correo electrónico y mensajes instantáneos, caballos de Troya que provienen de ciertos sitios Web y archivos infectados de virus que se descargan de conexiones P2P. El malware también buscará explotar en silencio las vulnerabilidades existentes en sistemas del equipo o la red. Las vulnerabilidades también pueden crearse por configuraciones incorrectas de seguridad o del equipo. Las amenazas explotan las debilidades de las vulnerabilidades que dan como resultado posibles daños al equipo o a los datos personales.

Cookie

Los cookies son archivos en los que almacena información sobre un usuario de Internet en su propio ordenador, y se suelen emplear para asignar a los visitantes de un sitio de Internet un número de identificación individual para su reconocimiento subsiguiente. La existencia de los cookies y su uso generalmente no están ocultos al usuario, quien puede desactivar el acceso a la información de los cookies; sin embargo, dado que un sitio Web puede emplear un identificador cookie para construir un perfil de

[4] "Malware", http://www.symantec.com/es/mx/norton/security_response/malware.jsp

un usuario y que dicho usuario no conoce la información que se añade a este perfil, se puede considerar al software que transmite información de las cookies, sin que el usuario consienta la respectiva transferencia, una forma de Spyware. Por ejemplo, una página con motor de búsqueda puede asignar un número de identificación individual al usuario la primera vez que visita la página, y puede almacenar todos sus términos de búsqueda en una base de datos con su número de identificación como clave en todas sus próximas visitas (hasta que el cookie expira o se borra). Estos datos pueden ser empleados para seleccionar los anuncios publicitarios que se mostrarán al usuario, o pueden ser transmitidos (legal o ilegalmente) a otros sitios u organizaciones[5].

Las cookies almacenan información que se utiliza con varios fines:

Para personalizar la página Web y su navegación para cada usuario. Para recoger información demográfica sobre cuántos usuarios visitan la página y su tiempo de estancia en ella. Para realizar un seguimiento de qué banners se muestran al usuario, y durante cuánto tiempo.

Estos usos no tienen un carácter malicioso, al menos en principio. Sin embargo, es necesario tener en cuenta que toda información personal que se introduzca en una página Web se puede almacenar en una cookie, incluyendo contraseñas y el número de la tarjeta de crédito.

Caballo de Troya

El término "caballo de Troya" procede de una fábula griega, según la cual los griegos ofrecieron a los troyanos un caballo de madera gigante como símbolo de paz. Sin embargo, los troyanos se llevaron una ingrata sorpresa cuando del interior del caballo de madera surgieron soldados griegos que capturaron Troya. De modo similar, un programa de caballo de Troya se presenta a sí mismo como un programa

[5] “Spyware”, http://es.wikipedia.org/wiki/Spyware

informático de utilidad, mientras que lo que hace en realidad es causar estragos y daños en el equipo a través del Spyware.

Cada vez con más frecuencia, los caballos de Troya se utilizan como primera fase de un ataque y su objetivo primordial consiste en mantenerse ocultos mientras descargan e instalan amenazas más poderosas, como por ejemplo un bot o Spyware. A diferencia de los virus y los gusanos, los caballos de Troya no pueden propagarse por sí solos. A menudo llegan a la víctima por medio de un mensaje de correo electrónico en el que se hacen pasar por una imagen o un chiste, o bien a través de un sitio Web nocivo, que instala el caballo de Troya en un equipo mediante las vulnerabilidades existentes en el software del navegador Web, como Microsoft Internet Explorer.

Tras su instalación, el caballo de Troya merodea sigilosamente por el equipo infectado y de manera “invisible” comete sus fechorías, como por ejemplo descargar Spyware, mientras la víctima continúa realizando sus actividades cotidianas al no percatarse de ello.

Spam

El spam es la versión electrónica del correo basura. Supone enviar mensajes no deseados a una gran cantidad de destinatarios y, por lo general, se trata de publicidad no solicitada. El spam es un tema grave de seguridad, ya que puede usarse para enviar caballos de Troya, virus, gusanos, software espía y ataques dirigidos de robo de identidad. Cómo sabe que lo atacan los mensajes que no incluyen su dirección de correo electrónico en los campos Para: o CC: son formas frecuentes de correo no deseado.

Cierto tipo de spam puede contener lenguaje ofensivo o vínculos a sitios Web con contenido inadecuado.

Robo de identidad o phishing

El phishing o robo de identidad es básicamente un tipo de estafa en línea, y los autores de estos fraudes son artistas del engaño con conocimientos técnicos y ladrones

de identidad. Utilizan spam, sitios Web falsos, mensajes de correo electrónico, mensajes instantáneos con los que engañan a los usuarios para que divulguen información confidencial, como los datos de la tarjeta de crédito o de cuentas bancarias.
Phishing: características y técnicas.

El phishing consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas Web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.

Existe un amplio abanico de software y aplicaciones de toda índole que quedan clasificados dentro de la categoría de robo de información personal o financiera, algunas de ellas realmente complejas, como el uso de una ventana Javascript flotante sobre la barra de direcciones del navegador con el fin de confundir al usuario.

Algunas de las características más comunes que presentan este tipo de mensajes de correo electrónico son:

Uso de nombres de compañías ya existentes. En lugar de crear desde cero el sitio Web de una compañía ficticia, los emisores de correos con intenciones fraudulentas adoptan la imagen corporativa y funcionalidad del sitio de Web de una empresa existente, con el fin de confundir aún más al receptor del mensaje.

Utilizar el nombre de un empleado real de una empresa como remitente del correo falso. De esta manera, si el receptor intenta confirmar la veracidad del correo llamando a la compañía, desde ésta le podrán confirmar que la persona que dice hablar en nombre de la empresa trabaja en la misma.

Direcciones Web con la apariencia correcta. Como hemos visto, el correo fraudulento suele conducir al lector hacia sitios Web que replican el aspecto de la empresa que está siendo utilizada para robar la información. En realidad, tanto los contenidos como la dirección Web (URL) son falsos y se limitan a imitar los contenidos reales.

Factor miedo. La ventana de oportunidad de los defraudadores es muy breve, ya que una vez que se informa a la compañía de que sus clientes están siendo objeto de este tipo de prácticas, el servidor que aloja al sitio Web fraudulento y sirve para la recogida de información se cierra en el intervalo de unos pocos días. Por lo tanto, es fundamental para el defraudador el conseguir una respuesta inmediata por parte del usuario. En muchos casos, el mejor incentivo es amenazar con una pérdida, ya sea económica o de la propia cuenta existente, si no se siguen las instrucciones indicadas en el correo recibido, y que usualmente están relacionadas con nuevas medidas de seguridad recomendadas por la entidad.

Para lograr su objetivo, este tipo de malware, además de la ocultación de la URL fraudulenta en un correo electrónico aparentemente real, también utiliza otras técnicas más sofisticadas.[6]

Rootkit

Originalmente, cuando se hablaba de sistemas de tipo UNIX, un rootkit se refería a un conjunto de herramientas propias del sistema operativo, como netstat, passwd y ps, que eran modificadas por un intruso para asegurarse el acceso ilimitado al ordenador, sin que pudiera ser detectado por el administrador del sistema.

Dentro de la terminología propia de un sistema UNIX, el administrador del sistema se denomina root, de ahí el nombre genérico con el que se denota a dichas herramientas: equipo para permanecer oculto en el sistema cuando se han obtenido privilegios de root. En Windows el concepto sigue siendo el mismo.

Un rootkit de Windows es un programa que oculta determinados elementos (archivos, procesos, entradas del Registro de Windows, direcciones de memoria, conexiones de red, etc.) frente a otros programas o el propio sistema operativo. Como se puede ver, esta definición no incluye en sí misma ningún efecto perjudicial sobre el sistema. Es una tecnología que puede utilizarse de una forma constructiva o

[6] http://www.pandasecurity.com/spain/homeusers/security-info/

destructiva. Los rootkits son empleados con objeto de garantizar la continuidad del acceso a una computadora remota previamente comprometida, para:

- Instalar puertas traseras mediante las cuales acceder a la computadora.
- Esconder las modificaciones realizadas en la configuración.
- Ocultar los registros dejados como consecuencia de la intrusión en el sistema.
- De modo que tanto su presencia como su ejecución pasen inadvertidos a los ojos del usuario e incluso del software de seguridad.

Hoaxes

Frecuentemente, circulan por Internet falsos mensajes de alerta sobre virus, conocidos como hoaxes o bulos. Su finalidad es generar alarma y confusión entre los usuarios. Son importantes para el contagio de Spyware ya que por lo regular vienen con un link o una liga a alguna página de Internet, para supuestamente instalar el software que lo corrige, siendo este no la vacuna si no un software espía.

Estas son las principales características de estas falsas alarmas sobre virus:

Se envían por correo electrónico, con la intención de extender falsos rumores por Internet.

Los mensajes suelen tener un tono alarmista y normalmente incitan al usuario a tomar medidas inmediatas para resolver la supuesta infección. No hay que seguir jamás estas instrucciones, ya que suelen acarrear efectos dañinos para la computadora.

Por regla general, siempre inciden en que el supuesto virus del que avisan no es detectado por ningún antivirus. Efectivamente, los antivirus no pueden detectarlo, porque el fichero del que habla el hoax no es un virus.

Para dar un aspecto verídico a los mensajes, normalmente incluyen en el encabezamiento el nombre de ciertas agencias de prensa, empresas de software, compañías de antivirus o de otros organismos de prestigio. Por la misma razón, los

mensajes no suelen estar fechados: así transmiten la impresión de que son mensajes recientes, aunque lleven mucho tiempo circulando por la Red.[7]

Backdoor

Una puerta trasera (también conocidos como Backdoor) es un software que permite el acceso al sistema de la computadora ignorando los procedimientos normales de autenticación o facilita la entrada a la información de un usuario sin su permiso o conocimiento. Como es el caso de e-mail, que aparentan ser ligas a actualizaciones y que al pulsarla conecta a páginas similares a las originales, descargando archivos backdoor que al instalarlos, abrirá un puerto del equipo, dejándolo a expensas del autor del malware o para poder descargar otros códigos maliciosos.

Según como trabajan e infectan a otros equipos, existen dos tipos de puertas traseras. El primer grupo se asemeja al Caballo de Troya, es decir, son manualmente insertados dentro de algún otro software, ejecutados por el software contaminado e infecta al sistema para poder ser instalado permanentemente. El segundo grupo funciona de manera parecida a un gusano informático, el cuál es ejecutado como un procedimiento de inicialización del sistema y normalmente infecta por medio de gusanos que lo llevan como carga.[8]

Keylogger

Son programas espías, que toman el control de los equipos, para espiar y robar información, monitorea el sistema, registrando las pulsaciones del teclado, para robar las claves y passwords, tanto de páginas financieras y correos electrónicos como cualquier información introducida por teclado, en el equipo utilizado para saber lo que la víctima ha realizado como conversaciones que la misma tuvo, saber donde ha entrado, qué ha ejecutado, qué ha movido, etc...

[7] http://www.pandasecurity.com/spain/homeusers/security-info/
[8] http://service1.symantec.com/SUPPORT/INTER

Pueden ser también aparatos o dispositivos electrónicos colocados intencionalmente en equipos, que se intercalan entre el dispositivo y la computadora.

1.1.3 Creadores del Spyware

Los creadores de los caballos de Troya y el Spyware son profesionales informáticos. Los caballos de Troya y el Spyware suelen ser creados por autores de crimeware profesionales, quienes venden su software en el mercado negro para su uso en los fraudes en línea y en otras actividades ilegales.

Los caballos de Troya y el Spyware forman parte del crimeware, y son dos de las herramientas esenciales que un criminal cibernético puede utilizar para obtener acceso no autorizado y sustraer información de una víctima como parte de un ataque. La creación y distribución de estos programas va en aumento.

El Spyware es desarrollado además por empresas que buscan obtener beneficios económicos por medios poco ortodoxos. Además de los hackers que obtienen muchas ganancias al acceder a las computadoras para obtener información, que muchas veces no les interesa de forma personal, pero si para venderlas a alguien que este interesado en ella. Y los cracker que a cambio de un número de serie para validar diferentes tipos de software instalan Spyware al momento de visitar sus páginas, que por lo general son más de tipo adware pero que aun así no dejan trabajar de una manera correcta el sistema operativo, ya que ocupan memoria de la computadora.

1.1.4 Cómo ataca el software espía o Spyware

El Spyware o software espía puede descargarse de sitios Web, mensajes de correo electrónico, mensajes instantáneos y de conexiones directas de uso compartido. Además, un usuario puede recibir, sin saberlo, Spyware cuando acepta un acuerdo de licencia de usuario final de un programa de software. Cómo sabe que lo atacan

frecuentemente, tratan de pasar inadvertidos, ya sea escondiéndose por medio de los caballos de Troya o simplemente ocultándose en un sistema conocido para el usuario. [9]

Es por eso que los caballos de Troya van ligados al Spyware, aunque algunas empresas de antivirus no lo consideren como tal, en este trabajo se le considerará al caballo de Troya como un Spyware, ya que, el Spyware viene oculto dentro de éstos, y al entrar actúa de las maneras antes descritas.

Es por eso que los caballos de Troya y el Spyware, son dos de los métodos más utilizados por los criminales cibernéticos, para cometer fraudes, robos de identidad y otros crímenes cibernéticos.

1.2 Medios de contagio

Para que el software espía se reproduzca necesita de medios de contagio, los cuales son portadores del Spyware y una forma de hacer que el Spyware sobreviva y más aún vaya en aumento. Uno de los medios de contagio son los dispositivos de almacenamiento de información.

1.2.1 Almacenamientos de información

La revolución tecnológica de las últimas décadas, las redes e Internet han cambiado nuestra percepción de la representación y el valor de la información. Internet ha sido un detonador que impulsó el manejo y circulación de la información. Sin embargo, la inmensa cantidad de información que proporciona no tiene ningún control ni estructura, esto provoca que el usuario se desespere y no encuentre un sentido claro de lo que implica tener acceso a tales volúmenes de información.

La información ha sido parte fundamental de todas las civilizaciones. La manera más común de transmitirla es a través de textos contenidos en algún objeto físico, tales como manuscritos, libros, periódicos, informes, etc. Hasta hace una década no se

[9] "Spyware", http://www.symantec.com/es/es/norton/security_response/Spyware.jsp

habían preocupado por analizar o interpretar la estructura, forma o significado de la información de cada objeto.

Con el surgimiento de textos electrónicos, las editoriales y las librerías están cambiando todos sus procesos editoriales y de distribución. Los inmensos volúmenes de papel y los grandes talleres de impresión están quedando atrás; los más audaces de esta industria están encontrando en Internet una nueva visión del nuevo manejo de información, lo que hasta hace no mucho tiempo era guardado en papeles hoy en día es guardado en archivos de procesador de palabras, los cálculos matemáticos que por lo regular eran demasiadas hojas con fórmulas son guardadas en archivos de hojas de calculo y así se puede enumerar cientos de distintas formas en como se almacena la información y en distintas áreas que es imprescindible el almacenamiento de la misma.

Y no es que nunca haya habido algún medio de almacenamiento para esta información en la computadora.

Pero si es distinta la manera en como han cambiado desde sus inicios. En la década de los ochenta era frecuente almacenar la información en disquete de 5¼ con capacidad de almacenamiento por debajo de 500 kilobytes, menos de la mitad de un mega, hoy por cierto, ya obsoletos y la capacidad de discos duros eran a lo máximo de 20 megabytes, si leyó bien, en la actualidad serviría posiblemente solo para almacenar la capacidad de un archivo de video, o peor aun ni eso. Por eso es que así como va evolucionando el mundo de la computación, de la misma manera o mucha más rápida va evolucionando la forma de almacenar la información teniendo en consideración para el bien de ellos mismos que cada vez son de mayor capacidad y más pequeños.

A continuación se describirán algunos unidades de almacenamiento, los cuales son comunes en computadoras personales con sistema operativo Windows, sin entrar a detalle en cuanto a funciones técnicas o tecnológicas, solo con el fin de saber que son una de las principales formas de contagio de Spyware, aún cuando las computadoras no se conecten a Internet.

Medios de almacenamiento

Las unidades de almacenamiento son aquellos dispositivos, ya sea internos o externos, donde se guardan físicamente los archivos de un sistema y son utilizados para la propagación del software espía.

Disco de 3 ½

Aunque ya son algo obsoletos son sin embargo un medio de contagio por el cual el Spyware puede contaminar a las computadoras por medio de archivos o semillas del Spyware.

Disco Duro

Es principalmente donde se aloja el software espía como tal y donde trabaja de una forma completa ya que por el hecho de ser grande la capacidad de almacenamiento y al estar siempre activo al momento de usar la computadora es la forma más conveniente por la forma en que se desarrolla el Spyware.

Unidad de CD-ROM y Unidad de CD-RW (Regrabadora)

Por lo regular es portador del Spyware cuando el CD-ROM es grabado en una máquina contaminada de Spyware, aunque tal vez no en un grado alto, aunque si cuando se instalan programas por lo regular gratuitos por este medio es probable que se instale el Spyware.

Unidad de DVD-ROM y Unidad de DVD-RW

Al igual que el dispositivo anterior solo que ya empieza a ser de mayor uso a nivel mundial por tener mayor capacidad que el CD-ROM siendo ésta una causa mayor para que se instale el software espía, y no solo su semilla si no un programa espía más robusto y con mayor capacidad.

Otros dispositivos de almacenamiento

Otros dispositivos de almacenamiento son las memorias flash y USB.

Memoria flash

La memoria flash. Es un tipo de memoria que se comercializa para el uso de aparatos portátiles, como cámaras digitales o agendas electrónicas. El aparato correspondiente o bien un lector de tarjetas, se conecta a la computadora a través del puerto USB o Firewire. La memoria flash es una forma evolucionada de la memoria EEPROM[10].

Los principales usos de este tipo de memorias son pequeños dispositivos basados en el uso de baterías como teléfonos móviles, PDA, pequeños electrodomésticos, cámaras de fotos digitales, reproductores portátiles de audio, etc.

Es por eso que se han convertido en presa fácil para la infección del Spyware haciendo que circule de una manera rápida y segura sin necesidad de tener Internet, además de que es mucha la demanda del uso de estas memorias por la nueva tecnología que se está manejando en estos momentos, al igual que las memorias USB.

Memorias USB

Una memoria USB (de Universal Serial Bus, en inglés pendrive o USB flash drive) es un pequeño dispositivo de almacenamiento que utiliza memoria flash para guardar la información sin necesidad de baterías (pilas). Estas memorias son resistentes a los rasguños y al polvo que han afectado a las formas previas de almacenamiento portátil, como los CD y los disquetes.

Estas memorias se han convertido en el sistema de almacenamiento y transporte personal de datos más utilizado, desplazando en este uso a los tradicionales disquetes, y a los CDs. Se pueden encontrar en el mercado fácilmente memorias de 1, 2, 4, 8 GB

[10] "Memoria flash", http://es.wikipedia.org/wiki/Memoria_flash

o más (esto supone, como mínimo el equivalente a unos 1000 disquetes) por un precio moderado.

Los sistemas operativos actuales como Windows XP y Windows Vista pueden leer y escribir en las memorias sin más que enchufarlas a un conector USB del equipo encendido, recibiendo la energía de alimentación a través del propio conector. La mayoría de las memorias USB son pequeñas y ligeras. Son populares entre personas que utilizan computadoras pesonales y necesitan transportar datos entre la casa, escuela o lugar de trabajo. Otra utilidad de estas memorias es que, si la BIOS del equipo lo admite, pueden arrancar un sistema operativo sin necesidad de otro disquete, CD, DVD ni siquiera disco duro. El arranque desde USB está muy extendido en computadoras nuevas y un USB ocupa mucho menos y es más rápido que una disquetera o incluso que un lector de DVD/CD-ROM.[11]

Es por eso que son un atractivo para los creadores del Spyware estos dos últimos medios de almacenamiento ya que están aptos para propagar el software espía con el simple hecho de que se conecten a la computadora ya que se instala el Spyware de tal manera que al conectarse automáticamente se ejecute el software espía.

1.2.2 Internet

Internet ha revolucionado el mundo de las comunicaciones y por lo tanto el manejo de la información de una manera innovadora e impensable en la humanidad.

Los beneficios que ha aportado a las personas, así como la nueva e inmensa gama de riesgos que conlleva.

Dentro de esos riesgos y uno de los más importantes hasta ahora es el Spyware tema de la presente investigación.

[11] Ibíd.

Que significa Internet

El nombre Internet procede de las palabras en inglés Interconnected Networks, que significa 'redes interconectadas'.[12]

La información viaja por cables de fibra óptica de un servidor a otro a gran velocidad, por lo que a Internet se le llama "la autopista de la información".

Que es Internet

Internet es la red de redes, la telaraña de la comunicación es un sistema de redes comunicadas entre si a nivel mundial que permiten compartir información entre si, unas a otras sin que sea requerido un contacto personal, es decir se pueden intercambiar archivos en alguna otra computadora en cualquier otra parte del mundo sin la necesidad de saber de quien es. De esta manera cualquiera puede obtener información y muchos más servicios con el solo hecho de conectarse a Internet.

El Internet es un medio y el más común y eficaz para que el Spyware se desarrolle con todo su potencial, aunque en este trabajo solo se mencionara como medio de contagio, ya que no es su finalidad explicarlo a detalle.

A continuación se mencionan algunos datos que fueron relevantes en el uso y/ mejora de Internet:

[12] "Internet." Microsoft Encarta 2007 [DVD]. Microsoft Corporation, 2006

Evolución del Internet

1988: Se produce el primer gran ataque vírico, nace el IRC (Internet Relay Chat), precursor de los Chat actuales y tan utilizados en estos días.
1990: Nace el primer proveedor de acceso a Internet comercial, y la EFF (Electronic Frontiers Foundation), una defensa de ciberderechos. Aparece la versión Windows 3.0
1991: Tim Berners-Lee publica el protocolo de la World Wide Web en el centro de investigación europeo.
1992: **N**ace la Internet Society, encargada de los aspectos técnicos de la Red.
1993: Aparece Mosaic, el primer navegador. En pantallas de todo el mundo y sobre fondo gris aparecen documentos con gráficos y enlaces en azul. Hasta ese momento la Red era sólo texto. Ese mismo año Marc Andreeseen, co-creador de Mosaic, funda Netscape junto al veterano ejecutivo de Silicon Valley, Jim Clarke.
1994: Nace el Spam y los banners. En la Universidad de Stanford dos estudiantes crean un directorio de cosas interesantes de la Red, al que bautizan Yahoo!. Ese mismo año se fundan Excite y Lycos, dos de los primeros buscadores de la Red.
1995: Se empiezan a cobrar los dominios, Sun crea Java, y RealAudio añade la música a la Red. Nace Windows 95 anunciando un giro estratégico a Internet.
1998: Windows tiene más del 80% de los navegadores, y es demandada por abuso de posición dominante. El gobierno EEUU anuncia un plan para privatizar Internet que es rechazado.
1999: Nace Napster, el primer programa de intercambio de ficheros (P2P).
2000: Se comienza a dar servicio de banda ancha para Internet a usuarios domésticos.
2001: Arranca con el recién lanzado pleito de las discográficas contra Napster por favorecer la piratería, pleito que acaba por provocar su cierre en julio por orden judicial.
2002: Un ataque concertado consigue desconectar a 8 de los 13 ordenadores de los que depende todo el sistema de dominios, lo cual acelera los planes para reforzarlo.
2003: Es el año de la música por Internet. Apple saca su tienda de música iTunes, asociada al reproductor iPod. WiFi despega como alternativa de acceso inalámbrico. Varias plagas barrieron Internet; desde Slammer, que se extendió en 10 minutos echando abajo 8 servidores raíz y

afectando bancos y tráfico aéreo, hasta SobigF y Blaster.
2004: Sale a bolsa Google, que lanza su correo Web de 1 GB Gmail. Guerra de buscadores: Yahoo! abandona a Google y compra varias empresas, Microsoft potencia MSN Search. En EEUU la banda ancha supera a los módem.
2005: Hay más servidores raíz fuera de los EEUU que allá. La Red tiene más de 300 millones de hosts, casi 60 millones de dominios activos, más de 4.000 millones de páginas Web indexadas por Google y más de 800 millones de navegantes. Varios accidentes y ataques revelan información privada en la Red y Apple presenta el iPod Shuffle, basado en memoria flash. El mercado de la publicidad online se despierta.[13]
2006: El 3 de Enero Internet alcanzó los mil cien millones de usuarios. Se prevé que en diez años, la cantidad de navegantes de la Red aumentará a 2.000 millones[14].

**Cuadro creado y recopilado por el autor

En el cuadro anterior se muestra lo rápido y acelerado que ha crecido Internet así como el crecimiento de sus usuarios, por tal motivo es atractivo para los creadores del Spyware para instalar sus programas espía.

Exploradores de Internet

Un navegador Web o explorador Web (del inglés, *navigator* o *browser*) es una aplicación software que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente descritos en HTML, desde servidores Web de todo el mundo a través de Internet. Esta red de documentos es denominada World Wide Web (WWW).

Cualquier navegador actual permite mostrar o ejecutar gráficos, secuencias de vídeo, sonido, animaciones y programas diversos además del texto y los hipervínculos o enlaces.

La funcionalidad básica de un navegador Web es permitir la visualización de documentos de texto, posiblemente con recursos multimedia incrustados. Los documentos pueden estar ubicados en la computadora en donde está el usuario, pero

[13] "Internet", http://www.giatica.info/item/internet-su-historia
[14] "Internet" http://es.wikipedia.org/wiki/Internet

también pueden estar en cualquier otro dispositivo que esté conectado a la computadora del usuario o a través de Internet, y que tenga los recursos necesarios para la transmisión de los documentos (un software servidor Web). Tales documentos, comúnmente denominados páginas Web, poseen hipervínculos que enlazan una porción de texto o una imagen a otro documento, normalmente relacionado con el texto o la imagen.[15]

El primer explorador de Internet fue Mosaic, creado en 1993 por el Centro Nacional de Aplicaciones de Supercomputación de la Universidad de Illinois (Estados Unidos). En un principio se desarrolló en UNIX, pero pronto se presentó en Windows.
En 1994 apareció Netscape Navigator, un explorador para Windows, Macintosh y diversas variantes de UNIX, de Netscape Communications Corporation. Pronto adquirió un rápido desarrollo, ya que permitía transferencias seguras en Internet. Inicialmente era un producto comercial, pero la dura competencia del explorador de Microsoft Corporation obligó a la empresa a facilitarlo de forma gratuita.

En 1995 Microsoft presentó su Internet Explorer; era un programa independiente, pero a partir de Windows 98 se ofreció integrado en el sistema operativo, lo que facilitó que se convirtiese en el explorador más extendido. Sus capacidades son similares a las de Netscape.[16]

A mediados del 2002 nace Mozilla en gran medida a que Nestcape Comunications Corporation libero su código fuente. A finales de 2004 aparece en el mercado Firefox, una rama de desarrollo de Mozilla que pretende hacerse con parte del mercado de Internet Explorer. Se trata de un navegador más ligero. El navegador Firefox v1.0 hace mella en el dominio del Explorer de Microsoft, arrebatándole un 5%.[17]

[15] "Navegador", http://es.wikipedia.org/wiki/Navegadores
[16] "Explorador de Internet." Microsoft Encarta 2007 [DVD]. Microsoft Corporation, 2006
[17] "Historia de Internet", http://www.giatica.info/item/internet-su-historia

Lo que si es un hecho es que gracias a la popularidad del Internet y a la gran cantidad de computadoras conectadas, hacen cada vez más atractivo el mercado para que el Spyware continúe y no desaparezca. Más aún que se están manejando velocidades más altas para la transmisión de datos además de distintas formas como los son de manera inalámbrica o a través de la telefonía celular.

