Universidad Don Vasco, A.C.

---- INCORPORACIÓN No. 8727 - 48 ----

a la Universidad Nacional Autonóma de México

Escuela de Informática

Análisis de la Seguridad Informática en la Administración Local de Recaudación en Uruapan, Mich; SAT;SHCP

TESIS

Que para obtener el título de:

LICENCIADA EN INFORMÁTICA

presenta:

Indira Quintero Silva

Uruapan, Michoacán, junio del 2004

ÍNDICE

Pag.

Pag.

AGRADECIMIENTOS

A Dios por ponerme constantemente en las mejores manos y permitirme vivir sanamente.

A mis padres, por apoyarme incondicionalmente en mis decisiones aconsejándome siempre lo mejor para mi, e impulsarme a que siga adelante, y por ser mi fuente de inspiración, porque algún día, quiero llegar a ser como ellos, profesionalmente y como los maravillosos padres que son para mi.

A Yunuen y Cony, por su ayuda académica y personal dada durante mis estudios, por su cariño y por estar siempre conmigo.

A Memo por su apoyo y amor.

A mis maestros, por la formación que me han dado en el transcurso de la licenciatura, y por no ser solamente mis maestros, si no también mis amigos.

INTRODUCCIÓN

Actualmente la información es uno de los recursos más importantes con los que puede contar una empresa, ya que de la información depende en gran medida el buen funcionamiento de los negocios. Un sistema informático se compone de hardware, software, personas que lo manejen y lo más importante, los datos. Con la información bien administrada, segura, objetiva, obtenida rápidamente y cuando se ocupa, se facilitan en gran medida la toma de decisiones para quienes las requieran realizar.

Los sistemas informáticos tienden a crecer cada vez mas al igual que la necesidad de su interconexión en redes, lo que lleva a tener mas puntos débiles debido a su mayor dimensión, pues el número de posibles atacantes crece, por la mayor conectividad que tienen las mismas firmas y el crecimiento de sus redes y comunicaciones. Los ataques pueden tener varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar a un sistema; esto puede ser hecho por personas internas de la empresa o por externos, radicando aquí la importancia de proteger la información de que pueda ser interceptada, modificada, interrumpida y de que le puedan agregar código a un programa, añadir programas completos mejor conocidos como virus, que pueden ser fácilmente adquiridos por medio de la red, a su vez transmitidos por Internet por medio de correos, links o ligas , puertas falsas que son generadas al instalar software que contienen "holes" (agujeros) y se ejecutan al acceder a Internet; el peligro que es tener instalado software ilegal, ya que hay leyes enérgicas en cuanto a los derechos de autor y es un deber de todos los usuarios de cumplirlas.

Otro elemento que repercute en daños al sistema, elementos informáticos, datos, programas o documentos electrónicos son las bombas lógicas creadas por programadores que al cumplirse una condición en el sistema, se ejecutan las instrucciones programadas. Las personas que manejan los sistemas informáticos también lo pueden dañar por medio de intercambio de dispositivos de almacenamiento previamente infectados por otros equipos.

Respecto a la seguridad del hardware aspectos a considerar son, ubicación del equipo (en caso de ser servidores que tengan el clima apropiado), el suministro de corriente debe ser la adecuada. Accidentes naturales tales como incendio pueden ocurrir y si no existía un respaldo, la información se perderá.

La Secretaria de Hacienda y Crédito Público a través de sus representaciones locales almacena información referente a ciudadanos, negocios y otras entidades, la mayor parte de la cual está protegida por las leyes que se refieren a la confidencialidad y a la divulgación. Toda la información bajo el control del Servicio de Administración Tributaria (SAT) deberá usarse y manejarse de conformidad con estas leyes, y con la mejor práctica y normas reconocidas para salvaguardar la información de acuerdo con su clasificación.

Los lugares físicos en donde se almacena la información, o en donde se tiene acceso a ella, debe tener la protección necesaria para que no sea utilizada de mal manera como en el caso de perjuicio de la misma empresa a la que le pertenece esa información. Si no se lleva a cabo, son en vano todas las demás medidas de seguridad para la información. Las computadoras en donde se almacena electrónicamente la información, sólo deberán estar accesibles para las personas autorizadas.

Es por esto que analizando el valor que tienen los sistemas informáticos y los ataques que puede tener, es muy importante el realizar una investigación y análisis en El Servicio de Administración Tributaria, para poder realizar una propuesta de solución a los problemas de seguridad que pudiera tener.

Para la realización de esta investigación se proponen los siguientes objetivos:

- Realizar el análisis de la situación de seguridad informática que se tiene actualmente en la Administración Local de Recaudación de Uruapan.
- Aplicar los conocimientos adquiridos en los estudios de Licenciatura en Informática.
- Analizar el conocimiento de los usuarios con respecto a la seguridad informática.
- Llegar a una propuesta sólida y objetiva.
- Que la propuesta obtenida sea de utilidad para la empresa.

La hipótesis planteada es: "Los usuarios de la red son una vulnerabilidad muy grande para ataques internos y/o externos de una empresa".

Para el desarrollo del presente trabajo de investigación se divide en cinco capítulos de los cuales los primeros cuatro son teóricos para poder sustentar el ultimo capítulo que es el caso práctico.

El primer capítulo habla de los conceptos de la empresa y sus características más importantes, referencias de la ciudad de Uruapan, así como una descripción de las empresas del gobierno, tratándose este tema por que el análisis es desarrollado sobre una paraestatal en la ciudad de Uruapan.

En el segundo capítulo se exponen los elementos de la Informática para marcar la evolución que se ha dado desde sus orígenes hasta estos tiempos, destacando la importancia que tiene en las empresas.

En el tercer capítulo se conceptualizan los términos relacionados con la seguridad informática, así como las amenazas físicas o lógicas, internas o externas que existen en contra de la empresa.

En el último capítulo teórico se habla de la división de los elementos de la seguridad informática y se dice qué aspectos pertenecen a cada termino, también se menciona las leyes existentes para la protección del software.

En el caso práctico situado en el último capítulo se realiza el análisis de los resultados obtenido en las encuestas y en la entrevista, pero primero se hace una breve explicación de los antecedentes generales del Servicio de Administración Tributaria para situarnos en la empresa que se va a estudiar.

CAPÍTULO I

LA EMPRESA

Es propio de cada sociedad contar con una empresa, pero para entender este concepto debemos formarnos primeramente una idea clara de entre las distintas definiciones existentes para de esta manera llegar a comprender las características que se desprenden de la empresa, dando lugar a la formación del marco teórico de esta tesis, ya que el análisis de la seguridad informática se realizará en la Administración Local de Recaudación de la ciudad de Uruapan Michoacán (ALR) dependiente del Servicio de Administración Tributaria (SAT), órgano desconcentrado de la Secretaria de Hacienda y Crédito Público (SHCP) .

1.1. REFERENCIAS DE LA CIUDAD DE URUAPAN

Ya que la investigación se hace en una empresa de la ciudad de Uruapan, es importante la descripción del lugar en que se encuentra ubicada la Administración Local de Recaudación.

1.1.1 HISTORIA

"Fray Juan de San Miguel fundó esta próspera entidad, en el ano 1533. Durante la guerra de Independencia, Uruapan fue asiento del Primer Congreso de Anáhuac y, a la consumación de ésta, alcanzó la categoría de municipio y cabecera de distrito". (http://www.michoacan.gob.mx/municipios/103historia.htm)

1.1.2 FISIOGRAFÍA

Es una de las ciudades más importantes de Michoacán, se encuentra a 62 kms al Oeste de Pátzcuaro, a una altura de 1,600 mts sobre el nivel del mar, con

clima templado húmedo y una temperatura media anual de 19 grados centígrados.

Su economía radica en la agricultura y fruticultura, y es uno de los principales productores de aguacate en la República. Es, además, notable región ganadera y forestal (http://www.ccu.umich.mx/mich/uruapan-inic.html).

1.1.3 LAS EMPRESAS EN URUAPAN

La industria está representada en un 95% por micro industrias como son talleres automotrices, taller metal - metálicos, fábrica de producción de alimentos y fábrica de materiales para la construcción.

Se cuenta con aproximadamente 1,158 comercios clasificados en 80 giros de los cuales el 11.6% son de abarrotes, el 8% farmacias, el 6.6% abarrotes con venta de vinos, el 5.7% tiendas de ropa, el 5.1% refaccionarías y accesorios para autos y aviones, el 4.8% son papelería e imprentas, el 4.5% de zapaterías y el 4.3 por ciento de ferreterías.

Actualmente hay 378 empresas de servicios representadas de la siguiente forma: 15% cafeterías y restaurantes, 9% hoteles, 7.5% constructoras, 7% de servicios profesionales y el 5% pensiones y estacionamientos. (http://www.michoacan.gob.mx/municipios/103economia.htm).

1.2. LA EMPRESA

La mayoría de las personas hemos escuchado o manejado el termino de empresa, pero realmente que es lo que abarca todo este concepto, veamos que dicen los profesionales.

1.2.1 CONCEPTO DE LA EMPRESA

Existen numerosos conceptos de empresa, aunque todos están encaminados a una definición en general, por lo que sólo se mencionarán algunas de ellas dadas por diferentes autores como lo son:

Joaquín Rodríguez Valencia (1999:71) la define como una entidad económica destinada a producir bienes, distribuirlos, venderlos, obtener un beneficio y ser el principal factor dinámico de la economía de una nación.

Es la unidad económico-social en la que el capital, el trabajo y la dirección se coordinan para lograr una producción que responda a los requerimientos del medio humano en el que la propia empresa actúa (GUZMÁN, citado por Fernández, 1977:85).

"Organización industrial o comercial que se hace funcionar para alcanzar metas propias de las mismas" (HERNÁNDEZ, BALLESTEROS, 1980:410)

1.2.2 ELEMENTOS DE LA EMPRESA

Para Agustín Reyes Ponce los elementos de la empresa son tres, los bienes materiales, los hombres y los sistemas.

- Bienes Materiales: Se refieren a las cosas que se procesan y combinan para producir el servicio, la información o el producto final (RODRÍGUEZ, 1999:85)
    - Bienes muebles e inmuebles como sus edificios, instalaciones, maquinaria, equipo, terrenos, etc.
    - Materias primas, materias auxiliares y productos terminados.
    - Dinero que es lo que se tiene disponible para pagos diarios, urgentes y representación del valor de todos los bienes.

- Hombres o Personal: Son el elemento eminente activo y el de máxima dignidad. Se clasifican en, obreros, empleados, supervisores, técnicos, altos ejecutivos.
- Sistemas: Es todo el cuerpo orgánico de procedimientos, métodos, etc.; por medio de los cuales se logran los objetivos de la empresa (RODRÍGUEZ, 1999:85). También se puede decir que son los bienes inmateriales como los sistemas de producción, de ventas, de finanzas, de organización y administración. (REYES, 1978:72).

A esta clasificación Joaquín Rodríguez Valencia agrega una cuarta clasificación que es el equipo, el cual Agustín Reyes Ponce lo agrupa en bienes materiales, llegando los dos a concordar en los elementos de la empresa.

1.2.3 OBJETIVOS DE LA EMPRESA

José Antonio Fernández Arena acepta tres categorías de objetivos, de servicio, social y económico. Ejemplo de ellos en una entidad industrial son:

- Objetivo de servicio. Satisfacer las necesidades de los consumidores ofreciendo buenos productos o servicios, en condiciones apropiadas.
- Objetivo social. Satisfacción del elemento personal, comunidad, por medio de buenas relaciones humanas y adecuadas relaciones públicas.
- Objetivo económico. Protección de los intereses económicos de la empresa, de sus acreedores y sus accionistas, logrando la satisfacción de estos grupos por medio de una generación de riqueza. (FERNÁNDEZ,1977:94).

1.2.4 IMPORTANCIA DE LA EMPRESA

La importancia de la empresa radica en el hecho de que se materializan la capacidad intelectual, la responsabilidad, la organización, factores involucrados en la producción , dando lugar a el crecimiento y desarrollo, proporcionan empleos, ofrecen la opción para una expansión económica, el campo experimental en donde se generan nuevos productos, ideas, técnicas y formas de hacer las cosas.(RODRÍGUEZ,1999:30,32).

1.2.5 CLASIFICACIÓN DE LA EMPRESA

Se clasifican en tres grandes ramas:

- De servicios. Son las que con el esfuerzo del hombre producen un servicio sin que el producto objeto del servicio tenga naturaleza corpórea. A su vez se clasifica en: Sin concesión, concesionadas por el estado y concesionadas no financieras.
- Comerciales. Se dedican a la adquisición de bienes o productos para revenderlos, aumentando al precio de costo.(Son intermediarios entre el productor y el consumidor).
- Industriales, que se dividen en:
    - Industrias extractivas. Las que se dedican a la extracción y explotación de las riquezas naturales, sin modificar su estado original, y se subdivide en: De recursos renovables y de recursos no renovables.
    - Industrias de transformación. Se dedican a la transformación o manufactura de la materia prima para la obtención de un producto con características diferentes a los adquiridos originalmente.

(RODRÍGUEZ,1999,82)

Existe otra clasificación que es de acuerdo con la Ley MIPYME (Micro, Pequeña y Mediana Empresa)

Tipo de Empresa	No. de Empleados	Activos Totales (en salarios mínimos mensuales vigentes)
Microempresa	Hasta 10	Hasta 500
Pequeña Empresa	De 11 a 50	De 501 a 5000
Mediana Empresa	De 51 a 200	De 5001 a 15000

Fuente: http://www.acopivalle.com.co/info/clasificacion.html

A esta clasificación se le puede sumar la empresa grande que puede tener un número aproximado de 1,000 trabajadores (REYES, 1978: 94).

1.3 GOBIERNO

Es una organización que provee bienes y servicios, y redistribuye ingreso y riqueza. Los servicios más importantes provistos por el gobierno son el marco de leyes y un mecanismo para su aplicación (los tribunales y las fuerzas policíacas). También proporcionan servicios como la defensa nacional, la salud pública, el transporte y educación. (PARKIN,1995:13).

1.3.1 EMPRESAS DEL GOBIERNO

"Una empresa paraestatal o del gobierno es aquella sociedad nacional, donde la organización del gobierno tiene participación. Teniendo como finalidad

satisfacer una necesidad de carácter general o social con la que puede obtener o no beneficios. Podrá trabajar obteniendo beneficios, pero puede ocurrir también que se haya planeado aun con base en pérdidas, porque el fin del estado como empresario no puede ser obtener lucros, sino satisfacer necesidades" (REYES, 1978:164).

Por lo que podemos señalar que la empresa es una unidad económica de producción de bienes y servicios, para su estudio se clasifica dependiendo del número de trabajadores y del giro de la empresa, cuenta con elementos distintos que la integran, todos ellos conjuntamente buscan lograr los objetivos para satisfacer una necesidad de la comunidad y cubrir la meta de la propia empresa; la paraestatal es financiada por el gobierno, teniendo como objetivo satisfacer una necesidad de carácter general o social. Ahora que tenemos un conocimiento mas sólido de la empresa, podremos dar paso al segundo capítulo que es "La Informática y su evolución".

CAPÍTULO II

LA INFORMÁTICA Y SU EVOLUCIÓN

El uso de las computadoras, sobre todo las computadoras personales, se ha extendido tan rápidamente que ya no es posible hacer caso omiso de su existencia, pero, ¿De cuándo datan sus inicios?, ¿Cómo se fueron mejorando?, ¿Quiénes impulsaron su desarrollo?, para dar respuesta a estas preguntas, en este capítulo se presentan los orígenes y la evolución del hardware y software.

2.1 CONCEPTOS

Para comprender de mejor manera el avance de la informática es importante definir los términos de hardware y software, ya que en base se presenta la mejora y además términos se mencionan durante todo la explicación del progreso de la Informática.

2.1.2. INFORMÁTICA

Conjunto de conocimientos científicos y de técnicas que hacen posible el tratamiento automático de la información por medio de computadoras. Además se encarga de aprovechar de la mejor manera la información, desde como conseguirla, utilizarla, procesarla y distribuirla, con una de las principales finalidades que es obtener decisiones coherentes, oportunas y confiables para una empresa o sociedad.

2.1.2 HARDWARE

Son los componentes materiales de un sistema informático, la función de estos componentes es importante para la información ya que es por donde se

ingresa, procesa, almacena y se da salida; algunos de los medios por el cual se ingresa la información son teclado, scanner, lápiz óptico, touch screen; se procesa por medio de la unidad de control(UC), unidad aritmético/lógica (UAL) ,área de almacenamiento primario(memoria); se almacena en floppy, CD-RW, Disco duro, cintas magnéticas; y se da salida por impresora y pantalla.

2.1.3. SOFTWARE

Son programas de computadoras que tienen instrucciones responsables de que el hardware realice su tarea y es indispensable para que el usuario puede interactuar con la computadora, este a su vez se puede dividir en varias categorías basándose en el tipo de trabajo que vaya a realizar. Es simplemente el conjunto de instrucciones individuales que se le proporciona al microprocesador para que pueda procesar los datos y generar los resultados esperados

2.2. HISTORIA DE LA INFORMÁTICA

Para hablar de los nacimientos y avances de la informática se tratan los temas de evolución del hardware, conjuntamente con el software y las generaciones de la computadora. Tanto software como hardware son elementos importantes para el desarrollo de este punto, por que no se puede decir que la informática es solo una de las dos partes, sino que es una interrelación de ambas y del ser humano.

2.2.1. EVOLUCIÓN DEL HARDWARE

"Los principios históricos del hardware datan desde hace 4,000 años con la creación del ábaco por los babilonios" (RADLOW, 1988:56), los antecesores mas recientes comienzan con la Pascalina.

