Administración de la seguridad informática y herramientas para plataforma Windows

Autor: Claudia Hassel Lozano García

Tesina presentada para obtener el título de:
Lic. En Sistemas Computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarra

UNIVERSIDAD VASCO DE QUIROGA

TESINA
ADMINISTRACION DE LA SEGURIDAD INFORMATICA Y HERRAMIENTAS PARA PLATAFORMA WINDOWS.

QUE PARA OBTENER EL TITULO DE:
LICENCIADO EN SISTEMAS COMPUTARIZADOS

ESCUELA DE SISTEMAS COMPUTARIZADOS
No. DE ACUERDO 952006 CLAVE 16PSU0014Q

PRESENTA:
Claudia Hassel Lozano García
ASESOR DE TESINA:
M.A. Ing. Sergio Francisco Barraza Ibarra

MORELIA, MICH. JULIO 2004.

DEDICATORIA:

AL SR. CURA J. TRINIDAD ROMERO:
Que me enseño lo que significa la verdadera Fe;
Y es el ángel, que me cuida desde el cielo...
Con todo el cariño del mundo... Para mi Tata.

A DAVID ARMANDO GARCIA MIRANDA:
Quien fue el primero de mis mejores amigos,
Y hasta el último de sus días fue el mejor de todos...
Descansa en paz.

A MI MAMA ALBINA:
Por ser la mejor viejita del mundo;
Gracias por haber existido.

AL ING. SERGIO FRANCISCO BARRAZA:
Que sin su apoyo, conocimientos y paciencia,
no hubiera podido lograr llegar hasta aquí.

A toda mi familia:
Mis papas Angelina y Jesús, por todo su apoyo;
Mis hermanos Tere, Jesús, Gely y Carlos;
Y mis niñas Mariana y Daniela.

A todos y cada uno de mis amigos que estuvieron conmigo en los momentos mas difíciles: Jessica, Moisés, Daniel, Oscar, Marisol, Katia, Armando, Mayté, Jazmin, Yuliana y Voris.

INFINITAS GRACIAS A TODOS.

ADMINISTRACION DE LA SEGURIDAD INFORMATICA Y HERRAMIENTAS PARA PLATAFORMA WINDOWS.

INDICE

ADMINISTRACION DE LA SEGURIDAD INFORMATICA Y HERRAMIENTAS PARA PLATAFORMA WINDOWS.

INTRODUCCION.

La meta como materia académica no existe, y es considerada como una herramienta dentro del ámbito en que se la estudia: relaciones internacionales-nacionales, estudios de riesgo, prevención de crímenes y perdidas, etc. Muchos sostienen que es una teoría tan amplia, compleja y abstracta como la pobreza, la belleza o el amor, y ni siquiera arriesgan su definición.

El amplio desarrollo de las nuevas tecnologías informáticas esta ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

El motivo del presente es desarrollar un estudio del estado actual y futuro posible de Seguridad Informática, que continuamente escuchamos mencionar y en realidad conocemos muy poco. Investigaremos planes de estrategias y metodologías, que si bien no brindan la solución total (como muchos estudiosos prometen), podrá cubrir parte de la brecha que hoy se presenta al hablar de Seguridad Informática.

La mayoría del mundo informático desconoce la magnitud del problema con que se enfrenta y, generalmente no se invierte ni el capital en recursos humanos, ni en recursos económicos; necesarios para prevenir, el daño y/o perdida de la información que, es el Conocimiento con que se cuenta.

Paradojamente, en el mundo informático, existe una demanda constante y muy importante que esta esperando a que alguien los atienda.

El presente trabajo esta integrado por 6 capítulos; el primer apartado describe El origen y Evolución de la Seguridad Informática, así como sus Objetivos, las Amenazas y los Elementos a proteger en un Sistema Informático, de los varios Tipos de Ataques que embisten las vulnerabilidades de los anteriores. El segundo capitulo se refiere a la Seguridad Física, los Ejemplos de Desastres y Acciones Hostiles a los que están expuestos los elementos tangibles de cualquier ente; también se refiere a un aspecto muy importante: El Control de Accesos y Protección Electrónica. La tercera parte aborda la Seguridad Lógica en un Sistema informático. El cuarto rubro desarrolla el tema Delitos Informáticos, sus ejemplares, el concepto de Delincuente y Victima además de como se castiga legalmente dichas agresiones. El quinto apartado no menos importante explica lo vital de la implementación de Políticas de Seguridad Informática, la Evaluación de Riesgos y las Estrategias de Seguridad; por último podrá encontrar una Introducción a la Seguridad en el Sistema Operativo Windows y algunas de sus herramientas como VNC (Virtual Network Computing) y MMC (Microsoft Management Console) de esta plataforma.

OBJETIVO GENERAL

Desarrollar un documento que describa un estudio del estado actual de la Seguridad Informática, que continuamente escuchamos mencionar y en realidad conocemos muy poco. Con la intención de proporcionar al lector, una idea general de lo significa tan importante cuestión en nuestros días. En cualquier entidad por pequeña que esta sea, cualquiera que sea su rama, la Seguridad Informática es de vital importancia para su existencia.

OBJETIVOS PARTICULARES

- Divulgar lo importante que es proteger nuestra Información y los recursos humanos, técnicos y económicos; de los cuales dependemos para llevar a cabo nuestras metas.
- Valorar cada uno de los riesgos a los que estamos expuestos como institución, y no pasarlos por alto.
- Invitar a las instituciones a considerar la definición de sus Políticas de Seguridad Informática y procedimientos subsiguientes.
- Contribuir al conocimiento de herramientas eficaces que permitan mejorar la calidad de la Información y el manejo de la misma.
- Concientizar a los lectores sobre la importancia de la Información para el desarrollo económico de las empresas.
- Investigar la mayor cantidad de métodos que si bien no brindan la solución total a la inseguridad de los datos, por lo menos cubran una parte.

CAPITULO 1.
ORIGEN Y EVOLUCION DE LA SEGURIDAD INFORMATICA

1.1 ORIGEN Y EVOLUCION DEL TERMINO SEGURIDAD

La Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, esto es tan antiguo.

Desde los inicios de la escritura (3000 AC.), aparecen autores de obras en donde afloran ciertos rasgos de la seguridad en la guerra y el gobierno. Los descubrimientos arqueológicos son pruebas de la seguridad de los antiguos. Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchaban o huían para eliminar o evitar la causa...

Como todo concepto, la Seguridad se ha desarrollado y ha evolucionado dentro de las organizaciones sociales y culturas. Los descubrimientos científicos han contribuido a la cultura de la seguridad.

Uno de los pasos de la Seguridad es la especialización, esto se refiere: nace la Seguridad Externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la Seguridad Interna (aquella preocupada por las amenazas de nuestra organización con la organización misma).

La seguridad moderna se origino con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en esa época. Un teórico y pionero del Management: Henry Fayol en 1919 identifica la Seguridad como una función empresarial.

Fayol al definir el objetivo de la Seguridad dice: "... salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso incluso de la vida del negocio. Es generalmente hablando todas las medidas para conferir la requerida paz y tranquilidad al personal"...

Hoy la seguridad desde el punto de vista legislativo, esta en manos de los políticos, para prevenir el crimen.
En cambio desde el punto de vista técnico, la seguridad esta en manos de los directivos de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este milenio. Es en este proceso en donde se aprecia que los conceptos son perfeccionamientos de los conocidos desde la antigüedad.

"La Seguridad es hoy día una profesión compleja con funciones especializadas".

Es importante mencionar que para la gran mayoría de las organizaciones y empresas, la Seguridad Informática, todavía no existe.

Este problema será solucionado satisfaciendo las necesidades de comprensión del concepto "Seguridad" y "sistema Informático" en torno de alguien (organización o particular) que gestiona información. Para esto es necesario acoplar los principios de Seguridad en un contexto informático y viceversa. En definitiva los expertos en seguridad y los expertos en informática deben interactuar interdisciplinariamente para que exista Seguridad Informática.

En el presente, cada vez que se mencione Información se estará haciendo referencia a la Información que es procesada por un Sistema Informático; definiendo este ultimo como el "conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, el medio donde actúan y sus interacciones.

1.2 OBJETIVO DE LA SEGURIDAD INFORMATICA

El OBJETIVO de la Seguridad Informática: Será mantener la Integridad, Disponibilidad, Privacidad (aspectos fundamentales), Control y Autenticidad de la información manejada por computadora.

ANALISIS DEL OBJETIVO.

La INFORMACION "Es una agregación de datos (Dato: "unidad mínima que compone cierta información"), que tiene un significado especifico mas allá de cada uno de estos"; y tendrá un sentido particular según como y quien la procese.
Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en la mayoría de los casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con la documentación.
Existe información que debe o puede ser pública: puede ser visualizada por cualquier persona; y existe aquella información que debe ser privada: solo puede ser visualizada por un grupo selecto de personas que trabaja con ella, en esta se deben maximizar los esfuerzos para preservarla.

La INTEGRIDAD de la Información, es la característica que hace que su contenido permanezca sin alteraciones, a menos que sea modificado por personal autorizado. La falta de integridad puede darse por anomalías en el hardware, software, virus informáticos o modificación por personas infiltradas,

La DISPONIBILIDAD, se refiere a la capacidad de estar siempre disponible para ser procesada por las personas autorizadas.

