UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

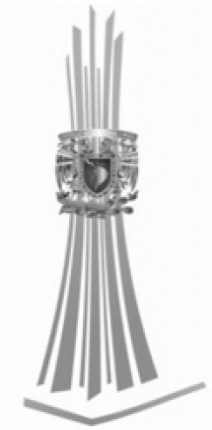
FACULTAD DE ESTUDIOS SUPERIORES ARAGON

"PRINCIPIOS Y CONSIDERACIONES PARA LA SEGURIDAD EN SISTEMAS INFORMÁTICOS"

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO EN COMPUTACIÓN
P R E S E N T A:

LETICIA REYES REYES



Asesor: Ing. Norma Raquel Soto Arredondo

MEXICO , 2008

El éxito es aprender a ir de fracaso en fracaso sin desesperarse
Winston Churchill

Por el apoyo que me otorgaron incondicionalmente mis padres Lidia Reyes y Fernando Reyes Cruz, les dedico esta tesis que es la culminación de una de mis metas, mas no es la única.

Gracias a ustedes, que han estado todo el tiempo a mi lado. He podido llegar al final de mi carrera.

A mis hermanos Lic. Miguel León,
Lic. Florida Alberta a ellos les doy las gracias por que me enseñaron que las cosas se pueden lograr si se tiene una meta en mente.

A mis hermanas Mónica Jazmín y Diana Violeta, que su juventud, carácter y decisión frente a la vida han sido una enseñanza para mí les agradezco por su apoyo.

A mis amigos les agradezco su apoyo y que siempre han sido incondicionales conmigo, han sido cómplices de mis aventuras y de mis triunfos, gracias por todo.

Gracias a todos.

“Una persona usualmente se convierte en aquello que el cree que es. Si yo sigo diciéndome a mi mismo que no puedo hacer algo, es posible que yo termine siendo incapaz de hacerlo. Por el contrario, si yo tengo la creencia que sí puedo hacerlo, con seguridad yo adquiriré la capacidad de realizarlo aunque no la haya tenido en el principio”.

(Ghandi)

¡Actúa en vez de suplicar. Sacrifícate sin esperanza de gloria ni recompensa! Si quieres conocer los milagros, hazlos tú antes. Sólo así podrá cumplirse tu peculiar destino.

Ludwig van Beethoven (1770-1827)

Todos somos muy ignorantes. Lo que ocurre es que no todos ignoramos las mismas cosas.

Albert Einstein (1879-1955)

Índice de contenido

Introducción

Se puede definir como seguridad a un estado de cualquier sistema que nos indica que éste se encuentra libre de peligro, daño o riesgo; sea el sistema de cualquier índole.

Se entiende como peligro o daño, todo aquello que pueda afectar el funcionamiento directo o los resultados que se obtienen del mismo.

Todos los sistemas necesitan contar con seguridad para el manejo de sus elementos y/o de su información.

En el mundo de las computadoras, y sobre todo, en aquellas que se manejan vía red, la necesidad de mantener la integridad de la información es muy fuerte, pues si los datos importantes son violados, alterados o robados, puede dar lugar a serios problemas para la organización a la que pertenecen.

Tratándose de computadoras, el elemento más importante resulta, justamente, la información, con la cual se realizan prácticamente todos los procesos; esto, a través de los dispositivos que se tienen para tal fin, ya sean dispositivos lógicos o físicos, así como las personas que manejan la información.

La seguridad informática consiste, generalmente, en asegurar que los recursos del sistema de información perteneciente a una organización, sean utilizados de la manera en que se decidió y que la información importante (toda, en realidad) no sea fácil de acceder por cualquier persona que no corresponda a los usuarios acreditados.

En el contexto de informática, se sabe que no existe el concepto de seguridad completa o sistema 100% seguro; y lo que se pretende, en estos casos, es minimizar las posibilidades de riesgo.

Estas medidas, por lo regular, se van implementando después de que el sistema ya está implantado y funcionando; sin embargo, debería preverse en el proceso de creación.

Para que un sistema se pueda llamar seguro, debe tener cuatro características básicas:

- ✓ Integridad
- ✓ Disponibilidad
- ✓ Irrefutabilidad
- ✓ Confidencialidad

La integridad se refiere al hecho de que la información no pueda ser modificada por quien no está autorizado.

La disponibilidad habla de que un sistema debe estar disponible cuando se requiera.

La irrefutabilidad se refiere a que no se pueda negar la autoría.

La confidencialidad marca que la información debe ser legible solamente para los usuarios autorizados.

La simpleza o sencillez de estas características a manera de lista, no tienen nada que ver con la complejidad tan grande que es el proveer de ellas a un sistema, trabajo que debe ser realizado por personas capacitadas para tal fin.

La seguridad informática puede ser de dos tipos: lógica o física, de acuerdo a las fuentes de las cuales provienen las amenazas.

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

Cabe mencionar que los sistemas informáticos no son estándar, ni no homogéneos, razón por la cual hay que poner mucha atención en sus características particulares para resolver necesidades específicas de seguridad.

En el presente trabajo, se pretende dar un panorama general sobre la seguridad en los sistemas informáticos y hacer énfasis en la importancia de tener sistemas seguros y confiables.

Objetivos:

- ✓ Identificar los problemas a los que se enfrenta cualquier sistema informático.
- ✓ Reconocer los tipos de agresores y riesgos debidos a las vulnerabilidades informáticas.
- ✓ Hacer énfasis en la importancia de la seguridad informática
- ✓ Marcar puntos a seguir en el desarrollo de la seguridad informática.

Justificación

A manera de justificación, se pueden marcar algunas estadísticas acerca de lo que implica tener sistemas informáticos vulnerables.

Desde hace cinco años, en los Estados Unidos existe una institución que realiza un estudio anual sobre la Seguridad Informática y los crímenes cometidos a través de las computadoras.

Entre lo más destacable del Estudio de Seguridad y Delitos Informáticos 2000 se puede incluir lo siguiente:

- ✓ Violaciones a la seguridad informática.
- ✓ No reportaron Violaciones de Seguridad 10%
- ✓ Reportaron Violaciones de Seguridad 90%

De lo anterior:

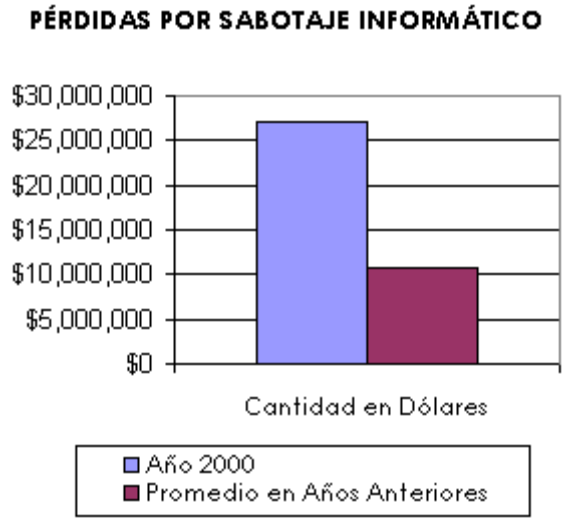
- ✓ 90% de los encuestados descubrió violaciones a la seguridad de las computadoras dentro de los últimos doce meses.

- ✓ 70% reportaron una variedad de serias violaciones de seguridad de las computadoras, y que el más común de estas violaciones son los virus de computadoras, robo de computadoras portátiles o abusos por parte de los empleados - por ejemplo, robo de información, fraude financiero, penetración del sistema por intrusos y sabotaje de datos o redes.

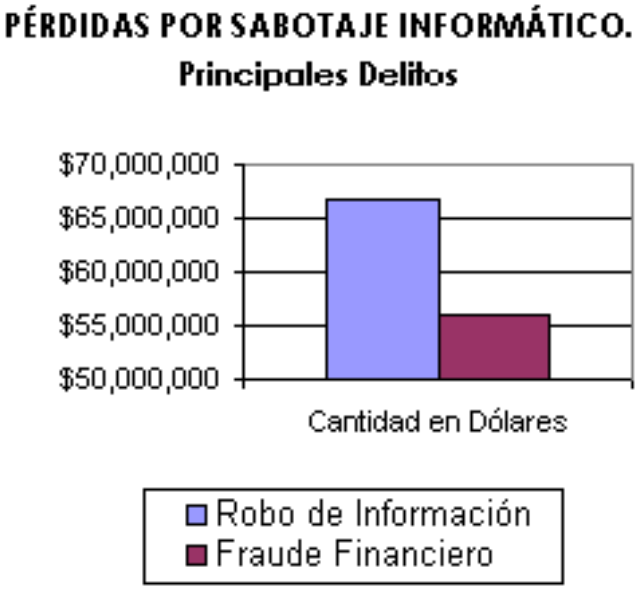
En cuanto a pérdidas financieras:

- ✓ 74% reconocieron pérdidas financieras debido a las violaciones de las computadoras.

- ✓ Las pérdidas financieras ascendieron a $265, 589,940 (el promedio total anual durante los últimos tres años era $120,240,180).



61 encuestados cuantificaron pérdidas debido al sabotaje de datos o redes para un total de $27,148,000. Las pérdidas financieras totales debido al sabotaje durante los años anteriores combinados ascendido a sólo $10,848,850. Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000). Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.



Como en años anteriores, las pérdidas financieras más serias, ocurrieron a través de robo de información (66 encuestados reportaron $66,708,000) y el fraude financiero (53 encuestados informaron $55,996,000).

Los resultados del estudio ilustran que esa amenaza del crimen por computadoras a las grandes corporaciones y agencias del gobierno viene de ambos lados dentro y fuera de sus perímetros electrónicos, confirmando la tendencia en años anteriores.

Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU.

En Singapur, el número de delitos cibernéticos detectados en el primer semestre del 2000, en el que se han recibido 127 denuncias, alcanza ya un 68 por ciento del total del año pasado, la policía de Singapur prevé un aumento este año en los delitos por Internet de un 38% con respecto a 1999.

En El Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen los programas (software) que utilizan. Esta proporción tan alta ha ocacionado que organismos Internacionales reacciones ante este tipo de delitos tal es el caso de BSA (Bussines Software Alliance).

Lo anterior hace de vital importancia para las organizaciones, la mayor difusión acerca de la seguridad en los sistemas informáticos.

Desafortunadamente, esta información no alcanza, en ocasiones a ser entendible para todas las personas, ya que se encuentra plasmada de una manera muy global. Frente a esto, se realiza esta investigación con la finalidad de llenar algunos huecos existentes en el tema.

Capítulo I:
Introducción a los sistemas informáticos

1.1 Generalidades

Desde la aparición del hombre, éste se ha visto en la necesidad de hacer cálculos y procesar la información para el desarrollo de sus actividades y la resolución de sus problemas.

A lo largo del tiempo, y movido por las necesidades existentes, el hombre ha recurrido a la invención de diferentes métodos que le permitieran organizar y manejar la información de manera eficiente; y tecnología que sea capaz de procesar los datos.

Este avance, determina dispositivos capaces de realizar cálculos con mayor facilidad y velocidad que como la realizaría el ser humano.

1.2 Conceptos básicos

Algunos de los términos básicos relacionados con los sistemas informáticos son:

- ✓ Sistema
- ✓ Computadora
- ✓ Información

Por supuesto, existen muchos más conceptos que tienen una relación con los sistemas de información, y cabe mencionar que ninguno de ellos es despreciable o irrelevante; pero por razones de espacio y tiempo, nos avocaremos a estos tres.

1.2.1 Sistema

En su definición más general, un sistema es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo.

Los sistemas son muy diferentes unos de otros Los sistemas reciben datos, energía o materia del ambiente; y proveen información, energía o materia. Es decir, posee entradas y salidas; como correspondiente, realiza un proceso .Esto se observa en la figura 1.1.

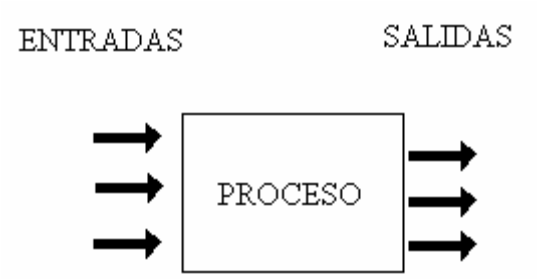


Figura 1.1 Funcionamiento de un sistema

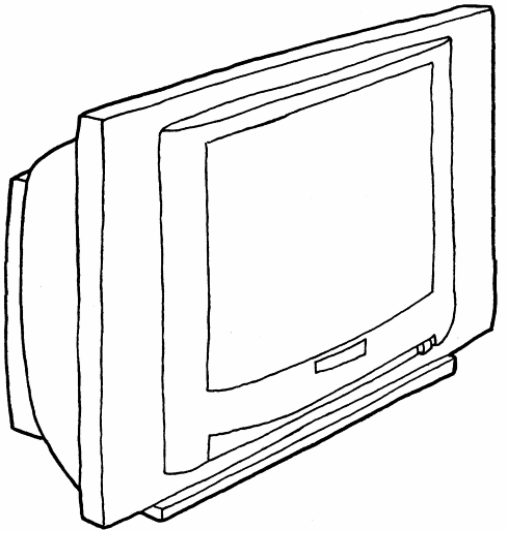
Un sistema puede ser:

- ✓ Físico o concreto
- ✓ Abstracto o conceptual

Un sistema es físico cuando es tangible, como ejemplos podemos mencionar: computadoras, televisores, humanos. Como muestra, está la figura 1.2

a) Computadora

b) Televisor



c) Ser humano

Figura 1.2 Ejemplos de sistemas físicos

Un sistema es abstracto si se refiere a elementos intangible, por ejemplo, el software de una computadora.

Los sistemas tienen límites o fronteras, que los diferencian del ambiente. Ese límite puede ser:

- ✓ Físico (el gabinete de una computadora)
- ✓ Conceptual.

Si hay algún intercambio entre el sistema y el ambiente a través de ese límite, el sistema es abierto, de lo contrario, el sistema es cerrado.

El ambiente es el medio en externo que envuelve física o conceptualmente a un sistema. El sistema tiene interacción con el ambiente, del cual recibe entradas y al cual se le devuelve salidas. El ambiente también puede ser una amenaza para el sistema.

Un grupo de elementos no constituye un sistema si no hay una relación e interacción, que dé la idea de un "todo" con un propósito.

En informática existen gran cantidad de sistemas:

- ✓ Sistema operativo
- ✓ Sistema experto
- ✓ Sistema informático
- ✓ Aplicación o software

Cabe mencionar que los usuarios (seres humanos) forman parte del sistema.

1.2.2 Computadora

La computadora se define como una máquina electrónica rápida y exacta que es capaz de aceptar datos a través de un medio de entrada, procesarlos automáticamente bajo el control de un programa previamente almacenado, y proporcionar la información resultante a un medio de salida.

En este contexto, una computadora puede considerarse como un sistema, y se puede representar gráficamente como lo muestra la figura 1.3

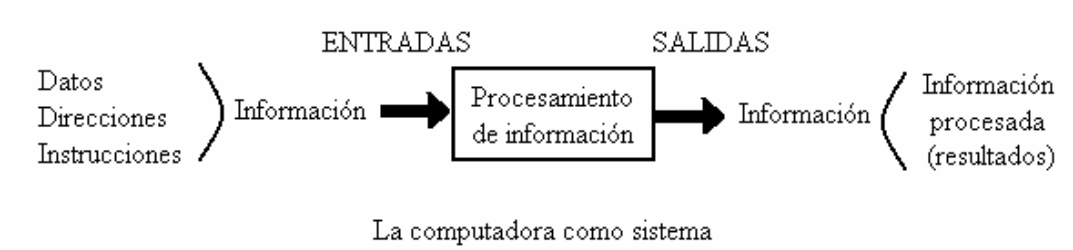


Figura 1.3 La computadora como sistema

Las computadoras pueden clasificarse en base a diferentes criterios; algunos de ellos son: por la forma en que trabajan; por su función o propósito; por su tamaño y potencia; por la manera en que se conectan.

De acuerdo a la forma que procesan los datos, las computadoras puede clasificarse en:

- ✓ Digital
- ✓ Analógica
- ✓ Híbrida

Las computadoras procesan datos discretos, trabajan contando números que representan cifras, letras o algunos otros símbolos especiales.

Las computadoras analógicas procesan datos que están medidos en una escala continua.

Las computadoras híbridas mezclan las características de las anteriores, utilizando simultáneamente las técnicas analógicas y las digitales en sus componentes.

De acuerdo a su propósito, se pueden clasificar en:

- ✓ De propósito especial o específico
- ✓ De propósito general

Las computadoras de propósito especial están diseñadas para un propósito específico, mientras que las de propósito general pueden almacenar diferentes programas y puede ser utilizada en distintas aplicaciones.