2.2.1.1 PASCAL Y LEIBNITZ

El inventor y pintor Leonardo Da Vinci (1452-1519) trazó las ideas para una sumadora mecánica, siglo y medio después en 1642 Blas Pascal invento la primera máquina de cálculo mecánica, la Pascalina, que era operada por palancas y engranajes, realizaba sumas; mas tarde Gottfried Wilhelm Von Leibniz logra que la máquina de Pascal realice las cuatro operaciones básicas: sumar, restar, multiplicar, dividir, pero en 1671 Leibnitz le agregó además la posibilidad de calcular la raíz cuadrada. Su máquina estaba formada sobre ruedas dentadas, cada una de estas ruedas tenía diez dientes, éstos correspondían a los números de 0 al 9.

2.2.1.2. EL TELAR DE JACQUARD

En 1804 Jacquard inventó un telar que podía crear diferentes diseños en telas por medio de tarjetas perforadas con hoyos que representaban números, estos se conocieron como telares de Jacquard. Introdujo 2 conceptos importantes para el desarrollo futuro de la computadora, uno es que la información por medio de tarjetas puede codificarse, y el otro es que la información almacenada en las tarjetas podía actuar como una serie de instrucciones al juntar las tarjetas.

2.2.1.3 MÁQUINAS DE BABBAGE

Con apoyo económico del Gobierno Británico, Babbage construyó la máquina diferencial con el objetivo especializado de compilar tablas matemáticas en forma automática, pero no fue terminada. Sin embargo concibió el diseño de una máquina mucho más poderosa a la que llamo máquina analítica, que es muy semejante al concepto de computadora moderna. La máquina analítica fallo por

que no existía la tecnología suficiente para llevar a cabo sus ideas. La máquina podría realizar las operaciones básicas en secuencia automática a una velocidad de 60 sumas por minuto, necesitaba energía de vapor, "Estaría formada por tres partes: el almacén, el molino y los mecanismos de secuencia" (RADLOW, 1988:58).

2.2.1.4. HOLLERITH Y LA MÁQUINA DEL CENSO

Para el censo de 1890 de Estados Unidos Hermann Hollerith logró realizar una máquina del censo la cual utilizaba tarjetas perforadas, electricidad y leía la información a través de unos contactos eléctricos. Los resultados del censo se dieran a conocer en solo 3 años, siendo que el censo anterior tardó cerca de 7 años. La idea de tarjetas perforadas fue tomada de observar a un conductor de tranvía que perforaba los boletos de los pasajeros y registraba los datos en tarjetas rectangulares. Esa máquina fue muy importante en el desarrollo de computadoras digitales. "También diseñó máquinas para clasificar, intercalar e imprimir los resultados de la tabulación" (RADLOW, 1988:58). Fundó la Tabulating Machine Company para manufacturar y comercializar sus inventos, mas tarde se une con otras compañías y se transforma en IBM (Internacional Business Machines Corporation).

2.2.1.5. MARK I

Howard Aiken, inspirado en las ideas de Babbage, inventó la primera computadora digital por completo automática en la Universidad de Harvard, junto con cuatro de los ingenieros mas calificados de IBM. "Podía realizar una multiplicación en aproximadamente 6 segundos y una división en 12 segundos" (PARKER, 1986:71). Se dedicó a problemas balísticos de la Marina. No está

considerada como computadora electrónica debido a que no era de propósito general y su funcionamiento estaba basado en dispositivos electromecánicos llamados relevadores.

2.2.1.6. ABC (Atanasoff – Berry Computer)

En 1939 Atanasoff y Berry diseñan y construyen la primera computadora electrónica digital, sin propósito general a gran escala. Empleaba tubos de vacío para almacenamiento y funciones básicas en aritmética y lógica. Utilizaba 300 bulbos y podía resolver un conjunto de 29 ecuaciones simultáneas con 29 variables.

2.2.1.7 ENIAC (Electronic Numerical Integrator and Computer)

Fue la primera computadora electrónica digital de propósito general a gran escala del mundo, tenía más de 18 000 tubos de vacío, tenía 30 metros de longitud, 3 metros de alto y 90 centímetros de profundidad consumía 200 KW de energía eléctrica y requería todo un sistema de aire acondicionado, pero tenía la capacidad de realizar cinco mil operaciones aritméticas en un segundo, podía ser programada para realizar una amplia variedad de cálculos complejos, también se empleo para predicciones meteorológicas, diseño de túneles de viento y estudios de rayos cósmicos. Las ideas de Von Neumann resultaron tan fundamentales para su desarrollo posterior, que es considerado el padre de las computadoras.

2.2.1.8. EDVAC (Eletronic Discrete-Variable Automatic Computer)

John Von Neumann en 1945 presentó dos ideas básicas para las computadoras, la primera fue que el sistema numérico binario se integrará a las

computadoras, y la otra se refiere al concepto de programa almacenado, que permitiría la lectura de un programa dentro de la memoria de la computadora, y después la ejecución de las instrucciones del mismo sin tener que volverlas a escribir. La EDVAC fue la primera computadora en utilizar estos conceptos, tenía aproximadamente cuatro mil bulbos y usaba un tipo de memoria basado en tubos llenos de mercurio por donde circulaban señales eléctricas sujetas a retardos, con esta máquina junto con su antecesora la EDSAC (Electronic Delay Storage Automatic Calculador) "se instituyo la etapa de la revolución de las computadoras y el crecimiento explosivo de la industria de la computación comercial" (PARKER, 1986: 76).

2.2.1.9. GENERACIONES DE LA COMPUTADORA

El desarrollo de las computadoras suele dividirse por generaciones y el criterio que se toma para esta clasificación son por la forma en que están construidas (hardware) y la forma en que el ser humano se comunica con ellas (software).

Para algunos autores son 4 generaciones y para otros 5, considerando a la quinta como el futuro, en las que las características en las que concuerdan y son más destacables de cada una de ellas son las siguientes:

Primera generación: Se considera aproximadamente de entre los años de 1951 y 1958. Las computadoras se basan en la tecnología de tubos de vacío o bulbos, que transmite corrientes eléctricas sólo en una dirección, generaban mucho calor, eran grandes y estaban propensos a fallas frecuentes, utilizados para el almacenamiento, procesamiento de la información; además utilizaban

tarjetas perforadas y almacenamiento interno por tambor magnético. Programadas en lenguaje de máquina, se caracteriza por ser tedioso, improductivo y muy sujeto a errores; y ensamblado. También se crean los traductores que convierten el código fuente a código objeto llamados programas ensambladores.

Segunda generación: El invento del transistor (cristal de germanio o silicio, que proporciona señal de encendido/apagado), viene a sustituir a los tubos de vacío dando lugar a una nueva generación, en la que las computadoras son más rápidas, más pequeñas y con menores necesidades de ventilación, la forma de almacenamiento en esta generación fue la memoria de núcleos magnéticos. Aparece el concepto de human interface que es la relación entre el usuario y su computadora, se ponen al alcance programas con menús (listas de opciones) que orientan en todo momento al usuario es desarrollado el lenguaje de programación llamada COBOL y FORTRAN.

Tercera generación: Se inaugura con la IBM 360 que podía realizar tanto análisis numéricos como administración ó procesamiento de archivos, el gran descubrimiento de este periodo fueron los circuitos integrados denominados CHIP ,las computadoras nuevamente se hicieron más pequeñas, más rápidas, desprendían menos calor y eran energéticamente más eficiente. Gracias a la gran capacidad de procesamiento se hizo posible el desarrollo del software y sistemas operativos. Se introduce el concepto de familias con el que "los usuarios comenzaron a sentir que podían solucionarse los problemas masivos de conversación" (PARKER, 1986:87). "El sistema operativo de la serie 360, se llamó OS que contaba con varias configuraciones, incluía un conjunto de técnicas de

manejo de memoria y del procesador que pronto se convirtieron en estánd ares"(http://www.monografias.com/trabajo/histocomp/histocomp.shtml). También se da origen al concepto de tiempo compartido, en donde varios usuarios comparten recursos de una computadora central. En respuesta a las necesidades de los lenguajes de programación surge BASIC (Código de instrucción simbólica de propósito general para principiantes) que dio la posibilidad a "millones de personas sin especiales conocimientos de que puedan programar para sus micros" (PARKER, 1986: 89).

Cuarta Generación: El tamaño reducido del microprocesador y de chips (micro miniaturización) hizo posible la creación de las computadoras personales (PC), los términos que se refieren a la micro miniaturización son VLSI (Very Large Sacale Integration) y LSI (Large Scale Integration), los microprocesadores son un gran adelanto de la microelectrónica, están integrados por circuitos de alta densidad y con una velocidad impresionante. "Es la primera generación en la que existe una variedad de computadoras y la primera en la que se tiende a apartarse a los usos puramente especializados en ciencias, defensa nacional o negocios y a inclinarse hacia el uso general" (RADLOW, 1988:68), las cuales requieren de un espacio mínimo y con una gran capacidad de almacenamiento y velocidad. Debido a estos avances la industria del software da un rápido crecimiento y en cuanto a lenguajes de programación se refiere están los de alto facilitando la tarea de escribir programas.

Quinta generación: Esta Quinta generación que recién comienza se denominará: Computadora inteligente o inteligencia artificial, donde las computadoras utilizarán mas bases del conocimiento, lenguaje natural, y necesitaran mucha mas circuiteria. "En vista de la acelerada marcha de la

microelectrónica, la sociedad industrial se ha dado a la tarea de poner también a esa altura el desarrollo del software y los sistemas con que se manejan las computadoras" (http://www.monografias.com/trabajos/histocomp/histocomp.shtml). Los componentes básicos de las capacidades propuestas para la generación son: base de conocimiento, que tiene la capacidad de inferir y generar nuevos hechos en el proceso de resolver un problema dado; datos de contexto, que son los hechos acumulados de la base del conocimiento; y la máquina de inferencia, es un programa que proporciona los métodos para extraer inferencias y obtener soluciones al problema que se considere.

2.3. IMPORTANCIA DE LA INFORMÁTICA EN LA EMPRESA

Actualmente no existe empresa que no esté ligada directamente con la informática, un ejemplo muy claro es: ¿Quién no utiliza un procesador de texto para sus labores diarias?, es una necesidad mínima que tiene que ver con informática. Una empresa logra cumplir con sus objetivos gracias a sus cuatro recursos indispensables que son materiales, financieros, humanos y el no menos importante que es la información, este elemento se complementa con el humano, ya que éste es quien la obtiene, ingresa, utiliza y distribuye la información, este recurso nos puede servir como arma competitiva a nivel empresarial y para innovar. La información utilizada de forma automatizada es más confiable, rápida, precisa, organizada y confiable, es utilizada, entre muchas cosas mas, para llevar controles, generar reportes, estadísticas, procesos masivos y la mas importante que es la toma de mejores decisiones, para quienes las tengan que tomar.

Hemos visto que durante los últimos años la evolución de la informática se ha dado a pasos agigantados, el software es quizá uno de los productos de la

ingeniería que más ha evolucionado en muy poco tiempo, pasando del software empírico o artesanal hasta llegar al software desarrollado bajo los principios y herramientas de la ingeniería del software debido a exigencias cada vez mayores en la capacidad de resultados, en el área de programación, los avances incluyen el desarrollo de lenguajes de programación y programas traductores (compiladores), mejoras en los sistemas operativos que controlan el funcionamiento general de los computadoras que han permitido aumentar la productividad y utilización del equipo, y en cuanto al hardware el costo y el tamaño se han reducido, en tanto que su velocidad, capacidad de almacenamiento y confiabilidad han aumentado, pero confiabilidad, ¿Hasta que punto se puede decir que es confiable?, se dará paso al siguiente capítulo que expone sobre "la seguridad informática".

CAPÍTULO III

LA SEGURIDAD INFORMÁTICA

En el capítulo anterior se destacó la evolución de la Informática así como la importancia de la información, ahora veremos por qué es necesario protegerla, de qué, y de quiénes, ya que es vital contar con la información adecuada y que conserve sus propiedades de confidencialidad, integridad y disponibilidad. También se verán cuales son los riesgos informáticos a los que se está expuesto, así como algunas posibles soluciones.

3.1 DEFINICIÓN E IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA

Para entender su importancia definamos primero lo que se entiende por seguridad informática; son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas.

Para asegurar que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados (confidencialidad), garantizar que la información no sea modificada, (integridad) y el grado en el que un dato se encuentre en el lugar, momento y forma en que es requerido por el usuario autorizado (disponibilidad) de la información es necesario protegerla, ya que de no ser así es susceptible a varios casos, como lo son los siguientes: ser intercepcionada por una persona, programa o proceso accediendo a una parte del sistema a la que no está autorizado; modificación, destrucción, reemplazamiento, cambio de los datos o del funcionamiento del

sistema; interrupción, impidiendo que la información llegue a su destino, o generación como de incluir campos y registros en una base de datos, añadir líneas de código a un programa, añadir programas completos en un sistema (virus), introducir mensajes no autorizados por una línea de datos .

Existen dos tipos de atacantes de la información de una empresa, los empleados disconformes que laboran en la empresa o personas externas con acceso a sistemas dentro de la empresa como los auditores de informática y los que atacan desde afuera de la ubicación física de la empresa que no tienen nada que ver con ésta, como son los hackers, crackers, etc., siendo los dos una razón para tomar en cuenta y aplicar los elementos de la seguridad informática.

3.2 RIESGOS INFORMÁTICOS

Lo que daña a la seguridad de información son varios factores, ya sean internos o externos las personas que lo hagan, los riesgos informáticos tratan de código específicamente diseñado para atacar las medidas de seguridad del sistema, pueden tener diversas motivaciones, entre ellas, simple diversión, robo de información, destrucción de la información o saturación del sistema. Un ataque también puede ser manipular al personal para obtener la información que requiere el atacante, esta técnica es conocida como ingeniería de software, pero el objetivo final de estos dos tipos de ataques es al software, tratemos algunos de ellos.

3.2.1 VIRUS

Los virus de las computadoras no son más que programas con algunas características muy especiales: como que son muy pequeños, casi nunca incluyen el nombre del autor, ni el registro o copyright, ni la fecha de creación, se

reproducen a sí mismos y toman el control o modifican otros programas. Los efectos que producen pueden ser destructivos o simplemente molestos: como provocar desde la pérdida de datos o archivos en los medios de almacenamiento de información (diskette, disco duro, cinta), hasta daños al sistema y, algunas veces, incluyen instrucciones que pueden ocasionar daños al equipo. Pueden introducirse en nuestro ordenador de formas muy diversas, mediante disquet, CD-ROM y otras unidades de disco extraíbles, transferencia de ficheros (FTP), grupos de noticias (News o Newsgroups), descargas, correo electrónico y copias ilegales o piratas. "En un estudio realizado por PriceWaterhouseCoopers se detecto que las empresas y organizaciones a nivel internacional reportaron pérdidas de 1.5 trillones de dólares por el concepto de virus" (MARTINEZ,2002:38).

3.2.2 CABALLO DE TROYA

Un caballo de Troya es un fragmento de código que se esconde en el interior de un programa aparentemente inofensivo, y que desarrolla actividades distintas del propósito aparente del programa que le sirve de anfitrión, es incapaz de replicarse (copiarse a si mismo o reproducirse) y su funcionamiento se basa en la ejecución del programa original que lo contiene. Los típicos programas anfitriones de los caballos de Troya son los juegos, editores de texto, hojas de cálculo, e incluso hay algunos casos muy curiosos en los que se esconden en supuestas nuevas versiones de conocidas herramientas antivirus. Son utilizados normalmente para instalar puertas traseras. (LEVIN, 1992:12).

3.2.3 BOMBAS LÓGICAS

Son los programas ocultos en la memoria del sistema o en los discos, o en

los archivos de programas ejecutables con tipo *COM* o *EXE*. Puede tratarse de una pieza de código o de un programa independiente preparado para atacar el sistema cuando se cumplan ciertas condiciones, como lo son: una fecha determinada, se haya arrancado el sistema un número dado de veces ó se pulse una secuencia definida de teclas.

3.2.4 GUSANOS

También conocidos como worms, son programas independientes capaces de autoreplicarse, por lo regular se desarrollan y actúan en entornos de red, se dedican a reproducirse y viajar entre los distintos ordenadores de la misma. Se cargan en la memoria y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borrados los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdida de datos. Su ejecución y distribución se basa habitualmente en errores o debilidades de los protocolos de red o de los programas incluidos en los sistemas operativos que los utilizan. (LEVIN, 1992:14).

3.2.7 BACKDOORS

Las puertas falsas son programas que permiten la entrada en el sistema de manera que el usuario habitual del mismo no tenga conocimiento de este ataque Su objetivo es ofrecer un modo de acceder al sistema esquivando todas las medidas de seguridad establecidas cuando se usa el procedimiento normal. Se trata pues de proporcionar una ruta directa y oculta de acceso al sistema. En algunas ocasiones en el desarrollo de aplicaciones complejas es normal que los

programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc, con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario estas rutinas no se eliminan del programa y proveen accesos o facilidades en su labor si las saben descubrir.

3.2.8 CRIPTOATAQUES

Estos tipos de ataques realizan diferentes hipótesis sobre la cantidad de información que podrá obtener un adversario en relación con el sistema criptográfico (se explica en 3.3.1) que se está atacando y la forma en que el adversario podrá manipular la información para comprometer la seguridad del sistema o de la aplicación.

Se pueden dividir en dos grandes grupos, los pasivos y los activos; los primeros son técnicas como supervisión y análisis del tráfico, que no requieren de una manipulación visible del texto cifrado, texto claro o de otros elementos o procesos del sistema criptográfico, estos ataques suelen estar orientados a comprometer la confidencialidad de los datos.; mientras que los ataques activos implican la falsificación de los mensajes, en la cual comprometen la integridad, la confidencialidad y autenticidad de los datos.(MCMCLURE,2002:672).