1.2.3 Vulnerabilidad

Otro medio para que se produzca el contagio de Spyware es la vulnerabilidad, es decir la posibilidad de ocurrencia de la materialización de un evento que puede desencadenar un incidente en la organización, produciendo daños materiales.

Agujero de seguridad

Un agujero de seguridad es un fallo en un programa que permite mediante su explotación violar la seguridad de un sistema informático. Esto también se ha comenzado a aplicar a los servicios Web, tales como páginas Web, correo, MSN, Chat, etc, con el objetivo de obtener información de personas que usen el servidor. A las personas que buscan errores en los sitios Web se les llama hackers.

Son principalmente los hackers en buscar agujeros de seguridad para violar la seguridad del sistema y acceder a la información de las computadoras con el fin de introducir programas de los cuales obtendrá un beneficio si no para el si para alguien más.

Un defecto de software (*computer bug* en inglés)[18], es el resultado de un fallo o deficiencia durante el proceso de creación de programas de ordenador o computadora. Dicho fallo puede presentarse en cualquiera de las etapas del ciclo de vida del software

[18] En 1945, los creadores de Mark II informaron del primer caso de error en un ordenador causado por un bicho. El Mark II, ordenador sucesor de ASCC Mark I, Construido en 1944, sufrió un fallo en un relé electromagnético. Cuando se investigo ese relé, se encontró una polilla que provocó que el relé quedase abierto. Este incidente es erróneamente conocido por algunos como el origen de la utilización del término ingles "bug" (Bicho) para indicar un problema en un ordenador. En realidad, la foto que se esgrime para dar forma a esa teoría es probablemente la primera referencia a el uso del término "bug" como causa de error en una computadora, siendo este un "bicho" de verdad y no el primero relativo a un error informático.

aunque los más evidentes se dan en la etapa de desarrollo y programación. Los errores pueden suceder en cualquier etapa de la creación de software. Los programas que ayudan a detección y eliminación de errores de programación de software son denominados depuradores (debuggers).

El factor humano

Cuando se habla de vulnerabilidad es preciso decir y mencionar al factor humano. Siendo utilizado como parte fundamental del contagio de Spyware gracias a lo vulnerable que representa el comportamiento humano.

El Spyware usa y utiliza técnicas de llamar la atención del usuario por medio de adware atractivos, tales como el que se ha ganado un premio, que alguien del sexo opuesto quiere conocerlo para realizar una amistad o algo más, así como la oferta de software gratuito, con la finalidad que la persona se interese e instale programas para continuar sin saber que es software espía ya mencionado con anterioridad.

Es así pues el humano parte fundamental para que el software espía siga en crecimiento por falta de conocimiento e información sobre la forma de atacar del Spyware.

Por tal motivo se ha desarrollado de manera paralela la forma de contrarrestar y mitigar los riesgos a causa del Spyware llamada seguridad informática.

1.3 Seguridad Informática

La seguridad informática generalmente consiste en asegurar que los recursos del sistema de información (programas) de una organización sean utilizados de la manera que se decidió y que la información que se considera importante no sea fácil de acceder por cualquier persona que no se encuentre acreditada.

Se puede entender como seguridad un estado de cualquier sistema (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende

como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro.

1.3.1 Características de la seguridad informática

Para que un sistema se pueda definir como seguro debe estar dotado de cuatro características:

- Integridad: La información no puede ser modificada por quien no está autorizado.
- Confidencialidad: La información solo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesita.
- Irrefutabilidad: (No-Rechazo o No Repudio) Que no se pueda negar la autoría.

Dependiendo de las fuentes de amenazas, la seguridad puede dividirse en seguridad lógica y seguridad física.

En estos momentos la seguridad informática es un tema de dominio obligado por cualquier usuario de la Internet, para no permitir que su información sea robada.

1.3.2 Términos relacionados con la seguridad informática

- Activo: recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- Impacto: consecuencia de la materialización de una amenaza.
- Riesgo: posibilidad de que se produzca un impacto determinado en un Activo, en un Dominio o en toda la Organización.
- Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

- Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- Desastre o Contingencia: interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

Aunque a simple vista se puede entender que un Riesgo y una Vulnerabilidad se podrían englobar un mismo concepto, una definición más informal denota la diferencia entre riesgo y vulnerabilidad, de modo que se debe la Vulnerabilidad está ligada a una amenaza y el riesgo a un impacto.

Los activos son los elementos que la seguridad informática tiene como objetivo proteger. Siendo el activo más importante la información:

Es el objeto de mayor valor para una organización, el objetivo es el resguardo de la información, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico. [19]

1.3.3 Seguridad en Internet

Si se habla de seguridad bien se sabe que se está hablando de un mecanismo:

Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente. En varias disciplinas por tal se maneja este concepto siendo tal vez de las más comunes la seguridad personal o de empresas, negocios o casas; las cuales tienen la función de salvaguardar lo que se considera de valor para el interesado y también hay muchos mecanismos, instrumentos, material y demás para procurar un buen funcionamiento en especial para prevenir una contingencia inesperada.

En la computación no podía ser una excepción ya que hay muchas cosas que se consideran de valor entre ellas la computadora misma o cualquier parte del hardware como puede ser la fuente de poder el disco duro, la tarjeta madre, etc, pero en este

[19] "Seguridad", http://es.wikipedia.org/wiki/Seguridad_informÃ¡tica

apartado se abocará solo la seguridad en el software es decir de los programas y muy en especial del sistema operativo Windows y de saber que tan seguro puede ser y de las vulnerabilidades que tiene.

Porque a decir de la seguridad no hay nada 100% seguro siempre se buscara una manera de hacerlo vulnerable y hacer que lo que parecía tan seguro no lo sea, tal es el caso de una alarma casera o empresarial no porque esta sea de lo mejor o de tecnología de punta evitara que se cometa un robo dentro de la caso o empresa.

Cuantas veces no se ha escuchado de robos aun teniendo todo tipo de seguridad llamado guardia, policía, cámara de video alarmas, etc. y aun así logran ser vulnerables de un ataque de un tercero para obtener algo que a el en lo particular le interese para su conveniencia. Lo mismo pasa en la seguridad informática, sale cada vez un mecanismo de seguridad mejor que el anterior y aun así no deja de ser vulnerable, tal es el caso de los antivirus, antiSpyware, firewall por mencionar algunos.

Siempre se busca la manera de sobrepasarlos muchos por el solo hecho de demostrar que no son seguros, otros tantos por simple distracción y otros muchos para poder acceder a la información de las computadoras para obtener un beneficio y es donde entran los Spyware.

Intentar tener un secreto en Internet es cada día más difícil ya que habiendo millones de usuarios la probabilidad de que alguien acceda a esa información es cada vez más riesgosa, más aún cuando en ese otro universo que se llama Internet hay tanta información como la que uno se pueda imaginar, entre ellas: números de tarjetas de crédito, autenticaciones de clientes, correos electrónicos, contraseñas, claves e incluso información personal que puede ser aprovechada por algún maleante o estafador que pueda obtenerla a través del Spyware es por ello que la seguridad es súper necesaria y más que obvia.

Dado que el Internet es un fenómeno mundial parte de la seguridad con la que cuenta la información al ser enviada es gracias a la criptografía. Todo usuario tiene derecho a su privacidad aún al conectarse al Internet a sabiendas que es una

interrelación de comunicación no le quita este privilegio de confidencialidad que en algún momento pierde al aceptar obligaciones a cambio de algunos derechos, por ejemplo al instalar software gratuito. Ahora que si el usuario no quiere exponerse a compartir información personal lo mejor sería rechazar el contrato y no instalarlo pero muchas veces por curiosidad o por conseguir las cosas gratuitamente acepta y peor aún sin siquiera haber leído el estar de acuerdo que la información que proporcione puede ser utilizada para conveniencia de terceros.

Hay muchas maneras de obtener seguridad en Internet y mucho de esa seguridad depende de la que nos brinde el sistema operativo en este caso el sistema operativo Windows XP que si es cierto es mucho más seguro que sus antecesores o al menos eso es lo que ha vendido la compañía siempre será necesario tener software de seguridad de terceros que brinden el servicio de antivirus, antiSpyware, cortafuegos (firewall), antispam. Por mencionar algunos, los cuales a veces una empresa o compañía de software incluyen juntos “todo-en-uno” los antes mencionados con el nombre de suites de seguridad.

1.4 Planteamiento del problema

El problema que se va a tratar es sobre el riesgo o los riesgos que conlleva el Spyware en un despacho contable.

1.4.1 La Organización

El despacho contable se especializa en impuesto legal, financiero, administrativo, la revisión comercial y el asesoramiento de la contabilidad además de la investigación y desarrollo y la puesta en práctica de nuevos proyectos.

Cuenta con una fuerza de trabajo de 33 empleados.

El despacho contable esta organizado de una forma vertical en el cual el dueño o gerente es quien dispone y toma las decisiones finales de que y como se deben de realizar las tareas.

Objetivos de negocio:

Aconsejar y brindar servicios en la contabilidad legal, comercial, financiera, judicial y administrativa a través de investigación y desarrollo con funciones sólidas y trabajo honesto para crear una infraestructura de crecimiento continuo hacia los clientes y firma.

Misión

Desarrollar comodidad y seguridad a la clientela en las operaciones cotidianas de su empresa dándole la ayuda y el soporte necesario a través de profesionales dedicados.

Filosofía del negocio:

Los clientes son la entidad más importante de la firma que es la razón de existencia y desarrollo, es a través de ellos que se crece profesionalmente para la imagen futura.

Actividades actuales:

- Asesoramiento, contabilidad, y operaciones cotidianas.
- La firma rinde actualmente servicios a 170 compañías de pequeña y mediana empresa, representan el 36% de la renta anual gruesa de la firma.
- Aproximadamente entre 30 y 180 compañías de grande tamaño requiere servicios del despacho contable para la puesta en práctica de nuevos proyectos, por ejemplo: licencias, investigación y desarrollo de lugares nuevos, intervenciones internas, intervenciones financieras y administrativas, e

intervenciones de impuesto, representan el 35% de la renta anual gruesa del despacho.

- Servicios de gobierno: bajo servicios que el gobierno ha creado recientemente hay varios sectores que dan la ayuda a los funcionarios de alto nivel para que puedan optimizar los recursos de sus componentes por medio del despacho contable de una manera personalizada para un control eficiente en sus gastos.

El despacho contable cuenta con:

- Red Lan de 13 computadoras de escritorio y 2 Laptop´s.
- 12 computadoras se conectan a Internet.
- 4 computadoras son solo para contabilidad y 1 para la secretaria.
- Conexión a Internet es por banda ancha y ruteador inalámbrico.
- 7 computadoras con WinXp, 6 con WinME y 2 con Win98.
- 10 Pc´s cuentan con antivirus y/o suites de seguridad.
- 4 impresoras láser, 2 inyección de tinta y 6 impresoras de matriz.

El problema del despacho contable es que últimamente se ha tenido un retraso en la operación de las computadoras, se han vuelto lentas, aparecen errores de librerías del sistema operativo, se pasman, es decir, se quedan trabadas en algún proceso en el cual se está trabajando.

No solo es que alguna computadora falle, si no que ha llegado a pasar que borra información importante, no solo contable si no direcciones, teléfonos, documentos, etc., a tal grado de tener que volver a capturar todo de nuevo, haciendo que haya un retraso en el trabajo y algunas veces se tenga que trabajar de forma más rápida de lo habitual para entregar los reportes a su debido tiempo.

Otras veces ha pasado que a causa de las fallas anteriores, las computadora se tengan que apagar de una forma incorrecta, debido a que no hay otra manera pues el sistema no funciona, los problemas se van extendiendo ya que empiezan a dañar de

alguna manera sectores en el disco duro, o peor aun en alguna “mal apagada” se dañe la tarjeta madre o el procesador haciendo que la computadora deje de funcionar.

Un riesgo más que se corre aparte de perder la información, y de dañar alguna parte del hardware es el tiempo que se pierde al no funcionar las computadoras de manera correcta, ya que además cuando no funcionan se le pide al compañero que le preste su computadora para realizar el trabajo, teniendo así una pérdida mayor de tiempo, ya que no solo es el tiempo del contador o auxiliar contable el que se pierde si no ahora además es el tiempo perdido de la otra persona que presta su máquina.

Hasta el momento se ha definido el problema, como es, la clasificación y descripción de los distintos tipos de Spyware parte del marco teórico conceptual del problema, así como los factores que inciden en su propagación e infección a las computadoras.

A continuación se plantearan las metas y fines que se pretenden realizar en el caso práctico del Spyware, para lograr el objetivo, después se identificaran las variables controlables y no controlables ya que éstas influyen en el proceso. Haciendo así que el proceso o procesos que se obtienen nos generen estrategias, es decir los caminos posibles a seguir para la solución del problema.

"Las matemáticas tienen varios aspectos. Desgraciadamente, para muchos estudiantes son un conjunto de reglas rígidas que hay que aprenderse antes del examen final y que pueden olvidarse después ... Para un matemático involucrado en la investigación, el quehacer en matemáticas es muchas veces como un juego de adivinanza: hay que adivinar el teorema matemático antes de probarlo, hay que adivinar la idea de la demostración antes de escribir en detalle la prueba rigurosa ... La primera adivinanza puede estar lejos de la verdad, pero después de varios intentos y modificaciones, seguidos por la observación y analogía, se llega a una conjetura más atinada ... "

"El resultado del pensamiento creativo de un matemático es el razonamiento demostrativo, una prueba rigurosa, pero la prueba se descubre por medio del razonamiento plausible, adivinando."[20]

[20] G. Polya, "Mathematics and Plausible Reasoning. Volume II Patterns of Plausible Inference". Princeton University Press, 1968. p. 158

Para solucionar el problema se tiene que desmembrar en partes, o componentes:

- Objetivos: Resultados que se desean.
- Variables controlables: Los cursos de acción.
- Variables no controlables: El ambiente.
- Y por último las relaciones entre las tres.

Ahora se enfocara a detectar las variables controlables y no controlables del problema, como lo conceptúa Russel L. Ackoff[21], quien plantea: Las variables controlables son aquellas en las que uno como tomador de decisiones tiene y ejerce un control sobre ellas, son variables que están dentro del proceso e interactúan en el sistema.

Las variables controlables son manejadas de tal manera que uno con el uso apropiado hará que el problema cambie, de tal modo que tenga otro resultado. Lo que uno debe de hacer es que ese resultado se mejore de acuerdo a lo planteado o se acerque y llegue porque no al diseño ideal.

Por tanto se minimizan los riesgos de pasar por alto consecuencias que vienen al caso, al formular un problema a uno o varios ideales.

Un diseño ideal tiene que ser factible además de que el estado que se diseña debe hacerse de tal manera que si llega a existir sobreviva. El diseño debe ser viable operativamente, además de ser flexible y susceptible al cambio con facilidad.

1.4.2 El ideal

El ideal como lo conceptualiza Ackoff[22] de acuerdo a este trabajo sería alcanzar que todas las computadoras estuvieran libres de Spyware, así como saber prevenir las diferentes formas posibles de contagio en un futuro, haciendo que el usuario deje de ser parte del problema y en cambio si sea parte de la solución a través de generar conciencia del riesgo que conlleva el Spyware.

[21] Ackoff, Russel L., "El arte de resolver problemas" Ed. Limusa. Pág. 69, 103 México 2007
[22] Ackoff, Russel L., "Planificación de la empresa del futuro" Ed. Limusa Pág. 131 México 2006

En este caso en particular, sobre el Spyware se planteara un Ideal que es erradicar el Spyware teniendo como consecuencia un aumento de seguridad en las computadoras personales.

A continuación se citaran algunas variables controlables que se encuentran el la problemática del software espía:

1.4.3 Variables controlables

Software antivirus El software antivirus es para tener mayor seguridad en las computadoras, de hecho las compañías de antivirus han expandido su manera de obtener una mayor seguridad convirtiéndose en suites de seguridad, es decir, muchos software en uno, como antispam, antiSpyware, firewall, antiadware, etc.

Actualizaciones automáticas: Las actualizaciones automáticas son proporcionadas por la empresa del sistema operativo por medio de updates o por archivos que corrigen los problemas de agujeros de seguridad comúnmente llamados “parches”.

El uso de la computadora: Esta dentro de las variables controlables puesto que si se usa de una manera correcta y razonable es más segura la forma de trabajar de la misma, no dando cabida a que entre fácilmente el Spyware.

El respaldo de información: Esta variable puede ser controlable puesto que mientras se creé una costumbre al usuario de respaldar la información periódicamente estará previniendo un desastre a consecuencia del Spyware.

Vulnerabilidad de software: son controladas por medio de parches, actualizaciones periódicas y software de terceros.

Deficientes e inseguras contraseñas: Éstas se consideran que pueden ser controladas si se cambia periódicamente, usando además combinación de caracteres alfabéticos y numéricos, siendo que estos no tengan relación personal.

Información que se envía por Internet: se puede manejar como variable controlable haciendo que no se envíe información detallada como nombres, direcciones tarjetas de crédito, etc. y que no se proporcionen a desconocidos en Internet.

En tanto las variables no controlables son aquellas en las cuales uno no puede inferir, y que no tiene el control sobre ellas, muchas variables incontrolables están no solo fuera del sistema sino dentro del sistema. Muchas veces se piensa que son variables incontrolables pero en realidad no lo son, solo que uno no ve las distintas aristas del problema.

1.4.4 Variables no controlables

Hacker, cracker, y demás delincuentes cibernéticos: Son usuarios muy avanzados que por su elevado nivel de conocimientos técnicos son capaces de superar determinadas medidas de protección.

La forma de atacar de los criminales cibernéticos ya que cada vez utilizan diferentes formas y recursos para enganchar al usuario de la computadora y los incitan a instalar sus programas sin que se den cuenta.

Comercio electrónico: Se considera como variable incontrolable, ya que trabajan de manera independiente las compañías de este tipo y que no tienen una homogeneidad en las formas de ejecución.

Las diferentes tecnologías de espionaje, ya que se van revolucionando de una manera igual o más rápida que la misma tecnología.

El usuario de la computadora puesto que no tiene buenos hábitos ni “cultura cibernética o informática”, el usuario es el eslabón principal pero también el eslabón más débil.

Internet y su evolución con sus grandes facilidades de conectividad, permite a un usuario experto intentar de forma anónima, y a veces conseguir, el acceso remoto a una máquina conectada.

Aspecto legal, Delito cibernético: Esta variable es difícil de controlar ya que se tiene que dar una legislación, la cual no se da muchas veces por falta de conocimiento

de quienes las laboran y éstos al estar desinformados no tienen alternativas para solucionarlas.

Tecnología e ingeniería social, puesto que va evolucionando muy rápidamente y cuando se tiene un mejor control es cambiada por una más eficaz y más difícil de erradicar.

Incremento de mensajería instantánea y blogs o páginas personales es una variable no controlable ya que puede enviar y recibir archivos de información sin algún control de seguridad, aun teniendo software de seguridad ya que uno es el que da el acceso de intercambiar archivos.

Programas P2P: Estos programas por el momento no se pueden controlar ya que tienen una infinidad de archivos que son manejadas por otra infinidad de computadoras, y no garantizan que la información que se comparte sea segura, exponiendo un gran riesgo para que la computadora se infecte de Spyware.

1.4.5 Disposiciones

- Detectar cuando el Spyware esta instalado en la computadora.
- Prevenir el contagio de Spyware.
- Reducir el nivel de contagio del Spyware.
- Planificación de desastres.
- Comprender la forma en que las amenazas siguen patrones de uso.
- Restringir acceso a sitios nocivos para su salud física y mental.
- Aumentar la seguridad del sistema operativo en la computadora.
- Instalar software antivirus.
- Instalar Suites de seguridad.
- Tener un control de las páginas Web que se visitan en Internet.
- Tener un control de la información que se comparte a través de los medios de almacenamiento.
- Tener en cuenta el avance tecnológico para nuevas formas de ataques.

- Detectar si el hardware falla ya que puede ser una consecuencia del Spyware.
- Incremento de medios de comunicación.
- Incremento de dispositivos móviles.
- Crear conciencia al usuario de los riesgos del contagio de Spyware.
- Capacitación al usuario.
- Monitoreo del uso y costumbres que tiene el usuario de la computadora.
- Crear buenos hábitos

1.4.6 Objetivo

Controlar el nivel de seguridad para hacerlo eficaz creando conciencia al usuario de los riesgos que conlleva el Spyware.

1.4.7 Metas

Realizar programas para actualizar e instalar software de seguridad.

Orientar a los usuarios de computadoras personales para que sus contraseñas sean eficaces, es decir, las claves de acceso deben resultar difíciles de adivinar.

Instalar software de seguridad en las computadoras de acuerdo al sistema operativo de cada computadora.

1.4.8 Estrategias

Creación de estrategias dirigidas a la minimización de daños productos del riesgo de contagio de Spyware:

- Evaluar los distintos caminos que se pueden utilizar para infectar las computadoras de Spyware, para un mejor control, comprendiendo la noción de que las amenazas siguen patrones de uso. Hacia donde la mayoría vaya, hacia allá irán los delincuentes cibernéticos. Cada vez que una nueva aplicación o dispositivo entre, surgirán nuevas amenazas.

- Cambiar la mentalidad de los usuarios de computadoras y capacitarlos para tener una posición activa, para compartir responsabilidades en materia de seguridad.
- La detección temprana del Spyware es factor clave para prevenir con éxito los riesgos y prepararse bien para ellos.
- La prevención del daño de Spyware y su preparación revisten importancia fundamental para reducir la necesidad del contagio de Spyware, debe considerarse como aspecto integral de la política y su planeación.
- Las medidas preventivas son más eficaces cuando entrañan la participación en todos los planos, desde el alto mando de la organización hasta el más bajo nivel de la organización.
- La evaluación del riesgo del Spyware es un paso indispensable para la adopción de una política y de medidas apropiadas y positivas para la reducción del contagio de Spyware.
- La vulnerabilidad puede reducirse mediante la aplicación de métodos apropiados de diseño y unos modelos de desarrollo orientados a los usuarios de computadoras, a través de la educación en materia de seguridad como prioridad. Para generar conciencia hacia los usuarios de computadoras.
- Fomentar la educación en seguridad informática mediante la incorporación de programas.

Es así como se ha cubierto el análisis de la planeación por medio de objetivos y estrategias, para dar un paso importante en el siguiente capítulo, la planeación.

La planeación, ¿que significa? ¿De que forma debe de suceder para resolver el problema?, ¿como hay que hacerlo?, ¿Qué actividades hay que desarrollar para cumplir las metas, fines y objetivos?, así como los costos del plan y los presupuestos con los que cuenta la empresa.

Luego entonces se espera que con la planeación se tengan varias opciones en las cuales se pueda elegir el camino que más satisfaga la resolución del problema por medio de la toma de decisiones, valorando y cuantificando la racionalidad, para beneficio de la empresa además de solucionar el problema.

Conclusiones

Todos los días uno se entera de posibles riesgos en diferentes dispositivos o sistemas de manejo de información. Para poder prevenir dichos riesgos es necesario conocerlos a fondo, así como conocer las medidas de seguridad necesarias para minimizarlos.

Es por eso que se necesita conocer y saber como trabaja el Spyware y sus riesgos implícitos que conlleva.

Saber que los diferentes tipos de Spyware y las diferentes tecnologías sociales que se usan son tan variadas y diversas para que el usuario de la computadora incurra en ella de una manera fácil, y es a través de algún programa, juego, chiste, y demás, que adquiere interés personal hacia el usuario utilizando como medio sus propios vicios dentro de Internet.

Hay un principio básico, que las abuelas de antaño comentaban: No le des ninguna información a nadie, no le abras la puerta a ningún desconocido, hoy en cambio se le da información a cualquier desconocido en un Chat, así como los gustos, las preferencias y los intereses personales por medio de la navegación en Internet.

Estos riesgos y estos puntos débiles comienzan con el usuario de las computadoras siendo éste el que abre las puertas para que el enemigo entre y espíe lo que pueda ser de su interés.

El riesgo es la probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando: La confidencialidad, la integridad y la disponibilidad de la información.

Siendo el activo más importante la información, la cual tiene un alto riesgo de pérdida al ser contagiada de Spyware.

Así pues, se ha dado el primer gran paso; conocer el entorno y el medio en que se rodea el Spyware, para posteriormente seguir con el siguiente paso poder atacarlo, y ese paso se podrá realizar gracias a la Planeación.

Capítulo 2
Planeación para la prevención y detección en el contagio de Spyware

En el capítulo anterior se describió el problema del despacho contable, existe un problema frecuente de infección de software espía en las computadoras. Lo que hace que las computadoras trabajen de una manera lenta y con un mal funcionamiento, haciendo que sean ineficaces e inoperantes por la problemática del Spyware.

En esta problemática están implicados todos los integrantes del despacho desde el cargo principal hasta el último usuario de las computadoras que vienen siendo los auxiliares contables.

El problema del Spyware ocurre en la mayoría de las computadoras del despacho contable con mayor incidencia en las máquinas que manejan los auxiliares contables, siendo este tal vez algo en lo que se tiene que analizar. El problema del Spyware sucede porque visitan páginas web que no debieran de visitarse, al abrir correos con archivos adjuntos por simple curiosidad, morbo e ignorancia. Las personas implicadas no miden las consecuencias de los riesgos que esto conlleva dado tal vez por que son sabedores que las computadoras no son de ellos sino de la empresa, además piensan que no hay riesgos y que no están implicados, cuando en realidad son los más implicados ya que son su herramienta de trabajo.

Pero a todo esto, después de describir la problemática hay que encontrar la resolución correcta sobre lo que esta sucediendo, y el porque se hace, estas respuestas se encontraron al analizar el medio ambiente, es decir ver como esta estructurado el despacho contable y así encontrar las variables controlables y las variables no controlables, para empezar a generar una serie de procesos que nos de una o varias estrategias como caminos viables para la resolución del problema, las cuales fueron descritas en el capítulo anterior.

Es aquí donde se utiliza la planeación como método de solución hacia el problema.

2.1 Filosofía de la planeación

Generalmente es una filosofía adaptativa, que pretende conciliar los diferentes intereses implicados para lograr los resultados de la organización, puede ser activa y pasiva.

La adaptación activa cambia el medio ambiente del sistema para obtener la eficiencia, en la adaptación pasiva cambia sólo el comportamiento para el logro del desempeño eficiente.

2.1.1 Herramientas

La planeación en este caso requiere hacer uso de metodologías, modelos, métodos y estándares existentes. Cuando no existen aspectos como los anteriores, es necesario realizar la creación de metodologías, modelos o sistemas que permitan establecer las reglas dentro la organización o sociedad.

Las áreas dentro de las organizaciones que utilizan la planeación, suelen ser las principales de las que depende otro sin número de áreas, debido a que marcan las líneas más generales de trabajo, brindan las pautas para que se alineen en torno a lo que van señalando. Son áreas independientes de las que dependen otras estructuras dependientes.

Para lograr una adecuada función de la organización, se necesita de una interrelación de todas las áreas hacia el cumplimiento de todos los objetivos, metas y fines realizando en cada tramo las adecuaciones pertinentes.

2.1.2 Otras Características

La planeación es muy necesaria que se realice en todos los ámbitos del ser humano, desde lo personal laboral, social, y en todo tipo de organización. La planeación cuenta con un principio de aplicación la racionalización, cumplir la máxima eficacia y eficiencia.

Todo tipo de planeación por su amplitud debe seguir un conjunto de pasos en su desarrollo. Se debe realizar una acotación del alcance, el tiempo, el lugar, la definición de los medios y los recursos con que se cuenta. Esto implica realizar un análisis previo del lugar en donde se aplicará la planeación.