De acuerdo a su tamaño y potencia, se clasifican en:

- ✓ Microcomputadoras PC
- ✓ Microcomputadoras mini
- ✓ Maxicomputadora mainframe
- ✓ Supercomputadora

Las microcomputadoras PC son los dispositivos más pequeños que pueden programarse; la minicomputadoras Mini son de tamaño medio, y mas costosas que una PC; una maxicomputadora puede puede controlar muchos dispositivos de E/S; mientras que las supercomputadoras son las más rápidas y costosas.

De acuerdo a la manera en que están conectadas, las computadoras pueden ser:

- ✓ Sistema monousuario
- ✓ Sistema multiusuario
- ✓ Sistema en red

Las computadoras en sistema monousuario están diseñadas para usarse por una sola persona a la vez, operan sistema operativo monousuario, utilizando una microcomputadora.

Un sistema multiusuario utiliza muchos de los microprocesadores que se encuentran en las PCs, pero pueden manejar varias tareas en forma concurrente.

Un sistema en red es un conjunto de computadoras conectadas entre sí para compartir recursos.

La figura 1.4 muestra la vista tradicional de una computadora.

Figura 1.4 Vista clásica de una computadora

1.2.3 Información

Cada persona tiene un concepto diferente de lo que es información; por ello, se dice que el concepto de información se puede definir de diversas maneras. Algunas de ellas se pueden mencionar como sigue:

> "Se entiende por información al elemento que hay que tratar y procesar cuando en una computadora ejecutamos un programa, y se define como todo aquello que permite adquirir cualquier tipo de conocimiento; por tanto, existirá información cuando se da a conocer algo que se desconoce."

> "Por información puede entenderse, con carácter general, un conjunto de símbolos- códigos - que representan hechos, objetos o ideas que se quieren comunicar"

> “Se utiliza el término información para referirse a todo aquello que está presente en un mensaje o señal cuando se establece un proceso de comunicación entre un emisor y un receptor"... "la información puede entonces encontrarse y enviarse en muchas formas, a condición de que quien la reciba pueda interpretarla"

En sí, la información son datos que se perciben por medio de los sentidos, quienes los integran para generar la información y producir conocimiento. Se reciben las señales informativas y quedan almacenadas en nuestro cerebro. El hombre usa su cerebro para procesar dicha información, modificarla y producir otra nueva.

Mediante la experiencia que ha acumulado la humanidad, se almacena la información y la transmiten de un ser humano a otro.

Todo, absolutamente todo lo que produce el hombre, es resultado de la información que a lo largo de los siglos ha conseguido acumular. Por ello, el hombre satisface sus necesidades específicamente humanas, mediante el uso de la información que le han proporcionado otros hombres.

1.2.3.1 Proceso de información

Para la que la información cumpla con sus funciones debemos procesarla, lo que implica almacenamiento, la organización, y sobre todo la transmisión de la misma.

La transmisión de la información está basada en tres elementos:

- ✓ Emisor
- ✓ Medio o canal de transmisión
- ✓ Receptor

El emisor es quien da origen a la información y que la codifica adecuándola al canal de transmisión; el medio permite que circule la información; el receptor es quien recibe la información y la decodifica.

Sin embargo, cabe mencionar que la información que se recibe nunca es igual a la que se ha emitido ya que se hace una aportación con el propósito de perfeccionarla y hacerla más completa.

En la figura 1.5 se muestra la secuencia de estos tres elementos:

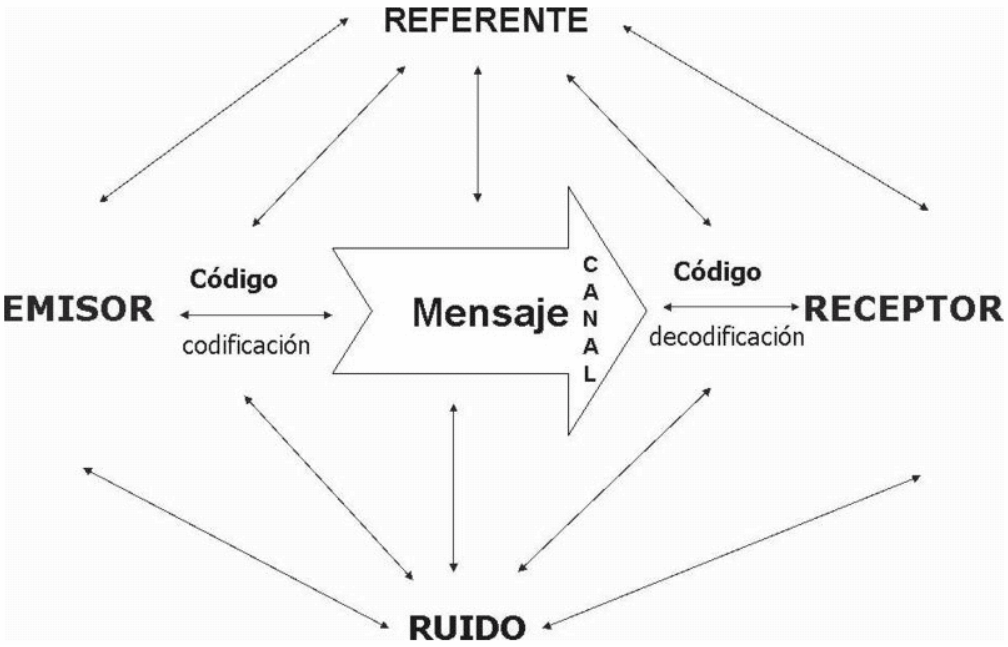


Figura 1.5 Secuencia de la transmisión de información

1.2.3.2 Tipos de información

La información se puede manifestar de cinco formas:

- ✓ Saber
- ✓ Conocimiento
- ✓ Tecnología
- ✓ Logística
- ✓ Derechos.

El saber es la información que almacena el cerebro; el conocimiento es la información del tipo saber que ha sido articulada y codificada en palabras e imágenes expresamente por un individuo para que sea interpretada por otro; la tecnología es el tipo de información del tipo saber que ha sido acumulada en objetos pero que no ha sido articulada y codificada.

En efecto, todo instrumento elaborado por un hombre contiene información que otro hombre puede interpretar y aprender en cierta medida; se le conoce como logística a la información codificada mediante el orden o distribución de instrumentos, personas y actividades en el espacio y en el tiempo; cuando se habla de derechos, se refiere a la información almacenada en los cerebros de los seres humanos que establecen relaciones de asignación entre instrumentos e individuos.

1.2.3.3 Funciones de la información

La información realiza muchas funciones, entre las que se encuentran:

- ✓ Aumentar el conocimiento de quien la usa.

- ✓ Proporcionar a quien Toma de decisiones la materia prima fundamental para el desarrollo de soluciones y la elección.

- ✓ Proporcionar una serie de reglas de evaluación y de decisión para fines de control.

- ✓ Nos permite construir lo que en general llamamos conocimiento que permite la resolución de problemas o la toma de decisiones.

- ✓ Procesa y genera el conocimiento humano.

Cabe aclarar que el individuo que hace uso de la información es quien valora lo significativo de la misma, la organiza y la convierte en conocimiento.

1.3 Definición de sistema informático

La informática es producto del encuentro de dos tecnologías: la de las máquinas de comunicar y la de las computadoras.

El proceso de información en la informática se resuelve de la siguiente manera:

- ✓ Lenguajes
- ✓ Códigos
- ✓ Representaciones.

Al lenguaje que es comprendido y utilizado por el ordenador se le denomina lenguaje o código máquina y consiste en instrucciones formadas por secuencias de "unos" (1) y "ceros" (0).

El ordenador trabaja con señales eléctricas, por lo que el canal por donde viaja la información son los circuitos electrónicos del ordenador. Los circuitos solo pueden dar dos situaciones: que pase corriente "1", o que no pase corriente "0".

Para el procesamiento y representación del lenguaje del ordenador se necesita de un sistema, al que se le denomina sistema informático.

De manera general, un sistema se define como el conjunto de elementos materiales necesarios (medios) e inmateriales (métodos) cuyos estados se encuentran relacionados entre sí.

De esta manera:

> "Un sistema informático es un conjunto de medios y métodos interrelacionados entre sí que permiten el tratamiento y flujo de la información, cuyo objetivo es el procesamiento de los datos para obtener información útil para el ser humano"

1.4 Composición de un sistema informático

Cada sistema existe dentro de otro más grande; por lo tanto, un sistema puede estar formado por subsistemas y partes; y, a la vez, puede ser parte de un supersistema.

En su forma más simple, un sistema informático se compone de tres elementos:

- ✓ Medios o hardware
- ✓ Métodos o software
- ✓ Soporte humano (usuarios)

Por otra parte, un sistema informático típico emplea una computadora, que utiliza dispositivos programables para realizar tareas tales como:

- ✓ Captura de datos
- ✓ Almacenamiento de información
- ✓ Proceso de datos

En este sentido, la computadora personal, junto con la persona que lo maneja y los periféricos que los envuelven, resultan un ejemplo de sistema informático. Esto se observa en la figura 1.6

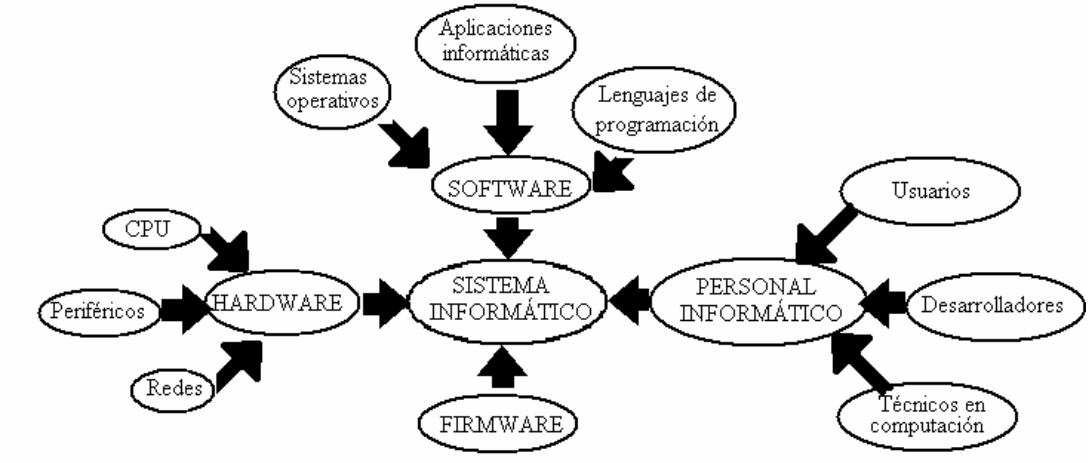


Figura 1.6 Interacción del sistema informático

Incluso la computadora más sencilla, se clasifica como un sistema informático, porque al menos dos componentes (hardware y software) tienen que trabajar unidos.

Sin embargo, el genuino significado de "sistema informático" viene mediante la interconexión.

Muchos sistemas informáticos pueden interconectarse, esto es, unirse para convertirse un sistema mayor. La interconexión de sistemas informáticos puede tornarse difícil debido a incompatibilidades. A veces estas dificultades ocurren a nivel de hardware, mientras que en otras ocasiones se dan entre programas informáticos que no son compatibles entre sí.

1.4.1 Medios

Los Medios, mejor conocido como hardware, se designa en un sistema informático a los componentes físicos del sistema. Constituido por un conjunto de elementos mecánicos, magnéticos, ópticos, eléctricos y electrónicos que forman parte del sistema informático.

La función de estos componentes suele dividirse en tres categorías principales:

- ✓ Entrada
- ✓ Salida
- ✓ Almacenamiento.

Los componentes de esas categorías están conectados a través de un conjunto de cables o circuitos llamado bus con la unidad central de proceso (CPU) del ordenador, el microprocesador que controla la computadora y le proporciona capacidad de cálculo.

El hardware, por consiguiente, está constituido por los dispositivos de entrada, las unidades de salida y los dispositivos de almacenamiento.

La figura 1.7 muestra la interacción entre las categorías de medios.

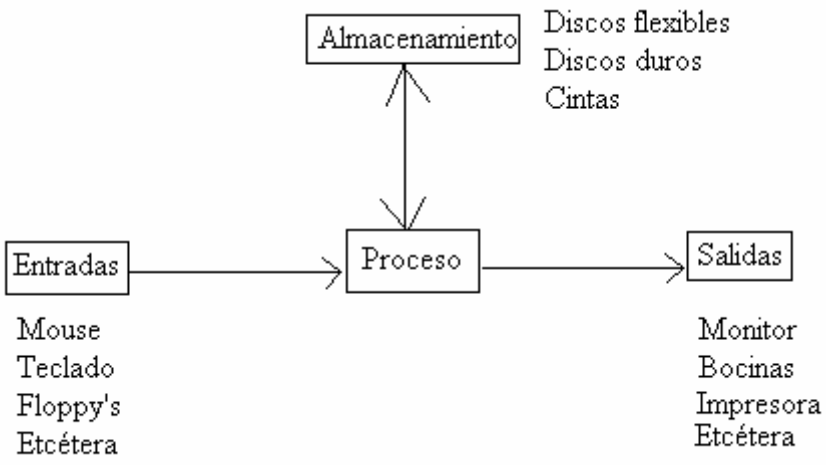


Figura 1.7 Interacción de medios

1.4.1.1 Dispositivos de entrada

Estos dispositivos permiten al usuario del ordenador introducir datos, comandos y programas en la CPU.

El dispositivo de entrada más común es un teclado, similar al de las máquinas de escribir. La información introducida con el mismo, es transformada por el ordenador en modelos reconocibles.

Otros dispositivos de entrada son:

- ✓ Los lápices ópticos, que transmiten información gráfica desde tabletas electrónicas hasta el ordenador.

- ✓ Los joysticks, el ratón o mouse, que convierte el movimiento físico en movimiento dentro de una pantalla de ordenador; los escáneres luminosos, que leen palabras o símbolos de una página impresa y los traducen a configuraciones electrónicas que el ordenador puede manipular y almacenar; y los módulos de reconocimiento de voz, que convierten la palabra hablada en señales digitales comprensibles para el ordenador. También es posible utilizar los dispositivos de almacenamiento para introducir datos en la unidad de proceso.

Los elementos de entrada más comunes se muestran en la figura 1.8

a) Teclado

b) Mouse

Figura 1.8 Vista clásica de los dispositivos de entrada más comunes

1.4.1.2 Unidades de salida

La pantalla es el dispositivo estándar de salida del computador, en el cual se presentan las respuestas del computador y los resultados de un proceso. También muestra la información ingresada mediante el teclado; se le denomina también monitor. Las características son similares a las de una pantalla de televisión.

Existen monitores monocromáticos (en blanco y negro) y a color. Las imágenes están formadas por puntos llamados píxeles. La nitidez y la calidad de la imagen dependen de la cantidad de píxeles que maneja la pantalla, o sea la resolución. La pantalla se conecta a la tarjeta controladora de video ubicada en la CPU.

La impresora es el dispositivo de salida más utilizado. Una impresora imprime series de caracteres, líneas o páginas con base en la información que le envía la CPU a través de un puerto (generalmente paralelo). La impresora puede ser de diversos tipos y funcionar de maneras diferentes.

Existe otra tecnología basada en rayo láser, más costosa y sofisticada, que imprime páginas completas; es similar a las fotocopiadoras, con mayor velocidad y resolución que las impresoras de chorro de tinta, llamadas impresoras láser.

La vista clásica de los periféricos de salida se muestra en la figura 1.9

a) Impresora

b) Monitor

Figura 1.9 Vista clásica de los periféricos de salida

1.4.1.3 Dispositivos de almacenamiento

Los sistemas informáticos pueden almacenar los datos tanto interna (en la memoria) como externamente (en los dispositivos de almacenamiento).

Internamente, las instrucciones o datos pueden almacenarse por un tiempo en los chips de silicio de la RAM (memoria de acceso aleatorio) montados directamente en la placa de circuitos principal de la computadora, o bien en chips montados en tarjetas periféricas conectadas a la placa de circuitos principal del ordenador.

Otro tipo de memoria interna son los chips de silicio en los que ya están instalados todos los conmutadores.

Tanto los primeros como los segundos están enlazados a la CPU a través de circuitos.

1.4.2 Métodos

Los métodos son mejor conocidos en el ámbito computacional como software. Se le designa de ésta manera a todo lo referente a los métodos que se emplean para el tratamiento de la información. Es el componente lógico del sistema.

El estudio del software abarca a:

- ✓ Los lenguajes para comunicarse con los ordenadores
- ✓ Los programas para darles instrucciones
- ✓ Los programas de utilidades y aplicaciones
- ✓ Los sistemas operativos
- ✓ Etcétera.