3.2.9 HOAX

Son mensajes de correo electrónico, en los que se advierte de un virus inexistente, con el único motivo de asustar a los usuarios, crear rumores o por simple broma. Estos mensajes deben ser ignorados, dado que hacen referencia a

virus que no existen, sus objetivos son: la propagación de una noticia inexistente, que puede causar temor a usuarios inexpertos, la divulgación de las direcciones de correo electrónico de nuestros conocidos, amigos, familiares y contactos de negocios que son enviados y reenviados hasta que alguien las elimine del mensaje original, así como la proliferación de información 'basura' por Internet.

3.2.10 INGENIERÍA SOCIAL

Consiste en mantener un trato social con las personas que custodian datos, indagar en sus costumbres o conocerlas más profundamente para perpetrar posteriormente un ataque más elaborado, incluye desde el reemplazo de identidades confiables hasta la búsqueda en papeleras y basuras de información relevante. Como ejemplo se cita el caso publicado el 16 de mayo del 2003 de la página www.vsantivirus.com, llamado "Un viejo truco de ingeniería social " se presenta un caso en el que un número indeterminado de personas recibía un correo electrónico no solicitado donde se les solicitaba rellenar el formulario de una página web, para ser clientes del servicio BBVAnet (Banco Bilbao Vizcaya Argentaria), se les pedían datos personales, número de tarjeta de crédito, fecha de caducidad e incluso el PIN y esta información iba a dar a la base de datos de los atacantes. De esta manera tan sencilla es que personas ajenas a la información pueden ingresar a ella obteniendo la contraseña de usuarios validos y para el sistema.

3.2.12 HACKER

"Es alguien capaz de manejar con gran habilidad un aparato, no necesariamente un ordenador, con el fin de sacarle más partido o divertirse. Raymond señala cinco características posibles que definen a un hacker:

- Una persona que disfruta al aprender los detalles de un lenguaje o sistema de programación.
- Una persona que disfruta al hacer la programación real en vez de sólo teorizar sobre ella.
- Una persona capaz de apreciar el hackeo de otro.
- Una persona que aprende rápidamente a programar.
- Una persona que es experta en un lenguaje o sistema de programación específico como "un hacker de UNIX"" (RAYMOND,1994:92).

3.2.13 CRACKER

"Es alguien que entra subrepticiamente en el sistema de ordenadores de otra persona, con frecuencia en una red. Un cracker puede hacer esto por ganancias materiales, malintencionadamente, por algún propósito o causa altruista o por el placer del desafío. Parte de estos allanamientos se han emprendido de manera ostensible para destacar las debilidades en el sistema de seguridad de algún sitio" (RAYMOND,1994:58)

3.3 SOLUCIONES DE AUTENTIFICACIÓN

Una vez vistos los ataques a los que se está expuesto, se puede apreciar la necesidad de la autentificación, la cual consiste básicamente en garantizar la originalidad tanto del mensaje como del remitente y del destinatario, es decir, el

mensaje recibido ha de ser realmente el enviado y el remitente/ destinatario han de ser realmente quienes dicen ser y no remitentes y/o destinatarios fraudulentos. Las técnicas de criptografía, esteganografía, funciones hash, firmas digitales y electrónicas son técnicas para conservar los 3 elementos indispensables a tomar en cuenta en la información, integridad, confidencialidad y disponibilidad.

3.3.1 CRIPTOGRAFÍA

Para establecer una comunicación de datos entre dos entidades hacen falta al menos tres elementos básicos: el emisor del mensaje (la fuente), el receptor del mismo (el destino) y un soporte físico por el cual se transfieran los datos (el medio). Hay ocasiones en las que nos interesa que dicho mensaje solamente pueda ser interpretado correctamente por el emisor del mismo y por el receptor al que va dirigido, por lo que la criptología ha demostrado con el tiempo ser una de las mejores técnicas para resolver esta cuestión (www.htmlweb. net/seguridad/cripto/cripto_#.html).

Algunos autores definen a la criptografía (del griego, escritura oculta), como arte, otros como ciencia, y algunos mas como técnica, pero coinciden en que sirve para proteger la confidencialidad, la integridad de los datos, enmascarando los mensajes de manera que no puedan ser entendidos más que por la persona a la que va dirigido el mensaje. El método o sistema empleado para encriptar el texto en claro (datos antes de aplicarle un sistema criptográfico) se denomina algoritmo de encriptación.

Por una parte podemos dividir los sistemas de cifrado según operen sobre bloques o sobre streams (flujos de bits). Los que trabajan sobre bloques dividen la

información a cifrar en bloques de un determinado tamaño y aplican una serie de operaciones sobre ese bloque para producir el criptograma. Los segundos, cifran la información bit a bit. A la palabra o serie base del mecanismo de cifrado se denomina clave de cifrado, y el número de letras que la forman se llama longitud de la clave. Por otra parte, podemos dividir los sistemas de cifrado en simétricos y asimétricos. Los simétricos también son conocidos como llaves privadas, en donde el emisor y el receptor tienen la misma llave para descifrar el mensaje, es decir, un mensaje es encriptado y desencriptado utilizando la misma llave. Y los asimétricos o de llave pública es donde el emisor tiene una llave para encriptar y el receptor tiene otra llave para desencriptar el mensaje. En cuanto a la longitud de las claves, para los sistemas de clave pública como RSA la longitud de clave recomendada es de 1024 bits. Para los sistemas simétricos las longitudes recomendadas son:

- DES: al menos 56 bits, siendo el tamaño óptimo de 128 bits.
- TDES: 168 bits.
- RC4: 128 bits.

Tanto la sustitución como la trasposición son técnicas básicas para ocultar la redundancia en un texto plano y forman la base de muchos de los sistemas criptográficos actuales; entendiendo como redundancia el hecho de que casi todos los símbolos de un mensaje en lenguaje natural contienen información que se puede extraer de los símbolos que le rodean. La redundancia puede ser el punto de partida para un ataque por Criptoanálisis.

La sustitución consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada de posición natural en el

alfabeto. Por ejemplo, fijar una equivalencia entre las letras del alfabeto original y una variación de él, como se muestra en la tabla a continuación.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

La trasposición en cambio consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada de posición en el orden del mensaje. Por ejemplo, si establecemos la siguiente regla de cambio en el orden de las letras en el texto: la frase "HOLA MUNDO" nos quedaría "OUDL HOAMN".

la letra	1	2	3	4	5	6	7	8	9
pasa a ser la	5	1	4	7	8	2	9	3	6

3.3.1.1 FIRMAS DIGITALES Y ELECTRÓNICAS

La división de las claves en pública y privada dan cabida a la existencia de lo que se ha venido a conocer como firmas digitales; que son un método de la criptografía asimétrica o de clave pública. Actualmente en el mundo de las computadoras se manejan dos tipo de firmas que vienen a sustituir a la firma común que todos conocemos que es la realizada en papel y estas firmas son la digital y la electrónica, cumplen las mismas propiedades que la firma manual; hablemos de la primera.

La firma digital es una cadena de datos creada a partir de un mensaje, suelen usarse en comunicaciones en las que no existe una confianza inicial total

entre los comunicantes, para autentificar mensajes, para validar compras por Internet, para realizar transferencias de fondos bancarios y para otras transacciones de negocios. La idea principal de la firma digital es que solamente el emisor la pueda producir y además se pueda demostrar que, efectivamente, es él quien la produce, también asegura el no repudio (que quien firma no niegue quien es), asimismo proporciona integridad de datos, ya que si el documento fuera accedido y modificado en el camino el resumen del documento cambiaría totalmente. El algoritmo que se utiliza para obtener el resumen del mensaje debe cumplir la propiedad de que cualquier modificación del mensaje original, por pequeña que sea, dé lugar a un resumen diferente. La firma digital de un usuario no es siempre la misma secuencia de bits, sino que depende del mensaje firmado. "El proceso de firma es el siguiente:

- El usuario prepara el mensaje a enviar.
- El usuario utiliza una función hash (se explica en el 3.3.1.1.1) segura para producir un resumen del mensaje.
- El remitente encripta el resumen con su clave privada. La clave privada es aplicada al texto del resumen usando un algoritmo matemático. La firma digital consiste en la encriptación del resumen.
- El remitente une su firma digital a los datos.
- El remitente envía electrónicamente la firma digital y el mensaje original al destinatario. El mensaje puede estar encriptado, pero esto es independiente del proceso de firma.
- El destinatario usa la clave pública del remitente para verificar la firma digital, es decir para desencriptar el resumen adosado al mensaje.

- El destinatario realiza un resumen del mensaje utilizando la misma función resumen segura.
- El destinatario compara los dos resúmenes. Si los dos son exactamente iguales el destinatario sabe que los datos no han sido alterados desde que fueron firmados."

(http://revista.robotiker.com/articulos/articulos45/pagina1.jsp)

Ahora veamos a lo que se refiera la firma electrónica, no es otra cosa que una técnica para verificar que un documento ha sido realizado por el poseedor de determinado algoritmo (lo que se conoce como llave privada), que se asocian inequívocamente a un documento electrónico; en realidad es simplemente un termino legal a la firma digital para asegurar que el titular de la llave privada es quien dice ser, e impedir que niegue posteriormente haber efectuado la declaración de voluntad. Firmar electrónicamente consiste en realizar una operación matemática que convierte el documento original en otro nuevo, cuyos caracteres guardan con el original una relación matemática basada en el algoritmo de cifrado Se debe acudir a un Prestador de Servicios de Certificación quien generará las claves pública y privada, y nos entregará la tarjeta o disquete que contenga esta clave privada, así como la aplicación informática o programa necesario para su uso, que se ha de instalar en nuestra computadora.

La clave privada por lo regular se encuentra incorporada en tarjetas inteligentes, que incorporan un chip que contiene información de su titular, la entidad que la ha emitido y el conjunto de bits en que consiste la clave, estas tarjetas son de uso personal e intransferible por estar protegida por un código secreto que sólo su titular conoce.

"La diferencia principal entre ambos tipos de firma, radica en el sistema criptográfico que se ha utilizado: para las firmas electrónicas en general se utilizan un sistema criptográfico simétrico o de clave secreta; mientras que para la firma digital el método utilizado es asimétrico o de clave pública." (htttp://revista.o botiker.com/articulos/articulos45/pagina1.jsp).

3.3.1.1.1 FUNCIÓN HASH

Al querer cifrar un documento extenso que queremos firmar digitalmente implica una pérdida de tiempo ya que los medios de encriptación de llave pública son lentos, pues precisan un gran proceso de cómputo, para solución de este problema aparecen las funciones Hash, que son unas funciones matemáticas que realizan un resumen del documento a firmar, su forma de operar es comprimir el documento en un único bloque de longitud fija, bloque cuyo contenido es ilegible y no tiene ningún sentido real, son irreversibles, es decir, que a partir de un bloque comprimido no se puede obtener el bloque sin comprimir, estas funciones son de dominio público. De esta manera se pude decir que las funciones Hash deben cumplir con las siguientes condiciones:

1. Transformar un texto de longitud variable en un bloque de longitud fija.

2. Ser irreversibles.

3. Conocido un mensaje y su función Hash debe ser imposible encontrar otro mensaje con la misma función Hash. Esto se debe cumplir para evitar que los criptoanalistas firmen un mensaje propio como si fueran otra persona.

4. Es imposible inventar dos mensajes cuya función Hash sea la misma.

El mecanismo de las funciones Hash es el siguiente:

1. El emisor Y aplica una función hash conocida al documento, con lo que obtiene un resumen hash del mismo.
2. Encripta (refiriéndonos a encriptación como un conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas) dicho resumen con su clave privada.
3. Envía al receptor X el documento original plano y el resumen hash encriptado.
4. El receptor X aplica la función hash al resumen sin encriptar y desencripta el resumen encriptado con la llave pública de Y.
5. Si ambos coinciden está seguro de que ha sido Y el que le ha enviado el documento. Si no coinciden, está seguro de que no ha sido Y o de que el envío ha sido interceptado durante el medio de envío y modificado.

Las funciones hash más conocidas y usadas son: MD2, MD4, MD5, SHA-1, RIPEMD-160.

3.3.2 ESTEGANOGRAFÍA

El término "esteganografía", que viene del griego stegos (cubierta), significa "escritura oculta" o "escritura encubierta" y es el arte o ciencia de comunicar de manera oculta un mensaje, camuflando la información entre otro conjunto de datos para que pase desapercibida, esto es, enviar mensajes invisibles en mensajes visibles. La esteganografía a diferencia de la criptrografía intenta ocultar un mensaje de forma que no despierte la más mínima sospecha. Una de las

primeras y sencillas técnicas esteganográficas era la tinta invisible que consistía en ocultar los mensajes escritos con zumo de limón en un papel en el que al calentarlo aparece lo escrito. Hoy en día las técnicas esteganográficas más comunes en informática se basan en ocultar la información en archivos gráficos o archivos de sonido, mezclando los bits del mensaje original entre los bits del archivo gráfico o de sonido

Cuando se oculta información en archivos de imágenes se aprovechan los bits menos significativos de los colores para introducir en ellos la información aunque tiene la desventaja de ser muy sensible al encontrarse en los bits menos significativos, ya que puede ser destruida por los siguientes motivos:

- Aplicación de cualquier filtro
- Cambios en brillo o contraste
- Un cambio de tamaño en la imagen
- Cualquier trazo o cambio en la imagen
- Recortar la imagen

Cuando se usan archivos de sonido la información oculta aparece como ruido de fondo, pudiendo confundirse fácilmente con una simple grabación con algo de ruido.

Para camuflar archivos hace falta tener un programa capaz de ocultar los datos, estos programas constan de una parte en la cual se ocultan los datos y otra que sirve para sacarlos, su uso es muy sencillo y algunos ofrecen la posibilidad de incluir un password de descifrado, actualmente existen tres software muy conocidos que son el Camuflage, el S-tools y el HIM.

3.4. ANTIVIRUS

Son programas diseñados por compañías con el firme propósito de contraatacar a los virus, siendo estos capaces de inmunizar o eliminar el virus de la computadora. Algunos programas antivirus intentan eliminar los virus detectados, pero a veces los resultados no son satisfactorios. En caso de ser atacado, se obtienen resultados más fiables desconectando la computadora infectada, arrancándola de nuevo desde un disco flexible protegido contra escritura, borrando los archivos infectados y sustituyéndolos por copias de seguridad de archivos legítimos y borrando los virus que pueda haber en el sector de arranque inicial, por lo que son importantes los respaldos, de no realizarlos, la información puede darse por pérdida. Para el correcto funcionamiento de los antivirus deben ser actualizados y configurados adecuadamente, ya que de no ser de esta manera es difícil que lleguen a cumplir con su objetivo.

3.5 REDES Y SEGURIDAD PERIMETRAL

Una red es un conjunto de computadoras independientes llamados host que son capaces de comunicarse electrónicamente. Básicamente consisten en compartir recursos, y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. Se clasifican principalmente en dos tipos, según su extensión: LAN (Local Area Network) y WAN (Word Area Network), la primera es una red área local, por ejemplo la interconexión de todas las máquinas dentro de una empresa o edificio y la segunda es la red de área mundial, que es el conjunto de varias LAN´s, el ejemplo mas conocido es Internet. Los componentes físicos para la formación de una red

son: tarjeta de red (Network Interface Cards), cable de red, tranceptor, hub, repetidor, puente, switch y router, utilizándose cada uno en diferentes casos. Para la identificación de cada equipo entre si conectado en una red es por medio de la dirección IP, que es un conjunto de números asignados por el administrador de la red, y también se pueden identificar por el número de la tarjeta de red llamada MAC por sus siglas en ingles. Otra variante del tipo de redes es la Intranet, que es una intercomunicación privada basada en tecnología Internet que posibilita a la empresa un canal exclusivo de comunicación intra-empresarial por el que pueden organizar, compartir y transmitir información entre los miembros de una organización.

Generalmente el lugar donde se concentran ó se deben de concentrar los servicios informáticos, es en el centro de computo, también llamado SITE, es aquí donde se realiza el procesamiento automático de la información de una entidad, además es responsable de centralizar, custodiar y procesar la mayoría de los datos con los que opera la compañía, prácticamente todas las actividades de los demás departamentos se basan en la información que les proporciona dicho centro.

Unas medidas que se pueden tomar para protegerse de los ataques informáticos en una red, son los Firewall (muros de fuego) ó las Redes Privadas Virtuales, ambas incluyen tanto software como hardware y determinan cierta área de restricción o de trabajo; si son configurados adecuadamente, dan resultados muy satisfactorios, veamos en que consiste cada unos de ellos.

3.5.1 FIREWALL

Llamados en español muros de fuego, es cualquier equipamiento de software o hardware utilizado para separar una máquina o una subred del resto de la red para protegerla de intrusiones externas o personas internas ajenas a la información que pueda suponer una amenaza a la seguridad. La zona protegida se llama "perímetro de seguridad" y la protección se realiza separándola de una zona externa, no protegida, llamada zona de riesgo. Su objetivo es mantener a los miembros de esa LAN al margen de las malignas intenciones de Internet, y garantiza que la información recibida de una fuente externa no contenga virus. Un problema de los cortafuegos es que restringen mucho el acceso a la Internet desde la red protegida, pero este mismo como ventaja, permite que los trabajadores no pierdan el tiempo y produzcan en su jornada de trabajo. Los Firewall protegen contra todos los ataques que pasan por el, obviamente, si esta correctamente configurado; por lo único que identifican a un usuario son por el número IP asignado a su estación de trabajo.