Se puede continuar realizando un diagnóstico de la situación, donde se vean:

- Los recursos.
- Lo interno y externo, entre ello el medio ambiente.
- Las variables controlables y no controlables.
- Las oportunidades y fortalezas, las debilidades y amenazas.

Toda planeación es acotada, por lo que es necesario el desarrollo de los puntos anteriores, para poder definir una forma de solucionar una problemática y lograr su alcance deseado mediante la planeación.

2.1.3 Diagnóstico

El problema del despacho contable es que las computadoras se infectan de Spyware a causa de instalar programas de Internet y de los cuales no se sabe su procedencia, de visitar páginas en las cuales es fácil adquirir el Spyware tales como juegos en línea, programas de supuesto software gratuito, páginas Web donde encontrar amistades y/o parejas, instalar programas piratas de software para ver video

y mp3 trayendo como consecuencia que las computadoras no trabajen de forma correcta y que el sistema operativo sea todo menos eso, operativo, puesto que no se puede trabajar dado que tiene problemas de librerías, de conexiones a Internet y de un buen funcionamiento tanto a nivel hardware como a nivel software.

Se ha gastado en estos dos últimos años más de $150,000 para reparar los equipos que han sido contagiados de virus y/o Spyware tanto en hardware como en software.

Siendo el 15% el gasto en hardware y el 85% en software.

El daño en hardware es principalmente en discos duros, memorias y mother board (tarjeta madre).

En los últimos 2 años (2006-2007) se han gastado en reparación de las computadoras en promedio poco más de $1500 semanales a causa de virus y/o Spyware por todas las computadoras del despacho haciendo un total de $80,000 anuales.

Ha habido pérdida de información total en 3 equipos habiendo que capturar de nuevo la información contable y en otras solo pérdida parcial de algunos archivos.

Se han consultado 9 distintas compañías de reparación en equipo de cómputo, debido a que no cubrían las demandas del despacho contable.

El promedio de la reparación de computadora para limpiarla de virus y/o Spyware es de $300 por computadora.

No ha habido ninguna computadora que no se haya infectado de Spyware, aún cuando no se conecte a Internet y a pesar de tener software de seguridad instalada

esto debido al intercambio de información ya sea por medio de la red o de dispositivos de almacenamiento.

El concepto relevante es la seguridad ya que si ésta aumenta se reducirá el riesgo de contraer o contagiarse de Spyware en las computadoras del despacho, teniendo así una menor exposición a perder información importante de la empresa tal como la contabilidad de los clientes que se tiene.

El tiempo en que esta escrito es reactivo ya que se están tomando datos del pasado de cuantas veces se infectan las maquinas, el costo que se tiene para repararlas y lo que cuesta el hardware dañado a causa de la infección.

A pesar de que el problema este descrito de una manera reactiva hay una combinación en la variable tiempo y en la cual se puede utilizar la planeación interactiva dado que se trata de ver el presente de acuerdo al pasado para un futuro ideal o deseable.[23]

El atacar este problema sirve para que las computadoras del despacho trabajen con la información veraz y oportuna, agilizando los reportes y las declaraciones contables se hagan en forma y tiempo debido.

Los beneficiados al corregir este problema aparte del mismo despacho serían los clientes para los que se trabaja, ya que sus declaraciones así como su contabilidad serán confiables y a tiempo.

A pesar de que se ha hablado y escrito del Spyware no se ha sido especifico a una empresa contable y menos con las características y el entorno de esta empresa, además de que solo se ve en un enfoque técnico de vulnerabilidades y seguridad.

[23] Ackoff, Russell L., "El paradigma de Ackoff"; Ed. Limusa Wiley, 2007

Y a pesar de tener software de seguridad, antivirus o cualquier tipo de protección el Spyware sigue haciendo estragos tantos físicos como lógicos. Por ejemplo dañando archivos, modificando librerías de Windows así como daños en los discos duros por mencionar algunos.

Al tratar de detectar y prevenir el Spyware se estima que no se gaste tanto dinero en reparación de equipo de cómputo o en la compra de hardware dañado a causa del Spyware, por eso la importancia de analizar y planear para una detección y prevención oportuna del Spyware.

Este tipo de problema es técnico por las vulnerabilidades del sistema operativo y del software que se utiliza además económico por los gastos que ocasiona en este caso también es organizacional dado que el despacho no tiene una organización en forma y esta integrada de una manera empírica siendo la empresa un elemento vulnerable para la seguridad de la información.

Se atacará la vulnerabilidad humana que es el eslabón más débil a través de políticas y normas, además se propone crear conciencia a los usuarios de las computadoras por medio de información de los daños que ocasiona el Spyware y así reducir los riesgos que conlleva.

2.1.4 Pronóstico

Se podría pensar que el despacho contable al tener más de 20 años se encuentra capacitado y comprometido para resolver este tipo de problemas, pero con lo rápido que ha evolucionado el Spyware y sus diferentes formas de contagiarse, el riesgo de contraer el Spyware ha crecido siendo la principal causa de reparación en el equipo de cómputo.

Si se crea conciencia a los usuarios de la empresa a través de un control de seguridad que implique una planeación estratégica, el Spyware disminuirá teniendo como consecuencia menores riesgos así como menores costos en la reparación además de servir como herramienta para detectar oportunamente el contagio, servirá como una medida de prevención.

2.1.5 Viabilidad

La viabilidad para realizar el proyecto es positiva ya que la organización esta dispuesta por iniciativa propia a contrarrestar o disminuir los riesgos que conlleva el contagio de Spyware siempre y cuando se utilicen los recursos tecnológicos (computadoras) con que se cuentan sin necesidad de adquirir otros por el momento.

2.1.6 Factibilidad

Dado que el mismo despacho contable lo considera viable también se considera factible puesto que esta dispuesto a aportar los recursos tanto humanos como financieros para realizar el proyecto teniendo en cuenta el valor extrínseco a través de su utilidad.

Una vez presentado el diagnóstico así como su pronóstico y puesto que es, tanto viable como factible se procederá con la planeación. ¿Pero qué es la planeación? ¿Cómo se da? O ¿Cómo se realiza? ¿A que se refiere cuando se habla de planeación?.

A continuación se dará una breve descripción de tal concepto siendo sus principales autores a tratar Ackoff[24], Tomas Miklos[25], y Churchman[26] para después

[24] Ackoff, Russell L., "El paradigma de Ackoff"; Ed. Limusa Wiley, 2007
[25] Miklos, Tomás y Tello Ma. Elena, "Planeación prospectiva"; Limusa Noriega, 1999.
[26] Churchman, C. West., "El enfoque de sistemas"; México: Editorial Diana, 1981

aplicarlos a la problemática del despacho contable, teniendo así ya no solo caminos hacia donde dirigirse sino el camino correcto o eficaz para la resolución del problema.

2.2 Planeación

La planeación en el sentido más universal implica tener uno o varios objetivos a realizar junto con las acciones requeridas para concluirse exitosamente. Va de lo más simple a lo complejo, dependiendo el medio a aplicarse. La acción de planear se refiere a planes y proyectos en sus diferentes, ámbitos, niveles y actitudes.

La Planeación se convierte en un factor gradual de cambio que debe crear las condiciones para afectar el presente y comprometer al futuro, implica el esfuerzo creativo y constante que asimile y proyecte, en los cambios la orientación y el ritmo de las variables socioeconómicas, en vías de que prevalezca una mayor racionalidad social.

Planear es diseñar un futuro deseado así como los medios efectivos para realizarlo. La planeación es un proceso de toma de decisiones; pero igualmente evidente es que la toma de decisiones no siempre es planeación.

La planeación es algo que se hace antes de emprender una acción, es decir, una toma de decisiones anticipada. Es necesaria cuando el estado futuro que se desea incluye un conjunto de decisiones interdependientes, es decir, un sistema de decisiones.

La planeación da dirección, reduce el impacto del cambio, minimiza el desperdicio y la redundancia y fija los estándares para facilitar el control. Anticipa cambios, desarrolla respuestas apropiadas y reduce la incertidumbre.[27]

La Planeación debe dividirse en etapas o fases que se lleven a cabo, puesto que las tomas de decisiones son demasiadas grandes para manejarlas todas de una vez. A esto se debe que la planeación debe de llevarse a cabo antes de emprender una acción.

La planeación es un proceso dirigido a producir uno o más estados futuros deseados y cuya materialización no es probable a menos que se haga algo al respecto.

Se ocupa por tanto de evitar las acciones incorrectas y de reducir el número de oportunidades que no se aprovechan.[28]

2.2.1 Etapas de la Planeación

Dado que a veces puede tratarse de un proceso de toma de decisiones, se pueden distinguir varias etapas:

- Identificación del problema.
- Desarrollo de alternativas.
- Elección de la alternativa más conveniente.
- Ejecución del plan.

En los casos de planeación reactiva, y operativa no se hace un enfático uso en la toma de decisiones, ya que es lineal y sólo administra los procesos en curso de alguna organización o sistema. El caso de la planeación táctica, estratégica y normativa, puede requerir los conceptos de toma de decisiones por lo complejo y amplio.

[27] Stephen P. Robbins, "Administración, Teoría y práctica"; Prentice Hall Hispanoamericana, México 1994
[28] Ackoff, Russell L., "El paradigma de Ackoff"; Ed. Limusa Wiley, 2007

Con relación a la toma de decisiones, un ejemplo, cuando por la mañana planeamos nuestro día y elegimos qué medio de transporte utilizaremos para ir al trabajo, estamos anticipando la decisión que de no haberlo planeado igual hubiéramos tenido que tomar. Estas acciones no se limitan a la organización temporal de conductas sino también a la planificación de pensamientos para realizarlo.

Lo anterior es un caso muy operativo, que se debe decidir en ese momento, y se hace en un tiempo inmediato, con relación a la planeación en el corto plazo, operativo, reactivo y adaptativo. De alguna manera se utiliza la planeación en la vida cotidiana, en sus diferentes expresiones, pero es muy importante distinguir las características en el entorno o medio ambiente que se desenvuelven, ya que no es lo mismo decidir por una persona que por miles de personas, cada escenario es muy diverso, de allí la importancia de la planeación.

2.2.2 Orientación de la Planeación

La Planeación en sí, posee una orientación en el tiempo, la cual se encuentra determinada por el siguiente esquema:

Orientación	Pasado	Presente	Futuro
Reactivista	+	-	-
Inactivista	-	+	-
Preactivista	-	-	+
Interactivista	+ / -	+ / -	+ / -

+ = actitud favorable - = actitud no favorable

Actitud frente a la planeación. La actitud de cada planeación, realizada en el nivel deseado, requiere una definición, puede ser:

Planeación reactiva

Es simplemente realizar acciones encaminadas a seguir cómo actualmente se encuentra la organización, no se piensa en el futuro, sino en mantener lo que actualmente tiene la organización, se está más preocupadas en regresar a como se trabajaba en el pasado dado que se piensa que como ya lo conocen las tareas es más fácil de manejar que el futuro que por lógica desconocen.[29]

Planeación inactiva

En esta etapa se considera solo en presente, el hoy es lo que cuenta sin mirar que se hizo con anterioridad ni que es lo que sucederá mañana.

En esta planeación solo se piensa en lo que se hace el día de hoy.

Planeación preactiva

Se realizan cambios para mantener vigente la organización, generalmente no trasciende, ni se realizan cambios de impacto, atiende actividades necesarias para poder continuar con el deseo que en futuro serán mejores.[30]

Planeación interactiva

Ésta última considera al pasado, presente y futuro como aspectos diferentes, pero inseparables de la problemática para la que se plantea; se concentra en todas las orientaciones al mismo tiempo. Esta basada en la creencia de que si no se toman en cuenta los tres aspectos temporales de una problemática, el desarrollo será obstruido.[31]

[29] Idem
[30] Ibid
[31] Ibid

Ackoff menciona que la planeación interactiva está orientada a tener el control sobre el futuro. Por consiguiente, este tipo de planeación consiste en el diseño de un futuro deseable y en la selección o invención de las formas para producirlo tan fielmente como sea posible.

De acuerdo a esta clasificación el problema que se está tratando será basado en la planeación Interactiva y sus cinco fases:

- Formulación de la problemática.
- Planeación de fines.
- Planeación de medios.
- Planeación de recursos.
- Implementación y control.

2.2.3 Tipo de planes

Por su marco temporal se dividen en: corto, mediano y largo plazo.

Por su especificidad y frecuencia de uso: específico, técnico y permanente por ejemplo.

La planeación por su amplitud se divide en: Estratégica, Táctica, Operativa y Normativa.

La primera y la última se realizan a largo plazo, la segunda en el mediano plazo y la tercera en el corto plazo.

Dependiendo de la naturaleza de la organización se deberán aplicar un conjunto de planes alineados para su actuación.

2.2.4 Los niveles de Planeación dentro de una Organización

Planeación Estratégica

Es el proceso mediante el cual los ejecutivos trazan la dirección a largo plazo de una entidad estableciendo objetivos específicos en el desempeño, tomando en cuenta circunstancias internas y externas para llevar a cabo .los planes de acción seleccionados. Esto suele llevarse a cabo dentro de las organizaciones en el nivel directivo, o el más alto nivel de mando. La cual se realiza por medio de tácticas y procedimientos empleados para el logro de un objetivo específico o determinado.

Planeación Táctica

La planeación táctica presenta características de ser un proceso continuo y permanente, orientado al futuro cercano, racionalizar la toma de decisiones, determinar cursos de acción, es sistémica ya que es una totalidad formada por el sistema y subsistemas, visto desde un punto de vista sistémico. Es iterativa ya que se proyecta y debe ser flexible para aceptar ajustes y correcciones, es una técnica cíclica que permite mediciones y evaluaciones conforme se ejecuta, dinámica e interactivo con los demás y es una técnica que coordina a varias actividades para conseguir la eficiencia de los objetivos deseados.

La incertidumbre provocada por las presiones e influencias ambientales debe ser asimilada por la planeación intermedia o táctica. Se debe convertir e interpretar en las decisiones estratégicas, del nivel más alto, en planes concretos en el nivel medio, se convierte en planes que se pueden emprender y a su vez, subdividir y detallar en planes operacionales a ejecutarse en el nivel operativo.

El nivel táctico es la toma de decisiones, el seguimiento y control parcial.

Planificación Operativa

Se da en los empleados, en el nivel más bajo de la organización. Realiza una micro planeación de las organizaciones de carácter inmediato, que detalla acerca de la forma en que las metas tendrán que ser alcanzadas, realmente quien realiza todos los puntos de la base de la planeación se dan en el nivel más bajo que es el operacional, en gran forma influye y determina en conjunto con la planeación táctica si las cosas se dan o no.

La parte operacional incluye esquemas de tareas y operaciones debidamente racionalizados y sometidos a un proceso reduccionistas típico del enfoque de sistema cerrado. Se organiza con base a los procesos programables y técnicas computacionales, se, convertir una idea en realidad, o el propósito de una acción que pueda ejecutarse por medio de varias vías posibles.

Planeación Normativa

Se refiere a la conformación de normas, políticas y reglas establecidas para el funcionamiento de una organización. Se va a apoyar en la conformación de estándares, metodologías y métodos para el correcto funcionamiento de las actividades dentro de la planeación.

La planeación normativa se refiere al establecimiento de reglas y/o leyes, y políticas dentro de cualquier grupo u organización. Principalmente para mantener el control, seguimiento y desarrollo de la planeación, así como el desarrollo de las mismas normas y políticas establecidas.

Esta planeación está estrechamente vinculada con el diseño de la Estructura organizacional.

La planeación normativa se aplica en áreas muy específicas, que generalmente son las que vigilan y definen aspectos que en otros niveles no son posibles delimitar y resolver la diferencia existente para llevar a cabo alguna actividad.

Derivado de esta descripción el tipo de planeación que se adecua a la empresa es la Estratégica, la cual será explicada más a detalle.

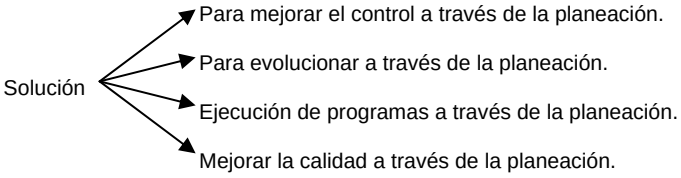
2.3 Planeación Estratégica

Es estudiar los procesos que generen estrategias. Siempre la estrategia tiende a tener mejor calidad, costo, tiempo, etc.

La planeación estratégica analiza el entorno de la organización cuyo funcionamiento busca de manera constante estrategias que mejoren: la calidad, la utilidad, oportunidad, desempeño, cantidad, costo, transparencia, tiempo, aplicación tecnológica, competitividad y desarrollo organizativo. Éste esquema metodológico de planeación permite analizar el conjunto de disposiciones que buscan resolver de forma racional el problema que se han planteado para alcanzar el objetivo.

La planeación estratégica se convierte en un pensamiento constante de evolución. Al obtener diversas soluciones, el análisis de las decisiones se presenta con horizontes de tiempo, racionalidad, costo, riesgo e innovación.

Toda planeación estratégica se orienta a una solución.



**Gráfica tomada de clases del seminario de Análisis y Planeación

2.3.1 La Teoría de los Sistemas y la Planeación Estratégica

Es importante destacar que la Teoría de los sistemas es plenamente aplicable a la Administración organizacional, y por ello es útil tenerla en cuenta cuando hablamos de planeación estratégica. Esta teoría considera que un sistema es un conjunto de elementos, interrelacionados, tendientes a cumplir un determinado conjunto de objetivos.[32]

Por ello, una empresa completa puede considerarse un sistema, pero un área específica (por ejemplo el departamento de informática) también es por sí solo un sistema, más acotado y con un objetivo más específico.

Esto es importante porque la definición de Planeación Estratégica y Planeación Operativa debería considerarse respecto del sistema bajo análisis, y no respecto a un ente rígido.

Por ejemplo, la definición de la visión y los objetivos de una organización pueden resultar estratégicos para la misma, mientras que la definición de las políticas relativas a los sistemas de información serán simplemente operativas. Sin embargo, como el sistema bajo análisis es el área de informática, la definición de las políticas anteriores pueden resultar estratégicas y serán operativas las definiciones sobre copias de seguridad o políticas de acceso a los computadoras.

Planeación Estratégica, Visión y Objetivos

En el ámbito empresarial, de organizaciones y sistemas, considerándolo como sistema bajo análisis, la Planeación Estratégica ayuda a que se tengan claros sus objetivos y así puedan definir un programa de acciones para realizarlos. De esa manera

[32] Churchman, C. West., "El enfoque de sistemas"; México Editorial Diana, 1981

se separa una problemática compleja en porciones pequeñas que se han de ir realizando poco a poco.

Durante la planeación estratégica se debería definir la visión y los objetivos de la organización.

La visión es la situación en la que se pretende que se encuentre la organización en un futuro de largo plazo. Por ejemplo, se quiere que el despacho contable sea líder con personal calificado y que se tenga una relación cordial y amable con la cartera de clientes que se tiene.

Los objetivos son más específicos que la visión, pero comparten un plazo similar. Podría decirse que el objetivo abarca una dimensión de la visión. Por ejemplo, los objetivos son: mejorar la imagen del despacho contable frente a los clientes potenciales disminuyendo el contagio de Spyware en las computadoras, mejorar la capacitación de los recursos humanos para tener un control del personal que se contrata, dando a conocer las políticas y normas de seguridad para la prevención del Spyware, etc.

Cabe hacer la salvedad de que algunos autores consideran a los objetivos y metas como sinónimos, otros consideran que los objetivos son como se definieron en el párrafo anterior y las metas son una medida puntual de los objetivos, y otros autores utilizan ambos términos en forma exactamente inversa.

En la mayoría de las organizaciones los objetivos de planeación se resumen en obtener beneficios para sus accionistas, empleados, la sociedad y el medio ambiente.

Asignar los recursos a cada tarea, ya sean tiempo, dinero u horas hombre es responsabilidad de los encargados de la planeación. Así como el orden en que se realizará cada tarea.

Desde el punto de vista de la planeación, existen objetivos, medios y fines que la empresa debe plantearse para establecer una o varias estrategias globales.

2.3.2 Objetivos

Disminuir el contagio de Spyware.

Prevenir y detectar oportunamente el contagio de Spyware en caso de adquirirlo.

Controlar el contagio de Spyware y como ideal tratar de erradicarlo.

Satisfacer las necesidades del cliente en tiempo y forma.

2.3.3 Medios

A través de crear conciencia a los usuarios del despacho contable que son el eslabón más débil.

Usar software de seguridad, específicamente suites de seguridad (antivirus, antispam, antispyware, etc., “todo en uno”).

Utilizar software anti-Spyware específicamente el Spybot –Search & Destroy.

Dar información de las distintas formas de contagio del Spyware.

2.3.4 Fines

Saber y conocer los síntomas para detectar el Spyware a corto plazo, tres meses.

Prevenir el Spyware a mediano y largo plazo, seis y doce meses respectivamente.

Controlar el contagio de Spyware durante los tres plazos a corto, mediano y largo plazo.

Erradicar completamente el Spyware de las computadoras a largo plazo.

2.3.5 Análisis Costo – Beneficio

Este tipo de análisis constituye una ayuda importante en la toma de decisiones, brinda información necesaria para determinar si la actividad es deseable, o si, por el contrario viene a construir un desperdicio.

Objetivo del costo-beneficio

La técnica de Costo – Beneficio, tiene como objetivo proporcionar una medida de los costos en que se incurren en la realización de un proyecto, y a su vez comparar dichos costos previstos con los beneficios esperados de la realización de dicho proyecto.

Utilidad del costo-beneficio

Su utilidad es la siguiente:

Valorar la necesidad y oportunidad de acometer la realización del proyecto.

Seleccionar la alternativa más beneficiosa para la realización del proyecto.

Estimar adecuadamente los recursos económicos necesarios en el plazo de realización del proyecto.

Para realizar un Análisis de Costo – Beneficio fiable, debemos seguir los siguientes pasos:

Producir estimaciones de costos – beneficios: Elaborar una lista que incluya lo requerido para llevar acabo el proyecto, así como los beneficios que este traerá consigo:

- Determinar la viabilidad del proyecto y su aceptación.

- Para determinar si el proyecto es conveniente o no realizarlo.
- Realizar un estudio de viabilidad donde se determina si el proyecto es factible o no; para lo cual los siguientes métodos pueden servir de base:
  - Retorno de la inversión.
  - Valor Actual.

De acuerdo a los métodos mencionados para este tipo de Análisis, el que mejor se adecua al problema por las características que presenta es el de Valor Actual.

Valor Actual

Este método permite tener en cuenta que un gasto invertido durante un cierto tiempo produce un beneficio. Con este método se podrá determinar la cantidad de dinero que es viable invertir inicialmente para que se recupere la inversión en un periodo de tiempo determinado por la Dirección.

Se debe calcular en primer lugar, el beneficio neto que se obtendrá cada año. Dicho beneficio no es real, ya que se debe estimar el valor real de dicha cantidad en el año *n*.

Para determinar la viabilidad del proyecto, se debe estudiar en cuantos años se recuperara la inversión realizada inicialmente y si esta inversión es retornada en un período de año fijado previamente por la Dirección.

Lo que se propone	Justificación	Costo	Beneficio	Que pasa si no se realiza
Instalar software de seguridad.	Porque no tienen software de seguridad en el mejor de los casos solo tienen antivirus.	$1100 por cinco licencias o 760 por cada computadora.	Tener una mayor seguridad en la información.	Las computadoras tendrán un mayor riesgo en contraer el Spyware.
Instalar Software Anti-Spyware Spybot. Search&Destroy.	Porque hay archivo o configuraciones que la suite de seguridad no detecta.	Software gratuito descarga desde su página.	Borrar desde raíz o en el registro la semilla del Spyware.	Como se instala en el registro de Windows cada que se reinicia la computadora. Automáticamente carga el Spyware.
Capacitar al usuario de la computadora.	Se necesita dar información de las diferentes formas de Ingeniería social para adquirir el Spyware.	---------	Tener un mayor conocimiento de las distintas formas de ataque además de crear conciencia de los riesgos que se corren.	A pesar de tener cualquier software de seguridad, suites de seguridad, anti Spyware, firewall, etc si el usuario instala un software sin conocimiento el Spyware se instalara sin su conocimiento pero si con su consentimiento.

Si se cuenta con una propuesta de solución, continúa la parte del desarrollo de la planeación, en la cual es necesario definir el enfoque de ésta a utilizar, señalando un bosquejo general de lo que se realizará.

Dentro de dicho enfoque es inevitable dejar de hacer mención de lo siguiente:

La incidencia del proceso administrativo como sistema dentro de la planeación y la organización.

2.3.6 Método FODA

El análisis FODA surgió de la investigación conducida por el Stanford Research Institute entre 1960 y 1970. Sus orígenes nacen de la necesidad descubrir por qué falla la planificación corporativa. La investigación fue financiada por las empresas del Fortune 500, para averiguar qué se podía hacer ante estos fracasos. El equipo de investigación consistía de Marion Dosher, Dr Otis Benepe, Albert Humphrey, Robert Stewart y Birger Lie. FODA (en inglés SWOT), es la sigla usada para referirse a una herramienta analítica que permitirá trabajar con toda la información que se poseamos sobre un negocio, útil para examinar las Fortalezas, Oportunidades, Debilidades y Amenazas.

Este tipo de análisis representa un esfuerzo para examinar la interacción entre las características particulares del negocio y el entorno en el cual éste compite. El análisis FODA tiene múltiples aplicaciones y puede ser usado por todos los niveles de la corporación y en diferentes unidades de análisis tales como producto, mercado, producto-mercado, línea de productos, corporación, empresa, división, unidad estratégica de negocios....., etc.

El análisis FODA debe enfocarse solamente hacia los factores claves para el éxito de la empresa. Debe resaltar las fortalezas y las debilidades diferenciales internas al compararlo de manera objetiva y realista con la competencia y con las oportunidades y amenazas claves del entorno.

Lo anterior significa que el análisis FODA consta de dos partes: una interna y otra externa.

1.- La parte interna: tiene que ver con las fortalezas y las debilidades del negocio, aspectos sobre los cuales se tienen algún grado de control.

2.- La parte externa: mira las oportunidades que ofrece el mercado y las amenazas que se debe enfrentar en el mercado seleccionado. Aquí es necesario desarrollar toda nuestra capacidad y habilidad para aprovechar las oportunidades y para minimizar o anular esas amenazas, circunstancias sobre las cuales se tiene poco o ningún control directo.

Análisis de la matriz FODA

Completar la matriz es sencillo, y resulta apropiada para talleres y reuniones de tormenta de ideas. Puede ser utilizada para planificación de la empresa, planificación estratégica, evaluación de competidores, marketing, desarrollo de negocios o productos, y reportes de investigación. La elaboración de una matriz FODA puede ser de utilidad en juegos de formación de equipos.

El análisis FODA es una evaluación subjetiva de datos organizados en el formato FODA, que los coloca en un orden lógico que ayuda a comprender, presentar, discutir y tomar decisiones. Puede ser utilizado en cualquier tipo de toma de decisiones, ya que la plantilla estimula a pensar pro-activamente, en lugar de las comunes reacciones instintivas.

En este trabajo se usara el análisis FODA para evaluar y analizar un cambio de procesos organizacionales dentro del despacho contable como una opción estratégica para el desarrollo de la empresa.

Las cuatro dimensiones son una extensión de los encabezados sencillos de Pro y Contra.

La plantilla del análisis FODA es generalmente presentada como una matriz de cuatro secciones, una para cada uno de los elementos: Fortalezas, Oportunidades, Debilidades y Amenazas.