De esta manera, el software puede dividirse en varias categorías según el tipo de trabajo realizado. Las dos categorías primarias de software son:

- ✓ Los sistemas operativos (software del sistema)
- ✓ El software de aplicación

Los sistemas operativos controlan los trabajos de la computadora. Procesa tareas tan esenciales, aunque a menudo invisibles, tales como el mantenimiento de los archivos del disco y la administración de la pantalla.

El software de aplicación dirige las distintas tareas para las que se utilizan las computadoras. Lleva a cabo tareas de tratamiento de textos, gestión de bases de datos y similares. Constituyen dos categorías separadas:

- ✓ El software de red, que permite comunicarse a grupos de usuarios
- ✓ El software de lenguaje, que es utilizado para escribir programas.

1.4.2.1 Sistema operativo

El Sistema Operativo es el programa que oculta la verdad del Hardware al programador y presenta una vista simple y agradable de los archivos nominados que pueden leerse y escribirse.

También, resguarda al programador y presenta una interfaz simple, orientada al archivo, disimula el trabajo concerniente a interrupciones, relojes o cronómetros, manejo de memoria y otras características. Su función es presentar al usuario con equivalente de una máquina virtual.

1.4.2.1.1 Objetivos del Sistema Operativo

Si bien un sistema operativo tiene a su cargo muchas funciones de la computadora y se considera como un elemento indispensable para cualquier sistema informático, se pueden enlistar sus principales objetivos de la siguiente manera:

- ✓ Transformar el complejo hardware de la computadora a una máquina accesible al usuario.

- ✓ Lograr el mejor uso posible de los recursos. Hacer eficiente el uso del recurso.

- ✓ Ejecutar los programas de los usuarios y facilitar la resolución de sus problemas.

1.4.2.1.2 Funciones del Sistema Operativo

Los objetivos y las funciones en un sistema operativo, suelen considerarse erróneamente como sinónimos, así que es importante mencionar que los objetivos son las metas que cubre y que las funciones son las acciones o tareas que lleva a cabo.

Entre las funciones de los sistemas operativos podemos destacar las siguientes:

- ✓ Aceptar todos los trabajos y conservarlos hasta su finalización.
- ✓ Interpretación de comandos
- ✓ Control de recursos
- ✓ Manejo de dispositivos de Entrada y Salida
- ✓ Manejo de errores
- ✓ Secuencia de tareas
- ✓ Protección
- ✓ Multiacceso
- ✓ Contabilidad de recursos

En la interpretación de comandos, el sistema operativo interpreta los comandos que permiten al usuario comunicarse con el ordenador

En el control de recursos, el sistema operativo coordina y manipula el Hardware de la computadora, como la memoria, las impresoras, las unidades de disco, el teclado o el Mouse.

En el manejo de dispositivos, organiza los archivos en dispositivos de almacenamiento, como discos flexibles, discos compactos o cintas magnéticas.

Para el manejo de errores, gestiona los errores de Hardware y la pérdida de datos.

En la secuencia de tareas, el Sistema Operativo debe administrar la manera en que se reparten los procesos, así como definir el orden que deben llevarse dichos procesos.

Se habla de protección, porque el sistema operativo es el encargado de evitar que las acciones de un usuario afecten el trabajo que está realizando otro usuario.

En el multiacceso, un usuario se puede conectar a otra máquina sin tener que estar cerca de ella.

En la contabilidad de recursos, el sistema operativo establece el costo que se le cobra a un usuario por utilizar determinados recursos.

1.4.2.1.3 Características de los Sistemas Operativos

Las características más relevantes de los sistemas operativos son:

- ✓ Conveniencia
- ✓ Eficiencia
- ✓ Habilidad para evolucionar
- ✓ Encargado de administrar el hardware
- ✓ Relacionar dispositivos (gestionar a través del kernel)
- ✓ Organizar datos para acceso rápido y seguro.
- ✓ Manejar las comunicaciones en red
- ✓ Procesamiento por bytes de flujo a través del bus de datos.
- ✓ Facilitar las entradas y salidas

Un Sistema Operativo hace más conveniente el uso de una computadora; asimismo, deberá construirse de manera que permita el desarrollo, prueba o introducción efectiva de nuevas funciones del sistema sin interferir con el servicio.

El Sistema Operativo se encarga de manejar de una mejor manera los recursos de la computadora en cuanto a hardware se refiere, esto es, asignar a cada proceso una parte del procesador para poder compartir los recursos; de la misma manera, se debe encargar de comunicar a los dispositivos periféricos, cuando el usuario así lo requiera.

También, se encarga de organizar datos para acceso rápido y seguro; también, permite al usuario manejar con alta facilidad todo lo referente a la instalación y uso de las redes de computadoras.

Provee un procesamiento por bytes de flujo a través del bus de datos; así como hacerle fácil al usuario el acceso y manejo de los dispositivos de Entrada/Salida de la computadora.

1.4.2.2 Software de aplicación

El Software de Aplicación se refiere a:

- ✓ Compiladores
- ✓ Sistemas de Bases de Datos
- ✓ Juegos de Videos
- ✓ Programas para negocios

Este software, define la forma en que los recursos se emplean para resolver los problemas de Computación de los usuarios.

1.4.3 Usuarios

Los usuarios de cualquier sistema informático son una parte fundamental para el funcionamiento de éste.

Existen diferentes tipos de usuarios, clasificados de acuerdo a sus características, a sus funciones o jerarquías, o al nivel de conocimientos que posean con respecto del sistema.

Capítulo II:
Generalidades en la vulnerabilidad de sistemas

2.1 Introducción

No existe un sistema que sea 100% seguro, todos tienen un punto vulnerable; de lo que se trata, es de minimizar los riesgos de que ataques ocurran en el sistema; éste es un proceso continuo y permanente.

Actualmente, los sistemas se han vuelto inestables debido a su incapacidad de impedir accesos "no autorizados"; esto ha provocado, a nivel empresa, pérdidas millonarias por robo de ideas, mercadotecnia, etcétera.

2.2 Términos relacionados

Algunos de los términos relacionados con la vulnerabilidad de sistemas son:

- ✓ Sistema
- ✓ Vulnerabilidad
- ✓ Activo
- ✓ Amenaza
- ✓ Impacto riesgo
- ✓ Ataque
- ✓ Desastre o contingencia

Algunos de estos conceptos suelen manejarse como sinónimos, aunque sí existen ciertas diferencias entre ellas.

2.2.1 Sistema

Se define como sistema a un conjunto de elementos organizados y relacionados que interactúan entre sí para lograr un objetivo.

Los sistemas poseen entradas; reciben datos, energía o materia del ambiente y proveen una salida.

Cada sistema existe dentro de otro más grande; así, un sistema puede estar formado por subsistemas y partes; y a la vez, puede formar parte de un supersistema.

La estructura del sistema se puede observar en la figura 2.1

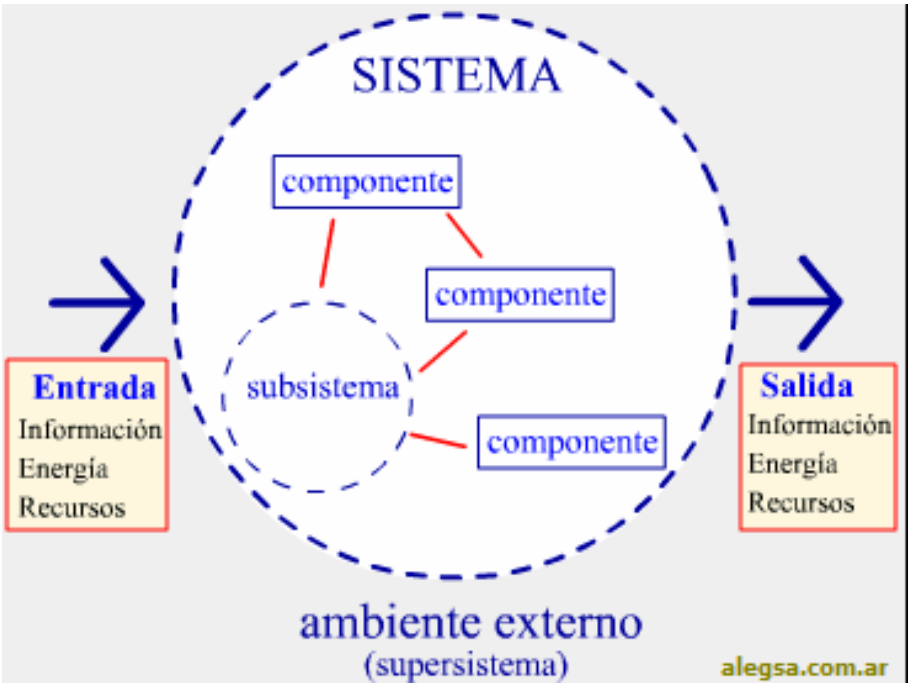


Figura 2.1 Estructura de un sistema

El ambiente es el medio externo que envuelve a un sistema. El sistema tiene interacción con el ambiente, del cual recibe entradas y al cual se le devuelven salidas. Cabe mencionar que el ambiente externo puede ser una amenaza para el sistema.

Un conjunto de elementos forma un sistema solamente si hay una relación e interacción, que dé la idea de un todo, y que éste lleve a un propósito.

2.2.2 Vulnerabilidad

Hablando de sistemas informáticos, la vulnerabilidad se refiere a una debilidad en un sistema, lo que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema y/o de sus datos y aplicaciones.

Se puede decir que la vulnerabilidad es el resultado de fallos en el diseño del sistema.

Sin embargo, puede ser también la consecuencia de las propias limitaciones tecnológicas; aquí retomamos la afirmación de que no existe un sistema que sea seguro por completo.

Bajo esa aseveración, se dice que las vulnerabilidades pueden ser teóricas o reales.

Por lo general, las vulnerabilidades en las aplicaciones suelen corregirse con parches o con cambios de versión; no obstante, algunas de éstas requieren de un cambio físico del sistema informático en cuestión.

Algunas vulnerabilidades comunes son:

- ✓ Desborde de pilas y otros buffer's
- ✓ Symlink races
- ✓ Errores en la validación de entrada
- ✓ Secuestro de sesiones
- ✓ Ejecución de código remoto
- ✓ XSS

A manera de esquema, se muestra en la figura 2.2 el seguimiento de estas vulnerabilidades:

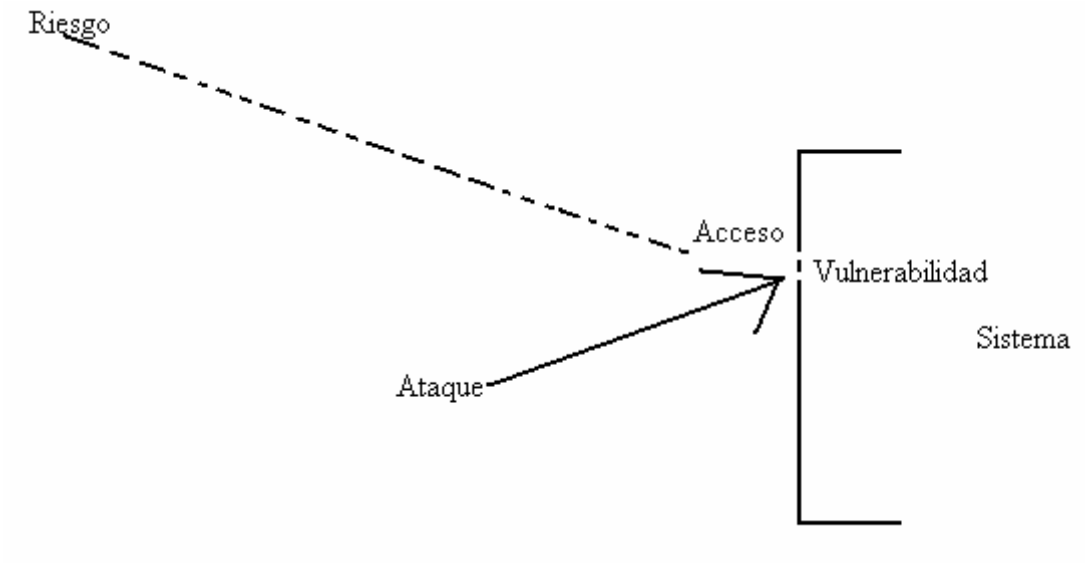


Figura 2.2 Riesgo y puerta de acceso a sistemas

2.2.3 Activo

Se define como activo aquel recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

2.2.4 Amenaza

Una amenaza es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

La amenaza no es un hecho y solamente es un enemigo potencial o latente en espera de una oportunidad.

2.2.5 Impacto

El impacto es la medición que se realiza para cuantificar la consecuencia al materializarse una amenaza.

El impacto depende de la organización afectada en particular.

2.2.6 Riesgo

El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

Se sabe que los riesgos pueden cuantificarse de acuerdo a la organización y a la afectación que se pueda hacer en ella.

2.2.7 Ataque

Se denomina como ataque a un evento que atenta sobre el buen funcionamiento del sistema, independientemente de que éste sea o no, exitoso.

2.2.8 Desastre o contingencia

El desastre, también llamado contingencia, es la interrupción de la capacidad de acceso a la información y al procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

2.3 Vulnerabilidades en ordenadores

La vulnerabilidad es un factor que no puede ser eliminado al 100% de ningún sistema, ya que no sólo los sistemas se actualizan en seguridad; también las personas interesadas en franquear los sistemas se actualizan.

Tan es así, que existe innumerable información acerca de estas vulnerabilidades y métodos de "corrección".

Cualquier persona que esté interesada en seguridad informática puede tener a su alcance una gran cantidad de información a este respecto; también es importante el conocer las versiones del software que se está usando y determinar si está actualizado.

Por otro lado, es indispensable en estos tiempos el conocer todas las posibilidades de la vulnerabilidad de sistemas y buscar formas de minimizarla.

Las personas para quienes es imperdonable el desconocimiento del tema son los administradores de sistemas y los responsables de la seguridad informática de las organizaciones, así como los investigadores de esta índole. También es un factor relevante en los auditores o personas encargadas de analizar el funcionamiento de los sistemas.

Como ya se comentó, una vulnerabilidad se define como un fallo en la concepción, desarrollo y/o implantación de un sistema informático, el cual puede permitir a un atacante eludir el planteamiento de seguridad del sistema en cuestión, posibilitándole la entrada o modificación de recursos a los que no debería de tener acceso, y que, en general, tiene fines maliciosos.

Un sistema informático puede ser software, hardware, o grupos de éstos.

2.4 Impacto debido a la vulnerabilidad

Una vulnerabilidad ofrece, de por sí, diversas desventajas en cuanto a acceso de usuarios no permitidos. Por otro lado, se puede determinar el grado de la vulnerabilidad de acuerdo con el impacto que provoca a la organización. Cabe mencionar que este impacto depende de la organización en particular. La vulnerabilidad, en este supuesto, puede ser:

- ✓ Alta
- ✓ Media
- ✓ Baja

Es alta si permite a un atacante remoto violar la protección de seguridad de un sistema; si permite a un atacante local ganar control completo del sistema; la pérdida de información es grande.

Se considera media como un punto de equilibrio entre alta y baja; en este sentido, se dice que es media si no es alta ni baja.

La vulnerabilidad es baja cuando el sistema no permite obtener información valiosa de por sí ni control del sistema; sin embargo, puede dar al atacante información que le permita encontrar otras debilidades en el sistema.

2.5 Ataques

Una vulnerabilidad puede permitir ataques de diversos tipos; una clasificación muy general sería:

- ✓ Local
- ✓ Remoto

Los ataques locales son aquellos que usan la vulnerabilidad pueden ser lanzados directamente en el sistema atacado. El intruso debe tener algún acceso previo al sistema para poder atacarlo. Esto se puede esquematizar como se observa en la figura 2.3.

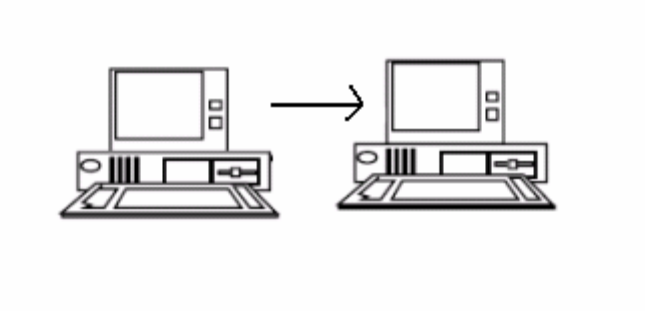


Figura 2.3 Ataque local

El ataque es remoto cuando el ataque se puede lanzar a través de una red contra un sistema en que el atacante no tuviera acceso previo.

