UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO Y DESARROLLO DE UNA METODOLOGÍA PARA LA DETERMINACIÓN Y EL ESTABLECIMIENTO DE NORMAS DE SEGURIDAD INFORMÁTICA

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A

JOSÉ URIEL RENDÓN CATAÑO

DIRECTORA DE TESIS
M. C. MA. JAQUELINA LÓPEZ BARRIENTOS

MÉXICO, D. F., CIUDAD UNIVERSITARIA, 2004

A DIOS:

Por todo.

A MIS ABUELOS:

Por ser el principio de mi historia, por ser el origen de todo, por su esfuerzo, por su sabiduría, por su afecto, a los que quiero y me siento orgullos de ellos.

A MIS PADRES:

Por darme la vida y enseñarme a vivirla, por su amor incondicional, por transmitirme sus experiencias a través de su cariño y cuidados, por permitirme vivir mi vida y dejarme ser yo mismo, por ayudarme a conseguir esta y otras metas, pero sobre todo por ayudarme a convertirme en lo que soy, esperando ser digno de merecer su esfuerzo y sacrificio, por ser mi luz en tiempos de oscuridad. A los que amo. Gracias.

A MI HERMANO OMAR:

Por ser un ejemplo a seguir, porque sé que siempre estarás ahí cuando te necesite, con quien nunca me sentiré solo ni asustado, con quien venceré las adversidades y en quien podré confiar hoy y siempre.

A VANESSA:

A la que el destino me unió y separó, a la que nunca olvidaré, a la que me enseño que la vida tiene sentido cuando conoces y vives el amor. Porque tú eres parte de mí y mis logros son tus logros
.(1 Corintios 13:4,5,6,7,8.)
Tu sabes, yo también. Que dios te bendiga.

A MIS AMIGOS:

A todos aquellos que han sido, son y serán parte de mi vida, que han reído y llorado conmigo. Nombrarlos sería injusto, olvidarlos imperdonable, pero cada uno sabe lo que para mí significa llamarlos amigo.

A LA M.C. MA. JACQUELINA LÓPEZ BARRIENTOS:

Por su guía, apoyo e impulso en la realización de este proyecto tan importante. Gracias.

INTRODUCCIÓN

La seguridad es uno de los aspectos más conflictivos del uso de las tecnologías de la información. Es suficiente comprobar como la falta de una política de seguridad global está frenando el desarrollo de Internet en áreas tan interesantes y prometedoras como el comercio electrónico o la interacción con las administraciones públicas.

Los recientes avances en las telecomunicaciones y en la computación en red han proporcionado la aparición de canales rápidos para la propagación de datos a través de sistemas digitales. Las redes abiertas están siendo utilizadas cada vez más como una plataforma para la comunicación en nuestra sociedad pues permiten rápidos y eficientes intercambios de información con un bajo coste económico asociado y con una fácil accesibilidad.

El desarrollo actual y las perspectivas de futuro de las "superautopistas de datos" y de una infraestructura global de información, es decir, de Internet y de la World Wide Web (WWW), crean toda una variedad de nuevas posibilidades. Sin embargo, la realización efectiva de tales posibilidades está influida por las inseguridades típicas de las redes abiertas: los mensajes pueden ser interceptados y manipulados, la validez de los documentos se puede negar, o los datos personales pueden ser recolectados de forma ilícita.

Como resultados, el atractivo y ventajas ofrecidas por la comunicación electrónica, tanto en el desarrollo de oportunidades comerciales entre organizaciones privadas como en las interrelaciones entre las organizaciones públicas y los ciudadanos, no pueden ser explotados en su totalidad.

Tanto los emisores como los receptores de información precisan de medios técnicos que aseguren la validación y autenticación de la información digital transmitida. De esa forma, tanto el comercio electrónico como otras muchas aplicaciones de la sociedad de la información podrán expandirse y darán lugar a beneficios económicos y sociales con un bajo coste.