Las fortalezas y debilidades corresponden al ámbito interno de la institución, y dentro del proceso de planeación estratégica, se debe realizar el análisis de cuáles son esas fortalezas con las que cuenta y cuáles las debilidades que obstaculizan el cumplimiento de sus objetivos estratégicos.

De esta forma, el proceso de planeación estratégica se considera funcional cuando las debilidades se ven disminuidas, las fortalezas son incrementadas, el impacto de las amenazas es considerado y atendido puntualmente, y el aprovechamiento de las oportunidades es capitalizado en el alcance de los objetivos.

FORTALEZAS internas	DEBILIDADES internas
• Capacidades fundamentales en actividades claves. • Recursos financieros adecuados. • Experiencia que respaldan 22 años de trabajo continuo. • Buena imagen ante los clientes. • Clientes que sirven como enganche para atraer más clientes. • Flexibilidad en costos. • Costos bajos en comparación a la competencia. • Asesoría legal acorde a los nuevos reglamentos y disposiciones gubernamentales.	• No hay una dirección estratégica clara. • Atraso en investigación y desarrollo. • Débil imagen en el mercado. • Habilidades de marketing por debajo de la medida. • Mala organización. • Cambio de personal constante. • Exceso de problemas operativos internos. • Equipo de computo no actualizado. • Falta de inversión en software. • Falta de comunicación en todos los niveles. • Falta de una visión a futuro.

OPORTUNIDADES externas	AMENAZAS externas
• Entrar en nuevos mercados ante el incremento de negocios. • Atender a grupos adicionales de clientes. • Satisfacer nuevas necesidades de los clientes. • Diversificación de productos relacionados. • Altos costos de la competencia. • Aumento de clientes potenciales. • Avance tecnológico. • Actualizaciones automáticas en línea. • Mayor protección de los diferentes software de seguridad.	• Efectos políticos. • Entrada de nuevos competidores constante y a la alza. • Crecimiento lento del mercado a causa de la situación actual. • Cambio en las necesidades y gustos de los consumidores. • Cambios en las diferente formas de contagio del Spyware. • Aumento de hacker y/o cracker. • Tecnología social adversa. • Aumento de usuarios en Internet. • Nuevas formas de comunicación para el manejo de la información.

**Cuadro diseñado por el autor

El análisis FODA es una de las herramientas esenciales que provee de los insumos necesarios al proceso de planeación estratégica, proporcionando la información necesaria para la implantación de acciones y medidas correctivas y la generación de nuevos o mejores proyectos de mejora.

En el proceso de análisis de las fortalezas, oportunidades, debilidades y amenazas, Análisis FODA, se consideran los factores económicos, políticos, sociales y culturales que representan las influencias del ámbito externo al Despacho contable, que inciden sobre su quehacer interno, ya que potencialmente pueden favorecer o poner en riesgo el cumplimiento de los objetivos. La previsión de esas oportunidades y amenazas posibilita la construcción de escenarios anticipados que permitan reorientar el rumbo de la empresa.

Es de importancia el tomador de decisiones, debido a que es quien debe contar con la capacidad de poder definir las diferencias existentes en alguna definición o actividad por realizar. También para que vigile el curso de las tareas y pueda aplicar los cambios adaptativos dentro de la planeación. Debe contar con cierto liderazgo y ser capaz de poder tomar las decisiones en el nivel respectivo.

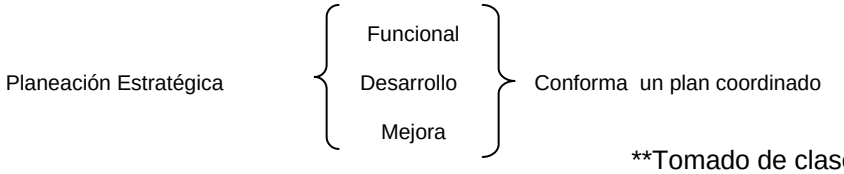
Otro tipo de características que distinguen a la planeación es la existencia del tomador de decisiones, cuando se realiza la planeación es necesario que exista un fuerte compromiso por parte de todos los integrantes en la organización; la planeación y el plan es lo más importante y todos los integrantes deben conocerlo.

2.4 Diseño Estratégico

Es el diseño de un plan a través de programas de acción a mediano y largo plazo que permite a la organización la consecución de los objetivos.

Un diseño estratégico es y se formula como un conjunto de previsiones sobre fines y procedimientos que forman una secuencia lógica para ser ejecutada y alcanzar los objetivos con eficiencia y eficacia.

El diseño estratégico es un conjunto de decisiones que conforman un plan coordinado bajo una sola estructura: pensar y resolver.



**Tomado de clases del Seminario

2.4.1 Tratamiento de riesgos de seguridad

La gerencia necesita evaluar los riesgos y decidir qué hacer con ellos. Tales decisiones deben documentarse en un Plan para tratar los Riesgos este plan se

denominara: PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN. Es aceptable que la dirección decida explícitamente no hacer nada con ciertos riesgos de seguridad de la información que se estiman dentro de la "tolerancia al riesgo" de la organización, sin que sea éste el enfoque por defecto.

2.4.2 PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN.

Es aquí donde el tomador de decisiones, en este caso el gerente general decide realizar un plan.

Este plan es originado por las estrategias originadas tomando en cuenta tanto las variables controlables como las no controlables, y es con la finalidad de minimizar los riesgos que provoca el Spyware.

Este plan es denominado PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN, se denominó así ya que involucra a todas las áreas del despacho contable por medio de unos programas a realizarse para la seguridad de la información.

El plan consta de cuatro etapas o programas:

- Programa de detección de Spyware.
- Programa de Prevención de Spyware.
- Programa de Control de Spyware.
- Programa de contingencia y desastres.

Con una amplitud en la planeación de tres meses a corto plazo, seis meses a mediano plazo y un año a largo plazo.

2.4.3 Programa de detección del Spyware

En esta etapa o programa tiene como propósito detectar que computadoras están contagiadas de Spyware.

El objetivo es que el usuario debe de ser capaz de saber detectar los signos y síntomas cuando la computadora esté infectada de Spyware.

A continuación se mencionan algunos signos y síntomas cuando la computadora esta infectada con Spyware:

- Cambia de página de inicio.
- Aparecen demasiadas ventanas emergentes.
- Internet trabaja de una manera más lenta.
- El correo se satura de spam.
- Aparecen leyendas de errores.
- No se puede conectar a Internet.
- No despliega de forma correcta las páginas Web.

Para solucionar:

- El programa consta primeramente de una regularización en las computadoras para que estén libres de virus y Spyware.
- En caso de detectarse el Spyware en la computadora ésta será aislada de la red hasta que este libre de Spyware.
- Instalar un anti-Spyware (Spybot).
- Instalar y actualizar la suite de seguridad.
- Luego se procederá a realizar el primer respaldo de información que se considere importante, dado que la computadora esta libre de virus y Spyware.
- Otra alternativa es realizar una imagen del disco duro.
- Reincorporar nuevamente la computadora a la red.

Este programa es de corto plazo, de una a dos semanas, para realizarlo una vez cada quince días, a mediano plazo y a un mes a largo plazo.

Su indicador es el número de máquinas infectadas con Spyware entre el número de computadoras que tiene el despacho.

Otro indicador es el porcentaje de riesgos de seguridad de la información para los cuales se han implantando totalmente controles satisfactorios entre el número de computadoras del despacho.

El porcentaje de cambios de riesgo son de: bajo, medio, alto y de emergencia.

2.4.4 Programa de Prevención

El programa de prevención tiene como objetivo principal crear conciencia de los posibles daños que puede ocasionar el Spyware y la importancia de prever un contagio.

- Capacitar al usuario.

En este punto el usuario debe tener cierto conocimiento de los riesgos, causas y consecuencias del Spyware.

- Informar de las nuevas tecnologías que se usan para adquirir el Spyware.

Aquí se le informara de los cambios, modificaciones y nuevas formas de tecnología social que usan los delincuentes cibernéticos para introducir el Spyware en las computadoras.

- El usuario estimará lo que puede suceder en la manera de ser atacado usando la creatividad.

En este punto se harán juntas con lluvias de ideas para estimar lo que puede suceder en la manera de ataque que usa el Spyware.

- Adquirir hábitos para respaldar información en tiempo y forma debida.

Es una de las actividades principales dentro de este plan ya que cuando estos hábitos sean constantes será más difícil de adquirir el Spyware.

- Crear contraseñas más seguras.

Otra manera de prevenir el contagio de Spyware es capacitar al usuario para generar contraseñas difíciles de adivinar usando longitud mayores a ocho caracteres usando caracteres alfanuméricos.

Su indicador es el número de computadoras con éxito entre el número de computadoras del despacho.

2.4.5 Programa de Control

Este programa tiene como objetivo principal controlar por medio de reportes la incidencia de los programas que constituyen el PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN.

- Monitoreo de las computadoras por lo menos cada tercer día a corto plazo y en forma aleatoria en mediano y largo plazo.
- Garantizar que los programas anteriores se cumplan.
- Esta actividad a través del control debe garantizar que los programas del plan se cumplan de acuerdo a sus especificaciones.
- Generar y verificar los datos.

Con esto se genera una confiabilidad en la información y un mayor alcance de la empresa. En esta actividad se deben generar y documentar los reportes de las computadoras que han tenido éxito al no contener ningún Spyware.

El indicador es por lo tanto el número de computadoras que han tenido éxito en no contener Spyware entre el número de computadoras del despacho.

Mientras más sea el éxito en las computadoras mayor es el control que se va a tener en este programa.

2.4.6 Programa de contingencia y desastres

En este programa el objetivo primordial es tener en cuenta que con los avances tecnológicos y la forma de evolucionar de los criminales cibernéticos tales como los hackers y crackers se puede sen víctima del Spyware con riesgos de pérdida total de la información o pérdida total de hardware.

- Aislar la computadora de la red.

La primera actividad a realizar es aislar la computadora de la red para que ésta no contagie a las otras computadoras.

- Detectar si el daño es físico o lógico.

Esta actividad es para detectar y valorar como es el daño producido por el Spyware que no estuvo al alcance de ser prevenido ni detectado por las nuevas formas de ataque.

- Documentar el origen y/o el modo del posible contagio.

Documentar la forma como se obtuvo el Spyware a través de lo último que se haya realizado en la computadora del usuario, para que sirva de prevención a las demás computadoras así como retroalimentar todos los programas.

- Evaluar el daño ocasionado en caso de desastre.

Esta actividad servirá para valuar el daño producido por el Spyware en tiempo y costo así como el impacto que haya ocasionado dentro del despacho.

- Mantener en forma impresa todos los reportes de los clientes.

Esta actividad es esencial en este programa ya que puede llegar a pasar que se dañe el equipo, el disco duro y/o el respaldo electrónico, y este punto es esencial es este programa ya que es el último recurso para volver a restaurar la información.

- Restaurar la información que con anterioridad se respaldo.

Una vez hecho las actividades anteriormente descritas se procede a restaurar la información por medio del respaldo o el último respaldo que se le realizo a la computadora.

Este programa se estima que sea a partir del mediano o largo plazo ya que cambia de una manera rápida y distinta las formas de contagio.

Su indicador es el número de fracasos entre el número de computadoras en total que tiene el despacho.

Es necesario evaluar el plan por cada uno de sus programas y ver si en realidad éste plan da solución a la problemática del despacho contable, pero éstos serán evaluados en el siguiente capítulo.

Conclusiones

Es así como en este capítulo se busca resolver el problema del Spyware dentro del despacho contable por medio de la planeación.

Entiéndase por este concepto como un proceso de reflexión sobre el qué hacer para pasar de un presente conocido a un futuro deseado. La definición de la situación futura y la selección del curso de acción integran una secuencia de decisiones y

eventos que, cuando se realizan de manera sistemática y ordenada, constituyen un ejercicio de Planeación.

La Planeación como técnica o instrumento se encuentra destinada a adecuar y racionalizar el proceso de toma de decisiones. Por lo tanto, la Planeación así concebida no significa solo crear planes de acción y ejercerlos; implica el esfuerzo creativo y constante que asimile y proyecte, en los cambios coyunturales, la orientación y el ritmo de las variables socioeconómicas, en vías de que prevalezca una mayor racionalidad. Este enfoque proporciona a la Planeación una connotación mucho más amplia: La Creación.

Como instrumento, la Planeación se convierte en un factor gradual de cambio que debe crear las condiciones para afectar el presente y comprometer al futuro.

Se utilizaron dos técnicas de la planeación el costo-beneficio y el análisis FODA que sirvieron como herramienta para el desarrollo del proyecto.

Planear es predecir la incertidumbre para mitigar los riesgos.

Una vez de haber formulado las estrategias harán que se forme un plan, denominado PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN para posteriormente designar los programas que integran el plan.

Capítulo 3
El futuro del Software Espía

Con la planeación estratégica se trata de prever un rumbo y orientarse a un destino, es convertir los objetivos estratégicos en acciones completas y concretas, es pasar de la planeación estratégica a la administración estratégica.

Puede decirse que la idea de planear responde a esta lógica inquietud de la humanidad por conocer su futuro, aunque con un enfoque más activo que la simple espera de su ocurrencia, lo que se busca con la planeación no es tan solo el diseño de escenarios, si no la forma de alterarlos y sacarles el mayor provecho.

Se trata, por tanto de planear el futuro en vez de padecerlo.

Es aquí donde se tiene que recurrir al proceso administrativo para poder ejecutar y controlar el plan, de manera tal que, el proceso administrativo sea realizado de una manera estratégica convirtiéndose así en administración estratégica.[33]

3.1 El proceso administrativo

Existen cuatros funciones fundamentales de la administración: planeación, organización, ejecución y control, que constituyen el proceso administrativo y son los medios por los cuales administra un gerente de otro que no lo es.[34]

Las funciones fundamentales de la administración son:

Planeación: para determinar los objetivos y los cursos de acción que deben tomarse.

Organización: Para distribuir el trabajo entre el grupo y para establecer y reconocer las relaciones y autoridad necesarias.

[33] Acle Tomasini, Alfredo, "Planeación estratégica y control total de calidad"; segunda edición Ed. Grijalbo.
[34] Terry, George R., "Principios de Administración"; Ed Continental, México 1984

Ejecución: Es necesaria por parte de los miembros de la organización para que lleven a cabo sus tareas con entusiasmo.

Control: Es necesario el control de las actividades para conformarlas con los planes.

Hasta el momento se han cubierto las dos primeras etapas del proceso administrativo, en este capítulo se llevara a cabo la ejecución y el control del plan para reducir el riesgo que conlleva el Spyware, y así obtener sus resultados para poderlos evaluar.

Para ejecutar el plan coordinado de seguridad descrito anteriormente y para efectuarlo de una manera responsable se recurrirá a efectuar algunas políticas y normas que conlleve al mejoramiento del plan.

3.1.1 Políticas y normas de seguridad de la información

Este manual de políticas de seguridad de la información contiene un conjunto coherente e internamente consistente de políticas, normas, y procedimientos.

La frecuencia de revisión de la política de seguridad de la información y las formas de comunicación a toda la organización será de forma semanal y mensual si es que se han reducido los riesgos.

La revisión de la idoneidad y adecuación de la política de seguridad de la información puede ser incluida en las revisiones de la dirección al momento de analizar si el plan se esta ejecutando correctamente.

La adopción de la política en la organización debe ser controlada por la gerencia o por una auto-evaluación.

Tener siempre en la mente el tema de la seguridad, hasta que sea algo innato en su proceder al conectarse a Internet.

3.1.2 Políticas a establecer

- Comprobar periódicamente el nivel de seguridad con el que se esta conectado (scan de puertos, antivirus, firewall, datos sensibles en la configuración de cuentas...)
- Realizar periódicamente copias de seguridad de los datos.
- Estar atento a las actualizaciones de los programas porque seguramente arreglaran agujeros de seguridad.
- Instalar y tener siempre activo un Antivirus y, por supuesto, actualizarlo periódicamente.
- Instalar un firewall y estar atento a las actualizaciones.
- Configurar en principio cualquier programa, y en especial el navegador de Internet, en el nivel más alto de seguridad.
- En las páginas web donde se tenga que introducir información sensible (por ejemplo el número de la tarjeta de crédito), procurar que sean siempre seguras (empiezan por https:)
- NUNCA ejecutar un adjunto de un correo con extensiones *.exe, *.bat, *.pif, *.reg, *.com ya que son programas que se ejecutan automáticamente por lo regular virus y/o Spyware y que muchas veces no son detectados por las suites de seguridad.
- Encriptar los mensajes y ficheros más sensibles.

- No aceptar nunca archivos que no se hayan solicitado cuando se esté en el chat (IRC) o grupos de noticias (NEWS).
- No instalar software que no sea el necesario con el que el despacho trabaja, sin excepción alguna.
- No instalar programas P2P.

3.1.3 Normas de seguridad

- Tener especialmente cuidado cuando se descargue software de sitios dudosos.
- No fiarse de los enlaces (links) de las páginas. Comprobar que se conduce a la página verdadera a donde se quiere ir, en caso de no estar seguro no dirigirse a tal link.
- No propagar los HOAX. Hay que romper las cadenas de mensajes. Actúan como un VIRUS donde uno mismo es el propagador además de causar alarma y pánico en los demás usuarios.
- Si no se quiere recibir SPAM, cuando se envié un mensaje a las NEWS, poner tanto en la dirección de correo de la cabecera del mensaje como en la firma algún identificador que haga imposible que pueda ser recogido de forma automática por programas informáticos.
- Si se va a ocupar una unidad de almacenamiento externa como memorias USB avisar al encargado antes de utilizarla.
- Revisar los dispositivos externos de información que no contengan virus.
- Leer siempre los contratos de licencia antes de instalar cualquier nueva aplicación del equipo.
- No visitar páginas de juegos en línea, pornográficas o de páginas que ofrecen archivos gratuitos de audio y video

- Hacer caso omiso a los mensajes o ventanas el cual dice que uno es el ganador de algún premio, dinero o regalo.
- No dar clic a los enlaces de supuestos antivirus, antiSpyware que según detectan en unos microsegundos o segundos que la computadora esta infectada.
- No visitar las ligas de supuestos usuarios que están buscando pareja y que por lo regular y casualmente viven cerca de la zona donde uno está.

Por último cabe hacer mención de algunas recomendaciones:

- ✓ Ante la duda, favor de abstenerse.
- ✓ Ayuda a los demás.
- ✓ Da a conocer estas normas y políticas de seguridad. a quién las desconozca.

3.1.4 Responsabilidades y obligaciones

Dentro de la planeación esta parte administrativa es importante ya que es la forma de integrar el plan dentro del despacho contable.

Aquí se hace una revisión de lo que se tiene y lo que no se tiene así como en que determinado plazo se va a realizar.

Las responsabilidades y obligaciones se necesitan para que los programas se produzcan y por consecuencia alcanzar a cumplir el plan coordinado de seguridad de la información.

3.1.5 Asignación de responsabilidades

El gerente general es responsable de que el plan se lleve a cabo por medio de reportes y diagnósticos que serán emitidos por los responsables de cada programa, además de ser critico y tener la visión de lo que puede o no puede realizarse de forma correcta.

El subgerente general estará a cargo del programa de control y su obligación es realizar un reporte de las actividades del programa ya descritas con anterioridad.

El área de informática estará a cargo de los tres programas restantes, de prevención, detección y del programa de contingencia y desastres por el simple hecho de tener más aptitudes en la materia. Pero con la idea de delegar responsabilidades a un nivel posterior del organigrama a un mediano plazo a tal grado que a largo plazo solo sea responsable del programa de contingencia y desastres.

Todas las responsabilidades de este plan y su programas deben estar soportadas por una clara definición de los resultados.

Además de reflejar y satisfacer las necesidades de los altos ejecutivos, y en caso de desviaciones de los planes correspondientes deberán ser informados debidamente en forma oportuna y clara.

Una responsabilidad que tienen todos los integrantes del despacho contable es respetar las políticas y seguirlas al pie de la letra, en caso de no hacerlo o de ser sorprendido de no efectuarlas será advertido de una posible sanción, si reincide una segunda vez, ésta vez será sancionado de acuerdo a como sea valorado el daño pero si por tercera vez volviera a ser sorprendido de no seguir las políticas será expulsado de la empresa no sin antes cubrir los daños que haya ocasionado.

Esto generará que los usuarios sean conscientes que los únicos responsables de las computadoras y lo que pase con éstas son ellos mismos. Por eso se le inculcara que fomenten los buenos hábitos solo con seguir las políticas y alinearse con las mismas.

Una vez ya aclaradas las políticas y normas de seguridad que servirán como lineamiento para una mejor ejecución y evaluación se dispondrá a llevar a cabo el denominado PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN y cada uno de sus programas.

3.2 Resultados

3.2.1 Primera evaluación: La detección

Dentro del plan se considerará primeramente evaluar el programa de detección de Spyware para determinar en que situación se encuentra el estado de las computadoras con respecto al numero de Spyware's que pudieran tener cada una de las computadoras.

Para ello se recurrirá al software Spybot Search&Destroy que se manejara para la detección y corrección del software espía, reconocido y recomendado por su facilidad y manejo así como su eficacia para solucionar problemas de Spyware. *(Figura 1)*

Después se le dará la opción de analizar problemas para iniciar el análisis del sistema en busca de software espía y otras amenazas. *(Figura 2).*

Una vez que termine el análisis de Spyware y otras amenazas desplegará el número de problemas que encontró, tales como cambios de registro, archivos que son parte del Spyware así como carpetas y cookies que tiene almacenadas la computadora.

A continuación se tiene que eliminar las entradas incorrectas del registro de Windows que detecta el Spybot, primeramente seleccionando o palomeando las entradas que se detectaron y a continuación se selecciona el botón solucionar problemas seleccionados *(figura 3)* desplegando luego una confirmación que menciona que esta a punto de eliminar las entradas seleccionadas se le dá un click del mouse a "SI" a la pregunta de si se desea continuar *(figura 4)* una vez hecho esto despliega una ventana del numero de entradas que corrigió *(figura 5)* esperando que sea el mismo número de entradas de Spyware que detectó.

Cuando esto no sucede, (corrección de todas las entradas que se detectaron) es probablemente porque el Spyware esta activo en memoria y puede ser que sea necesario modificar el registro de Windows haciendo que se pierda más tiempo en reparar la computadora, de tal modo que el Spyware podría provocar un daño mayor del esperado.

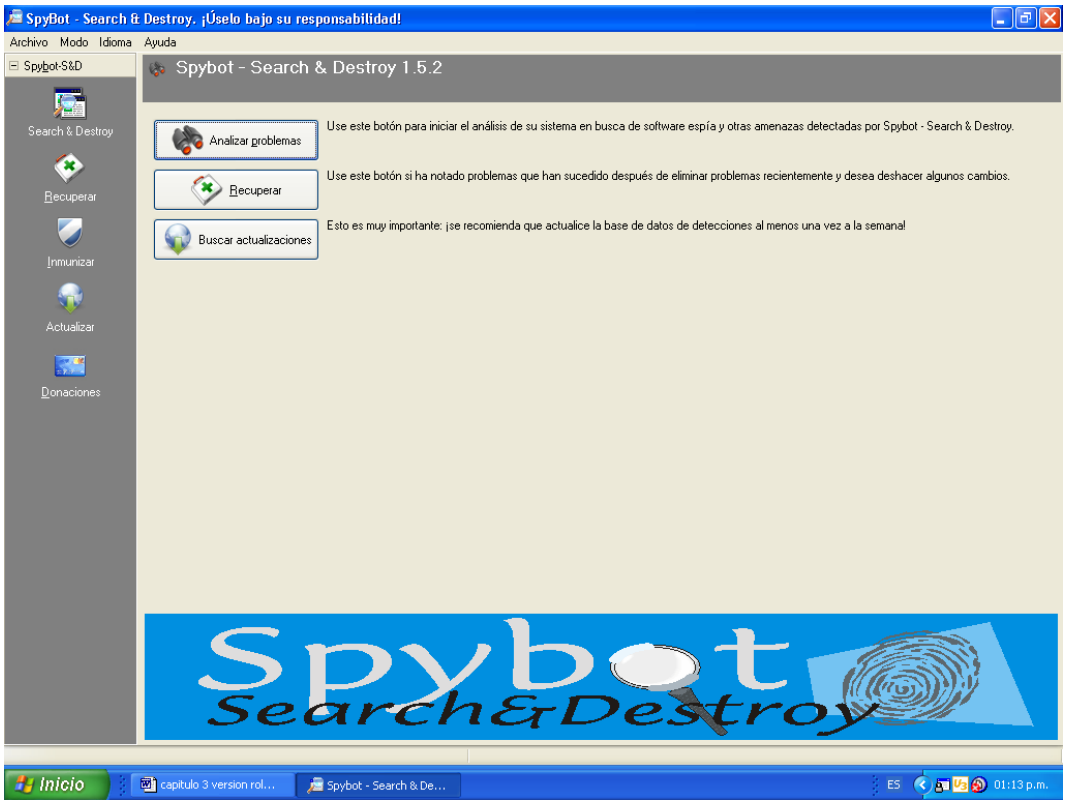

SpyBot - Search & Destroy, ¡Úselo bajo su responsabilidad!
Archivo Modo Idioma Ayuda
Spybot-S&D
Search & Destroy
Recuperar
Inmunizar
Actualizar
Donaciones
Spybot - Search & Destroy 1.5.2
Analizar problemas
Use este botón para iniciar el análisis de su sistema en busca de software espía y otras amenazas detectadas por Spybot - Search & Destroy.
Recuperar
Use este botón si ha notado problemas que han sucedido después de eliminar problemas recientemente y desea deshacer algunos cambios.
Buscar actualizaciones
Esto es muy importante: ¡se recomienda que actualice la base de datos de detecciones al menos una vez a la semana!
Spybot
Search&Destroy
Inicio
capitulo 3 version rol...
Spybot - Search & De...
ES
01:13 p.m.