Cabe mencionar que la víctima debe acceder de alguna manera a un sistema del atacante para que éste pueda explotar la vulnerabilidad. El caso más común es el de acceder, a través de un navegador, a páginas Web con código malicioso. Esto se observa en la figura 2.4

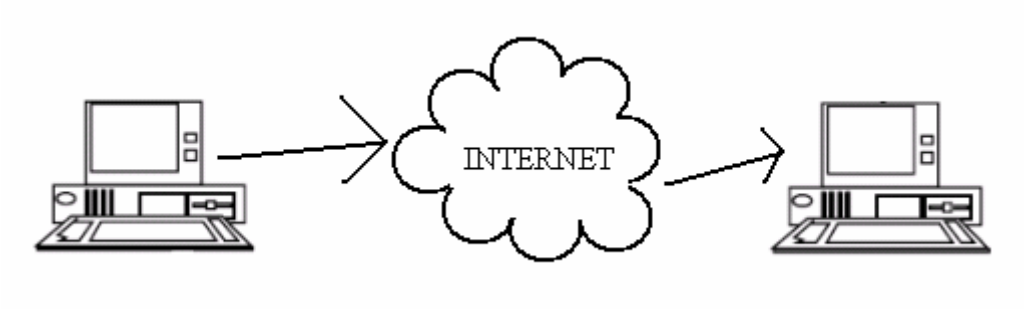


Figura 2.4 Ataque remoto

2.6 Pérdidas por vulnerabilidad

A las vulnerabilidades se le asignan las siguientes etiquetas no excluyentes entre sí:

- ✓ Disponibilidad
- ✓ Confidencialidad
- ✓ Integridad
- ✓ Protección de seguridad

Se habla de ataque a la disponibilidad si la vulnerabilidad permite un ataque que imposibilita directamente a un usuario, sea humano o máquina, el acceso a un recurso del sistema en particular. Los más comunes son los ataques de denegación de servicio (DoS).

Se refiere a ataque a la confidencialidad si permite el robo de información.

Un ataque a la integridad permite cambiar la información que reside o que pasa por un sistema.

Si el ataque elude la protección de seguridad, da al atacante privilegios en un sistema que el atacante no debería tener por la política de seguridad del sistema. En este apartado, los ataques se subdividen de acuerdo a los privilegios que obtiene el atacante; de esta manera, puede ser:

- ✓ Superusuario
- ✓ Usuario normal
- ✓ Otro tipo

2.7 Tipos de vulnerabilidad

Dependiendo del origen de la vulnerabilidad, ésta puede tener una o varias de las siguientes características:

- ✓ Error en validación de entrada
- ✓ Desbordamiento de límites
- ✓ Desbordamiento de buffer
- ✓ Secuencias de comandos en sitios cruzados
- ✓ Error de validación de acceso
- ✓ Error de manejo de condición excepcional
- ✓ Error de entorno
- ✓ Error de configuración
- ✓ Condición de carrera
- ✓ Error de diseño
- ✓ Otros

2.7.1 Error en validación de entrada

Es un error en la validación de entrada cuando la entrada que procesa un sistema no es comprobada adecuadamente de forma que una vulnerabilidad puede ser aprovechada por una cierta secuencia de entrada.

Este tipo de vulnerabilidad y sus subcategorías sólo se aplican a entradas formadas maliciosamente.

2.7.2 Desbordamiento de límites

El desbordamiento de límites ocurre cuando la entrada recibida por un sistema, sea de origen humano o máquina, hace que exceda los límites de funcionamiento normal y produzca una vulnerabilidad.

Por ejemplo, el sistema se queda sin memoria, sin espacio en disco, o colapsar la red. También podrían ser variables del sistema mal controladas, que lleguen a su máximo valor y salte al mínimo, o forzar una división por cero no tratada.

2.7.3 Desbordamiento de buffer

El desbordamiento de buffer es, sin duda, la más clásica de las fuentes de vulnerabilidades.

Ésta se produce cuando la entrada de un sistema es mayor que el área de memoria asignada para contenerla (buffer) y el sistema no lo comprueba adecuadamente. Entonces el buffer de entrada "se desborda" y escribe en zonas de memoria contiguas.

Construyendo inteligentemente el exceso de entrada, un atacante puede hacer caer el sistema e incluso ejecutar instrucciones de forma arbitraria.

2.7.4 Secuencias de comandos en sitios cruzados

Las secuencias de comandos cruzados (XSS o CSS), aplicable en principio a aplicaciones web o sitios web dinámicos, consiste en que se pueda ejecutar código de un dominio desde otro dominio, de forma que se perjudica a otro usuario, no al sitio web directamente.

Por ejemplo, supongamos un sitio Web de subastas que en el mensaje de error de "página no encontrada" incluye la página pedida, sin filtrar.

Un usuario malicioso puede poner un enlace a una página inexistente y con código (javascript, vbscript, activex o cualquiera que se pueda ejecutar en el ordenador de la víctima) de forma que en el mensaje de error se incruste ese código, que se ejecuta en el navegador de la víctima. Por ejemplo puede redirigirla a una falsificación del sitio de subastas y capturar su nombre de usuario y contraseña.

2.7.5 Error de validación de acceso.

Este error se produce cuando el mecanismo de control de acceso es defectuoso.

2.7.6 Error de manejo de condición excepcional

Se produce cuando el sistema se vuelve vulnerable cuando se produce una condición de funcionamiento no habitual, por ejemplo errores en la red, que el sistema no maneja adecuadamente.

2.7.7 Error de entorno

Una vulnerabilidad se caracteriza de esta manera si el entorno en que un sistema está instalado de alguna manera hace al sistema vulnerable.

Esto puede ser debido, por ejemplo, a una interacción no prevista entre una aplicación y el sistema operativo, o entre dos aplicaciones corriendo en el mismo anfitrión.

Este sistema probablemente es perfectamente seguro en las pruebas que ha hecho el desarrollador, pero en el entorno en que se ha instalado de alguna manera no cumple las condiciones de seguridad supuestas.

2.7.8 Error de configuración

Si la configuración controlable por el usuario es tal que el sistema es vulnerable. La vulnerabilidad no es debida al diseño del sistema si no a como el usuario final configura el sistema.

También se considera error de este tipo cuando la configuración por defecto del sistema es insegura, por ejemplo una aplicación recién instalada.

2.7.9 Condición de carrera

Se produce cuando la no atomicidad de una comprobación de seguridad causa la existencia de una vulnerabilidad.

Por ejemplo, un sistema comprueba si una operación es válida es permitida por el modelo de seguridad y luego la ejecuta.

Sin embargo, en el tiempo que pasa desde que se hace la comprobación hasta que se ejecuta la operación las condiciones cambian de forma que la operación ya no es válida.

Un atacante puede aprovechar esta pequeña ventana de oportunidad y hacer a un sistema efectuar operaciones no válidas, como escribir en un fichero de contraseñas.

2.7.10 Error de diseño

Una vulnerabilidad se caracteriza como "error de diseño" si no hay errores en la implementación ni en la configuración de un sistema, si no que el diseño inicial es erróneo.

2.7.11 Otros

Cuando se encuentra una vulnerabilidad que no cae en ninguna de las categorías anteriores.

2.8 Sistemas expuestos

Los sistemas tienen, aunque no explícitamente, un componente expuesto, que es la parte concreta que produce la vulnerabilidad. Los tipos posibles de componentes expuestos son:

- ✓ Sistema operativo
- ✓ Pila de protocolos
- ✓ Aplicación servidora
- ✓ Aplicación no servidora
- ✓ Hardware
- ✓ Protocolo de comunicaciones
- ✓ Módulo de cifrado
- ✓ Otro componente no definido

Los tipos de sistemas expuestos son:

- ✓ Servidor
- ✓ Estación de trabajo
- ✓ Dispositivo de red/seguridad
- ✓ Otro

Capítulo III: Importancia de la seguridad en informática

3.1 Introducción

Garantizar que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática.

Hablar de seguridad informática en el momento actual no parece que suponga un alarde de modernidad y novedad.

Con el desarrollo de los ordenadores personales, la vertiginosa evolución de Internet, la implantación del comercio electrónico y el impulso de la denominada "Sociedad de la Información", todo el mundo habla, sabe y se preocupa de la seguridad en estos ámbitos.

De una estructura informática basada en sistemas propietarios y grandes servidores manejada por personal técnico, con una formación muy específica y alejada del conocimiento del común de los mortales, se ha evolucionado a otra más amigable y cercana al usuario final.

Ello ha supuesto que los niveles iniciales de conocimiento sean rápidamente adquiridos por cualquier persona interesada, sin especiales conocimientos técnicos en la materia.

La "globalización" en el conocimiento ha supuesto una quiebra de la seguridad de tiempos pasados amparada, en gran medida, en un cierto ocultismo.

Cabe mencionar que los sistemas anteriores no eran más seguros que los actuales, tan sólo eran mucho más desconocidos.

3.2 Seguridad

En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

De esta forma, se define como seguridad informática a aquellas 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 los datos
- ✓ El acceso a bases de datos por personas no autorizadas.

Diversas técnicas sencillas pueden dificultar la delincuencia informática, al impedir que personas no autorizadas puedan observar la pantalla del ordenador, manteniendo la información y los ordenadores bajo llave o retirando de las mesas los documentos sensibles. Sin embargo, impedir los delitos informáticos exige también métodos más complejos.

En un sistema de los denominados 'tolerante a fallos' dos o más ordenadores funcionan a la vez de manera redundante, por lo que si una parte del sistema falla el resto asume el control.

Los virus informáticos son programas, generalmente destructivos, que se introducen en el ordenador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro. Existen programas antivirus que los reconocen y son capaces de 'inmunizar' o eliminar el virus del ordenador.

Para evitar problemas en caso de apagón eléctrico existen las denominadas UPS (acrónimo de Uninterrupted Power Supply), baterías que permiten mantener el sistema informático en funcionamiento, por lo menos el tiempo necesario para apagarlo sin pérdida de datos.

Sin embargo, la única forma de garantizar la integridad física de los datos es mediante copias de seguridad. El mayor problema que tienen que resolver las técnicas de seguridad informática es el acceso no autorizado a datos.

3.3 Parámetros de seguridad

La seguridad informática se encuentra condicionada por:

- ✓ La elección del sistema operativo
- ✓ Una versión estable de sistema operativo
- ✓ Una configuración estable

3.4 Errores característicos

Existe una cierta tendencia a minimizar el ámbito de actuación del aspecto de la seguridad en el mundo de la Informática. Se cae, habitualmente, en abordar la implantación de la seguridad como respuesta a un problema o situación específica sin estudiar todos los elementos que puedan estar relacionados.

Si se habla de una plataforma Web abierta a Internet, la seguridad no es responder si instalamos tal o cual cortafuegos, es mucho más que eso:

- ✓ Sistemas de alimentación ininterrumpida para máquinas críticas
- ✓ Duplicidad de almacenamiento
- ✓ Control físico
- ✓ Auditoria de conexiones internas y externas
- ✓ Blindaje de ficheros de sistema
- ✓ Control de modificación de ficheros
- ✓ Monitorización de tráfico de red
- ✓ Política de salvaguardas
- ✓ Etcétera

3.5 Sistemas seguros

Un concepto global de seguridad informática sería aquel definido como el conjunto de procedimientos y actuaciones encaminados a conseguir la garantía de funcionamiento del sistema de información, obteniendo eficacia, manteniendo la integridad, y alertando la detección de actividad ajena.

Si esto puede obtenerse (hecho que no es sencillo conseguir), se podrá decir que se dispone de un sistema seguro.

Es de aclarar que el sistema debe ser seguro en cuanto a todos sus elementos, el hardware y el software.

Dentro del área del Hardware los objetos de nuestra atención son fundamentalmente:

- ✓ Servidores
- ✓ Clientes
- ✓ Líneas de comunicaciones.

Dentro del área de Software los objetos de nuestra atención son:

- ✓ Sistema operativo
- ✓ Bases de datos
- ✓ Aplicaciones.

3.6 Agresiones a sistemas

Las agresiones potenciales a sistemas informáticos pueden ser de dos pisos:

- ✓ Maliciosas
- ✓ No maliciosas

3.6.1 Agresiones maliciosas

Las intervenciones maliciosas van ligadas a la manipulación humana. Las más peligrosas potencialmente, por el alcance del daño que se puede provocar y por la mayor dificultad en su detección, son las internas al propio sistema de información.

Los agresores se pueden dividir en:

- ✓ Interno
- ✓ Externo

Dentro de la agresión interna, el agresor queda enmarcado dentro de los administradores del sistema, programadores o usuarios privilegiados, también se incluye a aquel que, no teniendo acceso lógico al sistema, sí lo tuviese físico a elementos críticos del mismo.

Las grandes quiebras de seguridad han provenido siempre del interior de las estructuras atacadas y la mayor parte de las veces se han silenciado en un primer momento para no provocar reacciones incontroladas.

La mayor peligrosidad de este tipo de actuaciones viene derivada del mayor conocimiento que el agresor dispone del medio sobre el que actúa.

El otro tipo de intervención maliciosa es la de origen externo y que se produce casi siempre a través de línea de comunicaciones, como ejemplo más claro y actual podemos contemplar las intrusiones a través de Internet.

3.6.2 Agresiones no maliciosas

Las intervenciones no maliciosas, ya sean por manipulaciones humanas o no, son imprevisibles y de resultado incierto.

Las más habituales se refieren a cortes de corriente o alteraciones importantes en los niveles de tensión en la alimentación eléctrica que pueden provocar hasta daños irrecuperables en determinado hardware.

Los fallos en el hardware son muy comunes, de ello, no resulta extraño que los discos duros sean inutilizados por esta práctica, lo que implica la posibilidad de pérdida de información o el fallo de placas de sistema.

Otro tipo de fallo habitual es el que se deriva de funcionamientos anormales de software, principalmente cuando se encuentra en fase de prueba o validación.

Por otro lado, tampoco son extraños los accidentes que se pueden denominar como laborales:

- ✓ El cigarrillo sobre la cinta de salvaguarda que cuando reaccionamos ha fundido la tapa con el soporte magnético
- ✓ El café que tiene a bien explorar las interioridades de una CPU
- ✓ Los discos que pasan por el arco detector de metales
- ✓ Etcétera

3.7 La seguridad es importante

La seguridad es un factor imprescindible en cualquier organización; esto debido a la existencia de personas ajenas a la información que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos. Estas personas reciben, comúnmente, el nombre de “piratas informáticos” “piratas cibernéticos” o “hackers”.

Generalmente, estos personajes forman parte del personal administrativo o de sistemas de la organización en cuestión, aunque hay intrusiones que surgen de manera externa totalmente al sistema. De acuerdo con los expertos, más del 70% de las violaciones e intrusiones a los recursos informáticos son realizadas por el personal interno, debido a que estos tienen más facilidad e ello: tienen conocimiento de los procesos y las metodologías; también 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.

Esta situación se presenta como consecuencia de los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

El resultado, es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización, lo que puede representar un daño con valor de miles o millones de dólares.

3.8 Amenazas

Las amenazas (cuyo concepto ya vimos en el capítulo pasado), son el factor a evitar en todos los sistemas. Dado que los riesgos han evolucionado a la par de la misma seguridad informática, el evitarlas es una tarea muy complicada. No obstante, la seguridad debe llevarse a cabo si se quiere mantener la independencia de la información que se maneja.

En el área de la informática, existen siempre riesgos, tales como:

- ✓ Ataque de virus
- ✓ Códigos maliciosos
- ✓ Gusanos
- ✓ Caballos de Troya
- ✓ Hackers

Sin embargo, con la adopción de la Internet como instrumento de comunicación y colaboración, los riesgos han ido cambiando y mejorando y, actualmente, las empresas deben enfrentar amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

Específicamente, en los ataques de negación de servicio, el equipo de cómputo ya no es un blanco, sino el medio a través del cual es posible afectar todo el entorno de red; es decir, anular los servicios de la red, saturar el ancho de banda o alterar el Web Site de la compañía. Con ello, es evidente que los riesgos están en la red, no en la PC.

Es por la existencia de un número importante de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo.

Para ello, resulta importante establecer políticas de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos.

3.8.1 Ataque de virus

El ataque de virus suele ser un factor de ataque muy común en los sistemas informáticos.

Un virus informático es un programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Es decir, el virus es un pequeño software que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado o el sector de arranque sea leído. De esta manera, el programa del virus es activado y se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se replique a sí mismo.