Para poder acceder a Internet por detrás de un cortafuego se requiere de un servidor Proxy, que es un programa que permite o niega el acceso a una aplicación determinada dos redes, lo importante de ellos es que bien configurados, son completamente seguros, no dejan que nadie entre a través de ellos. Los clientes Proxy se comunican sólo con los servidores Proxy, que autorizan las peticiones y las envían a los servidores reales, o las deniegan y las devuelven a quien las solicitó, funcionan abriendo un socket en el servidor y permitiendo la comunicación con la Internet a través de él.

3.5.2 VPM (VIRTUAL PRIVATE NETWORK)

La red privada virtual utiliza en parte recursos de infraestructuras públicas o compartidas para establecer conexiones seguras entre dos o mas puntos, pero funcionan como redes restringida; normalmente esta red pública es Internet. Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. La técnica de tunneling consiste en que un paquete de datos pase de un extremo a otro de manera segura por medio de un "túnel". En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a su host remoto las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet público. En ocasiones puede ser interesante que la comunicación que viaja por el túnel establecido en la red pública vaya encriptada para permitir una mayor confidencialidad.

Las principales ventajas de usar una VPN es su gran cobertura y que permite disfrutar de una conexión a red con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de un ordenador en esa red privada, pudiendo acceder a la información publicada para esa red privada: bases de datos, documentos internos, etc. a través de un acceso público y además la reducción de costos en los sistemas de comunicación de la empresa. Entre los inconvenientes podemos citar una mayor carga en el host de una VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos. También se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al

cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas.

Con este capítulo ahora se comprende la importancia de la seguridad informática, así como los riesgos que puede tener por medio del software, creados por personas que buscan diversión, o realmente quieren provocar daños a la empresa; que éstos pueden ser prevenidos por algunas técnicas como lo son las de autentificación, instalación de antivirus, realización de una red privada virtual y /o la utilización de firewalls. Cabe mencionar que cualquier medida que sea tomada en contra de la vulnerabilidad de los sistemas debe de estar correctamente administrada, por que de no ser así, no tendrá los efectos esperados de protección, también se debe de tomar en cuenta otros aspectos para la seguridad, los cuales serán tratados en el capítulo "División y Legalidad de la Seguridad Informática".

CAPÍTULO IV

DIVISIÓN Y LEGALIDAD DE LA SEGURIDAD INFORMÁTICA

La seguridad en cuestión informática es un tema bastante extenso e interesante que día con día está teniendo mas importancia, aunque hablar de que se tiene una seguridad total, es casi un sueño; los empresarios se están dando cuenta de la vulnerabilidad de los sistemas, conforme más personal de la organización tiene acceso a mayor poder de cómputo, ésta se vuelve cada vez más difícil y compleja, por lo que la seguridad informática se divide en tres elementos para su estudio. En este capítulo también se mencionan las leyes que protegen a los autores para penalizar la piratería.

4.1 DIVISIÓN DE LOS ELEMENTOS DE LA SEGURIDAD INFORMÁTICA

"La seguridad tiene tres aspectos interrelacionados: físicos, lógicos y de conducta, los cuales deben operar en conjunto si se quiere que los estándares de calidad en seguridad permanezcan altos" (KENDALL et al, 1991:818). "La regulación depende de las herramientas de tecnología informática, de políticas y procedimientos y del factor humano" (ORIHUELA, 2002:31). Esta división puede dar lugar a conservar la integridad, confidencialidad y disponibilidad de la información de una forma mas clara.

4.1.1 SEGURIDAD FÍSICA

"La seguridad física se refiere a las instalaciones de cómputo, a nuestro equipo y al software, a través de elementos físicos" (KENDALL et al, 1991:818). "Establecer políticas, procedimientos y prácticas para evitar las interrupciones

prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc" (ECHENIQUE, 1992:109).

En el siguiente apartado son mencionados y explicados brevemente los puntos que se toman a consideración en lo que se refiere a seguridad física, tanto Leonard H. Fine, Kendall Kennett B y Echenique José Antonio coinciden en lo siguiente:

- Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.
- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible como un UPS (Uninterrupted Power Supply) ó No-Break, tanto en la computadora como en la red y los equipos de teleproceso. Los apagones son también una amenaza constante y muy grave, pues tienden a fundir y dañar el sistema de la computadora, lo que puede derivar en la pérdida de archivos, entre otras cosas. "En términos generales una computadora personal recibe en promedio 20 impactos de energía diarios, causados básicamente por las variaciones de voltaje; que van afectando los componentes internos y reduciendo su vida útil." (RAMIREZ, 2002:21).
- En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.

- Acceso controlado a la sala de cómputo, que puede ser por medio de lectores de tarjetas, gafetes o de un sistema de control de entrada y salida por firma de usuarios. Se debe de registrar todo el personal que sea ajeno al área, hasta el personal de limpieza y ser vigilados en sus actividades durante el acceso.
- Contar con alarmas de fuego y humo; deben ser capaces de detectar los distintos tipos de gases que desprendan los cuerpos en combustión, deben ser colocados cuidadosamente en relación con los aparatos de aire acondicionado, ya que los conductores de éste puede difundir el calor o el humo y no permitir que se active el detector. Deben ser instalados en la sala de cómputo, junto a las áreas de oficina y en el perímetro físico de las instalaciones.
- Las computadoras no se deben colocar en sótanos o en las áreas de la planta baja, donde el riesgo de inundación sea alto. Deben instalarse, si es el caso, detectores de agua o de inundación, así como bombas de emergencia para resolver inundaciones inesperadas.
- Respaldos y almacenamiento. Se debe guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad en un área a prueba de fuego e inundaciones. En caso de pérdida de la información por cualquier motivo que este haya sido se recurre a los respaldos para la recuperación. Los respaldos pueden ser de diferentes tipos como son: jerárquicos, Hot Back up, Cold Back up, respaldo a distancia, incrementales, respaldo por medio de redes SAN (Storage Area Network) y respaldo por dispositivos NAS (Network Atached Storge). La política mas tradicional es que pueden realizarse los

respaldos totales los fines de semana o incrementales diarios. En caso de haber una falla se cargan primero los respaldos totales, encima de estos los incrementales diarios y después se aplican los respaldos en línea, si es que se tienen, de esta manera solo se pierde el periodo entre el último respaldo semanal y la falla (VIADAS,2002:22).

- Piso falso con elevación de 40 cm, cableado aéreo, falso plafón, canaletas externas para cableado, flujo de aire de 15 ft^3/min. por persona en ocupación constante, procurar iluminación y atmósfera adecuada para el personal y evitar luz solar directa. Temperatura con un rango ideal de 18 a 22 ° C y humedad relativa de 50% mas- menos 10% para evitar condensación, como electricidad estática para el área de los servidores. (Administración de Centros de Computo, 2003).
- También se incluye la ergonomía, que es una disciplina a través de la cual se ayuda a promover sanas posturas corporales para realizar las diferentes tareas diarias, reduciendo así los riesgos de lastimaduras o de dolores crónicos.

4.1.2 SEGURIDAD LÓGICA

. Hace falta dar al factor humano el peso que tiene en temas relacionados con la protección de la información y considerar la importancia de crear y exigir el cumplimiento de políticas de prevención, por lo que la seguridad lógica tiene que ver con los password y con la asignación de las políticas de seguridad para los usuarios dentro de la empresa y políticas para los que accedan de forma externa, como en el caso de una auditoria informática.

Password: Son conocidos por los usuarios como contraseñas o códigos de autorización, para ingresar al sistema, los usuarios suelen olvidarla por lo que la pegan en un papelito junto a su PC para poderla recordar, la comparten con otros usuarios corriendo el riesgo de que dañen al sistema con su cuenta personal.

Políticas de Seguridad: "Las políticas deberán basarse en los siguientes pasos:

- Identificar y seleccionar lo que se debe proteger (información sensible).
- Establecer niveles de prioridad e importancia sobre esta información.
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles.
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red.
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla.
- Implementar respuesta a incidentes y recuperación para disminuir el impacto." (NAVA,2002: 23).

Para la fijación de las políticas se debe basar en los siguientes principios:

1) "Responsabilidad individual: las personas son responsables de sus actos. El principio implica que la gente que está plenamente identificada debe estar consciente de sus actividades, debido a que sus acciones son registradas, guardadas y examinadas.
2) Autorización: son reglas explícitas acerca de quién y de qué manera puede utilizar los recursos.
3) Mínimo privilegio: la gente debe estar autorizada única y exclusivamente para acceder a los recursos que necesita para hacer su trabajo.

4) Separación de obligaciones: las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. La separación de obligaciones funciona mejor cuando cada una de las personas involucradas tiene diferentes actividades y puntos de vista.

5) Auditoría: el trabajo y los resultados deben ser monitoreados durante su inicio y hasta después de ser terminado. Una revisión de los registros, donde se guardan las actividades, ayuda para realizar una reconstrucción de las acciones de cada individuo.

6) Redundancia: el principio de redundancia afecta al trabajo y a la información. Múltiples copias son guardadas con importantes registros y dichas copias son frecuentemente almacenadas en diferentes lugares.

7) Reducción de Riesgo: Esta estrategia debe reducir el riesgo a un nivel aceptable,

haciendo que el costo de la aplicación sea proporcional al riesgo" (www.geocities.com/fundamentosdeseguridad/SEMINARIO/TEMA_6.htm).

Algunos ejemplos de políticas son:

- *Procedimientos de compra.* Políticas escritas que cubran la forma en que los empleados solicitan software, personas responsables de la compra, proveedores autorizados, procedimientos de instalación, políticas personales y eliminación de activos de software.
- *Planeación de programas de desastre y su prueba.* Leonard H. Fine dice al respecto, los programas de planificación contra desastres tendrán que definir en forma detallada los arreglos que se hagan para cada caso, la organización y las responsabilidades para aplicarlos y un marco de trabajo para la

iniciación y aplicación paso por paso de los procedimientos de recuperación. Los tipos de desastres que pueden ocurrir son:

- Destrucción completa o parcial de los recursos centralizados y descentralizados de procesamiento de datos
- Destrucción o mal funcionamiento de los recursos ambientales destinados al procesamiento centralizado de datos.
- Destrucción total o parcial de los procedimientos manuales del usuario, utilizados para la captura de la información de entrada.
- Interrupción por huelga
- Pérdida del personal de cómputo clave.

- *Organización y división de responsabilidades.* Es la determinación del organigrama, analizar cuales son los sistemas con lo que trabaja cada persona, de esta manera se podrán establecer las reglas de acceso exclusivamente de acuerdo a las necesidades de operación de cada persona.
- *Soporte técnico.* Formar la conciencia en el usuario en que debe de modificar constantemente su password y que no sea identificable fácilmente, información de virus y facilitar la actualización de antivirus a los usuarios.
- *Seguridad en el manejo de información.* Para controlar este tipo de información se debe:

1) Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.

2) Sólo el personal autorizado debe tener acceso a la información confidencial.

3) Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.

4) Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.(http://www.monografias.com/trabajos/maudisist/maudisist.shtml) .

4.1.2.1 POLITICAS DE CONTRASEÑAS

Estas políticas, quizás sean de las mas importantes de la empresa, ya que con ellas se pueden evitar ataques humanos y para los hackers ó crackers, la tarea de adivinar passwords, se les complicaría. A continuación se enlistan las políticas que se deben seguir en la SAT, publicadas en la propia Intrasat (Intranet de SAT).

1. Cada clave de acceso asignada contará con una contraseña.
2. La contraseña asignada será personalizada y conocida únicamente por el usuario propietario.
3. La responsabilidad de pérdida o divulgación de las contraseñas será atribuible absolutamente a los usuarios propietarios de las claves de acceso correspondientes.
4. Todas las contraseñas deberán ser de al menos 8 (ocho) caracteres.
5. La contraseña debe ser lo suficientemente difícil de adivinar para los ajenos y al mismo tiempo fácil de recordar para el usuario propietario.
6. Si las contraseñas o los NIP son generados por un sistema, al dar de alta una clave; dichas contraseñas deben ser substituidas de manera inmediata por una contraseña personalizada por el usuario propietario.
7. Si los sistemas lo requieren, el usuario está obligado a cambiar substancialmente sus contraseñas cada que sea establecido por alguna función automática.

8. Si los sistemas no están programados para requerimientos automáticos de cambio de contraseña, el usuario deberá implementar un plan personal de cambio de contraseñas al menos una vez cada 30 (treinta) días.
9. Las aplicaciones que tengan la función automatizada controlarán que después de tres intentos consecutivos al entrar una contraseña incorrecta, la clave de usuario podrá ser:
    - Suspendida hasta que sea restablecida por el administrador.
    - Inhabilitada temporalmente por no menos de 5 minutos.
    - Desconectada en el caso de que se presuman conexiones con una red externa o a equipos sin autorización.
10. Los usuarios no deben definir una contraseña nueva de manera idéntica o substancialmente similar a la contraseña que venían utilizando previamente.
11. Composición alfanumérica y uso de caracteres especiales obligatoria de la contraseña.
12. Todas las contraseñas deberán contener caracteres alfabéticos, numéricos y/o caracteres especiales según la selección del usuario, pero necesariamente deberá existir la combinación, es decir no debe ser en su totalidad alfabético ni en su totalidad numérico. Se recomienda utilizar 4 caracteres alfabéticos, 2 numérico y 2 signos especiales (“., ?, ,, /, etc.).
13. Se permite el uso de 3 caracteres especiales como máximo.
14. En el ambiente UNIX no se recomienda el uso de letras mayúsculas
15. Los usuarios tienen prohibido el uso de contraseñas cíclicas. Llámese cíclicas a combinar un cierto número de caracteres que no cambian y otro cierto número de caracteres que se modifican periódicamente de forma predecible. Tradicionalmente relacionados con el mes en curso, el nombre de un

proyecto, la denominación de un área funcional o algún otro factor de fácil deducción.

Por ejemplo:

Contraseña~~1999~~

Contraseña~~2000~~

(http://intrasat/Dgti/dgti.htm)

4.1.3 CONDUCTA DE USUARIO

Actualmente se ha tomado conciencia de la creciente dependencia de la integridad, estabilidad y lealtad del personal para la seguridad de la información que manejan en la empresa. "La conducta interna de los miembros de la organización es decisiva para el buen éxito de los esfuerzos humanos" (KENDALL et al, 1991:819). Además se sabe que " Mas del 70 % de las violaciones e intrusiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización" (NAVA,2002:22), por otra parte Fabiola González en el articulo "Proteger la información es responsabilidad de todos" menciona el mismo porcentaje y también por causa del personal interno, agregando que se debe a un problema de ética laboral y de la falta de actividades que ayuden a generarla a nivel empresarial.

El 70% es una cifra muy alta por lo que se tiene que tomar en cuenta los siguientes puntos para la seguridad respecto a un usuario y poder disminuir este porcentaje:

- Selección y reclutamiento. Esto tiene como objetivo verificar que los intereses de la persona se ajusten con los de la empresa y de esta manera puedan entender por que se debe cumplir con las políticas de seguridad.
- Contratación del personal. "En la política de contratación las características mas importantes son: verificación de referencias y antecedentes de seguridad, pruebas psicológicas y exámenes médicos" (KENDALL et al, 1991:48).
- Las Políticas deben estar escritas de tal forma que sean perfectamente entendibles por las personas a quienes son dirigidas, ser distribuidas y actualizadas, de manera que los empleados estén enterados de que estas existen y de que hay que cumplirlas.
- Supervisión de la conducta con el objetivo de verificar que se sigan las políticas y corregir posibles conductas que después puedan ser perjudiciales a la empresa.
- Política sobre permisos. Es importante para asegurar que el personal expuesto al estrés descanse periódicamente de manera apropiada (FINE, 1988,50).
- Motivar al personal da lugar a que este se encuentre contento en la empresa y quiera seguir cumpliendo con los objetivos de la empresa cumpliendo con las políticas asignadas a éste.

4.2. LEGALIDAD

Los crímenes cibernéticos son los mismos delitos "tradicionales", siendo el instrumento lo único que cambia. "Existen delitos claros y precisos como el hackerismo, o la infección binaria que, por las características de la materia penal,

no pueden tener basamento en su persecución y castigo con los mismos silogismos jurídicos que los del mundo real y tradicional" (DE ANDA, 2002:88).

4.2.1 PIRATERÍA DE SOFTWARE

La piratería es un negocio multinacional que mueve inmersos recursos económicos. Al hablar de piratería de software debemos entender que es ilegal (sin licencia) utilizarlo o vender este software. El uso de programas piratas o duplicados de computación no solo conlleva múltiples problemas para el usuario, tales como falta de garantía, de soporte técnico, incompatibilidad entre programas, actualizaciones de productos, daño de reputación de la empresa, además del riesgo de adquirir virus informáticos que dañen ordenadores o la red, sino que también se incurre en un delito plasmado en las leyes mexicanas, con multas desde $400,000 pesos o penas que van desde 3 a 10 años de cárcel. (MOLINA,2002:66). El pirata no contrata a nadie, no emplea desarrolladores, publicistas o mercadólogos, solo se dedica a copiar y a vender, por lo que se dejan de pagar impuestos de 180 millones de dólares para el gobierno dejando de generar 3 mil empleos directos".(MOLINA,2002:94)

La piratería se puede presentar de las siguientes formas:

- Al adquirir una PC se vende con software ilícito preinstalado por parte de los distribuidores de computadoras.
- Falsificación tanto del software como del empaque y después es distribuido como legal.
- Uso de Internet para descargar o distribuir software no autorizado.
- Distribución inapropiada. Es el software distribuido impropiamente con descuentos especiales de licencias, ya sea a clientes que compran altos

volúmenes, fabricantes de computadoras o instituciones académicas o gubernamentales, el cual es distribuido posteriormente a otras personas o entidades que no tienen licencias o que no califican para este tipo de descuentos.