Figura 1

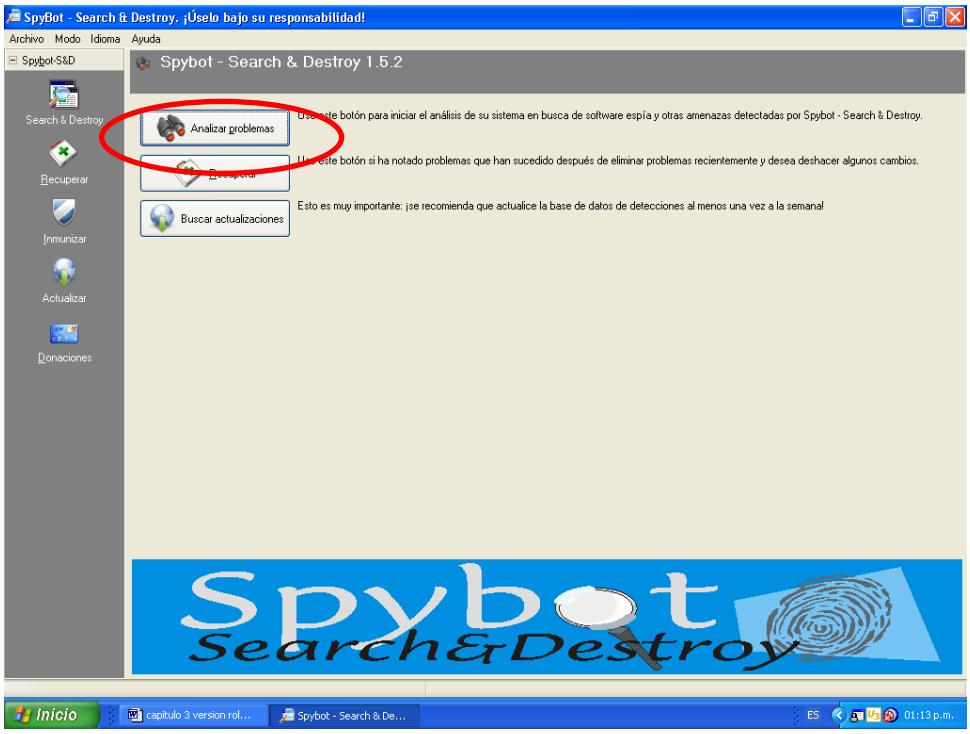


Figura 2

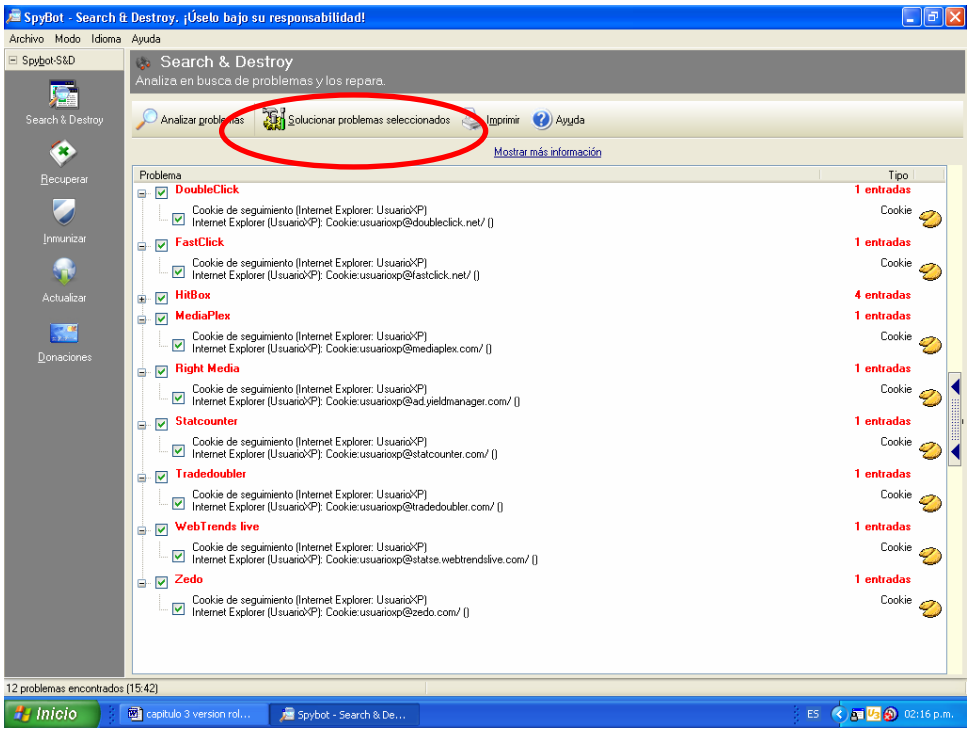


Figura 3

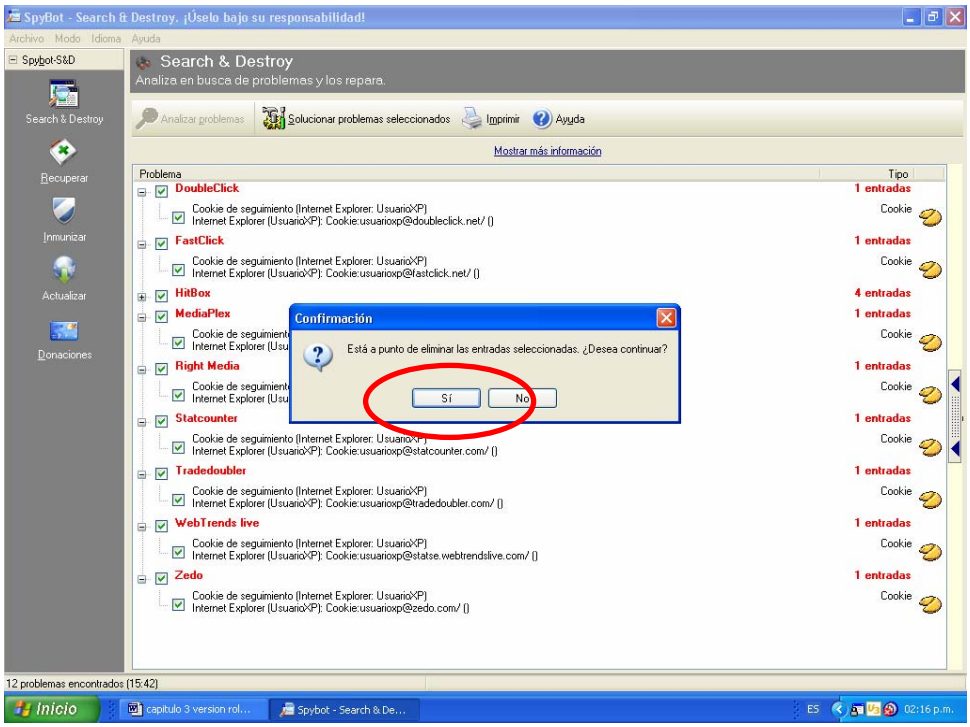


Figura 4

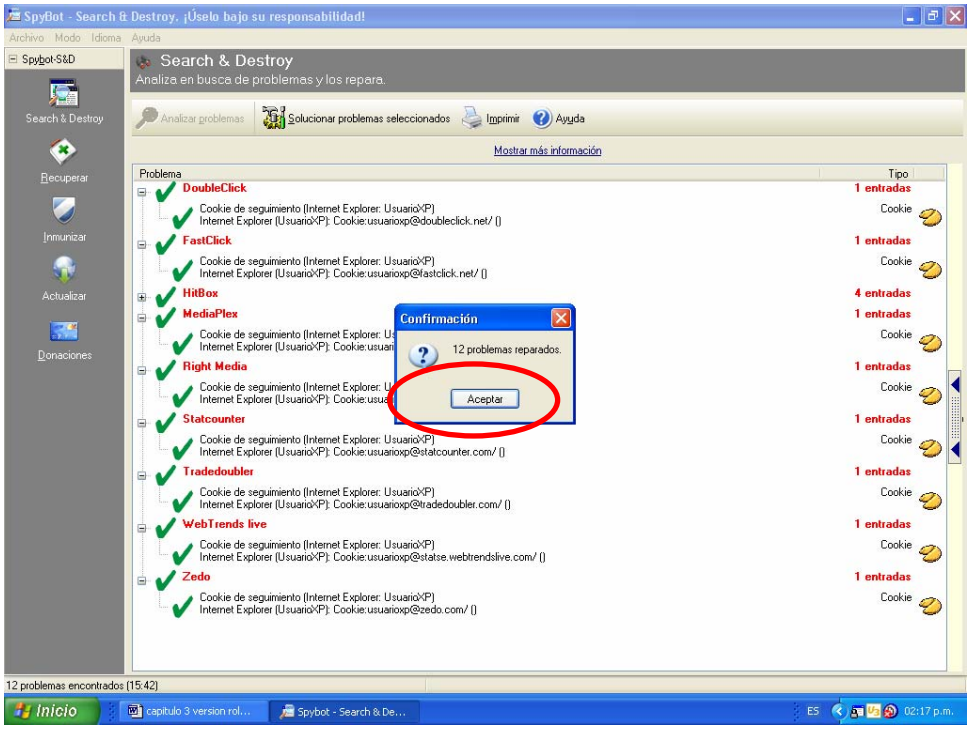


Figura 5

Una vez terminado el análisis de las computadoras del despacho contable se obtuvieron los siguientes resultados:

De las 15 computadoras con las que trabaja el despacho todas tuvieron alguna entrada de Spyware, pero cabe decir que en dos computadoras más que entradas de Spyware las entradas que se modificaron fueron que deshabilitó el antivirus y el firewall o cortafuegos, siendo esto uno de los primeros indicios de que el Spyware empieza a realizar algún daño en la computadora comenzando en desactivar el antivirus y/o cortafuegos para que en el momento en que se ejecute el programa espía no sea detectado por la protección que se tiene haciendo más sencilla su instalación en la computadora.

Por lo tanto siguiendo una simple ecuación de:

Número de computadoras infectadas de Spyware/Total del número de computadoras en la Organización

$$\frac{15}{15} = 1$$

Es decir el 100% de las computadoras del despacho tienen algún indicio de Spyware.

Éste el indicador para saber el porcentaje y el grado de infección de Spyware en las computadoras. Siendo que unas tienen mayor grado de infección que otras, dado que tienen más entradas de Spyware.

En la detección, 4 computadoras es decir, el 26.66% de los equipos, no corrigió todas las entradas de Spyware teniendo al menos 2 entradas que no se corrigieron, ya sea entradas de registro o carpetas por eliminar.

Aunque el tener más entradas de Spyware en la detección a través del Spybot no significa que sea más peligroso, ya que puede tener menos entradas pero la entrada detectada puede tener mayor riesgo de perder información o

dañar la computadora, sobre todo cuando el Spybot no logra eliminar las entradas que tiene que solucionar.

Después de detectar el Spyware se procede a realizar un análisis para verificar si contiene virus, claro está que una vez ya instalado el antivirus del cual por cierto no se instalo en 3 computadoras dado que estaban infectadas de virus a tal grado que no se pudo instalar el antivirus o suite de seguridad para ser más preciso.

Es decir el 20% de las computadoras estaban en un grado crítico, lo cual era de esperarse ya que eran éstas las que más fallas tenían, además de ser las que trabajaban más lento, aunque estas también se checaron para identificar los virus que contenían, aunque de una manera distinta y se requirió de un tiempo mucho mayor del que se llevaron las demás computadoras.

En cuanto a las demás computadoras de las 12 computadoras restantes 9 tenían virus, al igual que el Spyware unas más que otras pero lo que si sucedió es que curiosamente las que tenían más entradas de Spyware tuvieron de igual manera más archivos infectados de Virus.

Otra cosa que sucedió es que 2 de las 3 computadoras es decir, el 66% que no se conectan a Internet no contenían virus, posiblemente porque el virus se adquiere una vez instalado el Spyware o deshabilitado el antivirus y por medio de Internet.

En resumen el 80% de las computadoras contenían virus y solo el 20% no, el 13% de éstas últimas no se conectan a Internet, aunque si tenían un antivirus instalado.

Una vez hecho los dos procedimientos anteriores y estando libres de virus y Spyware se procede a realizar el respaldo de la información como parte del programa, con la garantía de que la información está limpia de Spyware.

Este procedimiento se realizó anteriormente, antes de realizar el proceso de detección como una manera de prevención por alguna circunstancia inesperada que pudiese ocurrir, aún con el conocimiento que al respaldar se corría el riesgo de también respaldar el Spyware y/o el virus o la semilla de ambos, pero se tenía que correr el riesgo por si sucedía alguna anomalía.

Cabe mencionar que exactamente las computadoras en las cuales no se pudo instalar la suite de seguridad son las mismas en las cuales no se pudo obtener un respaldo de archivo, dado que el proceso no terminaba de manera correcta.

Ya una vez con el conocimiento de que se han eliminado tanto el Spyware como el virus se procedió a realizar el respaldo de archivos con la idea de tener ahora si un respaldo seguro y que hubo una efectividad ahora si del 100% de éxito en el respaldo de información.

3.2.2 Capacitación e información al usuario

Es así como se termina la primera etapa del PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN que es el programa de detección de Spyware, para continuar con el siguiente programa del plan que es el programa de prevención del Spyware.

Como primer paso a dar, es la capacitación al usuario para prevenir el contagio de Spyware y sus riesgos que conlleva.

Esta capacitación esta a cargo de una persona con conocimientos en computación tales como:

- Manejo del sistema Operativo Windows nivel operativo pero sobre todo y fundamentalmente a nivel administrador.

- Conocer el software anti-Spyware Spybot Search & Destroy.

- Saber modificar el registro de Windows por alguna emergencia que pudiera ocurrir.

- Manejar comandos del sistema Operativo MS-DOS ya que se recurrirá a ellos si se quiere desactivar algún Spyware que no pueda eliminar el anti-Spyware o alguna(s) de su(s) semillas(s).

- Tener liderazgo dentro de la empresa.

- Conocer y manejar la(s) suite(s) de seguridad para detallarle a los usuarios el manejo apropiado del software.

Dentro de esta capacitación hacia los usuarios y a través de la lluvia de ideas que ahí se realizaron se notó que la manera en que más entendían de los riesgos que conlleva el Spyware era hacer similitudes así como analogías de casos prácticos y sencillos que cotidianamente pasan.

Como por ejemplo el decir que para no correr el riesgo de embarazo en una relación sexual era usar algún tipo de preservativo como el condón(en éste caso algún software de seguridad) pero eso no garantizaba que no saliera

embarazada ya que no es 100% seguro y había una probabilidad de que sucediera, tal vez mínima pero al fin y al cabo existía la posibilidad, al igual que el caso del Spyware que a pesar de tener todo tipo de seguridad y protección hablando en cuestión software no garantizaba que no se pudiera adquirir el Spyware. Otra forma de no embarazarse es la abstinencia en el caso específico del Spyware es no tener contacto con el Internet, el intercambio de información ó a través de medios de almacenamiento y demás formas explicadas en el capítulo 1.

O el de una casa o empresa que tuviera algún tipo de alarma, circuito cerrado o guardia de seguridad, no garantizaba que no fuera espiada para posteriormente ser robada con suma facilidad.

Cuantos casos no se han dado de que el mismo guardia es quien permite el acceso de los ladrones con su consentimiento, lo mismo pasa con las advertencias de seguridad tanto del anti-Spyware como de la suite de seguridad que indica que se realizará una modificación en el registro de Windows y si se acepta sabiendo que se corre el riesgo de instalar el Spyware se está permitiendo la entrada al igual que el guardia, dado que se esta consintiendo y permitiendo el acceso.

O el de la misma alarma que con solo el hecho de desactivarla la hace inservible y se pierde el control que se quería, lo mismo sucede con el Spyware que lo primero que realiza es desactivar el software de seguridad para poder entrar con facilidad y sin ningún problema.

Así como estos ejemplos hay muchos y variados, por ello la persona que dé la capacitación debe de tener ese don y esa creatividad necesaria e indispensable para buscar la manera de asemejar los grandes riesgos que se

corren a causa del software espía de una manera amena. Este punto es importante ya que una de las tantas soluciones que se tienen para crear conciencia en el usuario de los problemas que causa el Spyware es despertar el interés de las diferentes formas de contagio y sus similitudes reales de la vida cotidiana.

3.2.3 Análisis en la detección de Spyware

A continuación se muestran unas tablas con la información recopilada acerca del primer programa del PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN.

Computadora	Respaldo Satisfactorio	Sistema Operativo	Conexión a Internet	Instalación de Anti-Spyware	Instalación de Antivirus	Spyware	Entradas no corregidas	Archivos con Virus	Respaldo satisfactorio
1	SI	Windows XP	SI	SI	SI	SI	4	70	SI
2	SI	Windows ME	SI	SI	SI	SI	0	12	SI
3	SI	Windows ME	SI	SI	SI	SI	0	0	SI
4	SI	Windows 98	NO	SI	SI	SI	0	7	SI
5	NO	Windows XP	SI	SI	NO	SI	3	120	SI
6	SI	Windows XP	SI	SI	SI	SI	0	33	SI
7	SI	Windows 98	NO	SI	SI	SI	0	0	SI
8	SI	Windows ME	SI	SI	SI	SI	0	17	SI
9	NO	Windows XP	SI	SI	NO	SI	7	220	SI
10	SI	Windows ME	NO	SI	SI	SI	0	0	SI
11	SI	Windows XP	SI	SI	SI	SI	0	7	SI
12	NO	Windows XP	SI	SI	NO	SI	2	15	SI
13	SI	Windows ME	SI	SI	SI	SI	0	9	SI
14	SI	Windows ME	SI	SI	SI	SI	0	5	SI
15	SI	Windows XP	SI	SI	SI	SI	0	43	SI

Primer Análisis de detección de Spyware

Segundo Análisis de Detección de Spyware

Computadora	Sistema Operativo	Spyware	Entradas no corregidas	Archivos con Virus	Respaldo satisfactorio
1	Windows XP	SI	0	3	SI
2	Windows ME	SI	0	1	SI
3	Windows ME	NO	0	0	SI
4	Windows 98	NO	0	0	SI
5	Windows XP	SI	1	5	SI
6	Windows XP	SI	0	0	SI
7	Windows 98	NO	0	0	SI
8	Windows ME	SI	0	0	SI
9	Windows XP	SI	0	3	SI
10	Windows ME	NO	0	0	SI
11	Windows XP	SI	0	0	SI
12	Windows XP	SI	1	2	SI
13	Windows ME	NO	0	1	SI
14	Windows ME	SI	0	0	SI
15	Windows XP	NO	0	0	SI

Tercer Análisis de Detección de Spyware

Computadora	Sistema Operativo	Spyware	Entradas no corregidas	Archivos con Virus	Respaldo satisfactorio
1	Windows XP	SI	0	0	SI
2	Windows ME	NO	0	0	SI
3	Windows ME	NO	0	0	SI
4	Windows 98	NO	0	0	SI
5	Windows XP	SI	1	0	SI
6	Windows XP	NO	0	0	SI
7	Windows 98	NO	0	0	SI
8	Windows ME	NO	0	0	SI
9	Windows XP	SI	0	0	SI
10	Windows ME	NO	0	0	SI
11	Windows XP	NO	0	0	SI
12	Windows XP	SI	1	0	SI
13	Windows ME	NO	0	0	SI
14	Windows ME	NO	0	0	SI
15	Windows XP	NO	0	0	SI

En este momento se está realizando la siguiente etapa de detección de Spyware de acuerdo al Plan Coordinado de Seguridad, que servirá de comparativo para saber de que forma se redujo el contagio de Spyware así como de virus una vez que se le ha tratado de generar conciencia al usuario de los riesgos del Spyware.

Es así como se nota en los resultados anteriormente descritos que se puede reducir los riesgos de adquirir Spyware, de hasta un poco más del 70% en las computadoras con las que trabaja el despacho.

Además de que las computadoras han tenido un 100% de efectividad en los respaldos de información, cuando en un principio el 20% había fallado y otro 20% había sido respaldado pero con algún archivo infectado de virus.

Es decir que sólo el 60% de respaldo de información había sido efectivo al comienzo de la puesta en marcha del PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN.

Al obtenerse una reducción de contagio de Spyware, implícitamente también habrá una reducción de costo en reparación así como de mantenimiento a los equipos de cómputo.

Se diría entonces que ahora los costos de acuerdo a los resultados obtenidos serían de la manera siguiente:

[0.30 * (# Computadoras) * costo de reparación] - (costo de software seguridad) - (accesoria, capacitación).

Recuerdese que apenas esta por completar la primera etapa del PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN y que se espera llegar al ideal de que todas las computadoras estuviesen libres de Spyware, es decir que el 100% de las mismas no tengan ningún problema y por tal motivo ningún riesgo.

Con la ventaja de reducir el riesgo de perder información, que es el activo más importante de la empresa. Además no solo se beneficiaria la empresa si no se estaría contribuyendo a no expandir el contagio a otras computadoras por cualquier medio pero sobre todo en Internet.

3.3 Proyección

Una proyección es una característica de desempeño de una organización, sus partes o su ambiente desde su pasado reciente hacia el futuro, sin suponer cambios significativos en el comportamiento del sistema o su medio. Estos no son pronósticos del futuro; son proyecciones del tipo “que pasa si”.

Ponen de relieve los objetivos actuales que no se pueden obtener sin cambios en el funcionamiento de la organización o de su medio.

En esta investigación sobre Spyware, de no controlar el contagio y la contaminación de las computadoras de éste último se estaría llegando a un estado en el cual la empresa no trabajara eficientemente, es más tal vez ni con lo mínimo de lo que se pudiera obtener de las computadoras como herramienta para los cálculos contables, puesto que las computadoras estarían trabajando a un nivel bajo de productividad a causa del Spyware, como ya se ha comentado anteriormente.

Además de perder o dañar el hardware, que puede ir desde un disco de 3 ½ hasta un disco duro y en el peor de los casos hasta de la tarjeta madre y/o procesador.

Y se estaría perdiendo uno de los activos más importante de la empresa, “La información” de los clientes, lo cual para recuperarla se tendría que trabajar horas extra para poder recuperar lo que se pudiese perder.

En los últimos cuatro años, 58% de las Pymes en México ha padecido los estragos de algún tipo de ataque cibernético, hecho que ha llevado a la pérdida de información valiosa.

Douglas Wallace, director de Ingeniería de Sistemas para América Latina de Symantec, explicó que diariamente ocurren en el mundo siete millones de intentos de fraude electrónico o robo de información. Y, dentro del comercio electrónico, son las pequeñas y medianas empresas uno de los sectores más vulnerables a este tipo de ataques.

Hoy esta industria vive un aumento en el robo y fuga de datos, así como la creación de códigos maliciosos dirigidos con el fin de malversar información confidencial, que puede ser usada con fines económicos.

Y es que, según Wallace, “hoy día se lucra con la información que obtienen de manera ilícita y, además, no son los grandes corporativos de empresas multinacionales y bancos las únicas víctimas, porque ahora el tema acongoja a la Pyme, el que navega desde su casa o desde algún dispositivo móvil está siendo blanco de estas amenazas”.

Un estudio realizado por Symantec hace unos meses reveló que 80% de las Pymes en México padece la falta de presupuesto y los retos de recursos en sus empresas. En este aspecto, la falta de una mayor capacitación a sus empleados es el principal obstáculo para la implantación de soluciones integrales de seguridad y respaldo.

Durante 2007 surgieron en el mundo cerca de 1.2 millones de virus, lo que significa que cada dos minutos alrededor de cinco nuevas amenazas están circulando en la red (3,287 cada día; 136 cada hora y 2.28 cada minuto), advirtió el experto en códigos maliciosos Eugene Kaspersky, presidente de Kaspersky Lab.

Los virus y programas espía ya no sólo afectan a las PC, ahora han llegado hasta los dispositivos y redes móviles. Según la compañía McAfee 83% de los adolescentes descargan música digital, el tipo de búsqueda más riesgosa en la web.

3.3.1 Pérdidas Millonarias

Cada año los fraudes cibernéticos ascienden a 105 mil millones de dólares a nivel mundial, informó recientemente el director general de la Asociación de Usuarios de Servicios Bancarios de España, Carlos Hernández.

Además, según información de la Asociación Mexicana de Internet, de cada 100 quejas de fraudes que se realizan en México, el 80% está relacionado con operaciones electrónicas siendo denunciadas ante las instancias legales sólo el 0.3%. El monto promedio de quienes han sido defraudados por este sistema va de cinco mil a un millón de pesos mensuales

Al menos 18% de las computadoras que cuentan con una solución antivirus están infectadas con algún código malicioso, reveló la empresa Panda Security. Según una investigación que realiza en la dirección www.infectedornot.com.

En el caso del phishing a través del correo tradicional Reyes Krafft comentó que estos atacantes “pueden mandar una carta con el logotipo del SAT, por ejemplo, diciendo que el usuario tiene una devolución de impuestos; u o otra carta diciendo que se ganó un premio y entonces le piden el número de cuenta o de tarjeta o el NIP para supuestamente depositar ahí el dinero”.

Según un estudio elaborado por Consumer Reports, sólo en los Estados Unidos el malware generó unas pérdidas de 7.000 millones de dólares los dos últimos años.

El estudio afirma que uno de cada cuatro ordenadores está expuesto a convertirse en víctima de delincuentes virtuales, bien por la instalación de spyware, o bien por programas que convierten a los PCs en zombies y permiten su control a distancia.

Está claro que vale más gastarse algo de dinero en un buen antivirus que lamentar las consecuencias, aunque por mucho que se insita en la importancia de proteger correctamente el ordenador no parece que el mensaje termine de calar entre los usuarios. Según el estudio, nada menos que 3,7 millones de hogares con acceso de banda ancha ni siquiera tienen instalado una protección elemental ante las diversas amenazas que acechan en la Red.

Como consecuencia de todos estos ataques, nada menos que 1,8 millones de hogares decidieron cambiar de PC en los últimos dos años para liberarse del malware.

El incremento de la sofisticación de las amenazas y su impacto potencial en la organización es exponencial, no retrocede, no da tregua. Incluso la percepción de la intensidad de los ataques informáticos está repartida entre el phishing y el farming por un lado (53%), y los virus, el spyware, los troyanos y los gusanos por otro (51%), según deja ver la Encuesta Global de Seguridad 2006 de Deloitte.

El robo de identidad ha sido catalogado por Deloitte como el crimen del siglo 21, ya que los delincuentes actúan de manera más organizada y consiguen bases de datos completas por módicas cantidades.

Aunque el incumplimiento interno de políticas de seguridad sigue generando cuantiosas perdidas, 72% de quienes han experimentado lo anterior creen que los costos ascienden a por lo menos $1 millón de dólares.

58% de las instituciones financieras tienen como su principal prioridad prevenir el robo de identidad y los fraudes a cuentas de clientes, 59% no tiene un presupuesto para seguridad de la información, 95% de quienes tienen presupuesto de seguridad de la información lo han visto incrementarse, 8% creció el gasto en consultaría en seguridad con respecto al año pasado, 12% disminuyo el gasto en auditorías y certificaciones con respecto al año pasado, 48% de las políticas de seguridad versan sobre el uso de tecnologías inalámbricas

Con los virus se infectaban computadores, se bloqueaban sitios web, se borraba información y se causaba pánico, pero no se ganaba dinero. Pero ahora, "algunos programas de spyware se centran en espiar el comportamiento de una persona en Internet; los lugares que visita y las actividades que realiza en la red, los correos electrónicos que escribe y envía, así como sus conversaciones de mensajería instantánea. Tras recopilar toda esta información, el programa de spyware la transmite a otro equipo, por lo general, con fines publicitarios", explica Daniel Rojas, gerente de ventas de canal retail de Symantec.

Con cada máquina invadida y dependiendo de la cantidad de información y su calidad, se pueden hacer negocios que van desde US$500 hasta varios miles. De hecho, ya hay cibersubastas en las cuales se consiguen desde números y claves de tarjetas por US$7, hasta vulnerabilidades del nuevo Windows Vista por US$50.000, como en un gran bazar medieval de hechiceros y alquimistas.

La Ingeniería Social sigue siendo el elemento más explotado para engañar e infectar al usuario. Esto queda demostrado con la aparición de gran cantidad de malware que utilizan las tarjetas virtuales y los eventos de gran envergadura para incitar al usuario a que descargue un archivo dañino. La realización de los juegos olímpicos durante 2008 seguramente será una importante red para cazar usuarios desprevenidos.

La formación de grandes comunidades online (como MySpace, Orkut, FaceBook y diferentes juegos en línea) también se ha convertido en un importante punto para abusar de la confianza de los usuarios. Actualmente, ya existe gran cantidad de malware disponible para robar los datos privados a los usuarios que participan de estas comunidades.

La diseminación y posterior infección por intermedio de dispositivos de almacenamiento extraíbles [6] (USB, memorias, flash, etc) que aprovechan las bondades de ejecución automáticas de los sistemas operativos, se ha ido acrecentando desde mediados del 2007 y todo indica que seguirá creciendo aún más.

De hecho, según sus cifras, el malware creció un 61 por ciento entre 2006 y 2007, año en el que se produjeron 327 nuevas detecciones al día. Además, DeWalt afirma que, hoy por hoy, el 80 por ciento de los ataques tienen un motivo económico detrás.

Asimismo, es necesario proteger los datos corporativos, pues considera que la seguridad perimetral ya no es suficiente, ya que el 70 por ciento de las organizaciones experimentan pérdidas de datos causadas por sus propios empleados.

Por eso es que es tan importante que se tenga que resolver como hasta ahora el problema del Spyware, para no padecerlo en el futuro inmediato con todos sus riesgos que conlleva.