3.8.1.1 Funciones de los virus

Los virus pueden llegar a esconderse para evitar la detección y reparación; para ello, realiza las siguientes actividades:

- ✓ Mantiene un espacio mínimo para ser almacenado, esto le da la facilidad de esparcirse más rápidamente y reduce el riesgo de ser detectado.
- ✓ El virus reorienta la lectura del disco para evitar ser detectado.
- ✓ Los datos sobre el tamaño del directorio infectado son modificados en la FAT, para evitar que se descubran bytes extras que aporta el virus.
- ✓ El virus se encripta en símbolos sin sentido para no ser detectado, pero para destruir o replicarse debe desencriptarse, siendo entonces detectable.
- ✓ Los virus mutan, cambiando segmentos del código para parecer distintos en cada "nueva generación", lo que los hace muy difíciles de detectar y de destruir.

Los virus se transportan a través de programas tomados de diferentes partes, o copias de software no original, infectadas a propósito o de manera accidental. Cualquier archivo que contenga ejecutables o Macros, puede ser portador de un virus. Cabe mencionar que los archivos de datos, de texto o de html no pueden contener virus, pero pueden ser dañados por éstos

3.8.1.2 Clasificación de virus

Los virus informáticos pueden clasificarse de diversas maneras; en su forma más general, un virus se clasifica en:

- ✓ Aquellos que infectan a los archivos
- ✓ Aquellos que infectan el sector de arranque
- ✓ La combinación de los anteriores

Los virus más comunes son:

- ✓ Acompañante
- ✓ Archivo
- ✓ Jokes o virus de broma
- ✓ Hoaxes o falsos virus
- ✓ virus

Por otro lado, los virus más enviados según la ICVS (control informático de virus) se pueden enumerar como sigue:

- ✓ Troyanos
- ✓ Gusanos
- ✓ Boot
- ✓ Otros

La incidencia en la difusión de estos tipos de virus a través del tiempo se muestra en la siguiente tabla:

Tipo	**1998**	**2000**	**2003**	**2005**
Troyanos	20%	15%	22%	25%
Gusanos	22%	20%	25%	27%
Boot	5%	1%	4%	2%
Otros	52%	64%	49%	46%

Los virus informáticos afectan en mayor o menor medida a casi todos los sistemas más conocidos y usados en la actualidad.

3.8.1.3 Daños

Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como:

- ✓ Pérdida de productividad
- ✓ Cortes en los sistemas de información
- ✓ Daños a nivel de datos.

3.8.1.4 Métodos de contagio

Básicamente, existen dos métodos de contagio:

- ✓ En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus.
- ✓ En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos.

En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario podemos encontrar las siguientes:

- ✓ Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).

- ✓ Ingeniería social; es decir, mensajes tales como: “ejecute este programa y gane un premio”

- ✓ Entrada de información en discos de otros usuarios infectados.

- ✓ Instalación de software pirata o de baja calidad.

- ✓ Se puede dar el caso de que el ordenador pueda infectarse sin ningún tipo de intervención del usuario (versiones Windows 2000, XP y Server 2003), por virus Blaster, Sasser y sus variantes, por el simple hecho de estar la máquina conectada a una red o a Internet. cabe mencionar que este tipo de virus aprovechan la vulnerabilidad de desbordamiento del buffer y puertos de red para infiltrarse y contagiar el equipo; causar inestabilidad en el sistema, mostrar mensajes de error o reiniciar el equipo involuntariamente (sin autorización o petición del usuario); también puede reenviarse a otras máquinas mediante la red local o el Internet; por mencionar algunos casos.

3.8.2 Códigos maliciosos

Los códigos maliciosos son programas dañinos que se envían premeditadamente a las computadoras con la finalidad de causar algún daño. Estos códigos son, generalmente, recibidos vía Internet de diversas formas:

- ✓ Vía correo electrónico. Al abrir un correo, el código malicioso tiene la puerta abierta para entrar al sistema, ocultarse y causar todo el daño posible para el que fue programado.
- ✓ Vía Web. Al consultar páginas con códigos y/o querer bajar la información del portal en cuestión.

3.8.3 Gusanos

Los gusanos se registran para correr cuando el sistema operativo se inicia, ocupando la memoria y volviendo lento al ordenador, pero no se adhieren a otros archivos ejecutables.

Estos archivos utilizan medios masivos como el correo electrónico para esparcirse de manera global.

3.8.4 Caballos de Troya

Los virus del tipo gatillable también reciben el nombre de “Caballo de Troya” y se caracterizan por tener una combinación posible que los active. Estas combinaciones pueden ser:

- ✓ El cambio de fecha
- ✓ Una determinada combinación del teclado
- ✓ Una macro
- ✓ La apertura de un programa asociado al virus

Los troyanos suelen ser los más peligrosos, puesto que no existen muchas maneras de eliminarlos. Estos programas funcionan de manera similar que el “Caballo de Troya”; ayudan al atacante a entrar al sistema infectado, haciéndose pasar como contenido genuino (por ejemplo: salvapantallas, juegos o música). En ocasiones, tiene la facilidad de descargar otros virus para agravar la condición del equipo.

3.8.5 Hackers

Los piratas ya no tienen un parche en su ojo, ni un garfio en reemplazo de la mano. Y tampoco existen los barcos ni los tesoros ocultos debajo del mar. A la llegada del año 2000, los piratas se presentan con un cerebro desarrollado, curioso y con muy pocas armas:

- ✓ Una simple computadora
- ✓ Una línea telefónica.

Estos piratas reciben el nombre de Hackers o Crackers. Una palabra que aún no se encuentra en los diccionarios pero que ya suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún diario.

Proviene de "hack", el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida.

Observemos unas estadísticas:

- ✓ Durante 1997, el 54% de las empresas norteamericanas sufrieron ataques de Hackers en sus sistemas.

- ✓ Las incursiones de los piratas informáticos, ocasionaron pérdidas totales de 137 millones de dólares en 1997.

- ✓ El Pentágono, la CIA, UNICEF, La ONU y demás organismos mundiales han sido víctimas de intromisiones por parte de estas personas que tienen muchos conocimientos en la materia y también una gran capacidad para resolver los obstáculos que se les presentan.

- ✓ Un hacker puede tardar meses en vulnerar un sistema ya que son cada vez más sofisticados. Pero el lema es viejo: “hecha la ley, hecha la trampa”.

- ✓ Los medios de comunicación masivos prefieren etiquetarlos como delincuentes que interceptan códigos de tarjetas de crédito y los utilizan para beneficio propio. También están los que se intrometen en los sistemas de aeropuertos produciendo un caos en los vuelos y en los horarios de los aviones.

Los crackers (crack=destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etcétera. Adolescentes inquietos que aprenden rápidamente este complejo oficio.

Se diferencian con los Hackers porque no poseen ningún tipo de ideología cuando realizan sus "trabajos". En cambio, el principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema.

3.9 Afirmaciones erróneas comunes

La seguridad informática suele ser muy frágil; debido, principalmente, a las siguientes aseveraciones equivocadas:

- ✓ Mi sistema no es importante para un cracker. Esta afirmación se basa en la idea de que no introducir contraseñas seguras en una empresa no entraña riesgos pues ¿quién va a querer obtener información mía? Sin embargo, dado que los métodos de contagio se realizan por medio de programas automáticos, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes, etcétera. Por tanto abrir sistemas y dejarlos sin claves es facilitar la vida a los virus.

- ✓ Estoy protegido pues no abro archivos que no conozco. Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.

- ✓ Como tengo antivirus estoy protegido. En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamientos de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún.

- ✓ Como dispongo de un firewall no me contagio. Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos al sistema (de lo que protege un firewall) y otras de conexiones que se realizan (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones puede entrañar riesgos, además los firewalls de aplicación (los más usados) no brindan protección suficiente contra el spoofing.

- ✓ Tengo un servidor web cuyo sistema operativo es un unix actualizado a la fecha. Puede que este protegído contra ataques directamente hacia el núcleo, pero si alguna de las aplicaciones web (PHP, Perl, Cpanel, etcétera) está desactualizada, un ataque sobre algún script de dicha aplicación puede permitir que el atacante abra una shell y, por ende, ejecutar comandos en el unix.

3.10 Delitos informáticos

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como:

- ✓ Robos
- ✓ Hurtos
- ✓ Fraudes
- ✓ Falsificaciones
- ✓ Perjuicios
- ✓ Estafas
- ✓ Sabotajes

Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas.

3.10.1 Tipos de delitos informáticos

La Organización de Naciones Unidas (ONU) reconocen los siguientes tipos de delitos informáticos:

- ✓ Fraudes cometidos mediante manipulación de computadoras
- ✓ Manipulación de los datos de entrada
- ✓ Daños o modificaciones de programas o datos computarizados

3.10.2 Tipos de delincuente

Los delincuentes pueden ser pasivos o activos, de la misma manera que pueden considerarse como criminal debido a la conciencia de sus actos, o víctima de su propia ignorancia con respecto de los sistemas.

3.11 Organismos oficiales de seguridad informática

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales e internacionales.

La ONU señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y los delitos informáticos se constituyen en una forma de crimen transnacional.

En este sentido habrá que recurrir a aquellos tratados internacionales de los que nuestro país es parte y que, en virtud del Artículo 75 inc. 22 de la Constitución Nacional reformada en 1994, tienen rango constitucional.

Argentina también es parte del acuerdo que se celebró en el marco de la Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio, que en su artículo 10, relativo a los programas de ordenador y compilaciones de datos, establece que:

“Este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna, de julio 1971, para la Protección de Obras Literarias y Artísticas”

“Las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual” y que

“Para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales (los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias)”

Por otro lado, existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como el CERT/CC (Computer Emergency Response Team Coordination Center) del SEI (Software Engineering Institute) de la Carnegie Mellon University el cual es un centro de alerta y reacción frente a los ataques informáticos, destinados a las empresas o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.

Capítulo IV: Métodos de planificación y seguimiento

4.1 Introducción

La seguridad en los sistemas informáticos se ha convertido, a lo largo del tiempo, en un factor decisivo en todas las organizaciones.

En todas las áreas, por muy sencillas que sean, la seguridad es muy importante; aún así, la pérdida de información y de recursos, sigue siendo un problema muy común.

Partiendo del hecho de que no existe un sistema 100% seguro y de que las principales personas de quien se deben cuidar las organizaciones es de sus propios empleados, la seguridad en informática parece ser un cerco difícil de vencer.

Un primer paso para mejorar la seguridad informática y minimizar los riesgos, suele ser la implantación de políticas, acrecentar las restricciones para la mayoría de los usuarios, entre otras acciones como la actualización del software a utilizar, la capacitación del personal a cargo, etcétera.

4.2 Procedimientos

Un procedimiento muy básico pero funcional dentro de la seguridad en los sistemas informáticos se basa en la combinación de dos líneas de actuación muy claras:

- ✓ Establecimiento de políticas de seguridad
- ✓ Generación de auditorias

4.2.1 Establecimiento de políticas

En primer lugar, es recomendable establecer una política de seguridad que alcance a todo el sistema.

Debe plasmarse en un documento escrito donde se contemple la asignación de responsabilidades y refrendado al más alto nivel de dirección posible, lo que implicará a toda la estructura en su cumplimiento.

Se debe hacer un control riguroso de aplicación del mismo, pero también de su difusión para tener la certeza de que todos los afectados conocen su contenido.

Para su implantación es necesaria una adecuada generación de medios humanos y materiales específicos.

Y algo importantísimo: es fundamental la concienciación del personal afectado por las medidas a adoptar.

4.2.2 Generación de auditorias

Por otro lado, se hace necesaria la generación de auditorias periódicas, tanto de tipo interno como externo.

Las auditorias internas provienen de la propia estructura de seguridad del sistema. Las auditorias externas las realizarían personal de una empresa o contratados a tal efecto y no siempre los mismos.

El objeto de las últimas es la revisión del sistema por parte de elementos que no se encuentren "viciados" por la rutina o el conocimiento del funcionamiento del sistema, extremo que se da con el personal propio.

4.2.3 Aplicación de la política de seguridad

Los criterios implantados por la política de seguridad deben seguirse siempre, desde que el sistema es simple o sencillo hasta cuando su crecimiento lo transforma en uno complejo.

El mejor procedimiento es la escalabilidad, permitiendo de esta manera validar las políticas llevadas hasta el momento, afinando y optimizando las futuras.

4.2.4 Responsabilidades de la política de seguridad

De una manera genérica, la responsabilidad de implantación de la política de seguridad afecta a todos los usuarios del sistema de información, tanto los normales como los privilegiados, donde habría que englobar a:

- ✓ Administradores de sistemas
- ✓ Administradores de bases de datos y
- ✓ Responsables de comunicaciones.

De manera específica, debe existir un responsable de seguridad, con dedicación exclusiva caso de tratarse de sistemas de información importantes.

Para poder ejercer su labor, esta persona responsable debe contar con un equipo de seguridad que permita desarrollar la política determinada por escrito.

Es positivo establecer un equipo de supervisión compuesto por los usuarios privilegiados señalados anteriormente y el equipo de seguridad.

4.2.5 Seguridad informática y la Guardia Civil

Para poder situar a la guardia civil dentro de lo referido a la seguridad informática, podemos decir que, de una manera directa, encontramos una referencia importante en la Unidad de Delitos de Alta Tecnología encuadrada en la Unidad Central Operativa del Servicio de Policía Judicial como unidad operativa de investigación, en uno de sus ámbitos de actuación, de quiebras de seguridad maliciosas en sistemas de información.

Como otra referencia, se tiene un foro de encuentro en materia de seguridad en un portal especializado dentro de la web pública corporativa, al que se le pretende dar en la actualidad un impulso importante.

Es importante tener en cuenta que la Guardia Civil tiene como misión el garantizar el libre ejercicio de los derechos de los ciudadanos, es su misión, para ofrecer seguridad y la seguridad informática es una parcela de esa seguridad integral.

4.2.6 Bases para una política de seguridad

De manera recomendada y recomendable, las políticas deberán basarse en los siguientes pasos:

- ✓ Identificar y seleccionar lo que se debe proteger (información sensible de ataque).

- ✓ 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

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el manejo de incidentes y recuperación para disminuir el impacto, ya que previamente habremos identificado y definido los sistemas y datos a proteger.

Es importante tomar en consideración, que las amenazas no disminuirán y las vulnerabilidades no desaparecerán en su totalidad, por lo que los niveles de inversión en el área de seguridad en cualquier empresa, deberán ir acordes a la importancia de la información en riesgo.

Así mismo, cada dispositivo que conforma la red empresarial necesita un nivel de seguridad apropiado y la administración del riesgo implica una protección multidimensional (firewalls, autenticación, \ antivirus, controles, políticas, procedimientos, análisis de vulnerabilidad, entre otros), y no únicamente tecnología.

Un esquema de seguridad empresarial contempla la seguridad física y lógica de una compañía. La primera se refiere a la protección contra robo o daño al personal, equipo e instalaciones de la empresa; y la segunda está relacionada con el tema que hoy nos ocupa: la protección a la información, a través de una arquitectura de seguridad eficiente.

Esta última debe ser proactiva, integrar una serie de iniciativas para actuar en forma rápida y eficaz ante incidentes y recuperación de información, así como elementos para generar una cultura de seguridad dentro de la organización.

4.3 Consejos para la seguridad informática

Como es de saberse, el concepto de seguridad informática es muy amplio y abarca todas las esferas de la sociedad.

Cabe mencionar que cada organización es diferente y sus necesidades de seguridad también lo son.

Tratando de hacer un balance entre las organizaciones, se pueden realizar series de consejos, personalizados en cada caso. Pero, como el espacio aquí es reducido, nos limitaremos a algo más general.

4.3.1 Elementos básicos

Conforme la complejidad de los sistemas de información se incrementa, la seguridad decrece. Por ejemplo, los macrovirus de Microsoft Word y los virus programados en el correo electrónico se aprovechan de las habilidades intrínsecas de los productos Microsoft. Esos programas son muy complejos, y sujetos a contener muchos errores y vulnerabilidades en su seguridad.

Desafortunadamente, las tendencias actuales indican que esos programas se volverán cada vez más complejos y menos seguros (aún cuando tomen medidas para hacerlos más seguros).

Conforme el número de usuarios en casa y en las redes de las oficinas se incrementan de forma natural, la importancia de educar al usuario crece en la misma proporción. Las listas de consejos sobre seguridad ofrecen un marco de comportamiento seguro que puede y debe ser implementado para todos los usuarios pues, independientemente de su nivel de habilidad, la sofisticación de los programas utilizados fuera de contexto en el que se utilizan, ha crecido mucho.

Por ahora, sólo podemos ofrecer consejos y, dependerá de cada persona el seguirlos o no. Cabe mencionar que el llevar a cabo los consejos más sutiles, le permitirá a los usuarios y a los administradores incrementar el nivel de seguridad dentro de su organización sin ninguna inversión adicional.

Dado que las sugerencias que se harán a continuación están dirigidas a promover un comportamiento seguro por parte del usuario, son extremadamente efectivas para bajar los riesgos de una ruptura en la seguridad.