La PRIVACIDAD, es la necesidad de que la información solo sea conocida por personas autorizadas.

El CONTROL sobre la información permite asegurar que solo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

La AUTENTICIDAD permite definir que la información requerida es valida y aprovechable; nos asegura el origen de la misma.

1.3 AMENAZAS EN EL ENTORNO INFORMATICO.

Cabe definir AMENAZA, como cualquier elemento que comprometa el sistema. Dentro de las amenazas encontramos:

- ✓ Humanas
  - o Maliciadas: Externas e Internas.
  - o No maliciosas: Empleados ignorantes.
- ✓ Desastres naturales
  - o Incendios.
  - o Inundaciones.
  - o Terremotos.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo. Estos mecanismos conformaran políticas que garantizaran la seguridad de nuestro sistema informático.

1) Prevención (antes): Mecanismos que aumentan la seguridad de un sistema durante su funcionamiento normal.
2) Detección (durante): Mecanismos orientados a revelar violaciones a la seguridad (como los programas de auditoria).
3) Recuperación (después): Mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar a éste a su funcionamiento normal (como la recuperación de información desde las copias de seguridad realizadas).

Ningún sistema esta exento de Las Amenazas o Riesgos. Definiremos riesgo como "la proximidad de daño sobre un bien". Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

- ✓ Minimizar la posibilidad de su ocurrencia
- ✓ Reducir al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
- ✓ Diseño de métodos para la mas rápida recuperación de los daños experimentados.
- ✓ Corrección de las medidas de seguridad en función de la experiencia recogida.

La Seguridad indicara el índice en que un Sistema Informático esta libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir en un 100 % por lo que solo se habla de "Fiabilidad" y se la define como la "probabilidad de que un sistema se comporte tal y como se espera de él", y se habla de un Sistema Fiable en vez de Sistema Seguro. Entonces para garantizar que un sistema sea fiable se deberá garantizar las características ya mencionadas: Integridad, Operatividad, Privacidad, Control y Autenticidad. Debemos conocer "que es lo que queremos proteger", "de quien lo queremos proteger", "como se puede lograr esto"; para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución de los riesgos.

Comprender y conocer de seguridad ayudara a llevar a cabo análisis sobre los riesgos, las vulnerabilidades, amenazas y contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base de las necesidades de seguridad.

1.4 SISTEMA DE SEGURIDAD

Funciones que deben asegurar un sistema informático.

I. Reconocimiento._ Cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso se quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta también quede registrada.

II. Integridad._ Un sistema integro es aquel que todas sus parte funcionan en forma correcta y en su totalidad.

III. Aislamiento._ Los datos utilizados por un usuario deben ser independientes de los de otro, física y lógicamente (usando técnicas de ocultación y/o compartimiento).

IV. Auditabilidad._ Procedimiento utilizado en la elaboración de exámenes, verificaciones o comprobaciones del sistema. Estas comprobaciones deberían ser periódicas y tales que brinden datos precisos y aporten confianza a los directivos.

V. Controlabilidad._ Todos los sistemas y subsistemas deben estar bajo control permanente.

VI. Recuperabilidad._ Es la existencia de la posibilidad de recuperar los recursos perdidos o dañados.

VII. Administración._ La vigilancia nos permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una retroalimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra las amenazas.

1.5 ¿DE QUIEN DEBEMOS PROTEGERNOS?

Se llama INTRUSO o Atacante a la persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no. Los tipos de Intrusos se podrían caracterizar desde el punto de vista del nivel de conocimiento: existen desde los nuevos intrusos que solo prueban sus escasos conocimientos, hasta los Atacantes que entran a determinados sistemas a buscar la información que necesitan.

1.6 ¿Qué DEBEMOS PROTEGER?

En cualquier sistema informático existen 3 elementos básicos a proteger: el Hardware, el Software y los Datos.

Por Hardware, entendemos el conjunto de todos los Componentes Físicos del sistema informático: CPU, monitor, cableado, impresoras, CD-ROM, cintas, componentes de comunicación.

El Software, son los elementos lógicos que hacen funcional al Hardware: Sistemas Operativos, Aplicaciones, Utilidades.

Entendemos por Datos, al conjunto de información lógica que maneja el Software y el Hardware en conjunto: Bases de Datos, Documentos, Archivos.

De los anteriores, los Datos, que maneja el sistema serán el elemento más importante, ya que son el resultado del trabajo realizado. Si sufriera algún daño el Hardware o Software, estos podrían adquirirse nuevamente, pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y aun así es difícil de devolver los datos a su forma anterior al daño.

1.7 TIPOS DE ATAQUES

Para cualquiera de los elementos descriptos, existen multitud de amenazas y ataques que se pueden clasificar:

- Ataques PASIVOS: el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener la información que este siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Generalmente se emplean para:
  - Obtener el origen y destinatario de la comunicación.
  - Control del volumen de tráfico intercambiado entre las entidades monitorizadas.
  - Control de las horas habituales de intercambio de datos entre los entes.
- Ataques ACTIVOS: estos implican algún tipo de alteración del flujo de datos transmitido. Realizados por Hackers, Piratas informáticos o Intrusos remunerados.

1.8 RELACION OPERATIVIDAD-SEGURIDAD

Seleccionar las medidas de seguridad a implementar requiere considerar el equilibrio entre los intereses referidos a la seguridad, los requerimientos operacionales y la amigabilidad para el usuario.
La Seguridad y la Utilidad del Sistema, deberían ser igualmente proporcionados; aunque en la mayoría de los casos sucede que al incrementar la seguridad de un sistema informático, su operatividad desciende y viceversa; además de que el Costo para implantar un sistema seguro, se eleva por lo complejo del análisis para implementar y mantener este.

Hay que recordar que, el concepto de Seguridad es relativo, pues no existe una prueba total contra engaños, sin embargo existen niveles de Seguridad Mínimos Exigibles. Este nivel depende de un análisis de los riesgos que estamos dispuestos a aceptar, sus costos y las medidas a tomar en cada caso.

CAPITULO 2.
SEGURIDAD FISICA

La Seguridad Física es uno de los aspectos mas olvidados a la hora del diseño de un Sistema Informático. Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"; se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Computo así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

2.1 TIPOS DE DESASTRES

Este tipo de seguridad esta enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro de cómputo.

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

i. Desastres Naturales, incendios accidentales, tormentas e inundaciones.
ii. Amenazas ocasionadas por el hombre.
iii. Disturbios, sabotajes in ternos y externos deliberados.

Siendo sensatos, a veces es muy importante recurrir al sentido común para darnos cuenta que, el solo hecho de cerrar una puerta con llave o cortar la electricidad en ciertas áreas, siguen siendo técnicas muy validas en cualquier entorno.

A continuación se analizaran algunos de los peligros que se corren en un centro de procesamiento, con el objetivo de mantener una serie de acciones en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

2.1.1 INCENDIOS

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo numero uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputo.
Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputo son:

- El área en la que se encuentran las computadoras debe estar en un local que no sea inflamable.
- El área no debe situarse encima, debajo o adyacente a lugares donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- Construir un "falso piso", sobre el piso real de material resistente al fuego.
- No fumar en el área de proceso.
- Emplear mobiliario metálico para papelería. Evitar los materiales plásticos.
- El piso y techo del centro de cómputo y de almacenamiento de medios magnéticos, deben ser impermeables.

2.1.1.1 SEGURIDAD DEL EQUIPAMIENTO

Es muy importante proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos solo sea para PERSONAL AUTORIZADO. Además, es necesario que estas áreas cuenten con mecanismos de ventilación y detección de incendios.

Para protegerlos se debe de tomar en cuenta:

- La temperatura no debe propasar los 18° C aproximadamente.
- Los centros de cómputo deben estar provistos de equipo para la extinción de incendios, en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Instalar extintores manuales (portátil) y/o automáticos (rociador).
- Dar capacitación previa a todos y cada uno de nuestros colaboradores, del manejo de extintores y de cada una de las medidas de previsión implementadas.

2.1.2 INUNDACIONES

Se define como la invasión de agua por exceso de escurrimientos superficiales p por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputo.
Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable y acondicionar las puertas para contener el agua y evitar que pase por debajo de ellas.

2.1.3 CONDICIONES CLIMATOLOGICAS

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurra esta documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

TERREMOTOS.

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la perdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba,

2.1.4 SEÑALES DE RADAR

La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiado desde hace varios años. Los resultados de las investigaciones mas recientes son que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información.

2.1.5 INSTALACION ELECTRICA

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta, es una de las principales áreas a considerar en la seguridad física, además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

2.1.6 CABLEADO

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

Riesgos más comunes para el cableado:

- Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración de los datos que viajan a través de el por acción de campos metálicos, que si sufren los cables metálicos.
- Corte del cable: cuando la conexión establecida se rompe se impide el flujo de datos que circulan por el cable.

- Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar el propio cable, lo que hacen que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños frecuentes. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es interferir en su funcionamiento.
El cable de red ofrece también un nuevo frente para un determinado intruso que intentase acceder a los datos; por mencionar algunos casos:

- ✓ Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de acceso adecuado hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.
- ✓ Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse amenazados.
- ✓

Desgraciadamente, hoy en día no hace falta penetrar en los cables físicamente para obtener los datos que transportan.