Y la importancia de tener un PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN (PCSI) que incluye a todo el personal de la empresa para que trabaje en forma conjunta y de manera holística con la importancia de respaldar la información como elemento vital (forma pasiva)[31] y tanto evitar como anular riesgos (forma activa)[32] ante un posible desastre ya que como se ha comentado el Spyware por esencia tiene un grado de incertidumbre.

[31] Rodao Jesús de Marcelo, "Piratas Cibernéticos"; Ed. Rama
[32] Ibid

Por tal motivo el PCSI contempla abarcar los tres pasos de una protección informática[33]

Asumir el Riesgo

Minimizar el Riesgo

Transformar el Riesgo

Y de no realizarse una planeación para evitar esos riesgos, la empresa quedaría cada vez más expuesta a compartir información confidencial así como a perderla y lo peor aún sin el conocimiento de que esto estuviera sucediendo.

Además de contagiar con mayor facilidad a otras computadoras puesto que hay más maquinas infectadas, aumentando el riesgo de contraer el Spyware no solo dentro de la empresa si no fuera de ella.

3.3.2 Misión estratégica

Una vez de ver la proyección de que pasaría si no se soluciona el problema del Spyware así como sus riesgos implícitos, es necesario generar de nueva cuenta una misión para hacer que esto no suceda, esto gracias a la planeación estratégica que es flexible para modificar cuando se necesite para una mejora continua.

Luego entonces, la misión para el despacho contable sería:

Ser una empresa eficaz y eficiente que brinde a sus clientes información veraz, rápida y oportuna para una mayor comodidad y seguridad en los servicios que se brindan.

[33] Pierre Graton, "Protección Informática" Ed. Trillas

Por tal motivo para tener un nivel de seguridad alto es indispensable tener:

3.3.3 Diagnóstico de seguridad.

Objetivo: Identificar las brechas de seguridad existentes en una organización, así como desarrollar las recomendaciones necesarias para contar con un nivel adecuado en seguridad de la información.

Identificar las mejores prácticas y estándares de la organización respecto a controles, políticas y procesos de seguridad.

Evaluar los controles de seguridad existentes en la organización.

Revisar la organización de seguridad, sus roles, sus responsabilidades así como su estructura.

Elaborar Plan para reducir la exposición a los riesgos de seguridad.

Beneficios.

Conocer detalladamente las vulnerabilidades existentes en la infraestructura de TI, catalogadas por su severidad.

Disponer de información confiable para la toma de decisiones en cuanto a inversión de recursos en seguridad de la información.

Contar con las bases de un plan, diseñado para alinear los controles de seguridad y análisis de riesgos

Los activos de información en las organizaciones están sujetos a altos niveles de riesgo, desde la posibilidad de acceso a información confidencial por parte de personas no autorizadas, pasando por el desprestigio de su imagen hasta llegar a la paralización de las operaciones debido a la pérdida de información.

3.3.4 Detección de puntos débiles.

Objetivo: Determinar el nivel de seguridad de una organización identificando las amenazas y vulnerabilidades a la que están expuestos sus activos de información, valorando su impacto y la probabilidad de que ocurran.

Conocer el nivel de seguridad de la organización y las amenazas que enfrenta.

Identificar los principales activos de información y sistemas críticos.

Identificar las amenazas, vulnerabilidades y riesgos presentes en la organización.

Establecer la estrategia de protección.

Desarrollar los planes de mitigación de riesgos.

Beneficios

Determinar el nivel de seguridad deseado.

Contar con las bases de un plan, diseñado para alinear los controles de seguridad de la información con las prioridades, estrategia y objetivos del negocio.

Identificar, evaluar y minimizar los riesgos de seguridad.

Establecer las bases de una cultura preventiva de protección.

Enfocar recursos y esfuerzos en la protección de los activos de información críticos.

Cumplir con leyes y regulaciones de la Información con las prioridades, estrategias y objetivos de su negocio.

Contar con las recomendaciones necesarias para corregir las vulnerabilidades encontradas mitigando el impacto ante la ocurrencia de eventos.

3.3.5 Mecanismo de seguridad

La mejor manera de saber si su red esta segura es conociendo sus vulnerabilidades.

Objetivo: Conocer las brechas de seguridad existentes en la infraestructura de TI previo a que sean descubiertas y utilizadas por personal malintencionado y poner en riesgo la información, los procesos y servicios de la organización.

Identificar la información de la organización que esta visible desde Internet.

Identificar y documentar los servicios de red expuestos de forma interna y externa, y los riesgos asociados.

Probar los mecanismos de seguridad que protegen la infraestructura de TI de la organización.

Recomendar acciones para la eliminación de las brechas de seguridad.

Beneficios

Conocimiento de las brechas de seguridad actuales, tanto del perímetro como en la red interna.

Recomendaciones de acción inmediata con un alto nivel de detalle para corregir las brechas de alto riesgo.

Recomendaciones estratégicas orientadas a la arquitectura de la red.

Evaluación de la efectividad de los controles de seguridad existentes en la organización.

Cumplimiento de regulaciones y leyes al ejecutar periódicamente este servicio.

Acciones preventivas sobre las brechas de seguridad antes que sean descubiertas y utilizadas por intrusos.

Contar con un guía que permita la incorporación de la seguridad de la información en la organización, considerando, entre otros, los siguientes aspectos:

Organización de Seguridad de la Información.

Políticas, estándares y procedimientos de Seguridad.

Metodología de evaluación y tratamiento del riesgo.

Planes de contingencia y continuidad operativa.

Planes de sensibilización y formación en seguridad de la información.

Manejo de incidentes de seguridad.

Monitoreo y cumplimiento de la normativa de seguridad.

3.3.6 Normatividad y auditoría

OBJETIVO: Crear el marco normativo de seguridad de la información a través del desarrollo, documentación e implantación de políticas, estándares y procedimientos de seguridad, que permitan lograr un alto nivel de confidencialidad, confiabilidad (integridad) y disponibilidad de la información, así como también del cumplimiento normativo.

El marco normativo son las bases de cualquier programa de seguridad y permite la toma de decisiones en relación a:

Estructura y gestión de la seguridad.

Auditoría.

Control de acceso.

Manipulación de la información.

Uso aceptable de recursos.

Planificación ante desastres.

Manejo de incidentes.

Protección perimetral.

Capacitación y sensibilización del personal en seguridad.

Beneficios.

Contar con los objetivos estratégicos y la postura organizacional en seguridad de la información.

Marco de referencia para medir el progreso y el nivel de seguridad en la organización.

Contar con las bases para justificar una mejora continua de la seguridad de la información.

Alinear los esfuerzos en seguridad de la información con los requerimientos del negocio.

3.3.7 Prevención de riesgos

¡Todas las empresas son vulnerables!

El 90% de las empresas que han sufrido desastres sin tener un plan de contingencia, han dejado de operar en el corto plazo.

La continuidad de las operaciones no se garantiza solamente con disponer de un centro de cómputo alterno; adicionalmente, se requiere de procedimientos especiales de trabajo, roles y responsabilidades bien definidos, así como de personal disponible y capacitado.

Objetivo: La mejor inversión para su negocio es minimizar y prevenir los riesgos, la peor es ignorarlos

Muchos de los desastres, que ocasiona el spyware son mediante acciones humanas, muchas de ellas involuntarias e ignoradas; impactan fuertemente a las empresas, provocando pérdida de clientes, deterioro en la imagen, reducción de participación en el mercado, desventaja competitiva y sanciones, entre otros.

El objetivo es desarrollar acciones de prevención y estrategias de recuperación, que permitan minimizar el impacto de un desastre y recuperarse de la manera más eficiente y efectiva para asegurar la continuidad de las operaciones.

Beneficios.

Garantizar la continuidad de la operación durante una contingencia mayor.

Reducir el nivel de riesgo mediante el uso de una metodología probada.

Generar y fortalecer la concienciación en materia de prevención de riesgos.

Minimizar costos y pérdidas en caso de desastres.

Prevenir pérdida y daños.

Niveles de Seguridad

Alto	Cuando todos los puntos anteriores funcionen correctamente
Medio	Cuando al menos algún punto falte
Bajo	Cuando dos o más puntos fallen

3.4 Escenarios

Cuando se quiere plantear diversas estrategias para alcanzar futuros resultados exitosos para una organización, un proyecto e inclusive, una situación de índole mundial o nacional; se puede hacer uso de los Escenarios.

En este caso, se planteará distintos futuros para alcanzar el ideal, que consiste en erradicar el Spyware, para un aumento en la seguridad de computadoras personales. Ahora no solo dentro de la empresa si no en un ambiente mucho mayor, como lo es Internet. Ya que se sabe que el problema es de índole no solo nacional sino Internacional.

Y como se sabe que Internet es un mundo, se limitará solo a una parte de éste, se considerará solamente a México como el universo a estudiar dentro de los escenarios.

Los Escenarios son instrumentos para ordenar las percepciones acerca de entornos alternos en los cuales las decisiones pueden ser llevadas a cabo. Es lo que se pueda trabajar para interpretar una realidad.[34]

En los escenarios es importante tener en cuenta los tres tiempos, tanto pasado presente y futuro, por ello la importancia de haber usado una planeación interactiva así como estratégica.

[34] http://www.imss.gob.mx

3.4.1 PLANEACIÓN DE ESCENARIOS

Es un enfoque eficiente para la planeación eficaz empresarial estratégica. Es enfocarse en las ideas empresariales en un mundo incierto.

Y más aún en relación al Spyware que por su propia naturaleza es incierto y al momento de proyectarse a un futuro con relación a lo que puede pasar y puede ir cambiando aumenta el grado de incertidumbre, pero da una visión más amplia de sus posibles consecuencias como parte de una causa-efecto.

Es mejorar la capacidad para prevenir y disminuir el contagio de software espía y su adaptación para producir la respuesta más rápida y precisa posible ante los cambios en el ambiente.

Son un conjunto de futuros razonablemente plausibles, pero diferentes desde el punto de vista estructural.

Esta planeación de escenarios depende de un pensamiento causal cualitativo y no de la probabilidad.

La incertidumbre, convierte a la planeación de escenarios, a una actividad episódica, que ocurre una sola vez, en una propuesta de aprendizaje continuo.

La planeación debe basarse en la suposición de que algo es predecible, supone distintos futuros[35].

[35]Van Der Heijden. Kees, "Desarrollo de escenarios: El arte de prevenir el futuro"; Ed.Panorama México 2006

La importancia de la planeación de escenarios es predecir la incertidumbre para mitigar los riegos.

3.4.2 Selección de variables principales y secundarias

Los escenarios se clasifican en variables principales y variables secundarias.

A) Variables principales. Aquellas que se consideran de carácter dependiente (de las variables secundarias), y son las importantes debido a que prevalecerán durante toda la línea del tiempo de los escenarios, y la información que arrojará permitirá medir la sobrevivencia de la organización.

B) Variables secundarias. Son independientes, no sólo de las variables principales, sino de aspectos internos y externos que influyen en el comportamiento del sistema donde se ubica la problemática.

Clasificando el problema del software espía en estas variables se tiene:

Dos variables principales que son: la seguridad informática y la cultura informática. Y cada una depende de variables secundarias de las cuales depende en el comportamiento así como en el medio ambiente.

Seguridad informática

- ✓ Antivirus y software de seguridad.
- ✓ Hacker, cracker y demás delincuentes informáticos.
- ✓ Actualización de software (sistema operativo, programas).
- ✓ Tecnología social.
- ✓ Factor Humano.
- ✓ Respaldo de información
- ✓ Internet

Cultura Informática

- ✓ Factor humano.
- ✓ Usuarios de computadoras
- ✓ Moda informática
- ✓ Vicios en Internet
- ✓ Valores
- ✓ Educación
- ✓ Aprendizaje

3.4.3 Seguridad Informática

La seguridad informática es una práctica orientada hacia la eliminación de las vulnerabilidades para evitar o reducir la posibilidad que las potenciales amenazas se concreten en el ambiente que se quiere proteger. El principal objetivo es garantizar el éxito de la comunicación segura, con información disponible, íntegra y confidencial, a través de medidas de seguridad que puedan tornar factible el negocio de un individuo o empresa con el menor riesgo posible.

Las medidas de seguridad son acciones orientadas hacia la eliminación de vulnerabilidades, teniendo en mira evitar que una amenaza se vuelva realidad. Estas medidas son el paso inicial para el aumento de la seguridad de la información en un ambiente de tecnología de la información y deberán considerar el todo.

La identificación de las amenazas permitirá la visualización de los puntos débiles que se podrán explotar, exponiendo los activos a riesgos de seguridad.

Esta exposición lleva a la pérdida de uno o más principios básicos de la seguridad de la información, causando impactos en el negocio de la empresa, aumentando aún más los riesgos a que están expuestas las informaciones. Para que el

impacto de estas amenazas al negocio se pueda reducir, se toman medidas de seguridad para impedir la ocurrencia de puntos débiles.

Por lo tanto, la seguridad es…una actividad cuyo propósito es proteger a los activos contra accesos no autorizados, evitar alteraciones indebidas que pongan en peligro su integridad garantizar la disponibilidad de la información y es instrumentada por medio de políticas y procedimientos de seguridad que permiten: la identificación y control de amenazas y puntos débiles, teniendo en mira la preservación de la confidencialidad, integridad y disponibilidad de la información.

3.4.4 Cultura Informática

Generar conciencia

El hecho de generar conciencia es a través del aprendizaje y la comprensión de diferenciar entre lo que se considera bueno y lo que se considera malo, que si bien son términos muy relativos se basan en el bienestar tanto individual como colectivo, éstos dos elementos tanto el aprendizaje como la comprensión deben de ser a través del conocimiento, más en si al proceso de cómo llegar al él que al conocimiento mismo.

Es como aquella frase célebre que dice “Lo importante no es llegar a la montaña si no mantenerse en ella”, la cual se adecuaría de esta manera, “Lo importante no es llegar a la montaña si no saber como se llegó a ella”, ya que si en algún determinado momento ya no se estuviera en lo más alto de la montaña y por alguna razón, causa o circunstancia se descendiera, sería más fácil llegar nuevamente a la cima porque se conoce la forma de alcanzarla.

El aprendizaje

El aprendizaje tiene un valor tanto intrínseco (buscar aprender algo debido tan solo a la satisfacción que produce hacerlo) como extrínseco[36] (el progreso hacia los objetivos definidos).[37]

En el caso específico de esta investigación el aprendizaje se tiene que dar de una forma extrínseca, es decir de prevenir y disminuir el contagio de Spyware como un objetivo bien definido, y de manera intrínseca para que el usuario de la computadora aprenda tan solo por la pura satisfacción que le produce el evitar los riegos del Spyware haciendo que no sea una carga para el él por el simple hecho de darle éste valor.

La calidad

La calidad es el afán por conseguir la excelencia en la forma de ser y de relacionarse con las demás personas, es comprender su significado al igual que mostrar interés por una mejora constante.

Es por eso que si se tiene calidad, se evitará el contagio del Spyware aumentando el afán de superación como una mejora consecuente

Responsabilidad

Una persona responsable es aquella que toma las cosas con seriedad y cumple sus deberes que corresponde con lo que se ha comprometido en tiempo y forma establecidos. Así por ejemplo si el usuario es responsable de tener una disciplina de no caer en sus vicios dentro de Internet evitará por lo tanto el contagio del Spyware, ya que cuando se es responsable se plantean diversas alternativas ante un problema valorando sus consecuencias.

[36] Op. Cit i.
[34] Op. Cit i.

Así no solo evitará solo su trabajo sino el de los demás. Una persona responsable genera seguridad ante los demás siendo parte fundamental de las relaciones humanas.

Disciplina

Es realizar las cosas como se piden, en tiempo y forma de una manera correcta y eficaz, sin disciplina no se realizan las tareas encomendadas, es no desistir en un plan de acción.

Respeto

Es comprometerse a generar una actitud y conducta correcta ante las normas de convivencia El respeto es fruto del diálogo, sin respeto predominaría la ley del más fuerte. Por falta de respeto es que predominan los criminales informáticos autores del Spyware así como la piratería.

Compromiso

El compromiso es una obligación obtenida por medio de un acuerdo, promesa o contrato, es tener empeño y fuerza de valor para alcanzar los objetivos que se desean y proponen superando los contratiempos que pudiesen ponerse como obstáculos.

Cuando falta o falla el compromiso en un usuario de la computadora, el Spyware será más fácil de penetrar dentro de la misma por no quererse plantear ninguna obligación para su seguridad.

Comunicación

Proceso de trasmitir un mensaje estableciendo una relación y una interacción social. Es explicar a alguien más sus opiniones, pensamientos así como sus sentimientos

Unión, Colaboración

Es la relación conjunta de una acción, tarea o trabajo común entre varias personas que persiguen un mismo objetivo para alcanzarlo. Es decir mientras no haya unión para erradicar el Spyware, y solo sea uno el que quiera realizar ese trabajo será imposible alcanzar ese objetivo, dado que se necesita de colaboración de todas las personas implicadas.

Justicia

La justicia es una relación entre la verdad y las leyes.

.Es por ello que se considera que el generar conciencia en el usuario necesita ser adquirido como una parte esencial dentro de una “CULTURA INFORMÁTICA”

Esta cultura informática que se basa en la interrelación de los valores para un bien común.

3.4.5 Proyección de escenarios a futuro

Es la actualidad se adentra a una era que se caracteriza por las extraordinarias oportunidades e interacciones en línea. Tanto en un contexto social o político, como comercial o cultural, cada vez más personas usan Internet para intercambiar información, ideas y bienes. Es decir, se esta compartiendo la vida propia con más personas mediante la Web.

Es aquí donde el Spyware adquiere mayor interés, dado que cada vez la información es más personal como confidencial, lo cual resulta más interesante para espiar y sacar provecho de la información que se puede adquirir.

Es por eso que, junto con las crecientes interacciones y oportunidades se debe ser precavido en nuevos desafíos de seguridad, para crear estrategias, que lo protejan mientras interactúa en la Web. Una de esas estrategias es tener “cultura informática”, es decir tener y generar una serie de valores a nivel personal como medida de la seguridad de la información.

Estos valores son para actuar de manera firme y confiar en el trabajo mismo y en la capacidad de la condición humana a su entorno.

Los valores de esta cultura informática son necesarios para una mayor seguridad, ya que no hay seguridad si hay: Injusticia, Falta de comunicación e Irresponsabilidad. Y es aquí donde estos valores adquieren importancia.

Considerando la selección de 2 variables principales, se ubicarán en un plano de 2 dimensiones. Cada una se analizará de acuerdo al cuadrante donde se observe, en conjunto con las variables secundarias.

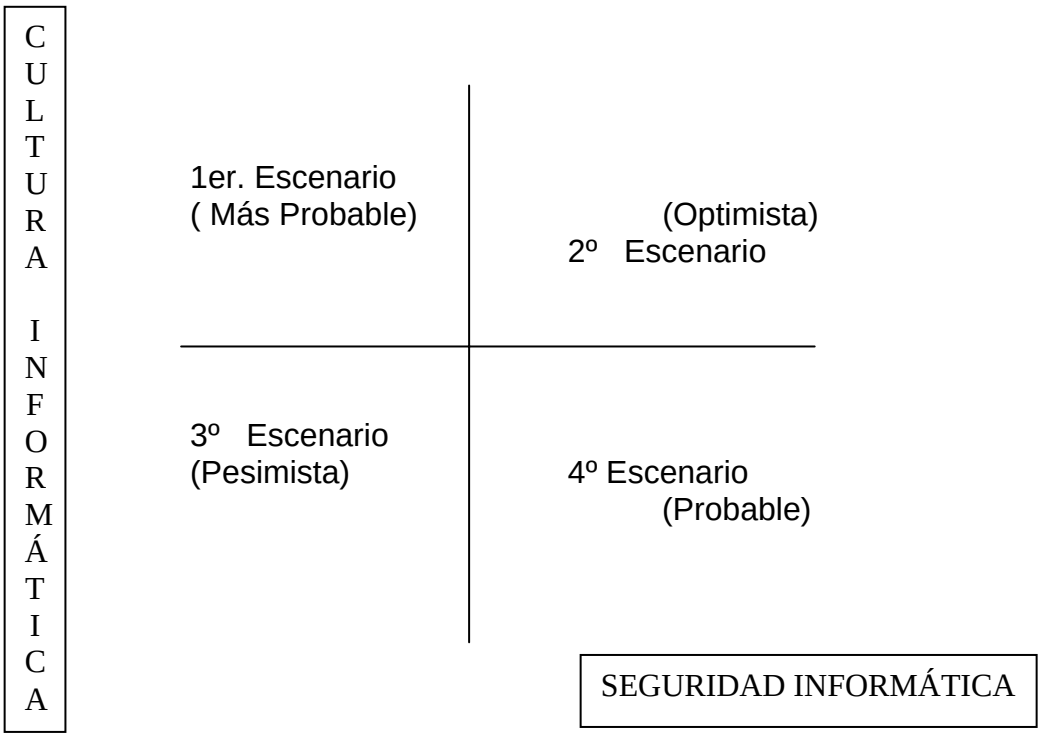


Figura 9[38]

A continuación se muestran los escenarios con un intervalo de periodo de 5 años hasta el año del 2025. Con cifras utilizadas del CONAPO[39], además de la página Web de AMIPCI[40] así como de las páginas Web de software de seguridad.[41] Siendo estos datos soporte principal para la creación de escenarios.

[38] Esta figura representa la forma de interpretar cada escenario del autor.
[39] http://www.conapo.gob.mx
[40] http://www.amipci.com.mc
[41] http://www.symantec.com, http://es.mcafee.com, http://www.pandasecurity.com

ESCENARIOS 2010 EN MÉXICO

TU INFAME ENGAÑO

Banda Ancha 5 millones, disminuye Dialup 700 mil.
108 millones de habitantes.
20 millones de computadoras.
11 millones de computadoras accesan a Internet.
6 millones son Pc's domésticas.
30 millones de internautas.
70 millones de teléfonos, comienza el Spyware.
Usa Antivirus.
Hacker: Reputación, ocio y dinero.
Software accesible.
No tienen actualizaciones por ser piratas.
El usuario respalda archivos importantes.
El usuario ocasionalmente expone sus vicios en Internet.
El usuario le interesa la información.
El usuario recopila datos acerca de ataques.
El usuario comparte información personal a conocidos.
Realiza trámites bancarios y compras en línea.
Chatea con audio y voz en tiempo real.
El usuario utiliza la computadora.
Spyware a través de Wi-Fi y memorias.
18-24 edad promedio que más usan la computadora.

VEN POR QUE TE NECESITO

Banda Ancha 5 millones disminuye Dialup 700 mil.
108 millones de habitantes.
20 millones de computadoras.
11 millones de computadoras accesan a Internet.
6 millones son Pc's domésticas.
30 millones de internautas.
70 millones de teléfonos en uso.
Usa suite de seguridad, "todo en uno".
Hacker ayudan a la seguridad informática.
Software barato y accesible.
Hay actualizaciones hasta para software pirata.
El usuario genera el hábito de respaldar información.
El usuario no expone sus vicios en Internet.
El usuario valora la información.
El usuario genera actitud.
El usuario no comparte información personal.
Sus trámites bancarios y compras en línea son seguros.
Visitar sitios seguros y comunicarse con personal calificado.
La computadora es herramienta para el usuario
Wi-Fi segura. Respaldan información.
25-34 edad promedio que más usan la computadora.

QUE NO QUEDE HUELLA

Banda ancha no crece, dialup aumenta 2 millones.
108 millones de habitantes.
19 millones de computadoras.
11 millones accesan a Internet.
5 millones Pc's domesticas.
25 millones de internautas.
65 millones de teléfonos móviles, ya hay Spyware.
Hacker ataca con mayor frecuencia por dinero.
Software caro y vulnerable.
No tienen actualizaciones por ser piratas.
El usuario no respalda información.
El usuario expone sus vicios en Internet.
Al usuario no valora información.
El usuario "le vale" lo que pasa en Internet.
El usuario ignora las amenazas informáticas.
El usuario comparte información personal a desconocidos.
Realiza compras en línea mostrando contraseñas.
Pierde información y daña hardware.
El usuario es herramienta de la computadora.
Spyware en computadoras, memorias, unidades de almacenamiento.
El usuario independientemente de la edad evita la computadora.

ORO

Banda ancha no crece, dialup aumenta 2 millones.
108 millones de habitantes.
19 millones de computadoras.
11 millones accesan a Internet.
5 millones Pc's domesticas.
25 millones de internautas.
65 millones de teléfonos, comienza el Spyware.
Hacker ataca con mayor frecuencia por dinero.
No tienen actualizaciones por ser piratas.
El usuario respalda archivos importantes.
El usuario escucha datos acerca de ataques y robos en línea.
Software caro y accesible.
El usuario "le vale" lo que pasa en Internet.
Realiza algunas compras en línea.
Moda: Chatea con audio y voz.
El usuario usa la computadora.
Spyware en WI-fi y medios de almacenamiento.
16-22 edad promedio que más usan la computadora.

ESCENARIOS 2015 EN MÉXICO

TU CARCEL

Banda Ancha: 25 millones, Wi-fi 25 millones.
113 millones de habitantes.
45 millones de computadoras.
20 millones de computadoras accesan a Internet.
15 millones son Pc's domésticas.
45 millones de internautas.
El CURP es única clave de identidad.
Teléfono móvil "todo en uno" es atacado por Spyware.
Autos nuevos con chip, rastreo satelital.
Hacker: Usurpación de identidad.
Contraseñas, cifradas. Reconocimiento de voz.
El Internet, así como la televisión están integrados en un mismo paquete.
La educación superior ya es a distancia.
Las familias compuestas están en aumento.
12-16 La edad promedio que usan la computadora.

COMO ME HACES FALTA

Banda Ancha: 50 millones Wi-fi 30 millones.
113 millones de habitantes.
50 millones de computadoras.
30 millones de computadoras accesan a Internet.
22 millones son Pc's domésticas.
55 millones de internautas.
El CURP ya es única clave de identidad.
Teléfono móvil y palm "todo en uno" es atacado por Spyware.
Autos nuevos con chip, rastreo satelital.
Hacker ayudan a la seguridad informática.
Contraseñas: cifrado y líneas de las manos.
El Internet, la radio así como la televisión están integrados en un mismo paquete.
La educación superior y media superior ya es a distancia.
Información gubernamental automatizada.
Los valores familiares son de respeto.
12-28 La edad promedio que usan la computadora.

LIBROS TONTOS

Banda Ancha aumenta 30 millones Wi-fi empieza a competirle y es insegura.
113 millones de habitantes.
50 millones de computadoras.
30 millones de computadoras accesan a Internet.
22 millones son Pc's domésticas.
55 millones de internautas.
El CURP ya es única clave de identidad.
Teléfono y palm "todo en uno" es atacado por Spyware.
Autos nuevos con chip, rastreo satelital.
Hacker usurpación de identidad y poder.
Contraseñas débiles y predecibles.
El Spyware se adueña del Internet, y demás medios de comunicación.
La educación superior y media superior va en decremento.
No hay relaciones sociales, solo virtuales.
Se carece de identidad personal.
Falta de preparación induce a robos.
Falta responsabilidad, disciplina y justicia.
12-16 La edad promedio que usan la computadora.

PASTILLAS DE AMNESIA

Banda ancha 30 millones, Wi-Fi es interceptado y espiado por software
113 millones de habitantes.
50 millones de computadoras.
30 millones de computadoras accesan a Internet.
22 millones son Pc's domésticas.
55 millones de internautas.
El Spyware se adapta a tecnología y se adueña del Internet, y demás medios de comunicación.
Los ataques son masivos y en cuestión de microsegundos se pierde tanto información como equipo
Faltan valores culturales.
No hay relaciones sociales, solo virtuales
Se carece de identidad personal.