"Algunos de los casos mas celebrados de infecciones víricas han sido asociados con la piratería del software. También algunos de los virus mas mortales han sido copias modificadas de aplicaciones muy conocidas."(LEVIN, 1992:83).

4.2.2.1 WAREZ

El costo elevado del software legal a dado lugar a un fenómeno llamado Warez, que son versiones completas de los paquetes de software y sistemas operativos mas populares del mercado puestos en Internet; aplicaciones plenamente operativas gracias a un crack (programa que hacer saltarse la seguridad del software). Muchas de las páginas de warez se financian por banners (publicidad de otras páginas) y enlaces (automáticos en su mayoría), que mientras se esta bajando una utilidad se empiezan a abrir cerca de 15 o mas ventanas del navegador, con el riesgo de que muchas de ellas pueden incluir un script (programa que realiza una acción) que nos descarga un marcador que se auto instala, cortando la conexión a Internet y conectándonos a un número internacional y además de que se puede adquirir virus en las utilidades que se están bajando (VAL, 2001:310).

4.2.2 LEY DE LA PROPIEDAD INTELECTUAL

Es el conjunto de derechos patrimoniales de carácter exclusivo que otorga el estado por un tiempo determinado, a las personas físicas o morales que llevan a cabo la realización de creaciones artísticas o que realizan invenciones o innovaciones y de quienes adoptan indicaciones comerciales, pudiendo ser éstos, productos y creaciones objetos de comercio.

Las partes que conforman a la propiedad intelectual son: propiedad industrial y propiedad autoral ó derecho de autor (www.impi.gob.mx/web/docs/bienvenida/index_preguntas.htmlción),que se explicarán a continuación.

4.2.2.1. LEY DE DERECHOS DE AUTOR

Constituido por 429 artículos y tiene por objeto la protección de los derechos de los autores, de los artistas intérpretes o ejecutantes, así como de los editores, de los productores y de los organismos de radiodifusión, en relación con sus obras literarias o artísticas en todas sus manifestaciones, sus interpretaciones o ejecuciones, sus ediciones, sus fonogramas o videográmas, sus emisiones, así como de los otros derechos de propiedad intelectual.

4.2.2.2. LEY DE LA PROPIEDAD INDUSTRIAL

Constituido por 229 artículos y regula, otorga patentes de invención, registra modelos de utilidad, diseños industriales, marcas, y avisos comerciales, publica nombres comerciales, declara protección de denominaciones de origen, y regulación de secretos industriales, previene los actos que atenten contra la propiedad industrial o que constituyan competencia desleal relacionada con la

misma y establece las sanciones y penas respecto de ellos. (http://www.imp i.gob.mx/web/docs/marco_j/3w002101.htm).

En este capitulo se vio que para lograr un buena calidad de la seguridad se debe de trabajar en tres aspectos importantes que son: seguridad física, lógica y conducta del ser humano. La seguridad física, como su nombre lo dice se refiere al aspecto tangible laboral, el lógica, es lo intangible como el manejo de la información y en lo que cabe con la conducta abarca las políticas de contraseñas y demás políticas que deben de tomarse en cuenta para tener reducir la vulnerabilidad de los sistemas informativos. Así como también se observo la legalidad del software y perjuicios que puede tener una empresa, ya que hay leyes que respaldan a los autores del software.

Con la información recopilada hasta este capitulo se puede dar continuidad a la siguiente parte que es la investigación documental, para poder aceptar o rechazar la hipótesis planteada y poder cumplir con los objetivos marcados.

CAPITULO V

CASO PRACTICO "ANTECEDENTES Y ANÁLISIS DE LA ADMINISTRACIÓN LOCAL DE RECAUDACIÓN"

En el presente capítulo primeramente se retomarán los antecedentes generales de la empresa de estudio, para situarnos y conocerla un poco, para posteriormente continuar con el análisis de las encuestas aplicadas y la entrevista aplicada al encargado de informática y de esta manera poder detectar los problemas y realizar una propuesta.

5.1 ANTECEDENTES GENERALES DEL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA

Mediante el decreto del 25 de enero de 1993 desaparecen las Coordinaciones de Administración Fiscal, las Administraciones Fiscales Federales y las Oficinas Federales de Hacienda, constituyéndose las Administraciones Regionales de Recaudación; de Auditoría Fiscal Federal; Jurídica de Ingresos y de Aduanas, así como las Administraciones Locales de Recaudación; Auditoría Fiscal Federal y Jurídica de Ingresos, con el propósito de promover una administración tributaria más eficiente que fortaleciera la recaudación, impulsara la fiscalización, aumentara la presencia fiscal, diversificara los controles y ampliara las fuentes de información.

El 30 de junio de 1997 se publican en el Diario Oficial de la Federación reformas en las que se establece la desincorporación de la Subsecretaría de Ingresos, con excepción de la Dirección General de Política de Ingresos, para

conformar el Servicio de Administración Tributaria con carácter de órgano desconcentrado de la Secretaría. De 1997 a la fecha han transcurrido cambios y desaparecido algunas unidades, las Administraciónes Locales de Recaudación no han tenido cambios, básicamente la estructura orgánica actual de la Secretaría de Hacienda y Crédito Público, queda conformada como se muestra en la figura 1.

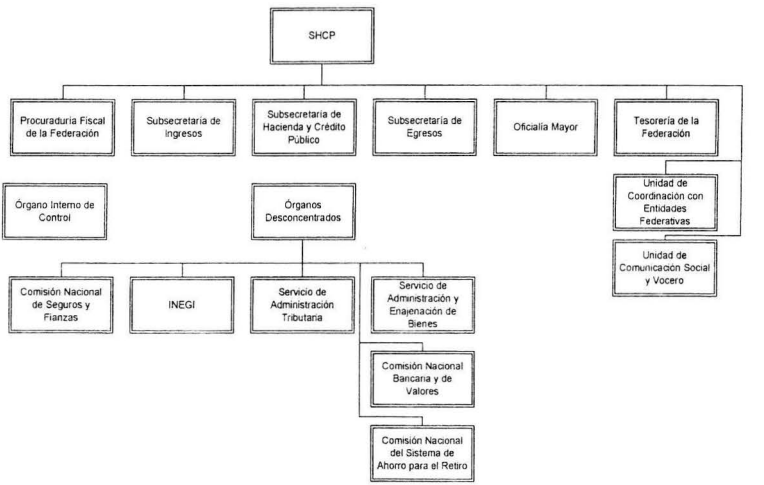


Figura 1. Fuente: http://www.shcp.gob.mx/index01.html

En la figura 1 se ubica el Servicio de Administración Tributaria como un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público. La Administración Local de Recaudación Uruapan dependiente del SAT, se encuentra ubicada en Ocampo #2 colonia Centro, con un número de personal, aproximadamente, de 57 trabajadores. La ALR de Uruapan atiende,

principalmente, a los municipios de: Apatzingán, Lázaro Cárdenas, La Piedad, Los Reyes, Sahuayo, Uruapan, Zamora, que se muestran en la figura 2.

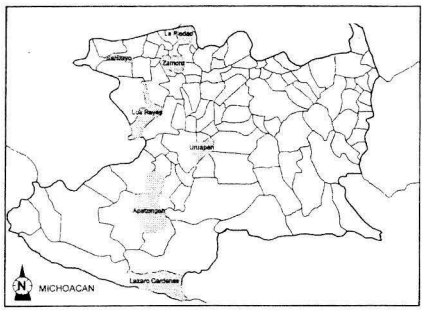


Figura 2. http://99.90.4.180/Presidencia/presidencia.htm

5.1.1. Software y Hardware de la Administración Local de Recaudación

La principal función de la Administración Local de Recaudación, como su nombre lo indica, es la recaudación de impuestos, para poder contar con recursos económicos y beneficiar a la sociedad. Por lo que requieren de software y hardware para lograrlo, dentro del software utilizan los siguientes programas.

- SQL cliente 6.5
- Esperant
- SIR Sistema Integral de Recaudación
- Dario
- Guardian
- Boveda expres
- Trend para server
- Informix cliente
- Tuxedo cliente
- Omniguard

- VDIMM cliente
- Impresión de declaraciones electrónicas
- Sistema de recepción de tramites
- Subsistema de tarjeta tributaria
- Sistema cuenta única nacional

En cuanto a Hardware se tienen las siguientes características de los servidores con sus respectivos servicios que realiza:

Servidor HP

Modelo HP Netserver LH4

524 MB en RAM

Procesador X86 Family6 Modelo 3

Steping 4AT/AT compatible

Disco duro de 18GB

Disco de 3.5"

CD-ROM

DDS Capacidad de GB por media de HPC1537A

Servicios:

Windows Nt 4.0

Price service pack 6ª

SITE Guardian configuración de sortorder de SQL

Subsistema VDIMM (validación de dispositivos numéricos)

Bodega express

SQL Server 6.5 Interprice

Parche SQL 5ª de SQL

Antivirus TREN para Server

Servidor COMPAQ

Modelo Proliant 1600

Disco duro de 18GB

DDS Capacidad de GB por media de HPC153A

Disco de 3.5"

CD-ROM

264 MB en RAM

Procesador X86 Family 6 Modelo 5

Antivirus TREND para Server

Servicios:

Sistema Dario (Altas de contribuyentes)

Servidor HP 9000 K370

2 Disco duros de 20GB c/u

Sistema Operativo 10.2 Unix

Informix 7.3

BD de toda la información

SIR (Sistema Integral de Recaudación)

DLT Sistema de respaldo Modelo 1/87000

Unidad de respaldo DDS

CD-ROM

Consola

Servidor de correos COMPAQ

Disco duro de 1 Gb

Procesador Pentium I a 233 MHz

Disco de 3.5"

Unidad de CD-R 24X

Con respecto a los dispositivos de red cuentan con la siguiente tecnología:

- Sistema VPN
- Enlace fibra óptica (Por ahora no se utiliza, pero se tiene)
- Router Cisco 3600 Martis DXX
- Router VAYNETWORKS Access Snack Bode
- Sistema de comunicación Promina 400 de voz y datos MD110 de Ericsson
- 4 Hubs
- 2 AT Alied telesyn (1 de 24 conexiones, 1 de 12 conexiones)
- 2 3COM
- 3 Modems
- 1 VPN (Sistema de comunicación en red) distribuidor UNITEC

  2 con enlace con Zamora
- 3 Switches IBM 8271-E24 con 24 conexiones cada uno
- 1 Conmutador (sistema de monitoreo de conmutador Eritar que es un tarificador.)
- Tarificador: Cuenta las llamadas realizadas, recibidas y proporciona una lista de esta, además de proporcionar identificador de la extensión que realiza la llamada.

5.2 METODOLOGÍA DE LA INVESTIGACIÓN

La técnica utilizada para la recopilación de la información fue por medio de entrevista al supervisor de informática, cuestionarios a los usuarios de la red y observación directa durante 6 meses, periodo que estuve realizando mis practicas profesionales, por lo cual puedo conocer en qué respuestas los usuarios no contestaron objetivamente.

5.2.1 ESQUEMA DE RECOPILACION DE LA INFORMACIÓN

El cuestionario (ANEXO 1) aplicado a los usuarios de la red se realizo de opciones múltiples para que no les fuera difícil contestar y/o tuvieran idea de las posibles respuestas, dándoseles también la opción de agregar otra posible respuesta, el objetivo era obtener la siguiente información:

- Saber si conocen lo que es la seguridad física y lógica
- Determinar en que medida aplican las políticas de seguridad informática.
- Saber si hay interés en conocer y aplicar las políticas de seguridad informática.
- Detectar qué políticas informáticas no cumple y cuales son las menos consideradas.
- Identificar qué hacen por mantener segura la información que manejan.

La entrevista al Administrador de Informática tuvo la finalidad de recopilar información acerca del SITE principalmente. Así como la posibilidad de proporcionar los datos utilizados en los formatos de control de acceso al área, al edificio, bitácoras de respaldos y pases de salida de equipo.

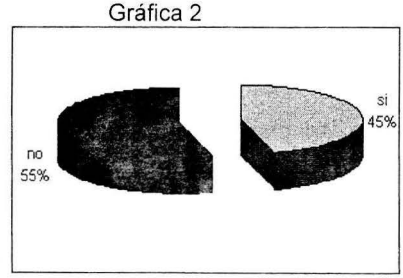
5.3 ANÁLISIS DE LOS RESULTADOS DE LA APLICACIÓN DE CUESTIONARIOS

Después de realizar el conteo (tomando en cuenta una muestra de 54 personas) de los cuestionarios, obtener resultados y de haber graficado se puede determinar lo siguiente.

A la pregunta de si conoce lo que es la seguridad física (Gráfica 1) el 58% contestaron afirmativamente, 42% no lo conocen, y en lo que respecta a seguridad lógica (Gráfica 2), más de la mitad, el 55%, no sabe a lo que se refiere este término, mientras que el 45% manifiestan sí saberlo, datos que serán probados o refutados con los resultados obtenidos de cada pregunta realizada.

Gráfica 1

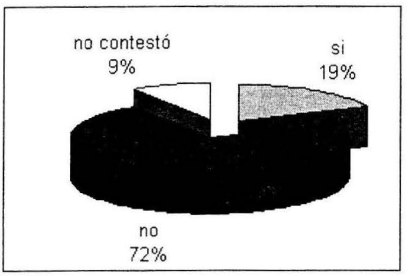
Gráfica 2



Fuente: Elaboración propia con datos del cuestionario

El 80% expresan no conocer las políticas y normas sobre seguridad informática (Gráfica 3) que se publican en la Intranet, por lo que aquí se puede notar un poco de contrariedad con las respuestas de la pregunta uno y dos, ya que dicen si conocer lo que es la seguridad física y lógica pero no conocen las políticas, que en realidad son estas las que pueden ayudar a definir cada término.

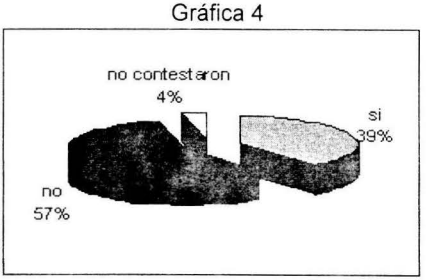
Gráfica 3



Fuente: Elaboración propia con datos del cuestionario

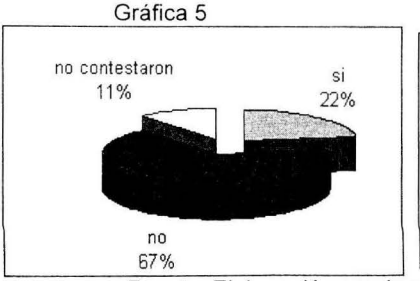
Sólo el 40% tienen el conocimiento de que existe un manual de políticas de seguridad (Gráfica 4) que se encuentra publicado en la Intranet, pero la mayoría, el 60% no lo saben. De los que saben que existe el manual, el 57% lo han leído (Gráfica 5) y comprendido (Gráfica 6), este manual explica de manera detallada lo que se debe de realizar para poder lograr la seguridad física y lógica, por lo que es importante que éste sea del conocimiento de todos los usuarios.

Gráfica 4

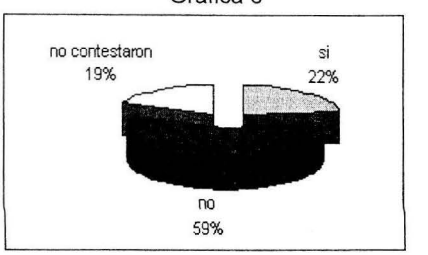


Fuente: Elaboración propia con datos del cuestionario

Gráfica 5



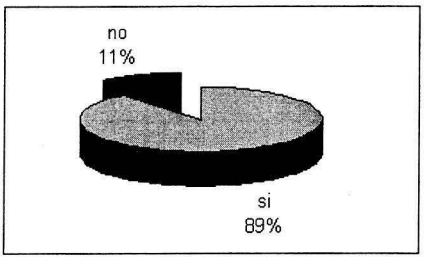
Gráfica 6



Fuente: Elaboración propia con datos del cuestionario

Aunque sólo el 57% ha leído y comprendido el manual, la mayoría, el 89% están enterados de que si se llegara a realizar una acción en contra de la empresa con su cuenta, la responsabilidad y consecuencias recaería sobre ellos (Gráfica 7).

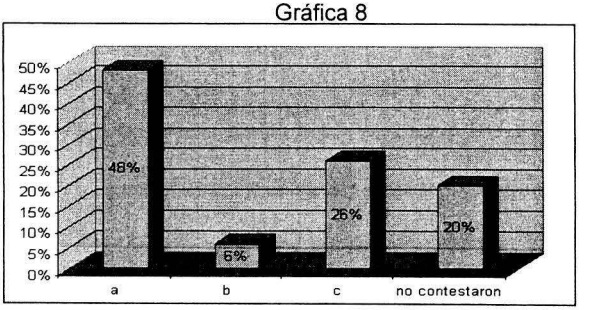
Gráfica 7



Fuente: Elaboración propia con datos del cuestionario

De los que han consultado algo referente a la seguridad informática (Gráfica 8), 60% dicen ponerla en práctica, aunque se ve que no es totalmente cierto por los resultados obtenidos en la encuesta, especialmente en seguridad de la información. 33% se muestran un poco mas interesados por lo que averiguan más y 8% no la pone en práctica, es decir que la ignora.

Gráfica 8



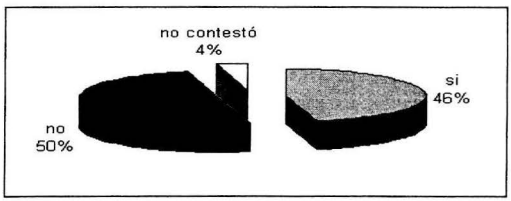
Fuente: Elaboración propia con datos del cuestionario

Nota: Estos porcentajes son tomando como universo 52 respuestas, ya que hubo quienes eligieron dos opciones y no se toma en cuenta a los que no contestaron.