2.1.7 SISTEMA DE AIRE ACONDICIONADO

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado, que se dedique a la habitación de las computadoras y equipos de proceso de datos en forma exclusiva.

2.1.8 ERGOMETRIA

No podía dejar de mencionar un componente muy importante en el adecuado funcionamiento de cualquier centro de procesamiento de información, el elemento humano.

"La ERGOMETRIA, es la disciplina que se ocupa de estudiar la forma que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible".
El enfoque ergonómico plantea la adaptación de los métodos, los objetos, las maquinarias, herramientas e instrumentos o medios y las condiciones de trabajo a la anatomía, la fisiología y la psicología del operador. Entre los fines de su aplicación se encuentra, fundamentalmente, la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro.

El lugar de trabajo debe estar diseñado de manera que permita que el usuario se encuentre demasiado cómodo, que su puesto de trabajo se adapte a las medidas y posiciones de su cuerpo de cada operador (como por ejemplo: el teclado y el mouse, la posición del monitor...).
No olvidemos que los ojos, sin duda, son las partes, mas afectadas por el trabajo con computadoras.

2.2 ACCIONES HOSTILES

2.2.1 ROBO

Las computadoras son posesiones valiosas de las empresas y es obvio que están expuestas; es frecuente que los operadores utilicen las computadoras de la empresa para realizar trabajos personales o para otras organizaciones y, de esta manera, robar tiempo maquina. La información importante o confidencial puede ser fácilmente copiada. Muchas organizaciones invierten fuertes sumas de dinero en programas y archivos de información, a los que dan menor protección que la que otorgan a una calculadora. El software, es una propiedad muy fácilmente sustraible y las cintas y discos son fácilmente copiados sin dejar rastro.

2.2.2 FRAUDE

Cada año, millones de pesos son sustraídos de empresas, y en la mayoría de ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.
Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.) tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

2.2.3 SABOTAJE

El peligro mas temido en los centro de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad, han encontrado que la protección contra el saboteador es unos de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son una herramienta a la que se recurre, ya que con una pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruídas en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o combustibles pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

2.3 CONTROL DE ACCESOS

El control de accesos no solo se refiere a la capacidad de identificación, sino también se asocia a la apertura de entradas (puertas), permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

2.3.1 UTILIZACION DE VIGILANCIA

El servicio vigilancia es el encargado del control de acceso de todas las personas al edificio. Este servicio coloca los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.
El uso de identificaciones es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.
Sin embargo, lo más recomendable es la utilización de sistemas biométricos para el control de accesos.

2.3.2 UTILIZACION DE SISTEMAS BIOMETRICOS.

Definimos a la Biometría como "la parte de la Biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos".

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.
La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos.
Los lectores biométricos identifican a la persona por lo que es (como sus manos, ojos, huellas digitales y voz).

BENEFICIOS DE UTILIZAR UNA TECNOLOGIA BIOMETRICA.

Pueden eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años, el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración. Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, que las características biométricas de una persona no son transferibles a otra.

- EMISION DE CALOR: Consiste en la medición de la temperatura del cuerpo (termograma), realizando un mapa de valores sobre la forma de cada persona.
- HUELLA DIGITAL: Basado en el principio de que no existen dos huellas dáctiles iguales, este sistema viene siendo utilizado con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias); características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona.
- VERIFICACION DE VOZ: La dicción de una frase es grabada y en el acceso se compara la voz (entonación, diptongos, agudeza, etc.); este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades, o también el envejecimiento, por mencionar algunos.
- VERIFICACION DE PATRONES OCULARES: Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados mas efectivos, en 200 millones de personas la probabilidad de coincidencia es casi 0.

2.3.3 VERIFICACION AUTOMATICA DE FIRMAS (VAF)

La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada. El equipamiento de colección de firmas es inherentemente de bajo costo y robusto.

2.4 PROTECCION ELECTRONICA

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de censores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos censores detectan una situación de riesgo, estos transmiten inmediatamente el aviso a la central; esta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

a) BARRERAS INFRARROJAS Y DE MICRO-ONDAS

Transmiten y reciben haces de luces infrarrojas y de micro-ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor; cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

b) DETECTOR ULTRASONICO

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generara una perturbación en dicho campo que accionara la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas.

c) SONORIZACION Y DISPOSITIVOS LUMINOSOS

Dentro de los elementos de sonorización se encuentran las sirenas, campanas, timbres, etc. Algunos dispositivos luminosos son los faros rotativos, las balizas, las luces intermitentes, etc. Estos deben ser colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar identificados para poder determinar rápidamente si el estado de alarma es robo, intrusión, asalto o aviso de incendio.

d) CIRCUITOS CERRADOS DE TELEVISION.

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista u ocultas.

e) EDIFICIOS INTELIGENTES

La infraestructura inmobiliaria no podía quedarse rezagada en lo que se refiere a avances tecnológicos.

El edificio inteligente, se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación. Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía. Una característica común de los Edificios Inteligentes es la flexibilidad que deben tener para asumir modificaciones de manera conveniente y económica.

CAPITULO 3.
SEGURIDAD LOGICA

Después de ver como nuestro 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 controla información por el almacenada y procesada.

Así, la Seguridad Física, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se menciono, el activo mas importante que se posee es la Información, y por lo tanto deben existir técnicas, mas allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo."
Los objetivos que procura cubrir:

- ✓ 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 utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- ✓ Que la información transmitida sea recibida solo por el destinatario al cual ha sido enviada y no a otro.
- ✓ Que la información recibida sea la misma que la transmitida.
- ✓ Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- ✓ Que se disponga de pasos alternativos de emergencia para la transmisión de información.

3.1 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 utilidad.

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. Al respecto, el Nacional Institute for Standard and Technology (NIST), ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

1) IDENTIFICACION Y AUTENTIFICACION

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

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

Al igual que se considero para la seguridad física, y basada en ella, existen 4 técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales se pueden usar juntas o por separado:

a. Algo que solamente el individuo conoce: por ejemplo un password o un numero de identificación personal
b. Algo que la persona posee: como una tarjeta magnética.
c. Algo que el individuo es y que lo identifica unívocamente: como las huellas digitales o la voz.
d. Algo que el individuo es capaz de hacer: como un patrón de escritura.

2) ROLES

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.

3) TRANSACCIONES

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

4) LIMITACIONES A LOS SERVICIOS.

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser, que en la organización se disponga de licencias para la utilización simultánea de un determinado software para determinado número de usuarios, en donde exista un control a nivel sistema que no permita la utilización del paquete a un usuario más.

5) MODALIDAD DE ACCESO.

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- LECTURA: El usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- ESCRITURA: Este tipo de acceso permite agregar datos, modificar o borrar información.
- EJECUCION: Este acceso otorga al usuario el privilegio de ejecutar programas.
- BORRADO: Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos).
- TODAS LAS ANTERIORES.

Además también pueden existir otras modalidades de acceso:

- CREACION: Permite al usuario crear nuevos archivos, registros o campos.
- BUSQUEDA: Permite listar los archivos de un directorio determinado.

6) UBICACIÓN Y HORARIO

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control mas restringido de los usuarios y zonas de ingreso. Estos tipos de controles van de la mano, de algunos de los anteriores.

7) CONTROL DE ACCESO INTERNO.

a. Passwords (Palabras Claves): Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica. Se podrá por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por esta razón: La elección de passwords débiles. Es importante considerar:

LA SINCRONIZACION DE PASSWORDS: Consiste en permitir que un usuario acceda con la misma clave a diversos sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada.

Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los

que tengan acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aun mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

CADUCIDAD Y CONTROL: Este mecanismo controla cuando pueden y/o deben cambiar sus passwords los usuarios. Se define el periodo mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un periodo máximo que puede transcurrir para que estas caduquen.

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

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

d. Limites sobre la interfase de Usuario: Estos limites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones especificas.

8) CONTROL DE ACCESO EXTERNO

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

b. Firewalls o Puertas de Seguridad: Permiten bloquear o filtrar el acceso entre dos redes, usualmente una priveda y otra externa (por ejemplo Internet). Los Firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de organización.

c. Acceso de Personal Contratado o Consultores: Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

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

9) ADMINISTRACION

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

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

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que producirá una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más criticas, y avanzar de acuerdo a u orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Un programa especifico para la administración de los usuarios informáticos desarrollado sobre la base de las consideraciones expuestas, puede constituir un compromiso vació, si no existe una conciencia de la seguridad organizacional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su perdida o apropiación de la misma por agentes extraños a la organización.

a. Administración del Personal y Usuarios:

ORGANIZACIÓN DEL PERSONAL._ Este proceso lleva generalmente cuatro pasos;

1. Definición de Puestos. Debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.

2. Determinación de la sensibilidad del puesto. Para esto es necesario determinar si la fusión requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.

3. Elección de la persona para cada puesto. Requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto; asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales.

4. Entrenamiento inicial y continuo del empleado. Cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tareas que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Solo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la organización.

CAPITULO 4
DELITOS INFORMATICOS

Ya hemos dejado en claro la importancia de la información en el mundo altamente tecnificado de hoy. También se ha dejado en claro cada uno de los riesgos "naturales" con los que se enfrenta nuestro conocimiento y la forma de enfrentarlos.

El 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.

4.1 LA INFORMACION Y EL DELITO

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.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún.