ESCENARIOS 2020 EN MÉXICO

PERO TE VAS A ARREPENTIR

Todos tienen la posibilidad de Banda y Wi-fi.
120 millones de habitantes.
105 millones de computadoras.
100 millones de computadoras accesan a Internet
70 millones son Pc's domésticas.
90 millones de internautas.
Aparatos nuevos con chip, rastreo satelital.
Contraseñas cifradas, las manos, pupilas de ojos.
Criminales informáticos usan tecnologías de simulación para descifrar contraseñas corporales, ataques a satélites.
Las relaciones sociales comienzan a desaparecer.
Se empieza a perder sentimiento en el ser humano.
La razón ya no es humana, ahora depende de lo que sugiera una máquina.

NUNCA VOY A OLVIDARTE

Todos tienen Banda ancha y Wi-fi comienza la transmisión satelital a casas.
120 millones de habitantes.
110 millones de computadoras.
105 millones de computadoras accesan a Internet.
75 millones son Pc's domésticas.
100 millones de internautas.
Aparatos con chip, rastreo satelital.
No hay criminales informáticos.
Casas Inteligentes.
Información nacional automatizada.
Contraseñas cifradas, las manos, pupilas de ojos.
El Internet, la radio así como la televisión están integradas en un mismo paquete vía satelital.
Toda la educación ya es a distancia.
Los valores familiares son de respeto, unidad y de concientización.
Todos usan la computadora.

CREO QUE VOY A LLORAR

Se resisten al uso del Internet un sector de México.
140 millones de habitantes.
105 millones de computadoras.
100 millones de computadoras accesan a Internet.
70 millones son Pc's domésticas.
80 millones de internautas.
Aparatos nuevos con chip, rastreo satelital, beneficia a las criminales informáticos.
Contraseñas cifradas, las manos, pupilas de ojos.
Guerra entre criminales informáticos, usan tecnologías de simulación para descifrar contraseñas corporales, ataques a satélites.
La tecnología móvil esta siempre espiada independientemente del medio de conexión.

CASTIGADOS

Se resisten al uso del Internet un sector de México.
140 millones de habitantes.
105 millones de computadoras.
100 millones de computadoras accesan a Internet.
70 millones son Pc's domésticas.
80 millones de internautas.
Criminales informáticos usan tecnologías de simulación para descifrar contraseñas corporales, ataques a satélites.
Las relaciones sociales comienzan a desaparecer.
Se empieza a perder sentimiento en el ser humano.
La razón ya no es humana, ahora depende de lo que sugiera una máquina.
Comienzan a surgir movimientos sociales en busca de lo humano.

ESCENARIOS 2025 EN MÉXICO

CORAZÓN DURO

Toda la información esta automatizada los impuestos información personal ya están incluidos en una base nacional para obtener la información desde cualquier punto en donde se encuentre.
Todos quieren ser piratas informáticos, da estatus social ya que son ellos los que obtienen prestigio, dinero y poder.
El usuario no sabe manejar la tecnología que tiene y le falta preparación escolar.

Aumenta el control de aparatos con localización satelital, para encontrar más fácilmente a alguien a quien robar.
El software espía cambia de manera tal que se instala en servidores que controlan y almacenan toda la información.
El trato máquina-hombre predomina.

LA PAREJA IDEAL

Toda la información esta automatizada los impuestos, información personal ya están incluidos en una base nacional para obtener la información desde cualquier punto en donde se encuentre.

No hay criminales informáticos, ayudan a desarrollar técnicas de seguridad. Son respetados nuevamente por la sociedad, por el bien que hacen a la sociedad.

El usuario maneja toda la tecnología que tiene y le saca el mayor provecho posible. Todos tienen educación universitaria.

Aumenta el control de aparatos con localización satelital, para encontrar más fácilmente mercancía robada.

LLORAR, LLORAR

Los criminales cibernéticos controlan el país.
Es un lujo la educación.
El gobierno se colude con la mafia y extorsión.
Se necesita pagarles a ellos para que no toquen ni compartan la información de la cual se hicieron dueños.
El fraude, chantaje, deslealtad son los valores con los que se viven en estos tiempos.
Los robots desplazan a los humanos en el sector laboral.
Se pierde la identidad personal.
Las relaciones humanas no existen.
Ya no se expresan los sentimientos humanos, se ha perdido toda sensación grata hacia los demás.
La realidad virtual es lo que predomina.
El trato máquina-máquina predomina.
El ser humano ya no razona, actúa solo con la inercia que lo lleva la tecnología.
La mitad del país tiene desempleo, el empleo informal es lo que predomina vendiendo software y hardware para poder acceder de forma ilícita algún sistema.

LAGRIMAS, SAL Y LIMON

La tecnología es necesaria para estar en contacto con el mundo.
Tecnología móvil interceptada por espías.
Realidad virtual, desvirtuada.
Los criminales cibernéticos controlan el país.
El gobierno se colude con la mafia y extorsión.
Se necesita pagarles a ellos para que no toquen ni compartan la información de la cual se hicieron dueños.
El fraude, chantaje, deslealtad son los valores con los que se viven en estos tiempos.
Los robots desplazan a los humanos en el sector laboral.
Se pierde la identidad personal.
Las relaciones humanas no existen.
Ya no se expresan los sentimientos humanos, se ha perdido toda sensación grata hacia los demás.

En el caso de los escenarios respecto al 2010, es el primer cuadrante titulado TU INFAME ENGAÑO lo más probable que ocurra, ya que como su nombre lo indica aún se van a padecer problemas de software espía con base en engaños de todo tipo, desde correos anunciando el mundial de fútbol, páginas Web instalando control activex sin que el usuario se de cuenta y hasta con su consentimiento, páginas Web simulando ser las páginas oficiales de marcas conocidas y confiables, y que varían solo por alguna letra, símbolo o logotipo, etc. Además de incrementar los fraudes en línea y el acceso de una charla en línea.

El otro escenario probable es el escenario titula ORO ya que es el dinero parte fundamental para que el software espía siga en curso así como en crecimiento. Ya que es el adware una manera fácil para entrar en la mercadotecnia, y el valor que se puede adquirir al tener información importante y trascendental de alguien. Se Empezará a cambiar contraseñas y ahora se tendrá que pagar dinero a los criminales cibernéticos por liberar cuentas y así poder acceder a la información personal requerida. Se dan cuenta los criminales informáticos de lo rentable que es venderle información su propia información al usuario.

Conclusiones

El futuro del software espía aún tiene mucho camino por recorrer, a pesar de que las compañías de software de seguridad cada vez le pongan más empeño en contrarrestarlo ya que usa tecnología social innovadora, teniendo como principal aliado al usuario de la computadora.

Ya que es el usuario el que abre las puertas para que entre el Spyware por medio de vicios y curiosidades personales y algunas veces por la falta de información respecto a éste tema. Además recuerde que hasta el software gratis a la larga siempre tiene algún costo.

Es por eso que hay que poner énfasis en adquirir la cultura informática y hacer de ella un hábito, trayendo como consecuencia minimizar los riesgos de adquirir el software espía y una manera de prevenirlo.

Los escenarios sirven de referencia para saber hacia donde se dirige el futuro del software espía, así como para generar nuevas estrategias para poder alcanzar el futuro que se desea.

Es en los escenarios donde se vislumbra que los criminales cibernéticos espiarán con mayor frecuencia no solos los hábitos de navegación que tiene el usuario, si no buscarán la manera de obtener información confidencial que se tienen el las bases de datos nacionales, como el padrón electoral de votación por mencionar alguno, sobre todo por dinero ya que se dieron cuenta la rentabilidad que tiene el Spyware.

Por tal motivo hay que tomar en cuenta la educación y el aprendizaje como parte fundamental de evolución a la cultura informática y que se tiene que valorar sobre todo en las personas más pequeñas, es decir los niños y jóvenes que serán los que usen las computadoras en mayor número.

Es así que si tiene el hábito de esta cultura informática uno será capaz de evitar adquirir el software espía en una extensión del tiempo e independientemente del desarrollo tecnológico ya que se usarán en éstos últimos los mismos patrones que se usan actualmente en la computadora.

Por último, hay que aprender del pasado, actuar de forma correcta en el presente para así tener un futuro deseado.

CONCLUSIONES

Conclusiones

Ésta investigación sirvió para comprobar que cuando una persona quiere tener el control absoluto sin el conocimiento debido, puede ocasionar un problema mayor.

Por tal motivo se crearon políticas y normas así como responsabilidades y obligaciones dentro del despacho contable, las cuales sirvieron para ser eficaces en la reducción del contagio de Spyware, teniendo como consecuencia una estructura adecuada en el organigrama para un mejor control.

Se notó que mientras más organizada este la empresa se tiene un mayor control en su propia estructura. Y sirvió para aprender que mientras se comparta el trabajo en forma conjunta tendrá mejores resultados para el beneficio de la misma, solucionando la vulnerabilidad que se tiene en la organización.

También se hizo notar a la seguridad como una variable relevante ya que soluciona el problema de las vulnerabilidades las cuales son aprovechadas por el Spyware para poder acceder a las computadoras y se recopile información que sea de su interés.

Sirvió también para que recapacite el usuario y no crea todo lo que está en Internet sin antes informarse adecuadamente, que el software gratuito a mediano o largo plazo tiene un costo, y que nadie regala algo sin obtener algo a cambio.

Aunque en un principio la idea era hacer la investigación en usuarios domésticos, la cual no se pudo realizar por no tener información que se tuviera al alcance, en cambio si en el despacho contable, se tomó éste último para mostrar la realidad que se está viviendo en la actualidad en cuanto se refiere al contagio y los riesgos que

produce el Spyware, y siguiendo el mismo objetivo de analizar sus principales causas para prevenirlas y detectarlas a tiempo.

Éste objetivo que de alguna manera se cumplió, por lo menos en la primera etapa de un plan denominado PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN, denominado así ya que involucra a todas las áreas del despacho contable por medio de cuatro programas descritos en el capítulo 2, confiando que las demás metas y objetivos de los programas faltantes se alcancen en un punto específico del tiempo o independientemente de éste.

El PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN fue creado gracias a la Planeación, la cual es un proceso dirigido a uno o más estados futuros deseados y cuya obtención no es probable a menos que se haga algo al respecto, sugiere una serie de pasos para la obtención de un objetivo, estos pasos son:

- ✓ Planteamiento del problema
- ✓ Objetivo u objetivos
- ✓ Diagnóstico del problema
- ✓ Pronóstico
- ✓ Identificación de variables controlables y no controlables.
- ✓ Creación de un Ideal
- ✓ Metas y fines
- ✓ Generar una serie de disposiciones, es decir acciones con buenos deseos
- ✓ Creación de estrategias para solución hacia el objetivo
- ✓ Viabilidad y factibilidad
- ✓ Seleccionar la planeación adecuada de acuerdo a su orientación, amplitud, por su frecuencia y por su marco temporal.
- ✓ Identificar fortalezas y oportunidades
- ✓ Realizar un plan

- ✓ Implementar el plan
- ✓ Evaluar el plan

La planeación estratégica es la indicada en casos como el Spyware, ya que al momento de extenderse en el tiempo existe la incertidumbre por el medio ambiente que lo rodea, y la planeación estratégica es flexible, es decir se puede adecuar como sea necesario y útil dado que es de largo plazo.

A pesar de que se utilizó la planeación estratégica como método fundamental, también se requirió de alguna manera de los otros tipos de planeación en cuanto amplitud se refiere, es decir que en algún momento cualquier tipo de planeación puede complementarse con otras.

Esta planeación estratégica se conformó tanto de un diseño como de una administración estratégica para la consecución del objetivo. Logrando así resultados favorables como los que se habían previsto, con una disminución de más del 70% de máquinas infectadas de Spyware.

Teniendo luego entonces que el PLAN COORDINADO DE SEGURIDAD DE LA INFORMACIÓN llegó a ser eficaz durante la primera etapa del plan y la mitad del primer programa, esperando que con los programas restantes del Plan siga con esa tendencia, la cual de ser así se disminuirá en un estimado de hasta un 95%, lo cual indica una mayor seguridad en la información.

De tal manera que si los usuarios, así como las empresas generen y apliquen un plan acorde al problema, se beneficiarán no solo a ellos si no a muchas más personas y empresas ya que no retroalimentaran el software espía. Teniendo como consecuencia una reducción mundial del contagio de Spyware.

El pronóstico del crear y generar conciencia a los usuarios para disminuir el Spyware y para su prevención se cumplió.

Los escenarios fueron útiles para generar una visión de lo que puede suceder en un futuro que por un momento parece lejano pero que está más cerca de lo que se pueda imaginar.

Dentro de estos escenarios compuestos por dos variables que son: tanto la cultura informática así como la seguridad informática se puede vislumbrar los posibles resultados.

La investigación aquí tratada quiere hacer énfasis en que la cultura informática es importante para evitar y prevenir no solo el daño del Spyware en computadoras personales, sino en distintos aparatos móviles que se usarán en los años que están por venir, usando los mismos patrones y la misma tecnología social que usa el Spyware tema del presente estudio, además de cualquier otra amenaza nueva que se origine es ese mismo transcurso del tiempo.

El mejor método para no contagiarse del Spyware es la prevención, es decir estar preparados para lo que pueda suceder en un futuro no muy lejano, y para lo cual se necesita tener creatividad e ingenio para detectar posibles técnicas de ataque. Que no se tenga que esperar a que se contagie la computadora para saber las nuevas formas de contagio.

Es por tal motivo que se tiene que trasmitir el conocimiento adquirido acerca de cómo prevenir el Spyware, ya que mucha gente desconoce o esta mal informada sobre este padecimiento mundial, y si bien los diferentes programas de software de seguridad son un mecanismo de defensa es necesario que se complemente con lo que en este trabajo se denomina cultura informática.

Por último, mientras no se genere la cultura informática que se necesita, se tendrán problemas del Spyware similares o peores aún y con mayores costos de reparación así como desastres que generen un caos informático no sólo en México si no a nivel mundial.

GLOSARIO

GLOSARIO

Acceso remoto
Acción de usar una máquina a la que no tenemos acceso físico mediante una utilidad o programa para este fin. El motivo más común para realizar esta acción es administrar los recursos de un sistema remoto. Esta mecánica no es adecuada, y por lo tanto no debe ser confundida con, compartir archivos o transferirlos entre sistemas.

ActiveX
Tecnología diseñada por Microsoft para el intercambio de información entre dos aplicaciones diferentes. Surgió de la combinación de dos tecnologías previas, OLE (Object Linking and Embedding - Inserción y vinculación de objetos) y COM (Common Object Model - Simulación de objetos comunes).

ActiveX Controls (Controles ActiveX)
Es un conjunto de reglas que indican como dos determinadas aplicaciones deben intercambiar información, en este caso, una de las aplicaciones, es un navegador, el cual descarga y ejecuta el ActiveX.

Los controles ActiveX pueden ser escritos en multitud de lenguajes, entre los que encontramos C, C++, C#, Visual Basic, Java, etc.

Adjunto
Archivo o fichero vinculado a un correo electrónico. Puede ser un texto, un gráfico, un sonido o un programa.

Administrador
Persona que se encarga de la gestión de equipos y redes en una determinada organización.
Usuario principal de Windows en los sistemas basados en el núcleo NT, entre los que encontramos Windows 2000, Windows XP y Windows 2003. Este usuario tiene, por defecto, los más altos privilegios a los que una persona puede acceder en condiciones normales.

Adware
Programa que es licenciado al usuario a condición de que acepte la publicidad que viene incorporada en vez de pagar por el.
Tipo de spyware que recolecta información del usuario sin notificación previa a fin de mostrar publicidad específicamente relacionada con determinadas actividades. Esta publicidad suele mostrarse al usuario mediante el uso de un navegador.
La segunda acepción es la distorsión que diversas empresas hicieron de un sistema legítimo de distribución de software de forma gratuita.

Agujero de Seguridad
Un agujero de seguridad, o una vulnerabilidad, es un error en una aplicación o sistema operativo por el cual se compromete de alguna manera la seguridad del equipo donde se está ejecutando dicho programa vulnerable.
Si un usuario malicioso se aprovecha de un agujero de seguridad, puede causar graves daños en un equipo, dependiendo el alcance de la vulnerabilidad.

Ancho de banda
Forma figurativa de referirse a la cantidad de información que pueden moverse por los canales de datos en tecnologías de transmisión superiores al RDSI (Red Digital de Servicios Integrados). Actualmente, este término se aplica comunmente a las variantes de ADSL (Asymmetric Digital Suscriber Line - Linea asimétrica digital del suscriptor).
La unidad de medida habitual de ancho de banda es el Kbps (Kilo bits per second - Kilo bits por segundo). 1 Kbps equivale a 1.000 bits por segundo. No debe confundirse con KBps (KiloBytes per second - Kylobytes por segundo), que equivale a 1024 bytes por segundo.

Anti-debug/Anti-debugger
Ver Antirastreo

Antirastreo
(En inglés Anti-debug/Anti-debugger) Se trata del conjunto de técnicas que los diseñadores de virus emplean para evitar ser investigados.

Antispyware
Es un programa desarrollado para el ámbito de la seguridad informática, el cual protege a los usuarios de programas maliciosos, tales como (Spywares, Adwares, Hijackers, entre otros Malwares), que voluntaria o involuntariamente se instalan en la computadora, detectándolos y eliminándolos de la misma.

Antivirus
Los antivirus son programas cuya función es detectar y eliminar virus informáticos y 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 computadores.
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).

Archivo Hosts
Es un archivo de texto que se utiliza para resolver nombres de dominio en direcciones IP de forma local, es decir, una libreta de direcciones. Fue concebido en tiempos en que sólo había unos pocos dominios que se enviaban en una lista (archivo hosts) todos ellos con sus respectivas Ips y para resolver nombres de dominio en redes locales (LAN).

Auditoría
Proceso sistemático, independiente y documentado para evaluar de manera objetiva las prestaciones de un sistema con el fin de determinar e que se cumplen los requisitos previamente especificados por la norma, política o regla contra la que se audita.

Autenticación
A) Procedimiento de comprobación de la identidad de un usuario.
B) Servicio de seguridad que se puede referir al origen de los datos o a una entidad homóloga.

Backdoor
Puerta trasera. Permite a un usuario aislado ingresar sin autorización a otros sistemas por medio de la instalación de un sistema de acceso considerado virus, permite revisar datos, borrar archivos, infectar con otro tipo de virus, todo esto sin que el usuario este enterado de lo que sucede en su ordenador.

Backup
Es una copia de los datos que se encuentran en nuestro disco duro, y que se preservan en otro medio de almacenamiento (discos duros / CD's / DVD's / cintas magnéticas, etc) con el fin de conservarlos y/o protegerlos en caso de posible daño y/o destrucción de la fuente original.

Base de Datos
Grupo de datos estructurado para facilitar su consulta y posterior tratamiento.

Bho
(Browser Helper Objects) El usuario descarga un software malicioso en apariencia inofensivo que se instala (el usuario acepta un largo contrato a través del cual permite al atacante efectuar cualquier acción en su ordenador sin opción a reclamar) en su propio sistema.
Una vez ha instalado la aplicación, el programa puede detectar, analizar y enviar de vuelta al fabricante (atacante) toda la información que se procese en nuestro explorador.

Bios
(Basic Input / Output System) Identifica al software o conjunto de programas que arrancan el ordenador (antes de encontrarse un disco de sistema) cuando se pulsa el botón de encendido. La BIOS, este programa, se encuentra siempre en la memoria principal, pero no en la RAM (Random Access Memory) pues al apagar el ordenador se borraría, sino en la ROM (Read Only Memory - Memoria de Sólo Lectura), cuyo almacenamiento es permanente.

Bit
Binary digit) Es la unidad más pequeña de la información digital con la que trabajan los sistemas informáticos, puede tener dos estados "0" o "1". La unión de 8 bits da lugar a un byte.

Blindaje
(En inglés Armouring) Técnica de autoprotección utilizada por algunos virus para impedir que los programas de depuración puedan abrir los ficheros infectados y analizar su contenido.

Bomba de Tiempo
(En inglés Time Bomb) Programa malicioso que se activa en una determinada fecha. Esta técnica la utilizan muchos virus como mecanismo de activación.

Bomba Lógica
(En inglés Logic Bomb) Programa malicioso que se ejecuta cuando existen condiciones especificas para su activación. Esta técnica la utilizan muchos virus como mecanismo de activación.

Bot
Tipo de troyano con el que el atacante se hace con el control de nuestro ordenador, habitualmente para atacar a otros ordenadores (lanzar ataques de denegación de servicios en forma distribuida, enviar correo electrónico no solicitado, etc.)
Los bots son propagados a través de Internet empleando un gusano como transporte, envíos masivos de ellos a través de correo electrónico o aprovechando vulnerabilidades en navegadores.

Bps
Es una abreviación de bits per second, bits por segundo, una medida de la velocidad a la cual son transmitidos los datos. Bps se utiliza normalmente para describir la velocidad de los modems o la velocidad de una conexión digital.

Búfer
Área de la memoria que se utiliza para almacenar datos temporalmente durante una sesión de trabajo.

Bug
Un error de software (computer bug en inglés), es el resultado de una falla de programación introducida en el proceso de creación de programas de ordenador o computadora (software).

Byte
Es una unidad que mide la cantidad de información, tamaño y capacidad de almacenamiento. Un Byte, equivale a 8 Bits.

Caché
Es un tipo de memoria R.A.M. perteneciente a la familia de las memorias Volátiles (se borra la información si se apaga el computador), que guarda una copia de la información que es usada con mayor frecuencia por el C.P.U. o microprocesador.

Certificado digital
Documento digital mediante un sistema seguro de claves administrado por una tercera parte de confianza, la autoridad de certificación, que permite a las partes tener confianza en las transacciones en Internet, garantizando la identidad de su poseedor en Internet.Permite realizar un conjunto de acciones de forma segura y con validez legal: firmar documentos, entrar en lugares restringidos, identificarse frente la administración, etc.

Chat
Se trata de conversaciones escritas en Internet. Mediante una conexión a la red y un programa especial, es posible conversar (mediante texto escrito) con un conjunto ilimitado de personas, al mismo tiempo

Códec
Son programas que permite comprimir y descomprimir vídeo y audio digital.
Su finalidad es obtener un almacenamiento substancialmente menor de la información de audio/video. Esta se comprime en el momento de guardar la información hacia un archivo y se descomprime, en tiempo real, en el momento de la visualización. Se pretende, por otro lado, que éste sea un proceso transparente para el usuario, es decir, que éste no intervenga o lo haga lo menos posible.

Código
Contenido de los ficheros de un virus -código del virus, escrito en un determinado lenguaje de programación-. También hace referencia a los sistemas de representación de información. En sentido estricto, puede definirse como conjunto de normas sistemáticas que regulan unitariamente una materia determinada, o combinación de signos que tiene un determinado valor dentro de un sistema establecido.

Código malicioso
(En inglés Malware) Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos son algunos ejemplos de código malintencionado.
Ver - Malwares

Contraseña
Una contraseña (password en inglés) o clave, es una forma de autenticación que utiliza una información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. Aquellos que desean acceder a la información se les solicita una clave, si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

Controlador
Es un programa informático que permite al sistema operativo interactuar con un periférico, haciendo una abstracción del hardware y proporcionando una interfaz (posiblemente estandarizada) para usarlo.
Es como un manual de instrucciones que le indica cómo debe controlar y comunicarse con un dispositivo en particular. Por tanto, es una pieza esencial, sin la cual no se podría usar el hardware.

Cookies
Son pequeños archivos que generan los sitios de Internet para facilitarle al usuario la utilización de algunas páginas. Existen componentes Adware y Spyware que revisan o archivan cookies para recopilar información que un usuario nunca desearía revelar o para facilitar el ingreso donde nunca buscaría ingresar.

Cortafuegos
Se trata de un mecanismo de protección, el cual puede ser construido mediante software, hardware o ambos. Su función es proteger un equipo o conjunto de ellos mediante el análisis de paquetes de datos entrantes y salientes.
Existen Cortafuegos que trabajan directamente a nivel de puertos de comunicaciones, permitiéndole al usuario autorizar o no la utilización de éstos por parte de aplicaciones o servicios. Otros, utilizan reglas para determinar que información debe transitar desde y hacia el equipo en cuestión.

Cracker
Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.
El término deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al termino hacker, en defensa de estos últimos por el uso incorrecto del término.
Se considera que la actividad de esta clase de cracker es dañina e ilegal.
También se denomina cracker a quien diseña o programa cracks informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo.

Craquear
Es el hecho de copiar y/o utilizar software comercial ilegalmente rompiendo las distintas técnicas de protección o registro que utilicen.

Criptografía
a) Diseño de procedimientos para cifrar los mensajes, de forma que si son interceptados no se pueda saber su contenido.
b) Disciplina que estudia los principios, métodos y medios de transformar los datos con objeto de ocultar la información contenida en los mismos, detectar su modificación no autorizada y prevenir su uso no permitido.

Cuarentena
Una función de protección de nuestro ordenador que nos permite dejar sin efecto a archivos que puedan estar infectados, hasta que nuestros sistemas de seguridad tengan una nueva actualización para poder desinfectarlos.

Defensa proactiva
Nueva tecnología implementada en Antivirus como Kaspersky.
La defensa proactiva se basa en comportamiento, una vez que ni las firmas, ni la capacidad heurística han detectado nada.

Dialer
Se trata de un programa que marca un número de tarificación adicional (NTA) usando el módem, estos NTA son números cuyo coste es superior al de una llamada nacional. Estos marcadores se suelen descargar tanto con autorización del usuario (utilizando pop-ups poco

claros) como automáticamente. Además pueden ser programas ejecutables o ActiveX (Estos programas sólo funcionan en Internet Explorer).

Dirección IP
El Protocolo de Internet (IP, de sus siglas en inglés Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados. Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

DLL (archivo)
Ejecutan acciones o rutinas de uso frecuente en Windows, y un mismo archivo DLL puede ser usado por varios programas al mismo tiempo (como el Kernel32.dll). Por ejemplo el procesador de palabras, la hoja de cálculo y otros programas pueden usar un mismo archivo DLL para desplegar el cuadro diálogo Abrir, cada vez que usted usa el comando Abrir.
Un DLL se carga en la memoria RAM y se ejecuta únicamente cuando un programa lo llama para que realice una función, mientras que otros módulos de rutinas que sí hacen parte del programa permanecen cargados en la memoria mientras trabaja con un programa.

Dns
Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet.
El Domain Name System (DNS), o Sistema de Nombres de Dominio, comprende personas, instituciones reguladoras, archivos, máquinas y software trabajando conjuntamente.

Dominio
Sistema de denominación de hosts en Internet el cual está formado por un conjunto de caracteres el cual identifica un sitio de la red accesible por un usuario. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. Comprenden una red 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. Los dominios se establecen de acuerdo al uso que se le da a la computadora y al lugar donde se encuentre. Los más comunes son .com, .edu, .net, .org y .gov; la mayoría de los países tienen su propio dominio, y en la actualidad se están ofreciendo muchos dominios nuevos debido a la saturación de los dominios .com.

Dos
Es una familia de sistemas operativos para PC. El nombre son las siglas de Disk Operating System (sistema operativo de disco).
Existen varias versiones de DOS. El más conocido de ellos es el MS-DOS, de Microsoft (de ahí las iniciales MS). Otros sistemas son el PC-DOS, DR-DOS y, más recientemente, el FreeDOS.

Dropper
Llamado cuentagotas. Es un fichero que al ejecutarse "gotea" o dispersa un virus. Un fichero "dropper" puede crear un virus e infectar el ordenador al ejecutarse. Cuando un "dropper" es escaneado por un antivirus, generalmente no se detectará un virus, porque el código viral no ha sido creado todavía. El virus se crea en el momento que se ejecuta el "dropper".