Para hacer esto importante y que llegue a más personas, se pueden llevar a cabo diversos métodos:

En las organizaciones, por ejemplo, los puestos directivos pueden instituir programas de seguridad acompañados por cursos sobre el tema en toda la organización, haciendo así que la lista de consejos de seguridad sea leída de manera obligatoria.

Hacer que los usuarios se den cuenta de las prácticas riesgosas es un elemento fundamental en cualquier programa de seguridad. Más aún, los empleados no sólo deberían leer la lista, sino que también deberían firmar un convenio en el se comprometen a cumplirla, antes de poder utilizar los sistemas de la organización.

Para un administrador, sería importante asegurarse de que empleados sigan los consejos porque así le ahorrarán dinero a la compañía en varias formas:

- ✓ Se baja el riesgo de infecciones por virus o programas malintencionados y así se ahorra dinero en la productividad perdida por el tiempo que lleva mitigar la infección.

- ✓ Establecer y fomentar el uso del e-mail por audio puede ahorrar a la compañía los gastos y la molestia del litigio legal. También protegerá a la organización de la publicidad dañina y negativa que puede resultar de un incidente de seguridad

- ✓ Proteger las máquinas de los usuarios con firewalls personales puede prevenir que la información confidencial sea husmeada por extraños

- ✓ Las operaciones en negocios críticos no serán interrumpidas con tanta frecuencia y, si lo son (dependiendo de otros factores), serán cuando los empleados practiquen computación segura en una organización orientada a la seguridad

La lista de consejos de seguridad deberá estar disponible para todos los usuarios de los sistemas. Deberá haber una copia en todos los sitios de la red y una copia impresa en papel junto a cada máquina. De la misma forma, los usuarios caseros deberán tener a su lado la lista de consejos junto a cada computadora. Los padres deberán tomarse un momento para leer y entender la lista cuidadosamente y luego, pacientemente, leersela a los niños para asegurarse de que todos los usuarios entienden la importancia de implementar prácticas de computación segura.

4.3.2 Programas malignos.

Los programas malignos (virus, gusanos, troyanos, etcétera), pueden causar:

- ✓ Pérdida de productividad
- ✓ Corrupción de archivos
- ✓ Lentitud en la red
- ✓ Negación del servicio (DoS)
- ✓ Retrasos o pérdida de los correos electrónicos
- ✓ Divulgación de archivos confidenciales
- ✓ Que los procedimientos de fumigación sean muy grandes y caros (algunos programas malignos incluso llegan a quedarse en los respaldos corporativos).
- ✓ Pasar programas malignos a otros usuarios u organizaciones puede causar una vergüenza tremenda y pérdida de credibilidad.

Los pasos a seguir para minimizar el riesgo son:

1. Comprar un antivirus de marca conocida, uno que permita revisar los mensajes de correo entrante y los archivos de manera automática.

2. Actualizar las firmas del antivirus al menos semanalmente. (En el caso ideal, los programas de antivirus se actualizan automáticamente). Las actualizaciones están disponibles en los sitios web de los fabricantes de antivirus y es, en general, muy simple de instalar.

3. Usar los programas antivirus para revisar todos los discos duros (es decir, toda la computadora) al menos cada mes. Las revisiones de los todos los discos duros deberán correr automáticamente de forma periódica.

4. Aprender cómo distinguir las bromas sobre virus de las amenazas reales. La sobre reacción a las bromas puede causar pánico innecesario y sobrecargar el ancho de banda de la red. Para determinar si una advertencia de virus es verdadera, se pueden visitar los siguientes sitios: F-Secure, biblioteca de información sobre virus de McAfeee, Trend, o Vmyts.

5. Instale un firewall o cortafuegos como ZoneAlarm que es gratuito para usuarios caseros e instituciones educativas para protegerse de los troyanos y otros accesos no autorizados a la máquina.

6. Revise todos los flopis, CDs y otros medios externos que hayan sido utilizados en sistemas externos o los archivos que recibe de otras personas (incluyendo amigos y familiares).

4.3.3 Correo electrónico

El correo electrónico puede ser el medio para enviar virus y otros programas malignos. Los correos electrónicos no solicitados pueden bajar la productividad. Más aún, los correos electrónicos no encriptados pueden conducir a fugas de información que pueden revelar información confidencial o conducir a problemas legales o publicidad negativa.

Para bajar los riesgos inherentes al correo electrónico, la lista de consejos es la siguiente:

1. No abra los archivos adjuntos a menos que sea absolutamente necesario, en especial si no conoce al remitente

2. Nunca abra archivos adjuntos con las extensiones EXE, BAT, VBS y SCR, ya que ellos son vectores de infección muy comunes. Considere instalar versiones actualizadas del Microsoft Office 2000 para bloquear dichos archivos adjuntos

3. Si es necesario abriir un archivo adjunto, revíselo con un programa antivirus antes de hacerlo.

4. Cuando abra archivos adjuntos ya revisados, como los archivos tipo DOC, hágalo a través del programa, en vez de simplemente oprimir un doble click sobre el archivo adjunto. Si duda de un documento tipo DOC, puede abrirlo con un programa como WordPad para ver el contenido sin correr el riesgo de una infección de macrovirus

5. Si utiliza los programas de correo electrónico Outlook u Outlook Express, configure los mensajes de correo como "Zona Restringida" (Vaya a "Herramientas/Opciones/Seguridad y luego elija "Zona" en la ventana inferior)

6. Considere utilizar un programa de correo con un lector de texto limpio (no-HTML) como Eudora The Bat.

7. Si es posible, ponga la opción a su programa de correo electrónico para que envíe los mensajes en texto limpio (para Outlook vaya a "Herramientas/Opciones/Formato del correo" y luego eliga Texto Simple de las ventanas inferiores). El correo escrito en HTML es un riesgo potencial y permite el fisgoneo y la infección con código malicioso

4.3.4 Servicios de correo electrónico en web

Los servicios de correo electrónico en web tales como Yahoo! y Hotmail tienen un riesgo adicional para los usuarios.

Esos riesgos pueden ser el aumento de correo no solicitado o "spam", violaciones a la privacidad y divulgación de información no autorizada. Más aún, en el lugar de trabajo puede conducir a pérdida de productividad debida al uso de correo personal.

Finalmente, debido a que son más presentes a un foro abierto de intercambio libre de correo electrónico, le agregan el riesgo de virus o infiltración de programas malignos.

Para minimizar estos riesgos, se recomienda lo siguiente:

1. No utilice sistemas de correo basados en web para la comunicación de temas sensibles.

2. Aún cuando puede parecer algo muy aburrido, deberá leer el acuerdo de licencia que viene con el servicio antes de presionar "Aceptar". Algunos servicios gratuitos de correo electrónico se convierten en los dueños del contenido de sus mensajes si los envía a través del web.

3. Siga la misma política con respecto a los archivos adjuntos tanto con los correos personales que con los de trabajo

4.3.5 Navegación del web

La navegación a través del web puede causar al usuario violaciones de privacidad, robo de datos y contraseñas y entrega de virus.

Lo recomendable para reducir esta incidencia, es seguir las siguientes recomendaciones:

1. Se recomienda encarecidamente deshabilitar las características de navegación peligrosas tales como ActiveX. Las aplicaciones ActiveX (o "controles" como los llaman) son programas que se pueden bajar y que corren en su sistema. A diferencia de los archivos EXE, los ActiveX pueden correr transparentemente en dentro del Internet Explorer y realizar acciones tales como borrar archivos o robar sus contraseñas.

2. Deshabilitar el JavaScript también se recomienda, pero puede ser poco conveniente para algunos usuarios ya que muchos sitios web lo utilizan para la navegación. JavaScript puede ser utilizado para robar contraseñas de correo, contenido de formas y aún modificar el registro de Windows en los lugares donde se guardan los ajustes del sistema y algunas contraseñas

4.3.6 Conexiones de red

La conexión a la red es la base del internet. Es prácticamente imposible obtener todos los beneficios de la computación sin tener una conexión a la red.

Desafortunadamente, la conexión a la red también conlleva que, todas las amenazas que existen dentro de ella, estén conectadas a su computadora. Esto puede crear vulnerabilidades:

- ✓ Ataques de los hackers
- ✓ Acceso no autorizado
- ✓ Robo de información
- ✓ Ataques con programas malignos
- ✓ Daños legales.

Para bajar el riesgo de las conexiones de red, se recomienda lo siguiente:

1. Desactive los archivos compartidos en su Windows. En Windows 98 vaya a "Inicio/ Configuración/ Panel de control", busque "Compartir archivos e impresoras" y seleccione el botón "desactivar". Si debe habilitar los compartidos, asegúrese de utilizar una contraseña y sólo comparta los directorios indispensables.

2. Instale un cortafuegos personal, como el “Zone Alarm”, para proteger su computadora de los intentos de intrusión y los troyanos.

3. Evite el uso de programas de red inseguros tales como ICQ, AIM o IRC para tratar información confidencial. El contenido de esa comunicación puede ser visto por terceras personas, y utilizarlo para atacar su sistema o entregarle virus.

4. Considere utilizar sistemas operativos más seguros tales como Windows NT, 2000 o el nuevo Windows XP.

4.3.7 Algunos otros programas peligrosos

Existen más amenazas informáticas de las que creemos; siguen avanzando a la par de las medidas de seguridad; de lo que se trata es de que la seguridad de los sistemas informáticos no sea rebasada por la capacidad de los atacantes para violarlos.

Un ejemplo es Windows Scripting Host (WSH), como se describe en los sitios de Symantec, Datafellows, y Sofos. El WSH fue utilizado por virus como el ILOVEYOU para esparcirse a través del correo electrónico.

Se recomienda:

1. Aunque borrar el WSH no detendrá todos los virus de correo electrónico, al menos evitará que riegue la infección.

2. Borre el servidor de acceso telefónico (dial-up). Si su computadora tiene un módem conectado a una línea telefónica y Windows tiene el servidor de acceso telefónico instalado, cualquiera puede conectarse a su sistema. Borre el servidor si no lo está utilizando. El servidor de acceso telefónico de Windows no es una solución de acceso remoto con calidad empresarial, por ello, su nivel de seguridad es muy débil. Para borrar esos programas vaya al Panel de Control y luego a "Agregar/Borrar Sofware", busque el "Servidor de acceso telefónico" y elimínelo.

4.3.8 Algunos consejos de manera general

Los consejos de seguridad general para usuarios caseros se enlistan a continuación:

1. Infórmese sobre los últimos acontecimientos relevantes sobre seguridad visitando los sitios de noticias sobre el tema en el internet, tales como SecurityFocus, HispaSec, y NTBugTraq.

2. Aplique con regularidad los parches al sistema operativo que vayan apareciendo.

3. Utilice formatos de bajo riesgo para intercambiar documentos, tales como RTF o archivos de texto simple, los cuales no son vulnerables a la transmisión de virus o fallas generales de hardware.

4. Respalde sus archivos con regularidad en una unidad de ZIP o CD-ROM. Esta medida le garantiza que su información vital no se perderá en el caso de virus o fallas generales de hardware.

5. Cree un disco de arranque de su computadora y consérvelo en un lugar seguro (eso se hace yendo a "Inicio/ Configuración/ Panel de Control/ Agregar/Borrar programas" y luego seleccione "Disco de arranque" e inserte un disco nuevo en su unidad de disquete.

6. Asegúrese de utilizar contraseñas efectivas. Utilice una contraseña larga y fácil de recordar: un método es utilizar contraseñas compuestas por las primeras letras de una frase que tenga significado para usted. Las contraseñas consisten en entre 6 y 9 carácteres y deberían incluir letras en altas y bajas así como símbolos y números. Las contraseñas se deben cambiar con regularidad.

7. Si utiliza Windows NT/2000 no utilice la cuenta del administrador para actividades rutinarias.

4.4 Seguridad en MAC

Los pasos para la seguridad en Mac son bastante sencillos de seguir y algunos bien aplican para otros sistemas operativos:

1. Utiliza la cuenta de administrador sólo para administración.
2. Desactiva el Inicio de Sesión Automático: Preferencias > Seguridad > Desactivar el inicio de sesión automático.

3. Guarda las imágenes de discos con el sistema de cifrado.
4. Cifra los archivos importantes (mejor PGP que FileVault).

5. Ata el ordenador con un cable de seguridad a la mesa.

Aunado a eso, se puede añadir: activar la petición de contraseña si se activa el salvapantallas (Preferencias > Seguridad > Solicitar contraseña para reactivar el equipo). Abandonar el equipo durante más tiempo de lo previsto es una forma típica de que un hostil pueda cotillearlo. Activando el salvapantallas a 5 minutos se minimiza ese problema.

4.5 Tipos de seguridad informática

La seguridad informática se puede tipificar en dos grandes grupos:

- ✓ Seguridad física
- ✓ Seguridad lógica

4.5.1 Seguridad física

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma, no.

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

Así, la Seguridad Física **co**nsiste en la ″aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Las principales amenazas que se prevén en la seguridad física son:

- ✓ Desastres naturales (Incendios accidentales, Tormentas, Inundaciones)
- ✓ Amenazas ocasionadas por el hombre(Disturbios, sabotajes internos y externos deliberados)

No hace falta recurrir a películas de espionaje para sacar ideas de cómo obtener la máxima seguridad en un sistema informático, además de que la solución sería extremadamente cara.

A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

4.5.2 Seguridad lógica

Después de ver como un sistema puede verse afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos, sino contra la información por él almacenada y procesada.

Por lo tanto, la seguridad física es solamente una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad.

Como ya se ha mencionado, el activo más importante que se posee es la información; y, por lo tanto, deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

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

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

4.5.2.1 Objetivos de la seguridad lógica

Los objetivos que se plantean serán:

- ✓ Restringir el acceso a los programas y archivos.
- ✓ Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- ✓ Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- ✓ Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- ✓ Que la información recibida sea la misma que ha sido transmitida.
- ✓ Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- ✓ Que se disponga de pasos alternativos de emergencia para la transmisión de información.

4.5.2.2 Controles de Acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

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

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso.

4.6 Evaluación de riesgos

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas.

Se debe poder obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis, versus el costo de volverla a producir (reproducir).

Se debe tener en cuenta la probabilidad que suceda cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

Se debe conocer qué se quiere proteger, dónde y cómo, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se deberá identificar los recursos (hardware, software, información, personal, accesorios, etc.) con que se cuenta y las amenazas a las que se está expuesto.

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización; pero se puede presupone algunas preguntas que ayudan en la identificación de lo anteriormente expuesto:

- ✓ "¿Qué puede ir mal?"
- ✓ "¿Con qué frecuencia puede ocurrir?"
- ✓ "¿Cuáles serían sus consecuencias?"
- ✓ "¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?"
- ✓ "¿Se está preparado para abrir las puertas del negocio sin sistemas, por un día, una semana, cuanto tiempo?"
- ✓ "¿Cuál es el costo de una hora sin procesar, un día, una semana...?"
- ✓ "¿Cuánto, tiempo se puede estar off-line sin que los clientes se vayan a la competencia?"
- ✓ "¿Se tiene forma de detectar a un empleado deshonesto en el sistema?"
- ✓ "¿Se tiene control sobre las operaciones de los distintos sistemas?"
- ✓ "¿Cuantas personas dentro de la empresa, (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?"
- ✓ "¿A que se llama información confidencial y/o sensitiva?"
- ✓ "¿La información confidencial y sensitiva permanece así en los sistemas?"
- ✓ "¿La seguridad actual cubre los tipos de ataques existentes y está preparada para adecuarse a los avances tecnológicos esperados?"
- ✓ "¿A quien se le permite usar que recurso?"
- ✓ "¿Quién es el propietario del recurso? y ¿quién es el usuario con mayores privilegios sobre ese recurso?"
- ✓ "¿Cuáles serán los privilegios y responsabilidades del Administrador vs. la del usuario?"
- ✓ "¿Cómo se actuará si la seguridad es violada?"

Una vez obtenida la lista de cada uno de los riesgos se efectuará un resumen del tipo:

Tipo de Riesgo	**Factor**
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus Informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Según esta tabla habrá que tomar las medidas pertinentes de seguridad para cada caso en particular, cuidando incurrir en los costos necesarios según el factor de riesgo representado.

4.7 Búsqueda de soluciones

Desde el punto de vista de soluciones tecnológicas, una arquitectura de seguridad lógica puede conformarse (dependiendo de los niveles de seguridad) por:

- ✓ Software antivirus
- ✓ Herramientas de respaldo, de monitoreo de la infraestructura de red y enlaces de telecomunicaciones
- ✓ Firewalls
- ✓ Soluciones de autentificación

- ✓ Servicios de seguridad en línea; que informen al usuario sobre los virus más peligrosos y, a través de Internet, enviar la vacuna a todos los nodos de la red empresarial, por mencionar un ejemplo.