En 1983, la Organización de Cooperación y desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales. Dicha organización publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define delito Informático, como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos".

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en si misma".

Adicionalmente, la OCDE 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. Por mencionar algunas:

- ✓ 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 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.
El autor Julio Téllez Valdez clasifica a los delitos informáticos en base a dos criterios:

1. Como instrumento o medio: Se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito. Ejemplos:

- Falsificación de documentos vía computarizada: tarjetas de crédito, cheques, etc.
- Variación de la situación contable.
- Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.
- Alteración del funcionamiento normal de un sistema mediante la introducción de código extraño al mismo: virus, bombas lógicas, etc.
- Intervención de líneas de comunicación de datos o teleprocesos.

2. Como fin u objetivo: Se enmarcan las conductas criminales se van dirigidas en contra de la computadora, accesorios o programas como entidad física. Ejemplos:

   - Instrucciones que producen un bloqueo parcial o total del sistema.
   - Destrucción de programas por cualquier método.
   - Atentado físico contra la computadora, sus accesorios o sus medios de comunicación.
   - Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.

4.2 TIPOS DE DELITOS INFORMATICOS

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

1. Fraudes cometidos mediante manipulación de computadoras:

   - Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

- La manipulación de programas: consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación.

- Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude del que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

- Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo.

2. Manipulación de los datos de entrada:

- Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumento: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

3. Daños o modificaciones de programas o datos computarizados.

- Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.

- Acceso no autorizado a servicios y sistemas informáticos: estos accesos se pueden realizar por diversos motivos, desde la curiosidad hasta el sabotaje o espionaje informático.

- Reproducción no autorizada de programas informáticos de protección legal: esta puede entrañar una perdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, se considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Adicionalmente a estos tipos de delitos reconocidos, el XV Congreso Internacional de Derecho ha propuesto todas las formas de conductas lesivas de la que puede ser objeto la información. Ellas son:

- Fraude en el campo de la Informática.
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos.

4.3 DELINCUENTE Y VICTIMA

4.3.1 SUJETO ACTIVO

Se llama así a las personas que cometen los delitos informáticos. Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre si es la naturaleza de los delitos cometido. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar retos tecnológicos, características de colaboradores del sector de procesamiento de datos. No es fácil descubrirlos ni sancionarlos, pero los daños económicos son altísimos. A los sujetos que cometen este tipo de delitos no se considera delincuentes, no se los desprecia, ni se los desvaloriza; por el contrario, es considerado y se considera a sí mismo "respetable"; estos tipos de delitos, generalmente, son objeto de medidas o sanciones de carácter y no privativos de la libertad.

4.3.2 SUJETO PASIVO

Este, la víctima del delito, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las victimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. Que usan sistemas automatizados de información, generalmente conectados a otros.

Es imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas.

Por lo anterior, *se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.*

La delincuencia informática, cada día tiende a expandirse más. Organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos, se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

4.4 LEGISLACION

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 ese sentido habrá que recurrir a aquellos tratados internacionales de lo que nuestro país es parte y que, en virtud del Articulo 75 inciso 22, de la Constitución Nacional tiene rango constitucional. Nuestra legislación regula Comercial y Penalmente las conductas ilícitas relacionadas con la informática, aunque aún no contempla en sí los delitos informáticos.

Por ejemplo, la Ley Penal de Propiedad Científica, Literaria y Artística, en el país; protege los lenguajes de bases de datos, planillas de cálculo, el software y su documentación dentro del mismo, pero, no tiene en cuenta la posibilidad de plagio ya que no hay jurisprudencia que permita establecer qué porcentaje de igualdad en la escritura de dos programas se considera plagio. Las copias ilegales de software también son penalizadas, pero por reglamentaciones comerciales.

Una de las más grandes dificultades es cuantificar los delitos informáticos. Si se considera Internet, el problema se vuelve aún mas grave ya que se caracteriza por ser algo completamente descentralizado; desde el punto de vista del usuario esto constituye un beneficio, puesto que no tiene ningún control ni necesita autorización para acceder a los datos, sin embargo, constituye un problema desde el punto de vista legal principalmente porque las leyes penales son aplicables territorialmente y no pueden pasar las barreras de los países.

Lo mencionado hasta aquí no da buenas perspectivas para la seguridad de los usuarios en cuanto a los datos que almacenan. Pero esto no es tan así, puesto que si la información es confidencial la misma tendrá, en algún momento amparo legal.

En cuanto a la actividad de los hackers, las leyes castigan el hurto de energía eléctrica y de líneas telefónicas, aunque no es fácil de determinar la comisión del delito, la dificultad radica en establecer dónde se cometió el delito y quién es el damnificado. Los posibles hechos de hacking se encuadran en la categoría de delitos comunes como defraudaciones, estafas o abusos de confianza, y la existencia de una computadora no modifica el castigo impuesto por la ley.

Estos vacíos en las legislaciones también se agravan debido a que las empresas que sufren ataques no los difunden por miedo a perder el prestigio y principalmente porque no existen conceptos claros para definir nuevas leyes jurídicas en función de los avances tecnológicos.

Como conclusión, desde el punto de vista social, es conveniente educar y enseñar la correcta utilización de todas las herramientas informáticas, impartiendo conocimientos específicos acerca de las conductas prohibidas; no solo con el afán de protegerse, sino para evitar convertirse en un agente de dispersión que contribuya, por ejemplo, a que un virus informático siga extendiéndose y alcance una computadora en la que, debido a su entorno crítico produzca un daño realmente grave e irreparable.

Desde la óptica legal, y ante la existencia de normas que tipifiquen los delitos cometidos a través de la computadora, es necesario y muy importante que la ley contemple accesos ilegales a las redes como a sus medios de transmisión. Lo gracioso es que existió el día que no había para nada, sanción legal para la persona que destruía información almacenada en un soporte, pero si para quien destruía la misma información impresa sobre papel.

Desde la Criminología debemos señalar que el anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, son 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 como lograr probar el delito. Este sigue siendo el principal inconveniente a la hora de legislar por el carácter intangible de la información.

Al final, la gente se dará cuenta de que no tiene ningún sentido escribir leyes específicas para la tecnología. El fraude es el fraude, se realice mediante el correo postal, el teléfono o Internet. Un delito no es más o menos delito si se utilizó criptografía... y el chantaje no es mejor o peor si se utilizaron virus informáticos o fotos comprometedoras... Las buenas leyes son escritas para ser independientes de la tecnología. En un mundo donde la tecnología avanza mucho más deprisa que las sesiones del Congreso, eso es lo único que puede funcionar hoy en día; mejores y más rápidos mecanismos de legislación, juicios y sentencias... tal vez algún dia...

CAPITULO 5.
POLITICAS DE SEGURIDAD

5.1 POLITICAS DE SEGURIDAD INFORMÁTICA

Como ya mencione, hoy es imposible hablar de un sistema 100% seguro, sencillamente porque el costo de la seguridad total es muy alto.
Las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concienciar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

En la mayoría de los casos, muchos documentos son ignorados por contener planes y políticas difíciles de lograr, o peor aún, de entender. Esto adquiere mayor importancia aún cuando el tema abordado por estas políticas es la Seguridad Informática. La Seguridad Informática no tiene una solución definitiva aquí y ahora sino que es y será el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son los responsables de nuestros sistemas.

Para continuar, hará falta definir algunos conceptos aplicados en la definición de una PSI:

DECISIÓN: Elección de un curso de acción determinado entre varios posibles.

PLAN: Conjunto de decisiones que definen cursos de acción futuros y los medios para conseguirlos. Consiste en diseñar un futuro deseado y la búsqueda del modo de conseguirlo.

ESTRATEGIA: Conjunto de decisiones que se toman para determinar políticas, metas y programas.

POLÍTICA: Definiciones establecidas por la dirección, que determina criterios generales a adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.

META: Objetivo cuantificado a valores predeterminados.

PROCEDIMIENTO: Definición detallada de pasos a ejecutar para desarrollar una actividad determinada.

NORMA: Forma en que realiza un procedimiento o proceso.

PROGRAMA: Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.

PROYECCIÓN: Predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas.

PRONOSTICO: Predicción del comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé influirá en los acontecimientos futuros.

CONTROL: Capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan.

RIESGO: Proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, etc., que puede tener un efecto adverso.

Una POLITICA DE SEGURIDAD, es "un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema"; también se define como "Una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán".

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero ante todo... una Política de Seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas, y debe:

- Adecuarse a las necesidades y recursos.
- Ser atemporal; el tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

Cualquier Política de Seguridad ha de contemplar los elementos claves de seguridad ya mencionados: la Integridad, Disponibilidad, Privacidad, Control, Autenticidad y Utilidad.

No debe tratarse de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que deseamos proteger y el porqué de ello.

5.2 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, contra el costo de volverla a producir.

- Se debe tener en cuenta la probabilidad que sucedan 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 presuponer 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 3 primeras preguntas?
- ¿se está preparado para abrir las puertas del negocio sin sistemas, por un día, una semana o 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?
- ¿Cuántas personas dentro de la empresa, están en condiciones de inhibir el procesamiento de datos?
- ¿a que se llama información confidencial?
- ¿la información confidencial, 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?; ¿Quién es el usuario con mayores privilegios sobre ese recurso?