Aun conociendo la responsabilidad de las cuentas de usuarios, el uso de las contraseñas no es muy adecuado como se puede ver a continuación.

Un poco mas de la mitad de los entrevistados, el 52% no conocen las políticas que se deben de seguir para tener una contraseña segura (Gráfica 9), mientras que el 48% dicen si conocerlas.

Gráfica 9



Fuente: Elaboración propia con datos del cuestionario

Los usuarios indican conocer las políticas, sin embargo, a la pregunta de con que relacionan su contraseña, la contestaron, siendo que no debe de decirse, además el campo que se dejó abierto para detallar cualquier otra opción, hubo quienes si lo especificaron con que la relacionan (Gráfica 10), los resultados fueron los siguientes: Gráfica 10

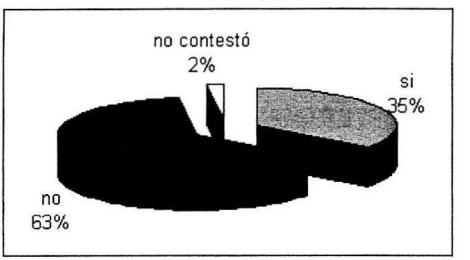
Término con qué lo relacionan	**%**
Nombre de su familia	21
Nombre de su pareja	10
Fechas de nacimiento	10
Siglas o nombres de su equipo de fútbol o béisbol	5
Nombres de famosos y grupos musicales	2
Su propio nombre, sus siglas o una combinación de siglas con fechas de nacimiento	29
Otro	23

Fuente: Elaboración propia con datos del cuestionario

Como se puede ver, el total de los encuestados no aplican las políticas de contraseña segura que se encuentran publicadas en la Intranet. El 23% que eligió la opción de otros, especifico que la relacionan con jugadores de fútbol, palabras fáciles de recordar, combinación de siglas, números y letras, fechas importantes, animal favorito, y sólo el 4% señalaron que era confidencial la relación de su contraseña.

36% han prestado o compartido alguna vez su contraseña (Gráfica 11) y 64% no lo han hecho, y eso es bueno, ya que esta es intransferible y única, por que si se presta, puede ser que otras personas, incluso los mismos compañeros o "amigos" hagan mal uso de la cuenta de usuario y contraseña.

Gráfica 11

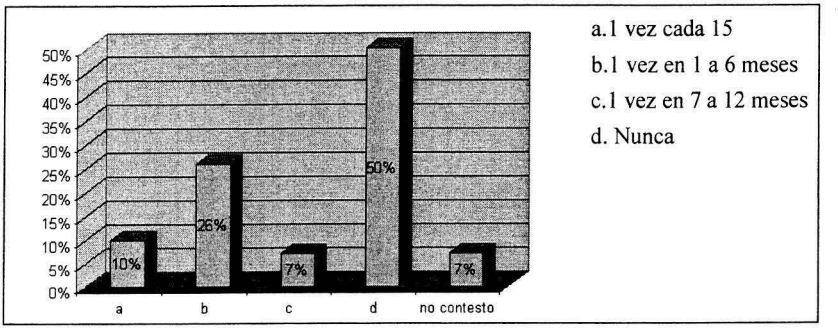


Fuente: Elaboración propia con datos del cuestionario

La frecuencia con que cambian su contraseña (Gráfica 12), un poco mas de la mitad, el 54% nunca lo hacen, dato preocupante, ya que sus contraseñas son fáciles de corromper, y una vez que puedan acceder a la red personas ajenas con esa cuenta, podrán hacerlo por el tiempo que quieran, así como los mismos compañeros a los que alguna vez se les fue prestada una contraseña; el 28%

realizan el cambio una vez de 1 a 6 meses y tan sólo el 10% lo cambian mínimo 1 vez cada 15 días, siendo esta el mejor rango.

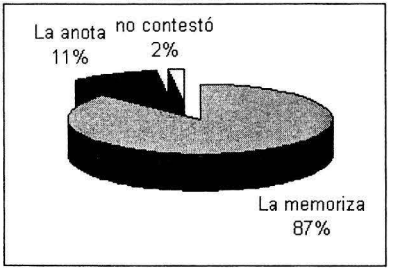
Gráfica 12



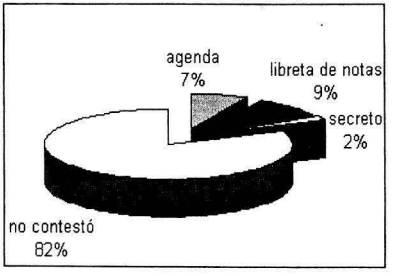
Fuente: Elaboración propia con datos del cuestionario

El 89% memorizan su contraseña (Gráfica 13), se puede ver por la relación que hacen de esta con situaciones cotidianas de su vida. Del 11% que la anotan, el 40% (Gráfica 14) lo hacen en su agenda, el 50% en libretas de notas, y sólo el 10% no lo especifico, sólo que era un lugar secreto.

Gráfica 13



Gráfica14

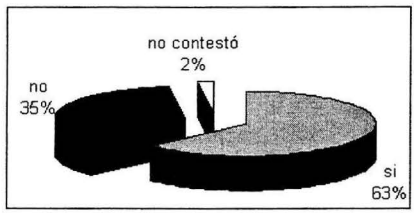


Fuente: Elaboración propia con datos del cuestionario

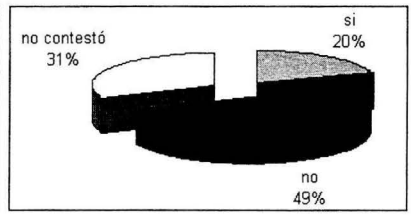
Las computadoras muchas veces no se utilizan durante un corto tiempo, a lo que un 64% utiliza protector de pantalla (Gráfica 15), esto es bueno, ya que se evita que los compañeros lleguen a ver información que no es de su atribución,

pero solo el 32% usa una contraseña para quitarlo (Gráfica 16), no del todo bueno, pues si no se usa, con un simple movimiento que reciba la computadora reacciona y desprotege la pantalla.

Gráfica 15



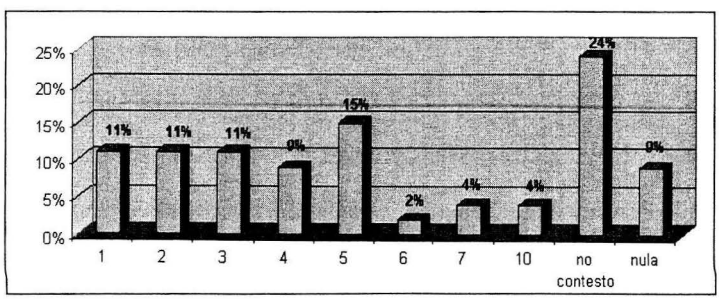
Gráfica 16



Fuente: Elaboración propia con datos del cuestionario

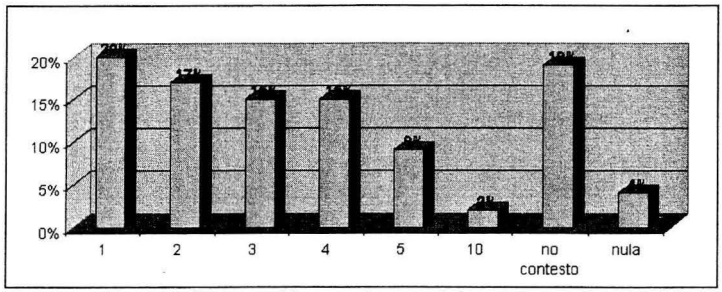
Se recomienda tener una contraseña por cada programa diferente que se use y la requiera; del 5% que tiene acceso a 10 programas (Gráfica 17), únicamente el 2% utiliza 10 contraseñas diferentes (Gráfica 18), del 22% que usan 5 programas, sólo, el 12% tienen 5 contraseñas diferentes, del 14% que utilizan 4 programas diferentes, todos tienen una diferente, ya que se ve que el 19% usan 4 contraseñas diferentes, 17% utilizan 1, 2 y 3 programas diferentes, todos ellos usan una contraseña diferente para cada programa. Los de 6 y 7 programas diferentes, ninguno usa una contraseña diferente para cada uno, esto quiere decir que tiene 1, 2 ó 3 contraseñas para los 6 ó 7 programas.

Gráfica 17



Fuente: Elaboración propia con datos del cuestionario

Gráfica 18



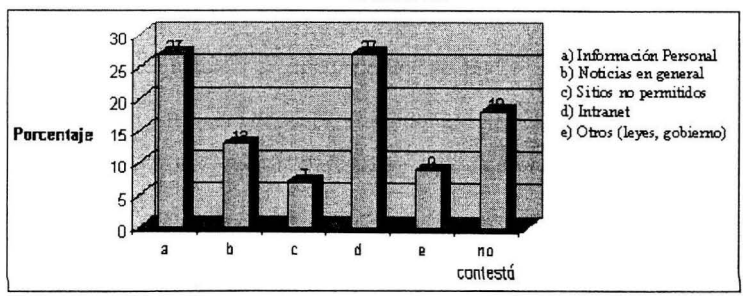
Fuente: Elaboración propia con datos del cuestionario

La mayoría de los entrevistados, el 63% sabe navegar por Internet (Gráfica 19), y el 37% no sabe, pero el acceso a es exclusivo para los administradores, o para quienes puedan justificar su necesidad de tenerlo ante el Administrador de la Unidad Administrativa. El 32% consulta la Intranet (Gráfica 20), dato que debería ser mucho más alto, ya que aquí se puede encontrar toda la información referente a su entorno de trabajo y a seguridad, y por la encuesta se ve que un bajo porcentaje la consulta.

Gráfica 19

Fuente: Elaboración propia con datos del cuestionario

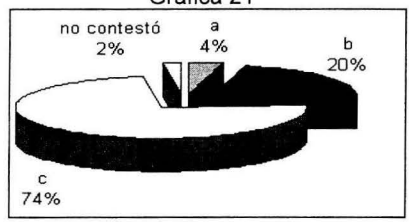
Gráfica 20



Fuente: Elaboración propia con datos del cuestionario

El servicio de e-mail aunque es únicamente para fines de la institución, una minoría de 25% tiende a reenviar cadenas (Gráfica 21), las cuales pueden ocasionar la saturación del servidor de correos y bajar el rendimiento del mismo y 76% atiende a la norma de enviar solo correos con fines institucionales.

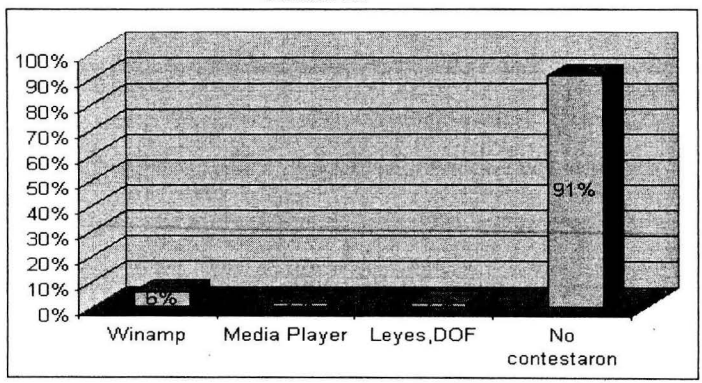
Gráfica 21



Fuente: Elaboración propia con datos del cuestionario

No pueden instalar nada que no sea software proporcionado por la empresa, así que en cuanto a legalidad, no infringen los derechos de autor, ni propiedad privada, a excepción del 8% que ha bajado programas como Winamp y Media Player (Gráfica 22), el 91% que se abstuvo de contestar es por que no tienen acceso a Internet en la empresa, cumplen con las políticas o desconocen el proceso de download (bajar warez de Internet).

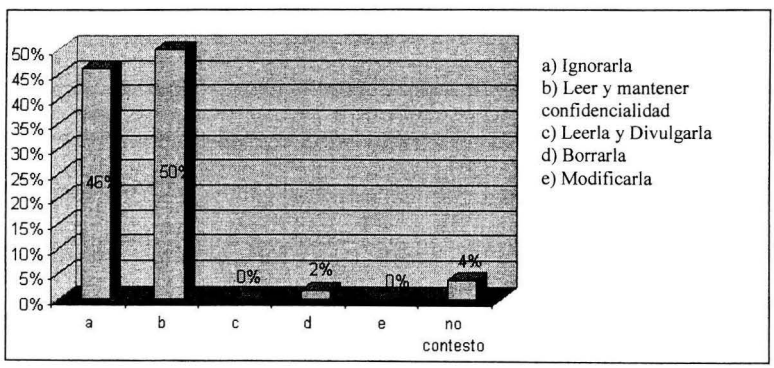
Gráfica 22



Fuente: Elaboración propia con datos del cuestionario

Un poco mas de la mitad, el 51% cuando encuentra información confidencial o vital para la empresa (Gráfica 23) y que no corresponda a sus tareas, la leen, pero la mantienen confidencial, el 47% la ignora, quizá lo hacen por que tienen mucho trabajo o no les importa saber mas que lo necesario para realizar sus tareas, tan sólo un 2% ha llegado a divulgarla, pero es muy bueno que el 0% realice modificaciones o borra esta información, ya que esta acción, podría repercutir en pérdidas para la empresa. Esto es lo que ellos expresan, pero muy posiblemente por miedo a que por medio de este cuestionario se les fuera a tomar alguna represaría en contra de los entrevistados, no contestaron con certeza.

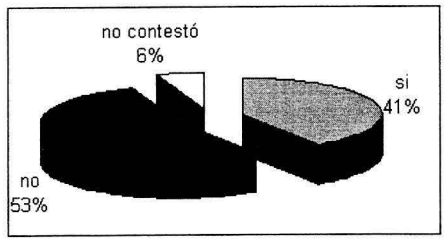
Gráfica 23



Fuente: Elaboración propia con datos del cuestionario

Sólo el 43% revisa sus discos con el antivirus antes de abrirlos (Gráfica 24), porcentaje alto, ya que no es difícil ni tardado este proceso y si puede evitar que nuestra máquina se contamine, ocasionando posteriormente virus en la red o pérdida de información valiosa y/o vital para la empresa

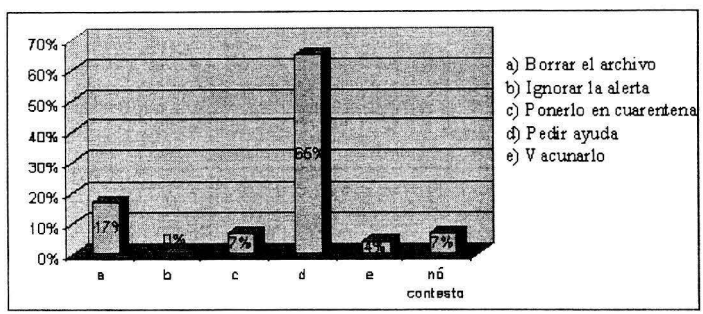
Gráfica 24



Fuente: Elaboración propia con datos del cuestionario

Cuando llega a detectar un virus el software antivirus (Gráfica 25), el 18% borra el archivo, siendo que puede ser un archivo irrecuperable e indispensable, el 8% lo pone en cuarentena, una gran parte, el 70% no sabe que hacer, por lo que pide ayuda y sólo una mínima parte lo vacuna para poder seguir utilizándolo.

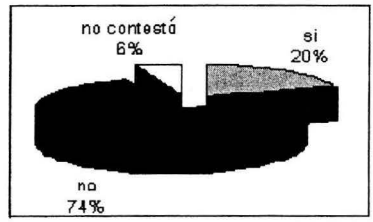
Gráfica 25



Fuente: Elaboración propia con datos del cuestionario

Un gran porcentaje, el 78% no saben realizar la actualización del antivirus (Gráfica 26), pero no es muy alarmante, ya que cuando llega una nueva versión, el departamento de informática se encarga de realizarla, aunque la versión que se tiene actualmente del software, trae automatizada esta opción, por lo que ya no requiere de una persona que lo haga.

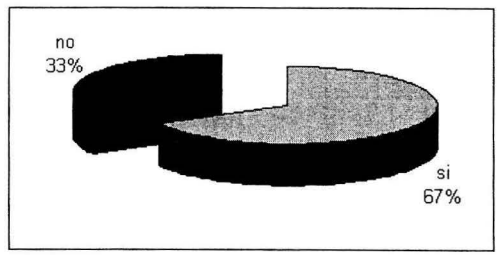
Gráfica 26



Fuente: Elaboración propia con datos del cuestionario

Al ingreso a la empresa, como nuevos empleados, se les capacita con respecto a como utilizar los programas que serán para realizar su labor (Gráfica 27), y cuando hay actualizaciones, se les manda un mail informándoseles dicho cambio, a lo que el 67% manifiesta que si se les da esta capacitación, y sólo un 33% no. Esta capacitación es con la finalidad de evitar posibles errores en el sistema y prevenir que estos ocasionen efectos al servidor.