Los métodos para disminuir o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

4.7.1 Activos

Los métodos activos pueden ser:

- ✓ Antivirus: los llamados programas antivirus tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad.

- ✓ Filtros de ficheros: consiste en generar filtros de ficheros dañinos si el ordenador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

4.7.2 Pasivos

Los métodos pasivos se enlistan a continuación:

- ✓ Copias de seguridad: Mantener una política de copias de seguridad o respaldos garantiza la recuperación de los datos y una solución cuando nada de lo anterior ha funcionado.

- ✓ Estudiar: Aprender cómo es el software de nuestra computadora, buscando y buscando información, en sitios en los que se pueda confiar, sobre software dañino, para así evitarlo.

- ✓ Desconfiar: Si no conocemos algo o no sabemos lo que hace, será mejor tenerle respeto y no tocarlo hasta aclarar nuestra duda, (en el uso de esta regla es recomendable no abrir archivos de correos de los que se desconoce el remitente, o se sospecha de que pueda contener código malicioso, o que no pidió usted. Aun así, si es de entera confianza, analice siempre con un antivirus el archivo antes de abrirlo).

- ✓ Es aconsejable complementar esta manera de proceder aplicando una política de contraseñas y de seguridad más seguras a su red local o a los parámetros de acceso a Internet. Lo que muchos creadores de virus desean es la sensación de vulnerabilidad al provocar las condiciones de contagio idóneas que permitan una infección del virus a nivel mundial y causar daños sin dejar rastro de su presencia. En algunos casos los virus de correo pueden ser predichos debido al asunto del mensaje, por ejemplo la mayoría de estos virus se predicen a partir de asuntos perfectamente escritos o en otros idiomas.

- ✓ Hacer reenvíos seguros de email: Cuando recibamos un mensaje de correo electrónico sospechoso de contener virus o que hable de algo que desconocemos conviene consultar su posible infección o veracidad (por ejemplo a partir de buscadores de la www).

- ✓ Informar a nuestros contactos: Conviene que hagamos saber lo mencionado en el punto anterior a nuestros contactos en cuanto nos reenvían mensajes con virus o contenido falso o sin utilizar la casilla CCO.

- ✓ Limpiar y eliminar el virus: En el caso de que nuestra máquina resulte infectada debemos proceder a su desconexion inmediata de la red, ya sea local o Internet (esto se hace para evitar contagios a otras máquinas) y, una vez aislada, aplicar un programa Antivirus actualizado para tomar la acción que se corresponda.

- ✓ Restauración completa: En caso de que el virus sea tan virulento que destruya la lógica de una unidad de almacenamiento, se deberá recurrir a la restauración completa con formateo completo. Téngase en cuenta que esta operación dejará la máquina tal y como estaba el día que se adquirió. Sus configuraciones y demás quedarán borradas hasta que se determinen nuevamente.

- ✓ Legislar la instigación al delito cometido a través de la computadora. Adherirnos, por nuestra parte, a los postulados de la ONU sobre los delitos informáticos, con el fin de unificar la legislación internacional que regule la problemática de la cibernética y su utilización tan generalizada en el mundo.

Desde la Criminología debemos señalar que el anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, es un factor criminógeno que favorece la multiplicación de autores que utilicen los medios electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley.

No solo debe pensarse en la forma de castigo, sino algo mucho más importante es como lograr probar el delito. Este sigue siendo el principal inconveniente a la hora de legislar por el carácter intangible de la información.

4.8 Evaluación de seguridad

Para lograr una explicación más eficiente acerca de la evaluación de la información, se hace necesario retomar y, en algunos casos, reexplicar algunos conceptos ya vistos.

4.8.1 Importancia de la Información

Cuando se habla de la función informática generalmente se tiende a hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos hardware, nuevas formas de elaborar información más consistente, etc.

Sin embargo se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la *información*.

Es muy importante conocer su significado dentro la función informática, de forma esencial cuando su manejo esta basado en tecnología moderna, para esto se debe conocer que la información:

- ✓ Esta almacenada y procesada en computadoras
- ✓ Puede ser confidencial para algunas personas o a escala institucional
- ✓ Puede ser mal utilizada o divulgada
- ✓ Puede estar sujeta a robos, sabotaje o fraudes

Los primeros puntos nos muestran que la información esta centralizada y que puede tener un alto valor y lo s últimos puntos nos muestran que se puede provocar la destrucción total o parcial de la información, que incurre directamente en su disponibilidad que puede causar retrasos de alto costo.

Pensemos por un momento que hay se sufre un accidente en el centro de computo o el lugar donde se almacena la información. Ahora preguntémonos: ¿Cuánto tiempo pasaría para que la organización este nuevamente en operación?

Es necesario tener presente que el lugar donde se centraliza la información con frecuencia el centro de cómputo puede ser el activo más valioso y al mismo tiempo el más vulnerable.

4.8.2 Riesgo

El riesgo es la proximidad o posibilidad de un daño, peligro, etcétera.
Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.
Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

4.8.3 Seguridad

Seguridad podría definirse como cualidad o estado de seguro
Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo.
Se dice también de todos aquellos objetos, dispositivos, medidas, etcétera, que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

Con estos conceptos claros podemos avanzar y hablar la criminología ya ha calificado los “delitos hechos mediante computadora” o por “sistemas de información” en el grupo de delitos de cuello blanco.

4.8.4 Crónica del crimen (o delitos en los sistemas de información)

Delitos accidentales e incidentales
Los delitos cometidos utilizando la computadora han crecido en tamaño, forma y variedad.

En 1994, los delitos cometidos tienen la peculiaridad de ser descubiertos en un 95% de forma casual. Podemos citar a los principales delitos hechos por computadora o por medio de computadoras estos son:

- ✓ fraudes
- ✓ falsificación
- ✓ venta de información

Entre los hechos criminales más famosos en los E.E.U.U. están:
El caso del Banco Wells Fargo donde se evidencio que la protección de archivos era inadecuada, cuyo error costo USD 21.3 millones.

El caso de la NASA donde dos alemanes ingresaron en archivos confidenciales.
El caso de un muchacho de 15 años que entrando a la computadora de la Universidad de Berkeley en California destruyo gran cantidad de archivos.

También se menciona el caso de un estudiante de una escuela que ingreso a una red canadiense con un procedimiento de admirable sencillez, otorgándose una identificación como un usuario de alta prioridad, y tomo el control de una embotelladora de Canadá.

También el caso del empleado que vendió la lista de clientes de una compañía de venta de libros, lo que causo una perdida de USD 3 millones.

4.8.5 Virus informático

El virus informático es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de diskettes o de la red telefónica de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas computarizados. Ejemplo: el virus llamado viernes trece o Jerusalén, que desactivó el conjunto de ordenadores de la defensa de Israel y que actualmente se ha extendido a todo el mundo.

Históricamente los virus informáticos fueron descubiertos por la prensa el 12 de octubre de 1985, con una publicación del New York Times que hablaba de un virus que fue se distribuyo desde un BBS y aparentemente era para optimizar los sistemas IBM basados en tarjeta gráfica EGA, pero al ejecutarlo salía la presentación pero al mismo tiempo borraba todos los archivos del disco duro, con un mensaje al finalizar que decía "Caíste".

Bueno en realidad este fue el nacimiento de su nombre, ya que los programas con código integrado, diseñados para hacer cosas inesperadas han existido desde que existen las computadoras. Y ha sido siempre la obra de algún programador delgado de ojos de loco.

Pero las primeras referencias de virus con fines intencionales surgieron en 1983 cuando Digital Equipament Corporation (DEC) empleo empleó una subrutina para proteger su famoso procesador de textos Decmate II, que el 1 de abril de 1983 en caso de ser copia ilegal borraba todos los archivos de su unidad de disco.

Los principales casos de crímenes cometidos empleando por virus informáticos son:

- ✓ 12 de diciembre de 1987. El virus de Navidad Una tarjeta navideña digital enviada por medio de un BBS de IBM atasco las instalaciones en los EE.UU. por 90 minutos. Cuando se ejecutaba el virus este tomaba los Adress Book del usuario y se retransmitía automáticamente, ademas que luego colgaba el ordenador anfitrión. Esto causo un desbordamiento de datos en la red.

- ✓ 10 de enero de 1988. El virus Jerusalén se ejecuta en una universidad hebrea y tiene como fecha límite el primer viernes 13 del año, como no pudieron pararlo se sufría una disminución de la velocidad cada viernes 13.

- ✓ 20 de septiembre de 1988 en Fort Worth, Texas, Donald Gene un programador de 39 años será sometido a juicio el 11 de julio por cargos delictivos de que intencionadamente contaminó el sistema de por ser despedido, con un virus informático el año 85. Sera la primera persona juzgada con la ley de sabotaje que entro en vigor el 1 de septiembre de 1985. El juicio duro 3 semanas y el programador fue declarado culpable y condenado a siete años de libertad condicional y a pagar USD. 12000. Su empresa que se dedicaba a la bolsa sufrió borro de datos, aproximadamente 168000 registros.

- ✓ 4 de noviembre de 1988 Un virus invade miles de computadoras basadas en Unix en universidades e instalaciones de investigación militares, donde las velocidades fueron reducidas y en otros casos paradas. También el virus se

propagó a escala internacional. Se estableció que la infección no fue realizada por un virus sino por un programa gusano, diseñado para reproducirse así mismo indefinidamente y no para eliminar datos. El programa se difundió a través de un corrector de errores para correo electrónico, que se movió principalmente en Internet (Arpanet) y contamino miles de computadoras en todo el mundo contando 6000 computadoras en centros militares en los EE.UU. , incluyendo la NASA, la Fuerza Aérea, el MIT, las universidades de Berkeley, Illinois, Boston, Stanford, Harvard, Princeton, Columbia y otras. En general se determino que la infección se propago en las computadoras VAX de DEC (digital equipament corp) y las fabricadas por Sun Microsystems, que empleaban Unix.

- ✓ Se halla al culpable Robert Morris, estudiante de 23 años, que declara haber cometido un error al propagar el gusano. Morris era el hijo de un experto en seguridad informática del gobierno. El caso fue investigado por el FBI. Posiblemente se sentencie a Morris por 5 años de prisión y una multa USD. 250000.

- ✓ 23 de marzo del 89 virus ataca sistemas informáticos de hospitales, variando la lectura de informes de laboratorio.

- ✓ Y los últimos pero recordados vaccina, hacker, cpw543, natas, antiexe, etcétera.

4.8.6 Ambiente propicio para el cultivo del crimen

En la actualidad se nota que los fraudes crecen en forma rápida, incluso mayor que los sistemas de seguridad. Se sabe que en los EE.UU. se cometen crímenes computarizados denunciados o no por más de 3 mil millones de dólares.)

Es importante para el auditor conocer las causas para que se cometan delitos, ya que una vez encontrado el problema se debe observar la raíz para sugerir su solución.

4.8.7 Paradigmas Organizacionales en Cuanto a Seguridad

Se entiende como paradigma un modelo o ejemplo de algo, En filosofía: Conjunto de ideas filosóficas, teorías científicas y normas metodológicas que influyen en la forma de resolver los problemas en una determinada tradición científica.

Del paradigma se desprenden las reglas que rigen las investigaciones. Cuando dentro de un paradigma aparecen anomalías excesivas, se produce una revolución científica que consiste precisamente en el cambio de paradigma

Es muy importante que el auditor conozca los paradigmas que existen en las organizaciones sobre la seguridad, para no encontrarse con un contrincante desconocido.

Entre los principales paradigmas que se pueden encontrar veamos los siguientes:

- ✓ Generalmente, se tiene la idea que los procedimientos de auditoria es responsabilidad del personal del centro de cómputo, pero se debe cambiar este paradigma y conocer que estas son responsabilidades del usuario y del departamento de auditoria interna.

- ✓ También muchas compañías cuentan con dispositivos de seguridad física para los computadores y se tiene la idea que los sistemas no pueden ser violados si no se ingresa al centro al centro de cómputo, ya que no se considera el uso terminales y de sistemas remotos.

- ✓ Se piensa también que los casos de seguridad que tratan de seguridad de incendio o robo que “eso no me puede suceder a mí” o “es poco probable que suceda”.

- ✓ También se cree que los computadores y los programas son tan complejos que nadie fuera de su organización los va a entender y no les van a servir, ignorando las personas que puedan captar y usarla para otros fines.

- ✓ Los sistemas de seguridad generalmente no consideran la posibilidad de fraude interno que es cometido por el mismo personal en el desarrollo de sus funciones.

- ✓ Generalmente se piensa que la seguridad por clave de acceso es inviolable pero no se considera a los delincuentes sofisticados.

- ✓ Se suele suponer que los defectos y errores son inevitables.

- ✓ También se cree que se hallan fallas porque nada es perfecto.

- ✓ Y la creencia que la seguridad se aumenta solo con la inspección.

El siguiente cuadro es una forma apta para llevar este tipo de información. Aunque no puede ser la mejor, pero permite distinguir las ideas que se pretender explicar.

	Viejo Equilibrio	Nuevo desequilibrio
RR.HH. Organización Operativo ..		

Se deben analizar estos y otros paradigmas de la organización, también es muy importante que el auditor enfrente y evalúe primero sus propios paradigmas y sus paradigmas académicos.

4.8.8 Consideraciones Inmediatas para la Auditoria de la Seguridad

A continuación se citarán las consideraciones inmediatas que se deben tener para elaborar la evaluación de la seguridad, pero luego se tratarán las áreas específicas con mucho mayor detalle.

4.8.8.1 Uso de la Computadora

Se debe observar el uso adecuado de la computadora y su software que puede ser susceptible a:

- ✓ Tiempo de máquina para uso ajeno
- ✓ Copia de programas de la organización para fines de comercialización (copia pirata)
- ✓ Acceso directo o telefónico a bases de datos con fines fraudulentos

4.8.8.2 Sistema de Acceso

Para evitar los fraudes computarizados se debe contemplar de forma clara los accesos a las computadoras de acuerdo a:

- ✓ Nivel de seguridad de acceso
- ✓ Empleo de las claves de acceso
- ✓ Evaluar la seguridad contemplando la relación costo, ya que a mayor tecnología de acceso mayor costo

4.8.9 Cantidad y Tipo de Información

El tipo y la cantidad de información que se introduce en las computadoras debe considerarse como un factor de alto riesgo ya que podrían producir que:

- ✓ La información este en manos de algunas personas
- ✓ La alta dependencia en caso de perdida de datos

4.8.10 Control de Programación

Se debe tener conocer que el delito más común está presente en el momento de la programación, ya que puede ser cometido intencionalmente o no, para lo cual se debe controlar que:

- ✓ Los programas no contengan bombas lógicas
- ✓ Los programas deben contar con fuentes y sus ultimas actualizaciones
- ✓ Los programas deben contar con documentación técnica, operativa y de emergencia

4.8.11 Personal

Se debe observar este punto con mucho cuidado, ya que hablamos de las personas que están ligadas al sistema de información de forma directa y se deberá contemplar principalmente:

- ✓ La dependencia del sistema a nivel operativo y técnico
- ✓ Evaluación del grado de capacitación operativa y técnica
- ✓ Contemplar la cantidad de personas con acceso operativo y administrativo
- ✓ Conocer la capacitación del personal en situaciones de emergencia

4.8.12 Medios de Control

Se debe contemplar la existencia de medios de control para conocer cuando se produce un cambio o un fraude en el sistema.

También se debe observar con detalle el sistema ya que podría generar indicadores que pueden actuar como elementos de auditoria inmediata, aunque esta no sea una especificación del sistema.

4.8.13 Rasgos del Personal

Se debe ver muy cuidadosamente el carácter del personal relacionado con el sistema, ya que pueden surgir:

- ✓ Malos manejos de administración
- ✓ Malos manejos por negligencia
- ✓ Malos manejos por ataques deliberados

4.8.14 Instalaciones

Es muy importante no olvidar las instalaciones físicas y de servicios, que significan un alto grado de riesgo. Para lo cual se debe verificar:

- ✓ La continuidad del flujo eléctrico
- ✓ Efectos del flujo eléctrico sobre el software y hardware
- ✓ Evaluar las conexiones con los sistemas eléctrico, telefónico, cable, etc.
- ✓ Verificar si existen un diseño, especificación técnica, manual o algún tipo de documentación sobre las instalaciones

4.8.15 Control de Residuos

Observar como se maneja la basura de los departamentos de mayor importancia, donde se almacena y quien la maneja. Establecer las Áreas y Grados de Riesgo

Es muy importante el crear una conciencia en los usuarios de la organización sobre el riesgo que corre la información y hacerles comprender que la seguridad es parte de su trabajo. Para esto se deben conocer los principales riesgos que acechan a la función informática y los medios de prevención que se deben tener, para lo cual se debe:

Establecer el Costo del Sistema de Seguridad (Análisis Costo vs Beneficio)
Este estudio se realiza considerando el costo que se presenta cuando se pierde la información vs el costo de un sistema de seguridad.