- ¿Cuáles serán los privilegios y responsabilidades del administrador contra la del usuario?
- ¿Cómo se actuará si la seguridad es violada?

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

Tabla 1: TIPO DE RIESGO-FACTOR

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

Es importante recalcar, los riesgos se clasifican por su nivel de importancia y por la severidad de su pérdida.

5.2.1 IDENTIFICACION DE AMENAZA

Una vez conocidos los riesgos, los recursos se deben proteger y como su daño o falta pueden influir en la organización es necesario identificar cada una de las amenazas y vulnerabilidades que pueden causar estas bajas en los recursos. Como ya se menciono existe una relación directa entre amenaza y vulnerabilidad a tal punto que si una no existe la otra tampoco.

5.3 ESTRATEGIA DE SEGURIDAD

Para establecer una estrategia adecuada es conveniente pensar una política de protección en los distintos niveles que esta debe abarcar y que no son ni mas ni menos que los estudiados hasta aquí: Física, Lógica, Humana y la interacción que existe entre estos elementos.

En cada caso considerado, el plan de seguridad debe incluir una estrategia Preactiva y otra Reactiva.
La Estrategia Proactiva (proteger y proceder) o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia.

La Estrategia Reactiva (Perseguir y procesar) o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia Preactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adoptarse ante los recursos compartidos:

- Lo que no se permite expresamente está prohibido: significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.

- Lo que no se prohíbe expresamente está permitido: significa que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás si lo estarán.

Estas posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no. Gracias a las acciones que atentan contra los sistemas informáticos se recomienda la primera política mencionada.

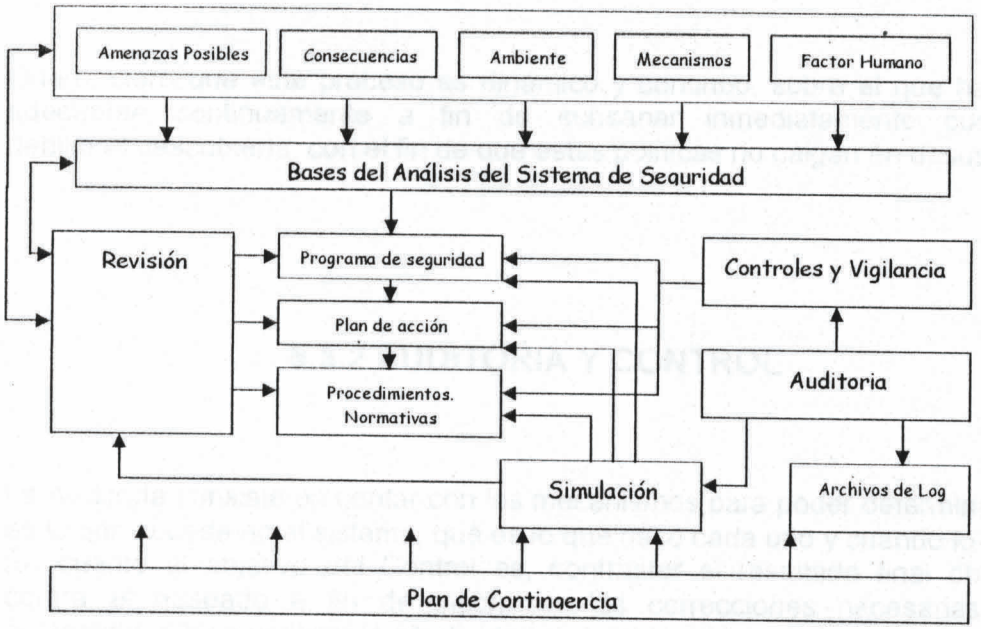
5.3.1 IMPLEMENTACIÓN.

La implementación de medidas de seguridad, es un proceso Técnico-administrativo. Como este proceso debe abarcar TODA la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.
Se deberá tener en cuenta que la implementación de Políticas de Seguridad, trae consigo varios problemas que afectan el funcionamiento de la organización. La implementación de un sistema de seguridad conlleva incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativamente.
Por esto, será necesario calcular cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.
Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Una PSI deberá abarcar:

- ✓ Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- ✓ Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- ✓ Responsabilidad de cada uno de los servicios, recursos y responsables en todos los niveles de la organización.
- ✓ Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- ✓ Definición de violaciones y las consecuencias del no cumplimiento de la política.
- ✓ Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer.
- ✓ Explicaciones comprensibles (libre de tecnicismos y términos legales pero sin sacrificar su precisión) sobre el porque de las decisiones tomadas.
- ✓ Como documento dinámico de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta, incremento de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc.

Una proposición de una forma de realizar una PSI adecuada puede apreciarse en siguiente diagrama.



Se comienza realizando una evaluación del factor humano, el medio en donde se desempeña, los mecanismos con los cuales se cuenta para llevar a cabo la tarea encomendada, las amenazas posibles y sus posibles consecuencias.
Luego de evaluar estos elementos y establecida la base del análisis, se originan un programa de seguridad, el plan de acción y las normas y procedimientos a llevar a cabo.

Para que todo lo anterior llegue a buen fin debe realizarse un control periódico de estas políticas, que asegure el fiel cumplimiento de todos los procedimientos enumerados. Para asegurar un marco efectivo se realiza una auditoria a los archivos Lógicos de estos controles.

Con el objeto de confirmar que todo lo creado funciona en un marco real, se realiza una simulación de eventos y acontecimientos que atenten contra la seguridad del sistema. Esta simulación y los casos reales registrados generan una retroalimentación y revisión que permiten adecuar las políticas generadas en primera instancia.

Por último el Plan de Contingencia es el encargado de suministrar el respaldo necesario en caso en que la política falle.

Es importante destacar que la Seguridad debe ser considerada desde la fase de diseño de un sistema. Si la seguridad es contemplada luego de la implementación del mismo, el personal se enfrentará con problemas técnicos, humanos y administrativos muchos mayores que implicaran mas costo para lograr, en la mayoría de los casos, un menor grado de seguridad.

Queda claro que este proceso es dinámico y continuo, sobre el que hay que adecuarse continuamente a fin de subsanar inmediatamente cualquier debilidad descubierta, con el fin de que estas políticas no caigan en desuso.

5.3.2 AUDITORIA Y CONTROL

La Auditoria consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno y cuando lo hace. En cuanto al objetivo del Control es, contrastar el resultado final obtenido contra el deseado a fin de incorporar las correcciones necesarias para alcanzarlo, o bien verificar la efectividad de lo obtenido.

5.3.3 PLAN DE CONTINGENCIA.

Pese a todas las medidas de seguridad puede ocurrir un desastre. De hecho los especialistas en seguridad afirman que hay que definir un plan de recuperación de desastres para cuando falle el sistema, no por si falla el sistema.

Por tanto, es necesario que el Plan de Contingencias que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles. Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

Un Plan de Contingencia de Seguridad Informática consiste los pasos que se deben seguir, luego de un desastre, para recuperar, aunque sea en parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas.

Se entiende por Recuperación, "tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información.

Se dice que el Plan de Contingencias es el encargado de sostener el modelo de Seguridad Informática planteado y de levantarlo cuando se vea afectado.
La recuperación de la información se basa en el uso de una política de copias de seguridad (Backup) adecuada.

5.3.4 EQUIPOS DE RESPUESTA A INCIDENTES

Es aconsejable formar un equipo de respuesta a incidentes. Este equipo debe estar implicado en los trabajos preactivos del profesional de la seguridad. Como:

- El desarrollo de instrucciones para controlar incidentes.
- Designación del Administrador de seguridad.
- La identificación de las herramientas de software para responder a incidentes y eventos.
- La investigación y desarrollo de otras herramientas de Seguridad Informática.
- La realización de actividades formativas.
- La realización de investigaciones acerca de virus.
- La ejecución de estudios relativos a ataques al sistema.

Estos trabajos proporcionarán los conocimientos que la organización puede utilizar y la información que hay que distribuir antes y durante los incidentes. Una vez que el Administrador de seguridad y el equipo de respuesta a incidentes han realizado estas funciones proactivas, el Administrador puede delegar la responsabilidad del control de incidentes al equipo de respuesta, que es capaz de controlar cualquier incidente por si mismo. Incidentes como virus, gusanos, invasión, engaños y ataques del personal interno; éste, también participa en el análisis de cualquier evento inusual que pueda estar implicado en la seguridad de los equipos.

5.3.5 BACKUPS.

El Backup de archivos permite tener disponible e integra la información para cuando sucedan los accidentes. Sin un backup, simplemente, es imposible volver la información al estado anterior al desastre.

Como siempre, será necesario realizar un análisis Costo/Beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirá el backup, etc.
Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

- Se debe de contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.

- Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de L/E, tipo de backup a realizar, etc.

- El almacenamiento de los backups debe realizarse en locales diferentes en donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.

- Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.

- Se debe de contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.

- Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios; por ejemplo, la información se debe encriptar antes de respaldarse.

- Se debe de contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.

- Mantener equipos de hardware, de características similares a los utilizados para el proceso normal en condiciones para comenzar a procesar en caso de desastres físicos.

5.3.6 PRUEBAS

El último elemento de las estrategias de seguridad, las pruebas y el estudio de los resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y preactiva. La realización de ataques simulados en sistemas de pruebas o en laboratorios permite evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia.