Gráfica 27

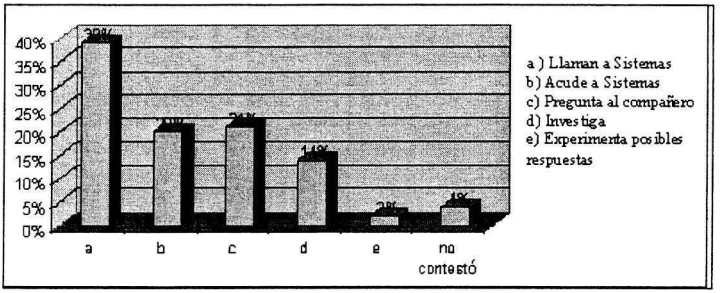


Fuente: Elaboración propia con datos del cuestionario

Completando a la gráfica 26, cuando tienen dudas del uso de una aplicación (Gráfica 28), el 41% llama al encargado de informática para que le ayude, el 20% acude personalmente, el 22% trata de resolver su duda preguntándole al compañero, el 15% investiga una solución y el 2% experimenta

posibles respuestas, este porcentaje es bueno, ya pueden llegar a dañar el equipo o sistema por acciones no debidas.

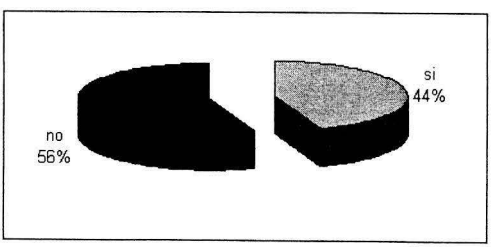
Gráfica 28



Fuente: Elaboración propia con datos del cuestionario

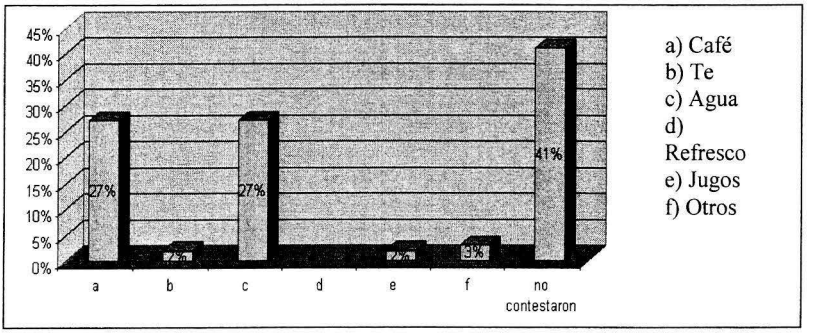
Los líquidos cerca del equipo de cómputo pueden derramarse y causar daños al equipo, y las comidas pueden llegar a ensuciarlo y perjudicar su funcionamiento, a lo que el 56% dicen no consumir nada cerca de los equipos (Gráfica 29). En contraparte el 61% dice consumir, café, te, agua, jugos e inclusive tortas (Gráfica 30) En las respuestas se noto un poco de contrariedad, ya que primero contestaban que no consumen nada y a la pregunta 25 contestaban que tipo de bebida ingieren.

Gráfica 29



Fuente: Elaboración propia con datos del cuestionario

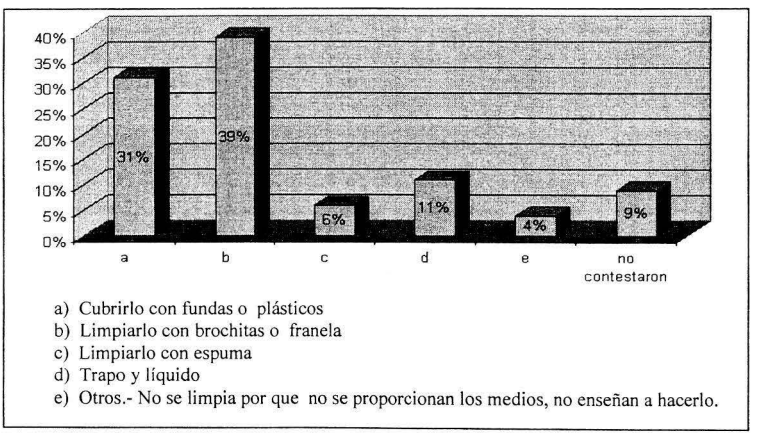
Gráfica 30



Fuente: Elaboración propia con datos del cuestionario

La mayoría cuida su equipo físicamente (Gráfica 31), ya que cada quien es responsable por él, a lo que 96% lo limpia o lo protege para mantenerlo en buen estado y solamente el 4% no hace nada justificándose con que no se les proporcionan los medios adecuados, ni los enseñan a limpiar o cuidar al equipo.

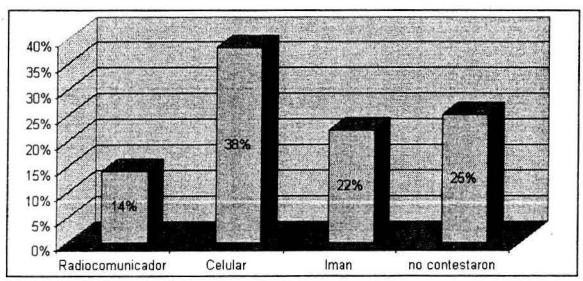
Gráfica 31



Fuente: Elaboración propia con datos del cuestionario

Continuando con el cuidado por parte de los usuarios, no es recomendable tener objetos cerca de la computadora que lleguen a generar interferencia, un poco mas de la mitad, el 52% tienen su celular cerca del equipo de cómputo (Gráfica 32), es decir, sobre la misma mesa, 30% objetos con imán y un 18% radio comunicador, pero este último porcentaje no es muy confiable, ya que confundieron un radio que toca música con el de comunicaciones.

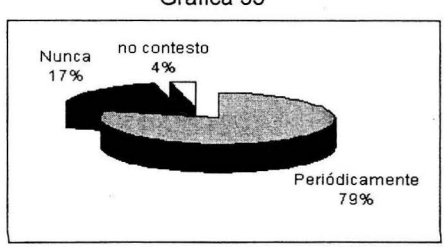
Gráfica 32



Fuente: Elaboración propia con datos del cuestionario

Es importante que se le de mantenimiento preventivo a las máquinas, el supervisor de Informática señala dárselos por lo menos cada 6 meses, dato que se comprobó preguntándoles a los usuarios, a lo que 82% contestaron que la revisión de sus computadoras es periódicamente (Gráfica 33) y tan solo el 18% dicen que nunca, tal vez sea por que ellos no se percaten de la revisión.

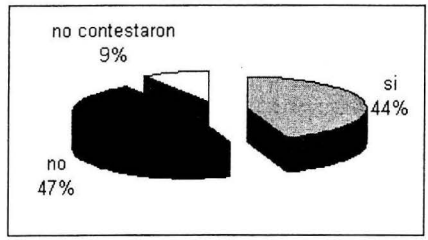
Gráfica 33



Fuente: Elaboración propia con datos del cuestionario

Es importante saber utilizar el extintor, esta disponible uno por cada departamento, ya que si se presenta un pequeño corto, se puede evitar algo mayor, el 51% no sabe utilizarlo (Gráfica 34), porcentaje grande, por que su uso es muy sencillo.

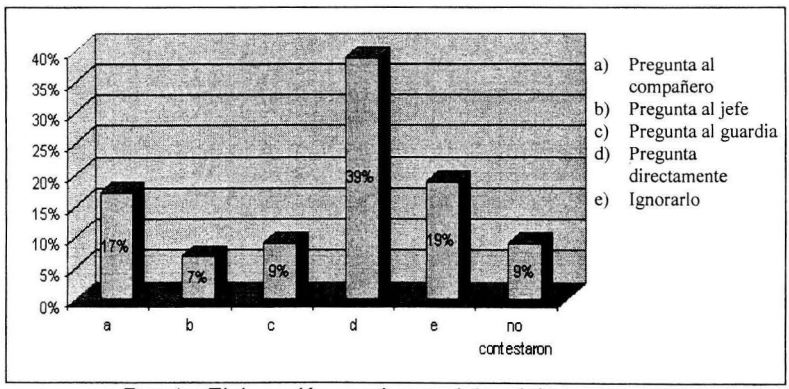
Gráfica 34



Fuente: Elaboración propia con datos del cuestionario

Cuando hay una persona extraña y no porta su gafete (Gráfica 35), el 43% de los usuarios se acerca a preguntarle personalmente al extraño quien es, el 21% se muestra indiferente ante tal persona, el 36% restante preguntan a compañeros, jefe o guardia, por lo que es importante portar el gafete que los identifique durante el tiempo que permanecen dentro de la empresa.

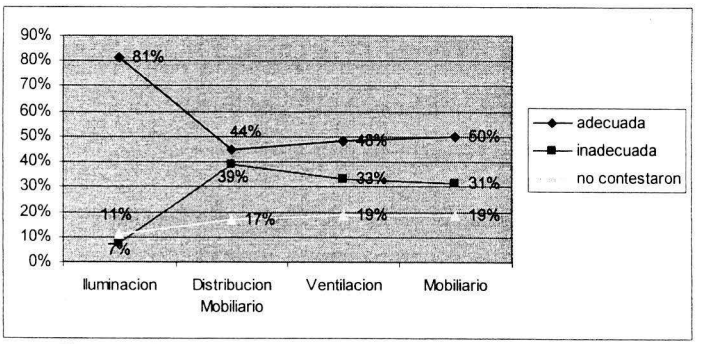
Gráfica 35



Fuente: Elaboración propia con datos del cuestionario

Respecto a como consideran en general su ambiente de trabajo se obtuvo que la mayoría están satisfechos con su lugar de trabajo (Gráfica 36), el 92% considera adecuada la iluminación, esta es importante para que no perjudique a la vista, el 53% dice que la distribución del mobiliario es adecuada, y se pudo ver (por observación directa) que si se tienen los espacios suficientes para cada persona, el 59% manifiesta que la ventilación es adecuada, ya que el edificio tiene unas grandes ventanas por la que entra mucho aire y además por la distribución de cada espacio, no se encierra el calor, el 61% considera adecuado el mobiliario, aunque se pudo ver que el teclado y el ratón no se encuentran muy ergonómicamente, ya que les quedan muy arriba de la distancia a la que deben de estar.

Gráfica 36

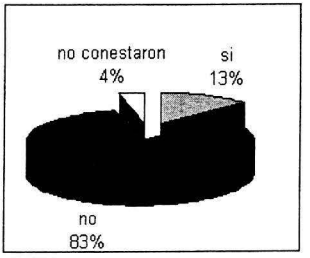


Fuente: Elaboración propia con datos del cuestionario

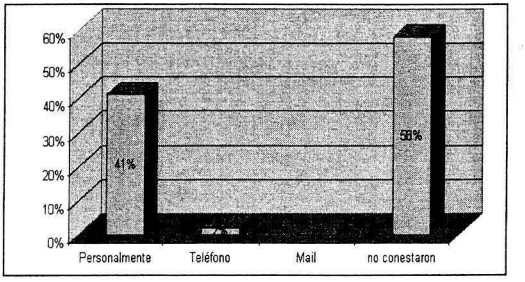
A la pregunta de si han dado su contraseña a cualquier otra persona que no sea al supervisor de informática (Gráfica 37), la mayoría a realizado lo correcto, pues el 83% no la a dado, tal parece que la pregunta no se entendió muy bien, ya que dice el 13% dijo que si la dio y haber recibido la solicitud personalmente o por teléfono (Gráfica 38), sumando un porcentaje de 329%, dato

imposible. Por lo que estas dos gráficas no son confiables para determinar si han sido victimas de la ingeniería social.

Gráfica 37



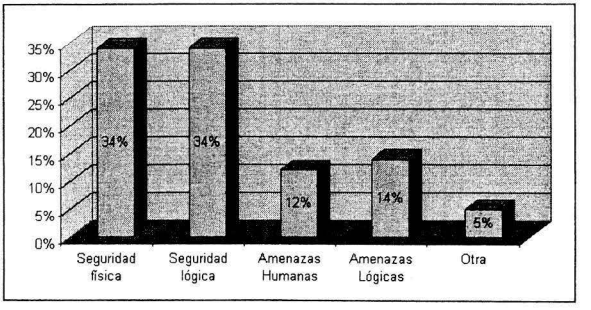
Gráfica 38



Fuente: Elaboración propia con datos del cuestionario

Los usuarios expresaron tener un poco de interés en conocer mas acerca de los siguientes temas (Gráfica 39), un 34% en seguridad física, otro porcentaje igual en seguridad lógica, un 12% en amenazas humanas y 14% en amenazas lógicas, solo un 5% eligió otra opción, la cual no fue especificada.

Gráfica 39



Fuente: Elaboración propia con datos del cuestionario

Nota: Para el análisis de la información el 100% se tomo en base a las respuestas contestadas, omitiendo los datos en blanco, que no son relevantes para la interpretación.

5.4 ANÁLISIS DE LOS RESULTADOS DE LA ENTREVISTA Y OBSERVACIÓN DIRECTA CON RESPECTO AL SITE

El centro de cómputo se encuentra ubicado en el segundo piso, esto para que no esté expuesto a posibles inundaciones, no sea fácil el acceso a personal ajeno, esta provisto de controles de acceso, muros de concreto, una puerta blindada y resistente al fuego para el acceso al SITE, tiene una solo entrada, pero las puertas son vidrios que permiten la visibilidad del exterior al interior del Centro de Cómputo. Para que pueda ser abierta la puerta blindada es por medio de una tarjeta magnética con contraseña. Además cuenta con: sistema contra incendios con detectores de partículas de humo, calor y supresión automática de fuego, extintores portátiles, alumbrado emergente, iluminación adecuada, alarmas auditivas y visuales, sistema de gas SFM200, falso plafón. Cuenta con equipos o sistemas auxiliares de soporte como: energía in-ininterrumpible (UPS), aire acondicionado y planta de emergencia. A grandes rasgos la temperatura promedio que tiene el SITE es entre 19 y 20 °C y cuenta con una humedad relativa del 34%.

En el caso de los respaldos de los servidores (WINDOWS NT) y/o estaciones de trabajo se establece que se debe cumplir con el cuadro siguiente:

Aplicación	Período Ordinario	Período extraordinario
Sistema Operativo	En caso de modificaciones a la configuración	En caso de actualización o instalación de nuevas versiones
Software de aplicaciones	En caso de modificaciones a la configuración	En caso de actualización o instalación de nuevas versiones
Software de Administración del Servidor (SMS)	En caso de modificaciones a la configuración	En caso de actualización o instalación de nuevas versiones
Bases de Datos (incluida la BD de SQL de SMS)	Cada 3er. día (de ser posible diario)	En caso de modificación a las estructuras o nuevas versiones
Información actualizada continuamente	Diario	

Además de que todos los respaldos serán generados en formato DAT de 4 mm y con los dispositivos del servidor. Los medios magnéticos utilizados en la realización de respaldos, deberán ser identificados con una etiqueta que describa claramente:

a. Fecha de generación: Día / Mes / Año, en el que se realizó el respaldo

b. Identificación del responsable: Nombre del encargado de la información a respaldar

c. Unidad Administrativa: Incluyendo la Dirección General a la que pertenece

d. Nombre del servidor: De acuerdo al esquema de redes del Servicio de Administración Tributaria

e. Número de orden secuencial: Por ejemplo, 1/1, 1/2, 2/2, etc.

f. Contenido del dispositivo: Descripción del contenido por directorios/subdirectorios/archivos

Finalmente deberá existir una bitácora para el control y registro de respaldos que contenga los siguientes datos:

a) Hora de inicio

b) Hora de conclusión

c) Contenido del respaldo

d) Nombre y firma del responsable informático

e) Número de orden secuencial del dispositivo (1/1, 1/2, 2/2)

f) Confirmación de conclusión exitosa

Todo el software que se maneja dentro de la ALR Uruapan tiene licencia, no se permite la instalación de nada mas, a menos de que se le haga una solicitud al supervisor de informática exponiéndole las razones por la que se desea instalar un nuevo software y el SAT debe aprobarlo y autorizarlo.

Para poder sacar/entrada material, mobiliario y equipo se utiliza un formato que lleva los siguientes datos:

a. El titulo de pase de salida/entrada

b. Número de secuenciación

c. Fecha

d. Dirigido al encargado de vigilancia

e. Descripción detallada del equipo

f. De que lugar esta saliendo /entrada del equipo

g. Lugar de destino/origen

h. Nombre y Firma del portador

i. Nombre y Firma de Autorización

5.5 PROBLEMAS DETECTADOS

- No se tiene la forma de constatar por que razón no contestaron algunas preguntas, pero las mas posibles son las siguientes:
    - Ignorancia, al no saber que contestar por desconocer el tema
    - Guardar la confidencialidad
    - Indiferencia
    - Por falta de dedicación o contestar rápido
    - No entender la pregunta
- No se hace una difusión suficiente de las políticas de seguridad informática que existen, por lo que los usuarios cometen acciones indebidas, por no tener el conocimiento de ellas.
- Las políticas se publican en la Intranet, son sencillas de entender, hay recordatorios para que realicen el cambio de sus contraseñas, pero pocos entran a revisar esta información.
- No hay una persona que vigile el cumplimiento de las políticas.

- Aunque están consientes de que si se comete un robo de información o ataque informático con sus cuentas, la responsabilidad es totalmente de ellos, no muestran interés por saber como protegerse o evitar esa situación
- Las contraseñas son fácilmente de corromper, ya que no cumplen con las políticas y precisamente hacen todo lo contrario.
- Por observación se constato que no portan su gafete que los identifique como personal de la empresa, siendo que en las políticas se indica que lo deben traer puesto y en un lugar visible.
- No se obliga a los visitantes a portar el gafete, sólo se registran (algunos) y pueden pasar.
- El principal problema son los usuarios, por que por parte del encargado de informática, cumple con las políticas de seguridad. Y de nada sirve tener la mejor administración si los usuarios cometen indiscreciones o no colaboran con la misma seguridad informática de la empresa.
- La información fue obtenida por una relación de confianza debido a que se tuvo una convivencia cercana laboralmente, aspecto que para la seguridad de la empresa, este tipo de información que permite acceder y conocer la manera en como operan para la determinación de sus contraseñas no debe de dársele a ninguna persona, ya que la mayoría de los ataques informáticos son realizados por el mismo personal de la empresa que labora o a estado ahí.
- Los extintores son de fácil uso pero no saben utilizarlos, sirviéndoles de nada.
- Tienen la bitácora de control de accesos al SITE pero no la utilizan si la persona ya es conocida.