Para realizar este estudio se debe considerar lo siguiente:

- ✓ Clasificar la instalación en términos de riesgo (alto, mediano, pequeño)
- ✓ Identificar las aplicaciones que tengan alto riesgo
- ✓ Cuantificar el impacto en el caso de suspensión del servicio aquellas aplicaciones con un alto riesgo
- ✓ Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera
- ✓ La justificación del costo de implantar las medidas de seguridad

Cada uno de estos puntos es de mucha importancia por lo que se sugiere clasificar estos elementos en áreas de riesgo que pueden ser:

- ✓ Riesgo computacional
- ✓ Consideraciones y cuantificación del riesgo a nivel institucional
- ✓ Disposiciones que acompañan la seguridad
- ✓ Higiene
- ✓ Cultura personal

4.8.15.1 Riesgo Computacional

Se debe evaluar las aplicaciones y la dependencia del sistema de información, para lo cual es importante considerar responder las siguientes cuatro preguntas:

1. ¿Qué sucedería si no se puede utilizar el sistema? Si el sistema depende de la aplicación por completo se debe definir el nivel de riesgo.
Por ejemplo citemos:

- ✓ Un sistema de reservación de boletos que dependa por completo de un sistema computarizado, es un sistema de alto riesgo.
- ✓ Una lista de clientes será de menor riesgo.
- ✓ Un sistema de contabilidad fuera del tiempo de balance será de mucho menor riesgo.

2. ¿Qué consecuencias traería si es que no se pudiera acceder al sistema? Al considerar esta pregunta se debe cuidar la presencia de manuales de respaldo para emergencias o algún modo de cómo se soluciono este problema en el pasado.

3. ¿Existe un procedimiento alternativo y que problemas ocasionaría? Se debe verificar si el sistema es único o es que existe otro sistema también computarizado de apoyo menor. Ejemplo: Sí el sistema principal esta diseñado para trabajar en red sea tipo WAN quizá haya un soporte de apoyo menor como una red LAN o monousuario. En el caso de un sistema de facturación en red, si esta cae, quizá pudiese trabajar en forma distribuida con un módulo menor monousuario y que tenga la capacidad de que al levantarse la red existan métodos de actualización y verificación automática.

4. ¿Qué se ha hecho en casos de emergencia hasta ahora? Para responder esta pregunta se debe considerar al menos las siguientes situaciones, donde se debe rescatar los acontecimientos, las consecuencias y las soluciones tomadas, considerando:

- ✓ Que exista un sistema paralelo al menos manual
- ✓ Si hay sistemas duplicados en las áreas críticas (tarjetas de red, teclados, monitores, servidores, unidades de disco, aire acondicionado).

- ✓ Si hay sistemas de energía ininterrumpida UPS.
- ✓ Si las instalaciones eléctricas, telefónicas y de red son adecuadas (se debe contar con el criterio de un experto).
- ✓ Si se cuenta con un método de respaldo y su manual administrativo.

Cuando se ha definido el grado de riesgo se debe elaborar una lista de los sistemas con las medidas preventivas que se deben tomar y las correctivas en casi de desastre, señalando la prioridad de cada uno. Con el objetivo que en caso de desastres se trabajen los sistemas de acuerdo a sus prioridades.

4.8.15.2 Consideración y Cuantificación del Riesgo a Nivel Institucional

Ahora que se han establecido los riesgos dentro la organización, se debe evaluar su impacto a nivel institucional, para lo cual se debe:

- ✓ Clasificar la información y los programas de soporte en cuanto a su disponibilidad y recuperación.

- ✓ Identificar la información que tenga un alto costo financiero en caso de perdida o pueda tener impacto a nivel ejecutivo o gerencial.

- ✓ Determinar la información que tenga un papel de prioridad en la organización a tal punto que no pueda sobrevivir sin ella.

Una vez determinada esta información se debe cuantificar, para lo cual se debe efectuar entrevistas con los altos niveles administrativos que sean afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que podrían causar estas situaciones.

4.8.15.3 Disposiciones que Acompañan la Seguridad

De acuerdo a experiencias pasadas, y a la mejor conveniencia de la organización, desde el punto de vista de seguridad, contar con un conjunto de disposiciones o cursos de acción para llevarse a cabo en caso de presentarse situaciones de riesgo. Para lo cual se debe considerar:

- ✓ Obtener una especificación de las aplicaciones, los programas y archivos de datos.
- ✓ Medidas en caso de desastre como pérdida total de datos, abuso y los planes necesarios para cada caso.
- ✓ Prioridades en cuanto a acciones de seguridad de corto y largo plazo.
- ✓ Verificar el tipo de acceso que tiene las diferentes personas de la organización, cuidar que los programadores no cuenten con acceso a la sección de operación ni viceversa.
- ✓ Que los operadores no sean los únicos en resolver los problemas que se presentan.

4.8.15.4 Higiene

Otro aspecto que parece de menor importancia es el de orden e higiene, que debe observarse con mucho cuidado en las áreas involucradas de la organización (centro de cómputo y demás dependencias), pues esto ayudará a detectar problemas de disciplina y posibles fallas en la seguridad.

También podemos ver que la higiene y el orden son factores que elevan la moral del recurso humano, evita la acumulación de desperdicios y limita las posibilidades de accidentes.

Además, es un factor que puede perjudicar el desarrollo del trabajo tanto a nivel formal como informal.

4.8.15.5 Cultura Personal

Cuando hablamos de información, su riesgo y su seguridad, siempre se debe considerar al elemento humano, ya que podría definir la existencia o no de los más altos grados de riesgo. Por lo cual es muy importante considerar la idiosincrasia del personal, al menos de los cargos de mayor dependencia o riesgo.

El fin de este punto es encontrar y evitar posibles situaciones de roce entre el recurso humano y la organización y lograr una mejor comunicación entre ambos.

4.9 Consideraciones para Elaborar un Sistema de Seguridad Integral

Como hablamos de realizar la evaluación de la seguridad es importante también conocer como desarrollar y ejecutar el implantar un sistema de seguridad.

Desarrollar un sistema de seguridad significa: “planear, organizar coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa.”

Por lo cual podemos ver las consideraciones de un sistema de integral de seguridad. Un sistema integral debe contemplar:

- ✓ Definir elementos administrativos
- ✓ Definir políticas de seguridad
- ✓ A nivel departamental
- ✓ A nivel institucional
- ✓ Organizar y dividir las responsabilidades
- ✓ Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
- ✓ Definir prácticas de seguridad para el personal:
- ✓ Plan de emergencia (plan de evacuación, uso de recursos de emergencia como extinguidores.
- ✓ Números telefónicos de emergencia
- ✓ Definir el tipo de pólizas de seguros
- ✓ Definir elementos técnicos de procedimientos
- ✓ Definir las necesidades de sistemas de seguridad para:
- ✓ Hardware y software
- ✓ Flujo de energía
- ✓ Cableados locales y externos
- ✓ Aplicación de los sistemas de seguridad incluyendo datos y archivos
- ✓ Planificación de los papeles de los auditores internos y externos
- ✓ Planificación de programas de desastre y sus pruebas (simulación)
- ✓ Planificación de equipos de contingencia con carácter periódico
- ✓ Control de desechos de los nodos importantes del sistema:
- ✓ Política de destrucción de basura copias, fotocopias, etc.
- ✓ Consideración de las normas ISO 14000

4.10 Etapas para Implementar un Sistema de Seguridad

Para dotar de medios necesarios para elaborar su sistema de seguridad se debe considerar los siguientes puntos:

- ✓ Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.

- ✓ Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.

- ✓ Elaborar un plan para un programa de seguridad. El plan debe elaborarse contemplando:

4.11 Plan de Seguridad Ideal (o Normativo)

Un plan de seguridad para un sistema de seguridad integral debe contemplar:

- ✓ El plan de seguridad debe asegurar la integridad y exactitud de los datos
- ✓ Debe permitir identificar la información que es confidencial
- ✓ Debe contemplar áreas de uso exclusivo
- ✓ Debe proteger y conservar los activos de desastres provocados por la mano del hombre y los actos abiertamente hostiles
- ✓ Debe asegurar la capacidad de la organización para sobrevivir accidentes
- ✓ Debe proteger a los empleados contra tentaciones o sospechas innecesarias
- ✓ Debe contemplar la administración contra acusaciones por imprudencia

Un punto de partida será conocer como será la seguridad, de acuerdo a la siguiente ecuación:

$$\text{SEGURIDAD} = \frac{\text{Riesgo}}{\text{Medidas preventivas y correctivas}}$$

Donde:

Riesgo (roles, fraudes, accidentes, terremotos, incendios, etc)

Medidas pre.. (políticas, sistemas de seguridad, planes de emergencia, plan de resguardo, seguridad de personal, etc)

4.12 Consideraciones para con el Personal

Es de gran importancia la elaboración del plan considerando el personal, pues se debe llevar a una conciencia para obtener una autoevaluación de su comportamiento con respecto al sistema, que lleve a la persona a:

- ✓ Asumir riesgos
- ✓ Cumplir promesas
- ✓ Innovar

Para apoyar estos objetivos se debe cumplir los siguientes pasos:

- ✓ Motivar. Se debe desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo, así como su impacto a nivel empresarial, de cargo y individual.

- ✓ Capacitación General. En un principio a los ejecutivos con el fin de que conozcan y entiendan la relación entre seguridad, riesgo y la información, y su impacto en la empresa. El objetivo de este punto es que se podrán detectar las debilidades y potencialidades de la organización frente al riesgo. Este proceso incluye como práctica necesaria la implantación la ejecución de planes de contingencia y la simulación de posibles delitos.

- ✓ Capacitación de Técnicos. Se debe formar técnicos encargados de mantener la seguridad como parte de su trabajo y que esté capacitado para capacitar a otras personas en lo que es la ejecución de medidas preventivas y correctivas.

- ✓ Ética y Cultura. Se debe establecer un método de educación estimulando el cultivo de elevados principios morales, que tengan repercusión a nivel personal e institucional.De ser posible realizar conferencias periódicas sobre: doctrina, familia, educación sexual, relaciones humanas, etc.

4.13 Etapas para Implantar un Sistema de Seguridad en Marcha

Para hacer que el plan entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguientes pasos:

- ✓ Introducir el tema de seguridad en la visión de la empresa.
- ✓ Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
- ✓ Capacitar a los gerentes y directivos, contemplando el enfoque global.
- ✓ Designar y capacitar supervisores de área.
- ✓ Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
- ✓ Mejorar las comunicaciones internas.
- ✓ Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
- ✓ Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

4.14 Beneficios de un Sistema de Seguridad

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que el la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- ✓ Aumento de la productividad.
- ✓ Aumento de la motivación del personal.
- ✓ Compromiso con la misión de la compañía.
- ✓ Mejora de las relaciones laborales.
- ✓ Ayuda a formar equipos competentes.
- ✓ Mejora de los climas laborales para los RR.HH.

Conclusiones

Después de haber dejado en claro la importancia de la información en el mundo actual y de manejar los riesgos con los que se enfrenta nuestro conocimiento y la posible forma de enfrentarlos, puedo decir que espero que, de alguna forma, esta información pueda ser de utilidad.

Haciendo un poco énfasis en la seguridad informática, cabe hacer mención de que el rápido y continuo desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La cuantía de los perjuicios así ocasionados es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o castigarse.

Como se ha mencionado, el delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes.

Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

La OCDE (organización contra los delitos informáticos) elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse un punto y notar lo siguiente:

- ✓ No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.

- ✓ No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.

- ✓ La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento. Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa. Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

Cabe mencionar que, si bien no existe un sistema 100% seguro, siempre es importante el mantener la información fuera del alcance de aquellas personas que intenten dañar a los sistemas de cualquier forma.

Es importante hacer mención de que la seguridad en los sistemas de información depende, en gran medida, de que las personas que los manejan no realicen actividades irresponsables ni permitan el acceso premeditado de personas no autorizadas.

Glosario de términos

ACOMPAÑANTE	Virus que basan su principio en que MS-DOS ejecuta en primer lugar el archivo con extensión COM frente al de extensión EXE, en el caso de existir dos archivos con el mismo nombre pero diferente extensión dentro del mismo directorio. El virus crea un archivo COM con el mismo nombre y en el mismo lugar que el EXE a infectar. Después ejecuta el nuevo archivo COM, creado por el virus, y cede el control al archivo EXE.
APLICACIÓN DE SOFTWARE	Programa informático que permite a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora, y suelen ejecutarse sobre el sistema operativo.
ARCHIVO	Los virus que infectan archivos del tipo *.EXE, *.DRV, *.DLL, *.BIN, *.OVL, *.SYS e incluso BAT. Este tipo de virus se añade al principio o al final del archivo. Estos se activan cada vez que el archivo infectado es ejecutado, ejecutando primero su código vírico y luego devuelve el control al programa infectado pudiendo permanecer residente en la memoria durante mucho tiempo después de que hayan sido activados.
CICLO DE PROCESAMIENTO DE LA INFORMACIÓN	Es el proceso mediante el cual se carga información a un sistema; ésta es procesada y se devuelven los resultados. Consta de entrada, procesamiento, salida y almacenamiento.

COMPUTADORA	Dispositivo electrónico compuesto básicamente de procesador, memoria y dispositivos de entrada/salida. Poseen parte física (hardware) y parte lógica (software), que se combinan entre sí para ser capaces de interpretar y ejecutar instrucciones para las que fueron programadas. Una computadora suele tener un gran software llamado sistema operativo que sirve como plataforma para la ejecución de otras aplicaciones o herramientas.
HOAXES O FALSOS VIRUS	Son mensajes con una información falsa; normalmente son difundidos mediante el correo electrónico, a veces con fin de crear confusión entre la gente que recibe este tipo de mensajes o con un fin aún peor en el que quieren perjudicar a alguien o atacar al ordenador mediante ingeniería social.
JOKES O VIRUS DE BROMA	No son realmente virus, sino programas con distintas funciones, pero todas con un fin de diversión, nunca de destrucción, aunque pueden llegar a ser muy molestos.
KLUGGERS	Aquellos virus que al entrar en los sistemas de otro ordenador se reproducen o bien se cifran de manera que tan sólo se les puede detectar con algún tipo de patrones.
OPERATING SYSTEM	Sistema tipo software que controla la computadora y administra los servicios y sus funciones como así también la ejecución de otros programas compatibles con éste.

SISTEMA EXPERTO (SE)	Sistemas que emulan el comportamiento de un experto en un campo concreto, su objetivo es lograr mejor calidad y rapidez en las respuestas y mejorar la productividad de un experto. Forma parte de la Inteligencia Artificial. Suelen basarse en el conocimiento declarativo (hechos sobre objetos, situaciones) y el conocimiento de control (información sobre el seguimiento de una acción). Un Sistema Experto está conformado por: * base de conocimientos (BC). * base de hechos (memoria de trabajo). * motor de inferencia: intentando modelar el proceso de razonamiento humano. * módulos de justificación: muestra el razonamiento seguido para llegar a una conclusión determinada. * interfaz de usuario.
SISTEMA INFORMÁTICO	Conjunto de partes (hardware y software) que funcionan relacionándose entre sí con un objetivo preciso. Los usuarios son parte del sistema informático
VIDDBERS	Aquellos virus que lo que hacen es modificar los programas del sistema del ordenador en el cual entran.
VIRUS DE ACCIÓN DIRECTA	Son aquellos que no se quedan residentes en memoria y se replican en el momento de ejecutar el fichero infectado.

VIRUS DE MACROS	Un macro es una secuencia de órdenes de teclado y mouse asignadas a una sola tecla, símbolo o comando. Son muy útiles cuando este grupo de instrucciones se necesitan repetidamente. Los virus de macros afectan a archivos y plantillas que los contienen, haciéndose pasar por una macro y actuarán hasta que el archivo se abra o utilice.
VIRUS DE SOBREESCRITURA	Son los virus que corrompen el fichero donde se ubican al sobrescribirlo.

Bibliografía

- ✓ Langefors, Börje (1973). Theoretical Analysis of Information Systems. Auerbach.

- ✓ Angell, I.O. and Smithson S. (1991) Information Systems Management: Opportunities and Risks

- ✓ Federal Standard 1037C, MIL-STD-188, and National Information Systems Security Glossary

- ✓ Rockart et. Al (1996) Eight imperatives for the new IT organization Sloan Management review.

- ✓ Ciborra, C. (2002) Labyrinths of Information, Oxford, Oxford University Press