La realización de pruebas y de ajustes en las directivas y controles de seguridad en función de los resultados de las pruebas es un proceso iterativo de aprendizaje. Nunca termina, ya que debe evaluarse y revisarse de forma periódica para poder implementar mejoras.

5.4 LA POLITICA

Como ya se ha mencionado, los fundamentos aquí expuestos no deben ser tomados puntualmente en cada organización tratada. Deberán ser adaptados a la necesidad, requisitos y limitaciones de cada organización (o usuario individual) y, posteriormente requerirá actualizaciones periódicas asegurando el dinamismo sistemático.

5.4.1 NIVEL FISICO

El primer factor considerado, y el más evidente debe ser asegurar el sustrato físico del objeto a proteger. Es preciso establecer un perímetro de seguridad a proteger, y esta protección debe adecuarse a la importancia de lo protegido.

La defensa contra agentes nocivos conlleva tanto medidas preactivas (limitar el acceso) como normativas de contingencia (que hacer en caso de incendio) o medidas de recuperación (realizar copias de seguridad). El grado de seguridad solicitado establecerá las necesidades: desde evitar el café y el tabaco en las proximidades de equipos electrónicos, hasta el establecimiento de controles de acceso a la sala de equipos. Lo más importante es recordar que quien tiene acceso físico a un equipo tiene control absoluto del mismo. Por ello sólo deberían accederlo aquellas personas que sean estrictamente necesarias.

5.4.1.1 AMENAZA NO INTENCIONADA (DESASTRE NATURAL)

Ejemplo de una posible situación:

Una organización no cuenta con sistemas de detección de incendios en la sala de servidores. El encargado del sistema deja unos papeles sobre el aire acondicionado de la sala. Durante la noche el acondicionador se calienta y se inicia un incendio que arrasa con la sala de servidores y un par de despachos contiguos.

Directivas:

1. Predecir ataque/riesgo: Incendio
2. Amenaza: Desastre natural, Incendio
3. Ataque: No existe
4. Estrategia Proactiva:
    a. Predecir posibles daños: pérdida de equipos e información.
    b. Determinar y minimizar vulnerabilidades: protección contra incendios.
    c. Evaluar planes de contingencia: backup de la información.
5. Estrategia Reactiva:
    a. Evaluar daños: perdida de hardware e información.
    b. Determinar su origen y repararlos: bloqueo del aire acondicionado.
    c. Documentar y aprender.
    d. Implementar plan de contingencia: recuperar backups.
6. Examinar resultados y eficacia de la directiva: Ajustar la directiva con los nuevos conceptos incorporados.

5.4.2 NIVEL HUMANO

5.4.2.1 EL USUARIO

Algunas consideraciones que se deberían tener en cuenta para la protección de la información:

1. Generalmente se considera que la máquina es poco importante para que un atacante la tenga en cuenta. Se debería recordar que este atacante no sabe quien está del otro lado del monitor, por lo que cualquier objetivo es tan importante como cualquiera.

2. Generalmente se sobrevalora la capacidad de un atacante, la mayoria de ellos comienzan solo por diversión o por un reto...

3. Convencerse de que todos los programas existentes tiene vulnerabilidades conocidas y desconocidas, permite no sobrevalorar la seguridad de un sistema. Ejemplo: Un usuario dice: "Yo utilizo Linux porque es más seguro que Windows"; esto es una mentira disfrazada: el usuario debería decir que Linux puede ser más seguro que Windows; de hecho cualquier sistema bien configurado puede ser más seguro que uno que no lo está.

4. Todo usuario debe tomar como obligación la seguridad de su computadora.

a) AMENAZA NO INTENCIONADA (EMPLEADO).

El siguiente ejemplo ilustra una posible situación de contingencia y el procedimiento a tener en cuenta:

Un empleado, no desea perder la información que ha guardado en su disco duro, así que la copia (el disco completo) a su carpeta particular del servidor, que resulta ser también el servidor principal de aplicaciones de la organización. No se han definido cuotas de disco para las carpetas particulares de los usuarios que hay en el servidor. El disco duro del usuario tiene 6 GB de información y el servidor tiene 6.5 GB de espacio libre. El servidor de aplicaciones deja de responder a las actualizaciones y peticiones porque se ha quedado sin espacio en el disco. El resultado es que se deniega a los usuarios los servicios del servidor de aplicaciones y la productividad se interrumpe. A continuación, se explica la mitología que se debería haber adoptado antes de que el usuario decida realizar su copia de seguridad:

Directivas:

1. Predecir ataque/riesgo: Negación de servicios por abuso de recursos.
2. Amenaza: No existe. Empleado sin malas intenciones
3. Ataque: No existe motivo ni herramienta, solo el desconocimiento por parte del usuario.
4. Estrategia Proactiva:
    a. Predecir posibles daños: pérdida de productividad por espacio de disco/memoria agotados.
    b. Determinar y minimizar vulnerabilidades: implementar cuotas de discos.
    c. Evaluar planes de contingencia: servidor backup.
    d. Capacitar al usuario.
5. Estrategia Reactiva:
    a. Evaluar daños: perdida de producción.
    b. Determinar su origen y repararlos: hacer espacio en el disco.
    c. Documentar y aprender.
    d. Implementar plan de contingencia:
6. Examinar resultados y eficacia de la directiva: Ajustar la directiva con los nuevos conceptos incorporados.

b) AMENAZA MALINTENCIONADA

Una empresa competidora ofrece a un usuario cierta suma de dinero para obtener el diseño del último producto desarrollado por su empresa. Como este usuario carece de los permisos necesarios para obtener el diseño se hace pasar como un administrador, y usando ingeniería, consigue el nombre de usuario y password de un usuario con los permisos que él necesita.
La política de seguridad asociada a este evento debería haber contemplado:

Directivas:

1. Predecir ataque/riesgo: Robo de información mediante el uso de ingeniería
2. Amenaza: Amenaza malintencionada.
3. Ataque: Ingeniería.
4. Estrategia Proactiva:
    a. Predecir posibles daños: pérdida de productividad y/o beneficios.
    b. Determinar y minimizar vulnerabilidades: concientización de los usuarios.
    c. Evaluar planes de contingencia:
5. Estrategia Reactiva:
    a. Evaluar daños: perdida de beneficios e información.
    b. Determinar su origen: revelación de login y password por parte del usuario.
    c. Recuperación de daños: implementar entrenamiento de los usuarios.
    d. Documentar y aprender.
    e. Implementar plan de contingencia:
6. Examinar resultados y eficacia de la directiva: Ajustar la directiva con los nuevos conceptos incorporados.

5.4.2.2 PERSONAS AJENAS AL SISTEMA

a) AMENAZA NO INTENCIONADA

Un virus ingresa a la empresa mediante un correo electrónico enviado a un empleado, y comienza a expandirse dentro de la misma tomando como base la libreta de direcciones de los usuarios:

Directivas:

1. Predecir ataque/riesgo: Negación de servicio del servidor de correo electrónico por la gran cantidad de mensajes enviados/recibidos.
2. Amenaza: Virus

3. Ataque: Virus de correo electrónico.
4. Estrategia Proactiva:

a. Predecir posibles daños: pérdida de productividad por negación de servicio.

b. Determinar y minimizar vulnerabilidades: actualización de antivirus y concientización de usuarios en el manejo del correo electrónico.

c. Evaluar planes de contingencia: evaluar la importancia de un servidor backup. Antivirus.

5. Estrategia Reactiva:
   a. Evaluar daños: perdida de producción.
   b. Determinar su origen y repararlos: caída del servidor por overflow de mensajes.
   c. Reparación de daños: implementar el servidor backup. Eliminación del virus causante del problema.
   d. Documentar y aprender.
   e. Implementar plan de contingencia: servidor backup.
6. Examinar resultados y eficacia de la directiva: Ajustar la directiva con los nuevos conceptos incorporados.

b) AMENAZA MALINTENCIONADA

Una persona ingresa al sistema de la empresa, con intenciones de recopilar información para su posterior venta:

Directivas:

1. Predecir ataque/riesgo: Ingreso al sistema por vulnerabilidades en los sistemas o política de claves ineficiente.
2. Amenaza: Outsider recopilando información significativa.
3. Ataque: Ingreso al sistema.
4. Estrategia Proactiva:
   d. Predecir posibles daños: Robo y venta de información. Daño a la imagen de la empresa.
   e. Determinar y minimizar vulnerabilidades: actualización de sistemas vulnerables. Concientización a los usuarios en el manejo de contraseñas.
   f. Evaluar planes de contingencia: implementación servidor backup para casos de daño de la información. Recuperación de imagen. Evaluar formas de minimizar el daño por la información robada.
5. Estrategia Reactiva:
   g. Evaluar daños: información susceptible robada.
   h. Determinar su origen: ingreso al sistema.
   i. Recuperación de daños.
   j. Documentar y aprender.
   k. Implementar plan de contingencia: servidor backup.
6. Examinar resultados y eficacia de la directiva: Ajustar la directiva con los nuevos conceptos incorporados.

CAPITULO 6.
INTRODUCCIÓN A LA SEGURIDAD EN WINDOWS 2000.