- Cualquier otro usuario que sepa login y password puede ingresar a otra máquina y ver toda la información y modificarla e inclusive borrarla, ya que los derechos no están restringidos.
- Nunca cambian su contraseña, por lo que si alguien logro entrar a la red, en un futuro de nuevo logrará volver a entrar sin ningún problema.
- Poner contraseña al protector de pantalla es muy sencillo y no lo hacen.
- Es difícil memorizar tantas contraseñas, y que cumplan con las políticas seguras, por lo que las relacionan con cosas cotidianas de su vida.
- No revisan todos los medios de almacenamiento que ingresan a su equipo de cómputo con el software antivirus, pensando que si un virus llegara a contaminar su computadora, sólo se formatea su máquina y ya, pero no están consientes de que el virus se puede expandir por toda la red.
- El consumo de bebidas cerca del equipo de cómputo es muy riesgoso y la mayoría lo hace, aunque contestaron que no, por observación directa se vio que la gran mayoría por el transcurso del día tienen, café, te o agua cerca de la computadora.
- Muchos tienen su celular cerca del equipo y genera interferencia, pudiendo dañar al equipo.
- Ergonómicamente el mouse no les queda bien a la mayoría, ya que tienen que tener levantada un poco el brazo para alcanzar el mouse que se encuentra en una posición nada cómoda.
- Las personas que están cerca de las ventanas, cuando se encuentran abiertas, se les llega a reflejar la luz natural en el monitor, ocasionando mas cansancio en la vista.

- Los usuarios no tienen interés por conocer y entender la seguridad informática, a pesar de que obtendrían un gran beneficio como usuarios.
- No hay conocimiento de la cultura informática.

5.6 PROPUESTA

A los usuarios se les debe de decir qué beneficios obtendrían al conocer y aplicar las políticas, porque si ni las conocen no es posible esperar que las vallan a aplicar.

Para los que tengan acceso a Internet deben estar restringidas ciertas direcciones IP donde puedan adquirir warez o aplicaciones no permitidas, o virus.

Instruir a los usuarios para que no respondan a ninguna pregunta sobre cualquier característica del sistema.

Presentarles casos reales de otras empresas que han sufrido ataques informáticos, y a aprovechar para recordarles cambiar sus contraseñas y demás políticas.

Hacerles entender sus responsabilidades legales y dentro de la organización con respecto a la información con la que trabajan, los procedimientos de seguridad asociados con dicha información y las razones por las que se han implementado.

Que se realice una evaluación del cumplimiento del reglamento.

Difusión de los manuales de seguridad y aplicarles un cuestionario que sea devuelto al encargado de informática, para asegurarse de que el material fue leído.

No dejar pasar a visitas si no se registran y portan su gafete, aunque sean conocidos.

Enseñarles a utilizar los extintores por lo menos una vez.

Aunque se conozca a la persona que ingrese al SITE debe de registrar su entrada.

Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, por lo que es importante la protección de cada máquina que se encuentra en la red, y no solamente de las que contengan la información mas valiosa

El software antivirus que tienen ahora ya realiza las actualizaciones automáticas, pero no revisa todos los archivos que se ingresen por las unidades de almacenamiento externas como por ejemplo el floppy, por lo que hay que invitar al usuario a que revise todo lo que ingresa a su equipo de cómputo.

El problema de las contraseñas y control de cuentas de los usuarios es muy grave, por lo que el uso de una SmartCard (Tarjeta Inteligente) resolvería muchos problemas relacionados con los usuarios y el uso de sus cuentas, ya que esta tarjeta tiene las ventajas de :

- Solo la persona que tiene la tarjeta y conoce la contraseña puede acceder a la red.
- No se tiene que escribir dominio, usuario y contraseña para la red ya que éste se encuentra en la tarjeta misma.
- Permite firmarse a la red desde cualquier localidad de la compañía y nos lleva directamente al dominio con "feel&touch"
- Sirve como identificación para la compañía y para control de asistencia.

- También como método para localizar a las personas, es decir, en que lectora se han firmado.
- Tiene antena de proximidad y cuenta con un chip para encripción.
- Cuesta aproximadamente 18 dólares.

Por lo que solamente se les indicaría que tiene que cuidar muy bien de esta tarjeta y ser realmente responsable de ella, advirtiéndoles que si se llegara a extraviar, se harían acreedores a una sanción.

CONCLUSIONES

La seguridad informática es importante para mantener la integridad, disponibilidad y confidencialidad de la información. Ya que este recurso es indispensable para el buen funcionamiento de una empresa y de una sociedad en general. Actualmente se ha extendido el cuidado de los sistemas haciendo conciencia de su importancia.

El Servicio de Administración Tributaria es una paraestatal que maneja gran cantidad de información muy importante para cada contribuyente, por lo que se debe de mantener la confidencialidad, integridad y disponibilidad, a través de una serie de políticas para llegar a lograr tales elementos, a través de la seguridad física, lógica y buena conducta de los usuarios, que por lo que después de haber realizado esta investigación se determina que de nada sirve la administración y protección, si los usuarios no colaboran.

Por parte del Departamento de Informática, se realizan las medidas adecuadas para la seguridad, pero los usuarios son un punto muy débil en la empresa, ya que no llevan a la práctica las políticas señaladas, ni mucho menos las conocen algunos, con esta información no se quiere dar una mala imagen de la empresa, si no que se pueda determinar puntos vulnerables y aprovecharlos de tal manera que sean de utilidad para realizar las oportunas correcciones que se determinen ser necesarias.

Se debe de considerar mas a los usuarios como parte integral para la seguridad informática, ya que de ellos depende en gran medida que la protección se lleve exitosamente o no. Y no solamente se habla de la seguridad lógica, si no que además es también muy importante el cuidado de los equipos, por que si les llegara a suceder algo y la información quedara irrecuperable, esto repercutiría en la empresa directamente.

Ergonómicamente una persona trabaja mejor cuando se encuentra en las posiciones adecuadas, y tendría menos errores a la hora de capturar información , por el contrario cuando está incomodo, puede tener trastornos futuros y rendirá menos por el estar sobandose algún dolor que sintiera a consecuencia de la máquina.

No se le puede dar a todos el mismo grado de protección de la información, ya que este factor depende del grado de confidencialidad que maneje cada persona, pero si es importante que todos se responsabilicen de la información a la que tienen acceso por seguridad de los propios contribuyentes.

El departamento de informática previendo incidentes inesperados, realiza un respaldo diario de la información que los DAT de respaldo son enviados a Celaya, por lo que si algo llegara a sucederle al SITE, existiría la posibilidad de recuperar la información.

En la actualidad no se conoce una red que sea 100% segura , siempre se está en peligro de ser atacados ya sea por personas externas a la empresa, que

tienen diferentes objetivos como desde entrar por simple diversión o reto, o para poder adquirir información, destruirla para perjudicar a la empresa; o ataques por propias personas que laboran en la empresa, que quieren venganza o perjudicar a la empresa, inclusive pueden hacer daño hasta por desconocimiento de lo que hace, llegar a borrar información por ignorancia o descuido.

La hipótesis planteada fue: "Los usuarios de la red son una vulnerabilidad muy grande para ataques internos y/o externos de una empresa", y ahora sí se puede decir que es cierto después de haber realizado el análisis, ya que los usuarios no conocen ni les es de su importancia conocer y aplicar la seguridad informática, se limitan a lo que es solamente su trabajo y no quieren dar mas de si mismos, para la colaboración de la empresa. Los objetivos planteados se cumplieron satisfactoriamente, ya que se realizó el análisis de la seguridad informática de la ALR, basándome en la investigación documental y los conocimientos adquiridos durante el estudio de la licenciatura, obteniendo de esta manera la práctica, así como la realización del análisis de los conocimientos de los usuarios para poder comprobar la hipótesis y llegar a una propuesta sólida y objetiva.

Con esto podemos determinar que no se puede eliminar por completo la inseguridad, pero si realizar una disminución de las vulnerabilidades. También es importante como encargado de informática saber identificar cada punto frágil de nuestra red para intrusos y evitar que éste llegue a generar destrozos o conozca información confidencial que pudiera utilizar para bien propio o para extorsionar a la empresa.

BIBLIOGRAFÍA

FERNÁNDEZ Arena José Antonio, El proceso administrativo, Editorial Diana, México, 1977

HERNÁNDEZ Rodríguez Sergio y Nicolás Ballesteros Inda, Fundamentos de administración, Editorial Mc Graw Hill, México, 1980

LEVIN, Richard B. Virus informáticos: tipos- protección - diagnosis - soluciones. MCGRA WHILL, MEXICO 1992.

MCCLURE Stuart, Scambray Joe!, Kurtz George, HACKERS 3, Secretos y soluciones para la seguridad de redes, España 2002, McGraw-Hill

PARKER, C,S. Introducción a la Informática, EditorialInteramericana, Madrid, 1986 PARKIN Michae1, Microeconomía, Editorial Pearson Educación, México, 1995 RADLOW James, Informática: las computadoras en la ,sociedad, Editorial Mc GrawHill, México, 1988

REYES Ponce Agustín, Administración de empresas. Teoría y Practica, Editorial Limusa, México, 1995.

RODRÍGUEZ Valencia Joaquín, Como administrar pequeñas y medianas empresas. Editorial Litograf, 3a edición, México, 1999.

SANDERS Dona1 d H. Informática: Presente y Futuro, Editorial McGrawHill, 3a edición, México 1990.

TEEL James, ."Embedded Firewalls La siguiente generación de seguridad informática", en Red, Año XI, Edición 143, Junio de12002, México

RAYMOND Eric. The New Hacker's Dictionary , MIT Press, Segunda edición 1994. Enciclopedia Microsoft@ Encarta@ 2000. (Q 1993-1999 Microsoft Corporation Administración de Centros de Computo, Prof. Armando Hugo López

Guzmán, 8° semestre de la Lic. En Informática, 2002.

Revistas

DE ANDA Y De Anda Lorenzo, "Delincuentes en Internet", en PC MAGAZINE EN ESPAÑOL, Vol. 13, N°8, Agosto 2002, México

FINE. H. Leonard, Seguridad en Centros de Cómputo, 1 era edición, México, 1988, Ed. Trillas

GONZALEZ Fabiola: "Proteger la información es responsabilidad de todos", en Red, Año XI, Edición 143, Octubre del 2002, México

KENDALL Kennett B., Kendall Julie E. Análisis y Diseño de Sistemas, México 1991, Editorial Prentice- Hal.

MARTINEZ Salcedo Claudia, "Seguridad en Redes", en Red, Año XI, Edición 143, Octubre del 2002, México

MOLINA Nadia:"CERO tolerancia no más piratería de software", en PC MAGAZINE EN ESPAÑOL, Vol. 13, N°9, Septiembre 2002, México

MOLINA Nadia: "La lucha contra la piratería del software", en PC MAGAZINE EN ESPAÑOL, Vol. 13, N°12, Diciembre 2002, México

NAVA L. Marlene, "Seguridad Informática ¿Qué, por qué y para qué?", en Red, Año XI, Edición Especial #2, Junio del 2002, México

ORIHUELA Álvarez Mauricio: "Cibercrimen: el enemigo está en casa", en Red, Año XI, Edición 143, Octubre del 2002, México

RAMIREZ José Antonio: "Ante los apagones, ¡UPS!", en Red, Año XI, Edición 141, Agosto del 2002, México

VAL Griera Luis: "Software ilegal", en PC ACTUAL, Año XIII, N°135, Noviembre

del 2001, España

VIADAS Díaz Virginia, "Plan de contingencia ante desastres", en Red, Año XI, Edición 135, Febrero del 2002, México

Páginas de Internet

www.michoacan.gob.mx

www. monografias. com

www.ccu.umich.mx

http://orbita.starmedia.com

www.acopivalle.com

www.geocities.com

http://penta2.ufrgs.br

www.htmlweb.net

http://revista.robotiker.com

www.monografias.com

www.impi.gob.mx

www.bsa.org

www.shcp.gob.mxlindex01.html

Intranet del SAT

http://99.90.4.180/Presidencia/presidencia.htm

http:// intranetlDgti/dgti. htm

Conferencias

Ignacio Mendívil, La Firma Digital, UNAM, Segunda Semana de Seguridad

Informática, 2002

Erika Sauceda, Roberto Gómez, La criptografia en la autenticación de procesos Linux,

ITESM-CEM, Segunda Semana de Seguridad Informática, 2002

M. C. Marcelo Pérez Medel, Esteganografia en Imágenes, Segunda Semana de Seguridad Informática, 2002

ANEXO 1

Cuestionario aplicado

a los usuarios

Objetivo: Recopilar información de seguridad informática por lo que se pide de favor contestar lo mas objetivo que pueda para que las estadísticas obtenidas sean lo mas confiable posible y puedan ser utilizadas para beneficio de usted.

1. ¿Sabe que es la seguridad física? SI NO
2. ¿Sabe que es la seguridad lógica? SI NO
3. ¿Conoce las políticas y normas que se dan a conocer en la Intranet de seguridad lógica y física? SI NO
4. ¿Conoce las políticas que deben seguirse para tener una contraseña segura? SI NO
5. ¿Ha compartido o prestado alguna vez su contraseña? SI NO
6. Con que frecuencia cambia su contraseña
   a. 1 vez en 15 días
   b. 1 vez en 1 a 6 meses
   c. 1 vez en 7 a 12 meses
   d. Nunca
7. Su contraseña, es algo relacionado con:
   a. Nombres de su familia
   b. Nombre de su pareja
   c. Fechas de nacimiento
   d. Siglas o nombres de su equipo de fútbol o béisbol
   e. Nombres de famosos y grupos musicales
   f. Su propio nombre, sus siglas o una combinación de siglas con fechas de nacimiento.
   g. Otro (especifique)

8. Usualmente la contraseña usted:

   a. memoriza

   b. La anota

9. En caso de anotarla, ¿en que lugar la anota y la guarda?

10. ¿A cuantos programas tiene acceso con contraseña?

11. ¿Cuantas contraseñas diferentes utiliza?

12. ¿Utiliza protector de pantalla? SI NO

13. En caso de si, ¿utiliza contraseña? SI NO

14. ¿Esta enterado de que si se realiza una acción en contra de la empresa con su cuenta de usuario, la responsabilidad recae sobre usted?

    SI NO

15. ¿Dan cursos de capacitación de manejo de programas informáticos, o por lo menos con los que van a trabajar?

    SI NO

16. ¿Revisa sus discos con el antivirus antes de abrirlos? SI NO

17. ¿Que hace cuando se detecta un virus?

    a. Borra el archivo

    b. Ignora la alerta

    c. Lo pone en cuarentena

    d. Pide ayuda

18. ¿Sabe realizar la actualización del antivirus?

    SI NO

19. ¿A que medio recurre cuando tiene dudas del uso de una aplicación?

    a. Llama a sistemas

    b. Acude a sistemas

    c. Pregunta al compañero

    d. Investiga

    e. Experimenta posibles respuestas

20. La revisión de sus computadoras, por parte de sistemas, es:

    a. Periódicamente

    b. Nunca

21. Cuando tiene acceso a información confidencial o vital para la empresa y que no corresponda a sus tareas, que hace con ella:

    a. Ignorarla

    b. Leerla y mantener confidencialidad

    c. Leerla y divulgarla

    d. Borrarla

    e. Modificarla

22. ¿Que consulta en Internet?

    a. Información personal (mail, cuentas de banco, etc)

    b. Noticias en general

    c. Sitios no permitidos

    d. Intranet

    e. Otros (especifique)

23. ¿Que programas ha bajado de Internet? Ejem: Winamp

24. ¿Consume alimentos o bebidas cerca del equipo de cómputo?

25. ¿Que tipo de bebida?

a. Café

b. Te

c. Agua

d. Refresco

e. Jugos

f. Otros

26. De que manera limpias y proteges tu equipo físicamente

a. Cubrirlo con fundas o plásticos

b. Limpiarlo con brochitas o franela

c. Limpiarlo con espuma

d. Trapo y líquido

27. ¿Que objetos generan interferencia cerca de la computadora?

a. Radiocomunicación

b. Celular

c. Imán

28. El lugar de trabajo es:

	Adecuada	Inadecuada
a. Iluminación		
b. Distribución de mobiliario		
c. Ventilación		
d. Mobiliario		

29. ¿Sabe utilizar los extintores? SI NO

30. ¿Que hace cuando ve a una persona ajena al área de trabajo?

a. Pregunta a compañeros

b. Pregunta a jefe

c. Pregunta al guardia

d. Pregunta directamente

e. Ignorarlo

31. ¿A dado su contraseña a cualquier otra persona que no sea el administrador de sistemas?

SI NO

32. ¿Por cual medio recibió tal solicitud?

a. Personalmente

b. Teléfono

c. Mail

33. Si a consultado la información referente a seguridad informática, usted:

a. La pone en práctica

b. La ignora

c. Averigua más

34. Le gustaría conocer más acerca de uno de los siguientes temas:

a. Seguridad física

b. Seguridad lógica

c. Amenazas humanas

d. Amenazas lógicas

e. Otra (especifique)

35. ¿Sabe utilizar el Internet? SI NO

36. ¿Tiene el conocimiento de que existe un manual de políticas de seguridad de la información? SI NO

37. ¿Lo ha leído? SI NO

38. ¿Lo ha comprendido? SI NO

39. ¿Tiende a reenviar cadenas por correo?

a. Siempre

b. A veces

c. Nunca