Ejecutable
Es el término genérico que se utiliza para definir a los programas o aplicaciones. Se utiliza sobre todo cuando se habla de ficheros, para diferenciarlos de aquellos que no se pueden ejecutar por sí mismos. Un ejemplo de fichero que no se puede ejecutar por sí mismo es un documento, una imagen o un fichero de sonido. Para poder abrir, visualizar o reproducir este tipo de ficheros se necesita un ejecutable. Los ejecutables tienen las extensiones "EXE" Y "COM".

Encriptar Es la acción de proteger archivos expresando su contenido en un lenguaje cifrado. Los lenguajes cifrados simples consisten, por ejemplo, en la sustitución de letras por números mediante complejos algoritmos. El proceso inverso se denomina desencriptar (decrypt). Los datos encriptados suelen llamarse "texto cifrado".

Exploit
(del inglés to exploit, explotar o aprovechar) es un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa (llamadas bugs)., uno de las herramientas mas utilizadas para realizar este tipo de ataque informático es el Metasploit que se encuentra en su ultima versión, El fin del Exploit puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.
Un "exploit" es usado normalmente para explotar una vulnerabilidad en un sistema y acceder a él, lo que es llamado como "rootear" tener privilegios de root (administrador). También es utilizado por los testers de seguridad informática para mejorar la seguridad de las compañías.

Fat
(File Allocation Table) Tabla de Asignación de Ficheros. Representa una sección del disco en la cual se almacenan las direcciones donde se encuentran los ficheros contenidos o guardados en dicho disco. Esta tabla se encuentra localizada en el Boot o sector de arranque del disco.

Fichero de proceso por lotes (.bat o batch)
Los ficheros de proceso por lotes o ficheros Batch se caracterizan por tener extensión BAT. Son ficheros de texto que contienen comandos de MS/DOS, uno por cada línea escrita. Cuando se ejecuta este tipo de ficheros, cada una de las líneas en él escritas se va ejecutando de forma secuencial. Un fichero muy importante de este tipo es el AUTOEXEC.BAT, el cual se encuentra siempre en la raíz del disco duro y se ejecuta automáticamente cuando el ordenador arranca, cargando una serie de controladores y programas.

Firewall
Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en las redes para prevenir algunos tipos de comunicaciones prohibidas por las políticas de red, las cuales se fundamentan en las necesidades del usuario. La configuración correcta de cortafuegos se basa en conocimientos considerables de los protocolos de red y de la seguridad de la computadora. Errores pequeños pueden dejar a un cortafuego sin valor como herramienta de seguridad.

Firma electrónica
Código encriptado que se usa en las redes de comunicaciones para autenticar la identidad del usuario emisor y la propiedad de un documento en circulación.

Formateo / Formatear
Borrar por completo la información existente en un dispositivo de almacenamiento. También se puede dar formato a una unidad de disco para eliminar todo su contenido o escribir un sistema de ficheros en dicha unidad de disco.

Freeware
Tipo de licencia de distribución un software que permite utilizar dicho software sin coste alguno.

Ftp
(En inglés File Transfer Protocol) Utilidad que permite extraer documentos, programas y otros datos contenidos en Internet, anónimamente y sin necesidad de códigos, contraseñas u otros sistemas de seguridad que limiten el acceso.

GSM
(Global System for Mobile communication) Sistema Global para comunicaciones Móviles. Sistema compatible de telefonía móvil digital desarrollado en Europa con la colaboración de operadores, Administraciones Publicas y empresas. Permite la transmisión de voz y datos.

Gusano
Los gusanos tienen ciertas similitudes con los virus informáticos, pero también diferencias fundamentales. Un gusano se parece a un virus en que su principal función es reproducirse, pero por el contrario de cómo lo hacen los virus, en lugar de copiarse dentro de otros archivos, un gusano crea nuevas copias de si mismo para replicarse.

Hacker
Hacker (del inglés hack, recortar), también conocidos como "white hats" (sombreros blancos) o "black hats" (sombreros negros), según una clasificación de sus acciones (según sean sólo destructivas o no, etc.). Es el neologismo utilizado para referirse a un experto (ver: Gurú) en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz, etc.
Se suele llamar hackeo y hackear a las obras propias de un hacker.

Hacking
Acción de piratear sistemas informáticos y redes de telecomunicación.

Heurística
Método de revisión de archivos y/o memoria basado en la búsqueda de patrones de actividad que puedan considerarse como un virus. Normalmente utilizados para la detección de nuevas versiones de virus ya conocidos o familias de virus.

Hijacker
(Secuestradores del Navegador) es el software encargado de cambiar la pagina de inicio de cualquier navegador, no dejando al usuario la posibilidad de cambiarlo.

Hipertexto
Documento digital que rompe la estructura lineal de un texto mediante 'enlaces', también llamados 'Vínculos' o 'Hipervínculos', que permiten saltar a otros temas relacionados, donde encontrar información ampliada. Las páginas Web de Internet son un ejemplo claro de Hipertexto.

Hoaxes
La palabra hoax viene del inglés y tiene dos interpretaciones. Por un lado, puede ser utilizado como un verbo que significa embaucar; en cambio, si se utiliza como sustantivo, se traduce como engaño, bulo o broma de mal gusto.

Html
El HTML, acrónimo inglés de HyperText Markup Language (lenguaje de marcas hipertextuales), lenguaje de marcación diseñado para estructurar textos y presentarlos en forma de hipertexto, que es el formato estándar de las páginas Web. Gracias a Internet y a los navegadores del tipo Internet Explorer, Opera, Firefox o Netscape, el HTML se ha convertido en uno de los formatos más populares que existen para la construcción de documentos y también de los más fáciles de aprender.
(Hyper Text Markup Language) Es el lenguaje de marcado usado como el estándar para especificar el formato y delimitar el contenido que permite la visualización de páginas Web, desde un navegador. Se basa en etiquetas (instrucciones que le dicen al texto como deben mostrarse) y atributos (parámetro que dan valor a la etiqueta). La versión más avanzada se conoce como XHTML (Extensible Hypertext Markup Language).

Ingeniería Social
Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ‘ingeniero social’.

Internet
Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación. Ofrece distintos servicios, como el envío y recepción de correo electrónico (e-mail), la posibilidad de ver información en las

páginas Web, de participar en foros de discusión (News), de enviar y recibir ficheros mediante FTP, de charlar en tiempo real mediante IRC.

Intranet

Red privada de una empresa de tipo Internet. Su aspecto es similar al de las páginas de Internet.

Intrusiones

Cuando un pirata informático, entra a la máquina de un usuario de forma que el usuario no se de cuenta, y ya con el control de ésa máquina, puede realizar cualquier tipo de actividades. También se pueden dar intrusiones a redes locales, por ejemplo, la de una empresa, y así obtener información sensible y confidencial.

IP (dirección)

La dirección IP está conformada por un número de 32 bits la cual identifica cada emisor y receptor de paquetes de información a través de Internet.

Cada paquete enviado dentro del protocolo TCP/IP incluye la dirección IP de origen y de destino para poder distribuir los datos de manera correcta y si fuese necesario confirmar al emisor la recepción de éstos.

Ésta consta de dos partes, una que identifica a cada red dentro de Internet y un identificador para cada dispositivo, el cual puede ser un router, un servidor o una estación de trabajo.

Java

Java es toda una tecnología orientada al desarrollo de software con el cual podemos realizar cualquier tipo de programa. Hoy en día, la tecnología Java ha cobrado mucha importancia en el ámbito de Internet gracias a su plataforma J2EE. Pero Java no se queda ahí, ya que en la industria para dispositivos móviles también hay una gran acogida para este lenguaje.

La tecnología Java está compuesta básicamente por 2 elementos: el lenguaje Java y su plataforma. Con plataforma nos referimos a la máquina virtual de Java (Java Virtual Machine).

JavaScript

Es un lenguaje de programación que aporta características dinámicas (datos variables en función del tiempo y el modo de acceso, interactividad con el usuario, personalización, etc.) a las páginas Web, escritas en lenguaje HTML.

Kernel

Es el corazón de un sistema operativo, su componente más importante. Su función es brindar servicios básicos para el resto del sistema y las aplicaciones que se ejecutan en él. Las tareas que el Kernel (o Núcleo) administra son, entre otras, todas las operaciones de entrada/salida con los dispositivos de hardware del ordenador, la memoria del sistema, la ejecución de procesos y servicios. Sin importar el sistema operativo, aquellos que se basan en un Kernel normalmente incluyen en éste las mismas funciones antes mencionadas, aunque en otros casos le agregan otras tareas, o quizás, manejan por separado la gestión de memoria. Algunos sistemas operativos basados en un Kernel son Windows y Linux, entre otros.

Keygen
Se denominan así, a los programas creados por Crackers, los cuales son capaces de generar las claves de registro de un programa shareware. Estos generadores de registro, normalmente muestran el número de serie a introducir en la aplicación que se quiere registrar.

Keylogger
(Capturadores de Teclado) Aplicaciones encargadas de almacenar en un archivo todo lo que el usuario ingrese por el teclado. Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados.

Lan
(Local Area Network) Es una red de área local, o grupo de ordenadores conectados entre sí dentro de una zona pequeña geográfica (generalmente en una misma ciudad, población, o edificio).

Linux
Sistema operativo gratuito y de código abierto para ordenadores personales derivado de Unix.

Macro / Virus de macro
Una macro es una secuencia de operaciones o instrucciones que definimos para que un programa (por ejemplo, Word, Excel, o Access) realice de forma automática y secuencial. Estas son 'microprogramas' que pueden ser infectados por los virus. Los documentos de texto, las bases de datos o las hojas de cálculo, no son programas y por ello no deberían ser infectados por ningún virus. No obstante, en cada uno de los ficheros creados con este tipo de aplicaciones se pueden definir macros y éstas sí son susceptibles de ser infectadas. Los virus de macro son aquellos que infectan exclusivamente documentos, hojas de cálculo o bases de datos que tienen macros definidas. El virus se propaga de un documento a otro y la infección tiene lugar cuando se abre el documento.

Malware
Es la abreviatura de Malicious software, término que engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Trojan (Caballo de Troya), Gusano (Worm), Parásito, Spyware, Adware, Hijackers, Keyloggers, etc….

Mbps (Megabits por segundo)
Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits.

Mbr
(Master Boot Record) En castellano, Sector de Arranque, o Sector Maestro de Booteo. Es una pequeña parte de memoria cuyo contenido se ejecuta en el inicio del ordenador. Puede contener un programa cargador, y normalmente se encuentra en el primer sector del disco rígido. Los virus residentes suelen alojarse en el MBR para ejecutarse desde el inicio mismo del sistema. Algunos ejemplos son el Stoned, Michelangelo y Jersusalem, entre otros.

MHz (Megahertzio)
Unidad empleada para medir la 'velocidad bruta' de los microprocesadores equivalente a un millón de hertzios.

Microprocesador / Procesador
Es el corazón electrónico e integrado de un sistema informático. Se trata del chip (pastilla o circuito integrado -CI- de silicio, con elementos electrónicos microscópicos -transistores, resistencias, etc.-) que gobierna todas y cada una de las operaciones que se realizan en el sistema.

Módem
Es un elemento físico (un periférico), también conocido como MOdulador DEMmodulador, que se utiliza para convertir las señales eléctricas (analógicas y digitales). Su objetivo es facilitar la comunicación entre ordenadores y otros tipos de equipos. Su utilidad más habitual, en la actualidad, es conectar los ordenadores a Internet.

Modo Seguro
El modo seguro permite al usuario ingresar en su ordenador dejando sin funcionamiento alguno a determinadas aplicaciones para que el usuario pueda determinar que es lo que no funciona adecuadamente.

Monitor de Red
(En inglés Sniffer) Programas que monitorizan la información que circula por la red con el objeto de capturar información. Las placas de red tienen un sistema de verificación de direcciones mediante el cual saben si la información que pasa por ella está dirigida o no a su sistema. Si no es así, la rechaza. Un Sniffer consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer). Existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo contraseñas de acceso a cuentas, aprovechándose de que generalmente no son cifradas por el usuario. También son utilizados para capturar números de tarjetas de crédito o direcciones de correo. El análisis de tráfico puede ser utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto). Los buenos Sniffers no se pueden detectar, aunque la inmensa mayoría, y debido a que están demasiado relacionados con el protocolo TCP/IP, si pueden ser detectados con algunos trucos.

Ms-dos
(Disk Operating System). Sistema operativo desarrollado por los primeros ordenadores compatibles IBM, en el que se trabaja escribiendo órdenes para todas las operaciones que se desean realizar. Muy difundido como sistema operativo básico hasta que ha sido reemplazado por los sistemas operativos Windows.

Multimedia
Información digitalizada de varios tipos como texto, gráficos, imagen fija, imagen en movimiento y sonido.

Navegador
Un navegador (también llamado navegador Web o de Internet) es el programa que permite visualizar los contenidos de las páginas Web en Internet. También se conoce con el nombre de browser. Algunos ejemplos de navegadores Web son: Internet Explorer, Opera y el mas rápido y seguro de hoy en día Firefox

Ntfs
NT File System (Sistema de Archivos de NT). Es el sistema de archivos utilizado incorporado a partir del sistema operativo Windows NT, y utilizado también en Windows 2000 y Windows XP. Permite un mayor nivel de seguridad que los sistemas de archivos anteriores en las plataformas Windows, pudiendo agregar permisos de acceso por usuario/grupos a archivos y carpetas almacenadas en el disco duro del equipo.

P2p
Es un modelo de comunicaciones en el cual cada parte tiene las mismas capacidades y cualquiera de ellas puede iniciar la comunicación. Otro modelo totalmente opuesto es el cliente/servidor en donde el servidor se encuentra a la espera de una comunicación por parte del cliente. Este modelo se basa en que ambos nodos actúen como servidores y clientes a la vez.
Actualmente, este tipo de comunicaciones es utilizado por aplicaciones de intercambio de archivos en donde los usuarios pueden comunicarse uno con el otro o mediante un servidor intermedio.

Parche
También conocidos como actualizaciones (en inglés patches o updates), son soluciones a problemas o agujeros de seguridad en aplicaciones o sistemas operativos. En el ambiente Windows son normalmente programas ejecutables que reemplazan los componentes fallados por otros sin problemas; en otras plataformas también son conocidos como PTFs (Program Temporary Fixes).
Existen conglomerados de parches, más estables, que incluyen varias actualizaciones a diversas fallas, que suelen ser llamados Service Packs, y son liberados cada cierto tiempo por las empresas responsables de las aplicaciones y sistemas operativos más utilizados.

Phishing
Se utiliza el término "phishing" para referirse a todo tipo de prácticas utilizadas para obtener información confidencial (como números de cuentas, de tarjetas de crédito, contraseñas, etc.).
La gran parte de estos ataques son llevados a cabo a través de un e-mail falso (scam), enviado por el atacante, que notifica al usuario la necesidad de que confirme cierta información sobre su cuenta.
Estos mensajes pueden parecer muy reales ya que muchas veces incluyen logos de la entidad bancaria y una gráfica muy profesional.
Debido a ciertas vulnerabilidades en los principales navegadores, los atacantes puede redireccionar al usuario a un servidor falso sin que este note la diferencia.

Plug-In
Extensión de programa: Un componente de software que incorpora funciones no previstas en el desarrollo original. Significan para el usuario la posibilidad de agregar funciones especiales, generalmente muy específicas. Pueden también mostrar comportamientos indeseados como redirecionar resultados de búsqueda o supervisar el comportamiento de búsqueda de los usuarios, la historia de las conexiones, o instalar otro software indeseado o código dañino. Son muy utilizados en los navegadores,

Polimórfico (Virus)
Este tipo de virus tienen una cualidad muy importante: pueden cambiar de forma. Pero, ¿qué quiere decir que un programa informático, como un virus, pueda cambiar de forma? Lo que realmente hace el virus es copiarse en memoria, volver a compilarse tras cambiar su estructura interna, tal como nombres de variables, funciones, etc, y volver a compilarse, de manera que una vez creado nuevamente un espécimen del virus, es distinto del original.
Existen virus de un polimorfismo avanzado que no sólo cambian variables y funciones sino mucho más, e incluso hay algunos nuevos tipos de virus polimórficos que son llamados metamórficos por su capacidad de cambiarse casi completamente creando una copia nueva de si misma, que puede no ser detectada por la mayoría de los antivirus. Para los fanáticos de los virus informáticos, los polimórficos son uno de los especimenes más interesantes dada su capacidad camaleónica.

Pop-up
El término anglosajón popup denota un elemento emergente.
En Internet se utiliza a menudo para referirse a ventanas Web que se abren sobre la ventana en uso. A menudo, esto se utiliza como técnica para poner publicidad que, al tapar la página que veíamos, no podemos evitar mirarla. Otra técnica algo menos intrusiva es la de pop-under, que consiste en ventanas que se abren en el fondo, detrás de las ventanas en uso.
Algunas de estas ventanas, a su vez, activan otras ventanas emergentes, lo que puede dar lugar a un bucle infinito intencionado o no. Algunas se abren en pantalla completa o, en general, hacen más difícil que el usuario las cierre.

Proxy
Software que permite a varios ordenadores acceder a Internet a través de una única conexión física y puede permitir acceder a páginas Web, FTP, correo electrónico, etc., y también, servidor de comunicaciones, responsable de canalizar el tráfico entre una red privada e Internet, que contiene un cortafuegos.

Puerto:
Puerto: Un puerto es una conexión lógica utilizada específicamente por el protocolo de Internet (TCP/IP). Los programas que requieren de la utilización de un servidor se conectan a éstos mediante un puerto.
Algunas aplicaciones poseen puertos ya asignados, éstos son llamados "puertos ya conocidos" y han sido asignados por IANA (Internet Assigned Numbers Authority) organismo encargado de regular la asignación de números de puertos.
Otras aplicaciones utilizan números dinámicos, los cuales son establecidos en cada conexión.

Los números de los puertos pueden ir desde el 0 al 65.536, de los cuales los primeros 1024 están reservados para ciertos servicios privilegiados.
Un ejemplo es el puerto 80 utilizado por el servicio HTTP, que nos permite navegar por sitios Web.

Ram
(Random Access Memory) Se trata de una memoria de semiconductor en la que se puede tanto leer como escribir información. Es una memoria volátil, es decir, pierde su contenido al desconectar la energía eléctrica. Se utiliza normalmente como memoria temporal para almacenar resultados intermedios y datos similares no permanentes.

Registro de Windows
El Registro de Windows, también llamado Registry (en inglés) o Registro del Sistema, contiene información de configuración del sistema operativo. Entre dicha información podemos encontrar las definiciones de las extensiones de archivos, las librerías dinámicas instaladas, configuraciones de software propio del sistema operativo o de terceros, etc.
Muchos gusanos, virus y troyanos utilizan el registro para agregar la configuración que necesitan para ejecutarse automáticamente con cada inicio del sistema. También toman información necesaria para su ejecución, como las rutas de los directorios del sistema, que están almacenadas en el sistema.

Residente (Virus)
Se denomina un virus residente cuando es capaz de mantenerse en memoria desde el inicio del equipo infectado, ya sea cargándose desde el sector de arranque del mismo o como un servicio del sistema operativo, hasta que el mismo se apaga.
Un ordenador infectado por este tipo de virus suele ser difícil de limpiar, dado que en muchos casos requieren que se reinicie el equipo con un disco de arranque (bajo Windows 9x/Me) o con el disco de emergencia (Windows NT/2000/XP) para evitar que se carguen en memoria.

Rom
(Read Only Memory) Es una memoria de semiconductor no destructible, es decir, que no se puede escribir sobre ella, y que conserva intacta la información almacenada, incluso en el caso de interrupción de corriente (memoria no volátil). La ROM suele almacenar la configuración del sistema o el programa de arranque del ordenador.

Rootkit
Los rootkits se iniciaron bajo los sistemas operativos Unix, basándose en un conjunto de herramientas específicamente modificadas para ocultar la actividad de quien las utilizará.
Por esto, se define a rootkit como un conjunto de herramientas especiales que permiten esconder procesos activos, archivos en uso, modificaciones al sistema, etc., de manera que las utilidades de seguridad tradicionales no puedan detectarlas una vez en el sistema.
Cuando se habla de “técnicas rootkit” en un código malicioso, básicamente nos referimos al hecho de que el malware en cuestión es capaz de aprovechar funciones propias o de herramientas externas para esconder parte o todo su funcionamiento.

Shareware
Tipo de licencia de un software que permite distribuir un software gratuitamente para ser probado, pero que posee ciertas limitaciones en su funcionalidad o disponibilidad.

Spam
Spam: Es llamado Spam al correo basura, el cual llega a nuestras casillas de correo sin que nosotros lo hayamos solicitado.
Generalmente estos mensajes contienen anuncios publicitarios sobre productos, sitios Web, o cualquier otra actividad comercial que puedan imaginarse. Con estos envíos masivos el "anunciante" logra llegar a una gran cantidad de usuarios que de otra manera no se enterarían de su producto o servicio.
Los Spamers, personas dedicadas al envío de correo basura, van generando base de datos de direcciones de correo electrónico las cuales son obtenidas de diferentes formas.

Spyware
Software espía. Es todo aquel programa o aplicación que sin el conocimiento del usuario recolecta información de su equipo o de lo que hace al utilizar Internet. Normalmente utilizado con fines de publicidad o marketing. Son programas que invaden la privacidad de los usuarios y también la seguridad de sus computadoras.
Actualmente, este tipo de software es incluido junto a aplicaciones gratuitas de gran difusión, como las utilizadas herramientas de intercambio de archivos.
Podría considerarse una rama de la familia de los troyanos dado que básicamente su función es similar a la de estos. Tema de la presente investigación.

Tcp/ip
(Transfer Control Protocol / Internet Protocol) Protocolo de control de transmisión/Protocolo de Internet. Conjunto de protocolos sobre los cuales funciona Internet, permite la comunicación entre los millones de equipos informáticos conectados a dicha red.
El protocolo IP, que se ocupa de transferir los paquetes de datos hasta su destino adecuado y el protocolo TCP, se ocupa de garantizar que la transferencia se lleve a cabo de forma correcta y confiable.

Troyanos
(Caballos de Troya) Programas que, enmascarados de alguna forma como un juego o similar, buscan hacer creer al usuario que son inofensivos, para realizar acciones maliciosas en su equipo.
Estos troyanos no son virus ni gusanos dado que no tienen capacidad para replicarse por si mismos, pero en muchos casos, los virus y gusanos liberan troyanos en los sistemas que infectan para que cumplan funciones especificas, como, por ejemplo, capturar todo lo que el usuario ingresa por teclado (keylogger).
La principal utilización de los troyanos es para obtener acceso remoto a un sistema infectado a través de una puerta trasera. Este tipo de troyano es conocido como Backdoor.

Unidad de red Unidad de red es un término utilizado para definir un espacio donde puede almacenarse información, pero en lugar de encontrarse en el propio equipo, éste es generado en un equipo remoto. Cuando una estación de trabajo se conecta al servidor de su red, se

puede crear una unidad de red con los documentos del usuario que ha iniciado la sesión, pero que físicamente se encuentran en el servidor u otro equipo.

Url
(Uniform Resource Locator) Localizador Unificado de Recursos. Dirección a través de la cual se accede a las páginas Web en Internet (o a otros PCs).

Virus
Son sencillamente programas creados para infectar sistemas y otros programas creándoles modificaciones y daños que hacen que estos funcionen incorrectamente.

Wan
(Wide Area Network) Es una red de área extensa, o grupo de ordenadores que se encuentran conectados entre sí, pero distantes geográficamente. La conexión se realiza mediante línea telefónica, radioenlaces, vía satélite o cualquier sistema de intercambio de paquetes.

Webmaster
Es una persona encargada del mantenimiento de un sitio Web. Esto puede comprender escribir ficheros HTML, establecer programas más complejos, y responder a los correos electrónicos. Muchos sitios animan a que se les envíen comentarios y preguntas al webmaster acerca del sitio Web por medio del correo electrónico.

Wep
(Wired Equivalent Privacy) Protocolo para la transmisión de datos 'segura'. El cifrado puede ser ajustado a 128 bits, 64 bits o deshabilitado. La configuración de 128 bits da el mayor nivel de seguridad.
También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de cifrado. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado, aunque requiere tiempo.

Wi-Fi
Abreviatura de Wireless Fidelity. Es el nombre “comercial” conque se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica.

Zip
(Compactar) Es un formato correspondiente a los ficheros comprimidos con la herramienta WinZip.

Zombie
Un ordenador generalmente infectado con un troyano de acceso remoto, capaz de recibir órdenes externas, y de actuar, generalmente en actividades maliciosas, sin el conocimiento de sus dueños.

FUENTES DE CONSULTA

BIBLIOGRAFíA

Ackoff, Russell L. "El arte de resolver problemas"; Ed. Limusa, México 2007.

Ackoff, Russell L. "Planificación de la empresa del futuro"; Ed. Limusa, México 2006.

Ackoff, Russell L. "El paradigma de Ackoff"; Ed. Limusa Wiley, 2007.

Ackoff, Russell L. "Rediseñando el futuro"; Ed. Limusa, México 1981.

Acle Tomasini, Alfredo. "Planeación estratégica y control total de calidad"; segunda edición Ed. Grijalbo.

Churchman, C. West. "El enfoque de sistemas"; Editorial Diana, México1981

Miklos, Tomás y Tello Ma. Elena. "Planeación prospectiva"; Ed. Limusa Noriega, 1999.

Pierre Graton. "Protección Informática"; Ed. Trillas

Rodao Jesús de Marcelo. "Piratas Cibernéticos"; Ed. Rama

Stephen P. Robbins. "Administración, Teoría y práctica"; Prentice Hall Hispanoamericana, México 1994

Terry, George R. "Principios de Administración"; Ed Continental, México 1984

Van Der Heijden. Kees. "Desarrollo de escenarios: El arte de prevenir el futuro"; Ed. Panorama México 2006

PÁGINAS WEB

http://es.mcafee.com/
Mcafee Antivirus español
http://es.wikipedia.org/wiki/Memoria_flash
Wikimedia La enciclopedia libre
http://es.wikipedia.org/wiki/Spyware
Wikimedia La enciclopedia libre
http://service1.symantec.com/SUPPORT/INTER
Soporte Symantec
http://www.alambre.info/2007/
Página de Tecnología y sociedad
http://www.amipci.com.mc
Asociación Mexicana de la Industria Publicitaria y Comercial en Internet
http://www.conapo.gob.mx
Consejo Nacional de Población
http://www.forospyware.com/
Foro de información de Infospyware
http://www.giatica.info/item/internet-su-historia
Giatica blog sobre educación tecnológica y proyectos técnicos
http://www.imss.gob.mx
Instituto Mexicano del Seguro Social
http://www.inegi.gob.mx
Instituto Nacional de Estadística y Geografía
http://www.infospyware.com/
InfoSpyware
http://www.microsoft.com/latam/athome/security/Spyware/
Microsoft Latinoamérica

http://www.pandasecurity.com

Panda Antivirus

http://www.pandasecurity.com/spain/homeusers/security-info/

Panda Antivirus español

http://www.seguridad.unam.mx/usuario-casero/Spyware.dsc

Seguridad UNAM

http://www.spybot.info/es/index.html

Spybot

http://www.symantec.com/

Symantec

http://www.symantec.com/es/es/norton/security_response/Spyware.jsp

Symantec Norton Antivirus España

http://www.symantec.com/es/mx/norton/security_response/malware.jsp

Symantec Norton Antivirus México

ENCICLOPEDIA ELECTRÓNICA

Microsoft Encarta 2007 [DVD]. Microsoft Corporation, 2006