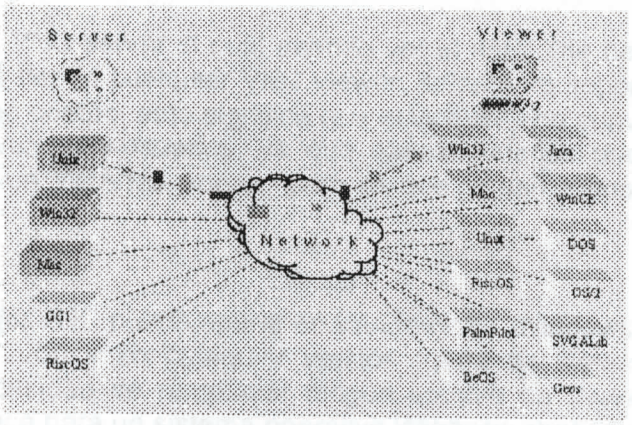
6.1 VNC (Virtual Network Computing)

RealVNC es una compañía del Reino Unido, fundada en 2002 por un equipo de los laboratorios de AT&T. La compañía fue fundada para desarrollar, aumentar y promocionar VNC, el software de acceso remoto innovador. El software de VNC es de plataforma múltiple, admitiendo el control remoto entre diferente clases de computadoras.

La fuente de VNC ha estado libremente disponible desde 1998, y más de 20 millones copias del software han sido descargadas. El software también ha aparecido en discos de portada de revistas, y durante varios años versiones populares de Linux han incluido VNC. Hoy, el equipo de RealVNC ha rediseñado y re-implementado el sistema de VNC, el sistema es ahora una plataforma sumamente flexible y modular y escalable para el desarrollo y la integración.

6.1.1 ¿QUÉ ES VNC? ¿PARA QUE SIRVE?

VNC es un programa el cual es la solución para trabajar en cualquier tipo de plataforma y poder ver y controlar nuestra PC desde cualquier otra maquina conectada a Internet. VNC son las iniciales de Virtual Network Computing (Red virtual de Computo), el programa funciona en varias plataformas. Consta de dos partes, un cliente y un servidor. El cliente se puede ejecutar como una aplicación cualquiera y el servidor puede funcionar en plataformas Windows, Windows CE, Macintosh, y varios tipos de Unix.



6.1.2 ¿CÓMO FUNCIONA?

El servidor se instala en la máquina a monitorear, luego aparecerá un icono al lado de la hora de Windows que te indica que se encuentra activado. Y el cliente se instala en la máquina desde donde se va a trabajar, todo lo que hay que hacer, es indicarle al cliente el IP de tu máquina en Internet o red interna y la contraseña que hayas configurado.

VNC es totalmente independiente, sea cual sea la plataforma en la que esta instalado, puede verse desde cualquier plataforma distinta sin problemas. Por ejemplo, si lo instalamos en Linux, podemos ver el escritorio de Linux desde el Internet Explorer desde PC.

No es totalmente necesario instalar el programa cliente en la máquina desde la cual se quiere trabajar, hay otra opción un poco más lenta pero muy compatible. Se puede usar el Internet Explorer o cualquier navegador para acceder a la otra máquina, solo se debe poner en la dirección (http://) la dirección IP de la maquina, si suponiendo que es 5900 se debe poner, por ejemplo http://000.000.000.000:5900, y automáticamente se va a cargar un applet hecho en Java solicitando la contraseña.

Con el VNC se puede conectar remotamente y tener el control de una PC que se encuentre con el VNC servidor ejecutándose. En algunas configuraciones se puede, también, tener múltiples usuarios conectados a la vez, usar comandos remotos, copiar y pegar texto ASCII entre el servidor y el cliente, etc.

6.1.3 WINVNC - EL VNC SERVER PARA WINDOWS NT

WinVNC es un VNC server el cual permite ver el ambiente de escritorio de un server windows desde cualquier VNC viewer, solamente soporta una conexión remota al mismo tiempo, esto significa que el WinVNC no convierte un servidor NT en un server multi-usuarios. ya que varios usuarios podrían acceder al mismo tiempo un WinVNC server; pero lo que verían todos seria el mismo escritorio.

Por otro lado Win VNC puede operar en Windows 95, Windows98, Windows NT 4.0, Windows 2000 y en cualquier versión futura de sistemas basados en Win32, sin necesidad de remplazar ningún archivo de system o instalar un versión especifica para un sistema operativo Windows especifico.

WinVNC puede iniciarse como un servicio, lo cual significa que es posible tomar control remoto de una estación remota aunque nadie hubiese iniciado una sesión local, perfectamente puedes validarte e iniciar la sesión e igualmente salir y luego cerrar la conexión remota.

6.1.4 INSTALACIÓN

WinVNC es fácil de instalar y usar:

Ejecutando el programa de Instalación. (si obtienes el VNC como un archivo ZIP o TAR será necesario desempaquetarlo inicialmente)

Usando WinVNC

Cuando el WinVNC server ha sido iniciado, este adicionara un pequeño icono en la barra de tareas. Un clic derecho sobre este icono desplegara un menú con las siguientes opciones:

- Properties - esta opción despliega las propiedades del usuario, permitiendo asi que este modifique sus parámetros
- Add New Client - esta opción te permite especificar el Nombre o la Direccion IP de un host que tu deseas que tome control remoto del equipo en el que te encuentras en este momento; para que el equipo especificado pueda tomar control remoto, deberá estar ejecutando el Viewer en "Listening Mode".
- Kill All Clients - esta opción desconectara a todos los clientes actualmente conectados al server.
- About WinVNC - esta opción nos proporciona información acerca del producto.
- Close - baja el servidor.

VNC es software libre, con licencia GPL y disponible para la mayoría de las plataformas. La distribución original de VNC se puede conseguir en la página de AT&T.

6.1.5 ¿QUÉ ES TIGHTVNC?

TightVNC es una versión mejorada de VNC, optimizada para conexiones lentas ya que comprime el tráfico usando un algoritmo de compresión propio. En redes donde VNC es lento porque la conexión no es lo suficientemente rápida, TightVNC puede funcionar prácticamente en tiempo real.

Además de estas optimizaciones de compresión, TightVNC también incluye otras muchas mejoras y optimizaciones, y es compatible con el VNC estándar.

Características

Movimiento local del cursor	Los movimientos del cursor no generan una actualización de la pantalla, sino que éste es procesado localmente por el visor.
Algoritmos eficientes de compresión	El algoritmo de compresión Tight está optimizado para conexiones lentas, y genera mucho menos tráfico que la compresión tradicional de VNC.
Nivel de compresión configurable	Puedes elegir el ratio de compresión, dependiendo de las velocidades de tu procesador y de tu conexión.
Compresión JPEG opcional	Si no te importa demasiado la calidad de imagen, puedes activar este tipo de compresión que comprime las partes de muchos colores más eficientemente.
Acceso desde navegador	TightVNC incluye un visor Java.
Funcionamiento desde Unix y desde Windows	Todas estas características están disponibles tanto para la versión Unix como para la versión Windows.
Opciones avanzadas desde WinVNC	TightVNC te da la posibilidad de configurar muchas opciones avanzadas directamente desde el GUI WinVNC, y aplicar los cambios inmediatamente. No hace falta ejecutar regedit para configurar algunas opciones como en el VNC estándar.
Túnel SSH automático en Unix	La versión Unix del visor TightVNC puede hacer un túnel ssh automáticamente usando cliente SSH o OpenSSH.
Y mucho más	Un gran número de mejoras, optimizaciones para mejorar el rendimiento y corrección de errores, para ver todo esto lee el fichero WhatsNew.

6.1.6 ¿QUÉ HACE VNC DIFERENTE DE LOS OTROS SISTEMAS?

VNC es diferente de otros sistemas de visualización remotos en tres maneras cruciales:

Es completamente de plataforma múltiple. Un desktop que funciona en una computadora de Linux puede ser exhibido sobre un PC de Windows, sobre una computadora de Solaris, o sobre cualquiera de las otras arquitecturas. La sencillez del protocolo lo hace fácil al puerto para nuevas plataformas.
Es pequeño y simple. El telespectador de Windows, por ejemplo, está sobre 150 kb. en tamaño y puede ser operado directamente de un disquete. El telespectador de Java entero es considerablemente menor que 100 kb.

¡Es libre! Usted puede descargarlo, usarlo, y redistribuirlo.

6.2 MMC (MICROSOFT MANAGEMENT CONSOLE)

Implante sus directivas de seguridad mediante plantillas de seguridad personalizadas

Uno de los mayores retos a los que tienen que hacer frente los administradores de sistemas es el de asegurarse de que en todos los equipos de la red se aplique una misma política de seguridad. Microsoft ha desarrollado numerosas herramientas y plantillas de seguridad cuyo fin no es otro que el de facilitarles a los administradores dicha tarea.

Puede utilizar Microsoft Management Console (MMC) para crear, guardar y abrir herramientas administrativas (denominadas consolas MMC) que administran los componentes de hardware, software y de red del sistema Windows. MMC es una característica del sistema operativo Windows 2000, pero también puede ejecutar MMC en los sistemas operativos Windows NT, Windows 95 y Windows 98. Además, MMC es una característica de varias aplicaciones de software diseñadas para Windows.

MMC no realiza funciones administrativas, pero incorpora herramientas que sí lo hacen. El principal tipo de herramienta que puede agregar a una consola se denomina complemento. También puede agregar controles ActiveX, vínculos a páginas Web, carpetas, vistas de cuadro de tareas y tareas.

Existen dos formas generales de utilizar MMC: en el *modo de usuario*, que le permite trabajar con consolas MMC existentes para administrar un sistema, o bien, en el *modo de autor*, que le permite crear consolas nuevas o modificar las consolas MMC ya existentes.

Con el paso del tiempo, dichas herramientas y plantillas han ido evolucionando hasta alcanzar el alto grado de madurez y funcionalidad que presentan las que incluye Windows 2000, en adelante. Pero, sorprendentemente, son muchos los administradores que aún no tienen noticia de la existencia de dichas herramientas y plantillas, y todavía son más los que, teniendo noticia de ellas, no son plenamente conscientes de su potencial.

6.2.1 PLANTILLAS DE SEGURIDAD

Una plantilla de seguridad es un archivo de texto que contiene parámetros de seguridad tales como las directivas de cuentas y las directivas locales, el registro de sucesos, los grupos restringidos, los servicios del sistema, la configuración del registro y los permisos del sistema de archivos.

Por defecto, Windows guarda estos archivos con la extensión .inf.

Microsoft ha puesto a disposición de los administradores tres plantillas de seguridad básicas: una para estaciones de trabajo, otra para servidores y otra para controladores de dominio. Dichas plantillas contienen las configuraciones de seguridad predeterminadas que se utilizan cuando se instala el sistema operativo de cero y se aceptan todas las opciones predeterminadas que ofrece el programa de instalación.

Las plantillas de seguridad básicas establecen los permisos del sistema de archivos y del registro que se van a utilizar de forma predeterminada en el sistema. Para que el sistema pueda beneficiarse del nivel de seguridad que les ofrecen las plantillas de seguridad básicas, las particiones deberán ser NTFS en lugar de FAT. Si considera que el nivel de seguridad que le ofrecen las plantillas de seguridad básicas no es suficiente para su entorno, utilice las plantillas seguras (cuyos nombres incluyen la palabra «secure») o las plantillas de alta seguridad (cuyos nombres incluyen la palabra «hisec») que Microsoft ha desarrollado para estaciones de trabajo y controladores de dominio.

Las configuraciones de seguridad que le ofrecen las plantillas seguras son incrementalmente más estrictas que las que le ofrecen las plantillas básicas, y definen aspectos tales como las directivas de contraseñas, los sucesos auditables y las opciones de seguridad. Por su parte, las configuraciones de seguridad que le ofrecen las plantillas de alta seguridad son incrementalmente más estrictas que las que le ofrecen las plantillas seguras, de modo que la lista de sucesos auditables es mayor, y las opciones de seguridad existentes son aún más estrictas.

El orden por el que se deben utilizar las plantillas de seguridad a la hora de auditar o configurar la seguridad de un sistema es el siguiente: primero las plantillas básicas, a continuación las plantillas seguras y, por último, las plantillas de alta seguridad.

Es recomendable, antes de instalar cualquier plantilla de seguridad, las adapte a las necesidades de su entorno y que no las aplique sin saber lo que contienen ni cómo pueden afectar a sus sistemas y a su red.

Las plantillas de seguridad son una potente herramienta de configuración y análisis de las directivas de seguridad de la empresa

El complemento «Plantillas de seguridad»

No modifique en ningún caso las plantillas que incluye el sistema operativo de fábrica; limítese a utilizarlas como base para crear sus propias plantillas personalizadas. Para crear una plantilla personalizada a partir de una plantilla ya existente, guarde ésta última con otro nombre. Con el fin de que, después, pueda identificarla sin problemas, le recomendamos que incluya en el nombre información sobre el entorno.

TABLA. Plantillas de seguridad más importantes

Nombre	Origen	Descripción
Basicdc.inf	Windows 2000	Configuración básica de seguridad para controladores de dominio.
Basicsv.inf	Windows 2000	Configuración básica de seguridad para servidores de archivos e impresión.
Basicwk.inf	Windows 2000	Configuración básica de seguridad para estaciones de trabajo (W2000 Prof.).
Securedc.inf	Windows 2000	Configuración segura para contro ladores de dominio.
Securews.inf	Windows 2000	Configuración segura para estaciones de trabajo.
Hisecdc.inf	Windows 2000	Configuración de alta seguridad para controladores de dominio.
Hisecwk.inf	Windows 2000	Configuración de alta seguridad para estaciones de trabajo.
Compatws.inf	Windows 2000	Configuración de Basicwk.inf para aplicaciones heredadas.
Notssid.inf	W2000 Server	Plantilla que permite eliminar los privile- gios adicionales que se otorgan a los usuarios de los «Servicios de Terminal Server» de Windows 2000 Server.
Hisecweb.inf	Microsoft W2000 Server	Configuración de alta seguridad para sedes web.
Secureinternetwebserver.inf	Microsoft W2000 Server	Configuración segura para el uso de servidores web en Internet.
Secureintranetwebserver.inf	Microsoft W2000 Server	Configuración segura para el uso de servidores web en Intrarnets.

El complemento «Configuración y análisis de seguridad»

El complemento «Security Configuration and Analysis» (Configuración y análisis de seguridad) le permite auditar y configurar la seguridad del sistema.

Es preciso agregarlo a la consola MMC para poder usarlo, ya que no se encuentra disponible en dicha consola por defecto.

El elemento más importante del complemento «Configuración y análisis de seguridad» es un motor de bases de datos que crea y utiliza una base de datos con la extensión .sdb. Cuando se analiza la seguridad de un sistema, dicho complemento guarda en la base de datos la configuración de seguridad que tenga el sistema en ese momento.

De ese modo, cuando se configure la seguridad del sistema, el motor de la base de datos comparará la configuración de seguridad del sistema almacenada en la base de datos con la de las distintas plantillas y decidirá cuál es la plantilla que se debe aplicar al sistema.

CONCLUSIONES Y RECOMENDACIONES.

Después de haber desarrollado este documento, he podido llegar a la conclusión, de lo necesario que es en la actualidad, la implementación de mecanismos de seguridad debido al gran numero de ataques a los que están expuestos todos los sistemas informáticos sin excepción.

En estos mecanismos de seguridad computacional, se deben considerar las políticas particulares que sean convenientes para cada organización. Estas políticas deben proteger al sistema del robo, divulgación y modificación no autorizada de información; para que dichas políticas cumplan con los objetivos de una organización, deben ser establecidas de manera precisa para evitar confusiones.

Sin embargo como ya he hecho hincapié, resulta muy difícil hablar de seguridad, ya que la seguridad absoluta no existe. Para poder establecer que un sistema informático es seguro seria necesario identificar todas las amenazas a las que puede verse sometido y tomar todas las medidas preventivas y de seguridad correspondientes.

En este instante puedo definir la seguridad de un sistema informático como "el estado de protección del mismo, establecido con el fin de evitar la aparición de las distintas amenazas posibles que puedan alterar su normal funcionamiento, o de aminorar las consecuencias negativas de los distintos riesgos, una vez producidos".
No podemos dejar de tomar en cuenta que la seguridad informática no solo se implanta dentro de los sistemas mediante la modificación de la configuración de los equipos y la instalación de programas internos (seguridad interna), sino que hay que considerar otros problemas que son ajenos al medio informático, y por tanto se abordan con otras técnicas (seguridad externa).

Actualmente la sociedad no esta consciente de lo importante de establecer medidas que garanticen la seguridad de los Sistemas informáticos tanto como en el sector privado como en el público, lo que puede traer como consecuencia grandes pérdidas tanto de información como de recursos indispensables para su correcto funcionamiento, esto exige una concientización, por parte de todos, la información es conocimiento y como tal debemos atribuirle la importancia que merece. Esta importancia incluye por supuesto, estudiar.

Es imprescindible establecer una correspondencia y pertenencia entre las técnicas adoptadas conformando un sistema de seguridad; y no procedimientos aislados que contribuyan al caos general existente. Esto puede lograrse al integrar la seguridad desde el comienzo, desde el diseño, desde el desarrollo.
La tarea de implementar este tema, es vital para el éxito de todos los entes, y es problema de todos, por eso cada uno de nosotros debemos de cooperar con nuestro granito de arena para lograr llegar a un mundo mas seguro, confiable, honesto y por supuesto productivo, en todos los aspectos de nuestras vidas.
Todos por un futuro mejor...

BIBLIOGRAFIA.

http://www.sapmania.com

http://www.delitosinformaticos.com

http://www.symantec.com

http://www.ausejo.net

http://www.kriptopolis.com

http://www.google.com.mx

http://www.geocities.com

http://www.monografias.com

CRIPTOGRAFIA Y SEGURIDAD EN COMPUTADORAS.
Lucena López, Manuel José.
3ª. Edición Virtual.
España, 2001.

AUDITORIA EN INFORMÁTICA.
Echenique, José Antonio.
Editorial Mc Graw Hill.

MANUAL DE SEGURIDAD INFORMATICA.
Soler de Arespacochaga, José Antonio.
España, 1998.

SEGURIDAD EN LOS SISTEMAS INFORMATICOS.
Royal P. Fisher.
Editorial Díaz de Santos
Octubre 1991.

DERECHO INFORMATICO.
Télles Valdez, Julio.
2ª. Edición.
Editorial Mc Graw Hill.
México, 1996.