Millones de empresas, entidades y particulares confían sus datos empresariales y personales más críticos a las computadoras, y no toman ninguna medida para protegerlos más allá de sencillas copias de seguridad... con frecuencia extremadamente inseguras.

Parecen no darse cuenta de que, con mucha frecuencia, una copia de seguridad "perdida" de uno de nuestras computadoras puede proporcionar a potenciales adversarios una auténtica "fotocopia" de quiénes somos.

En cualquier empresa típica de la actualidad, al menos la contabilidad y la facturación se llevan mediante el uso de computadoras. Una sencilla copia de dos o tres carpetas, que normalmente cabrá en un par de disquetes, contendrá ni más ni menos que nuestro estado contable y financiero, la lista completa de nuestros clientes, sus compras y precios y posiblemente la lista completa de nuestros proveedores. Otro disquete puede utilizarse para copiar el archivo de nóminas. ¿Se imagina lo que puede hacer un competidor con toda esa información? Mucha gente anda muy preocupada con los virus, que son programas cuya

acción es muy fácil de prevenir, pero nadie parece preocuparse de que un adversario humano husmee en sus datos más confidenciales.

La **Información** es el bien más preciado de nuestro tiempo. Toda información. La suya, también. Quien tiene la información tiene el poder, a menos que sea perfectamente incapaz. Quien posee su información, tiene poder sobre usted. Y las computadoras, que se definen como "máquinas para el tratamiento automático de la información", contienen la mayor parte de los datos de utilidad de nuestro mundo.

En esta época no es un secreto la importancia de implementar un programa completo para la seguridad de la información en la empresa. Sin embargo, crear un programa de seguridad con base en los componentes de "bloqueadores de cookies" rara vez produce resultados efectivos.

Lo más efectivo es utilizar una metodología comprobada que diseñe un programa de seguridad con base en las necesidades de la empresa.

El presente trabajo presenta una forma de diseñar y desarrollar una metodología que permita establecer las normas de seguridad de la información; determinando y estableciendo las políticas de seguridad de la información que rijan, regulen y hagan valer los compromisos y responsabilidades de todas las personas, desde niveles directivos hasta el de empleados, que trabajen en una organización, sin importar la actividad que ésta desempeñe. Para esto, el trabajo realizado cubre los siguientes puntos:

- Definir los aspectos importantes que se deben considerar en materia de seguridad, de acuerdo a los fundamentos de la seguridad en la información, identificando las amenazas y vulnerabilidades que se presentan en una organización en los sistemas informáticos y recursos humanos.

- Definir una estrategia de análisis que permita identificar los principales riesgos o faltas en materia de seguridad en la información, la cual sea flexible en su aplicación a cualquier organización sin importar su actividad.

- Definir las políticas de seguridad en información que serán aplicadas a la organización y que establecerán los compromisos y obligaciones que tendrá cada uno de los integrantes de la misma, según sea su nivel laboral establecido por su organigrama.

- Definir los puntos que deben cubrir los planes de acción que permitan la aplicación de las políticas de seguridad de la información para las organizaciones.

- Determinar con base a las políticas desarrolladas los mecanismos y las herramientas tecnológicas que permitirán poner en marcha la protección y brindar la seguridad requerida a la información de la organización.

A continuación se muestra un panorama general del trabajo, dividido en cinco capítulos, cada uno ligado entre sí, pues como se observará, el tema de la seguridad en la información no puede ser solucionado a través de un solo procedimiento o respuesta única.

La **Información**, en nuestra actualidad es un recurso valioso para todas las personas, organizaciones y empresas sin importar su actividad, nos proporciona los conocimientos necesarios para tomar una decisión o seguir una serie de pasos con el fin de obtener un beneficio o cubrir una necesidad, a la vez de proporcionarnos una retribución por la oportuna acción que hayamos tomado.

Hoy en día utilizamos redes de computadoras en prácticamente todas las actividades laborales, empresariales y educativas de nuestra vida. Realizamos compras, inversiones bancarias, transacciones de dinero, transmisiones de datos importantes para nuestro negocio, contactamos personas que se encuentran en otros países con el fin de expandir el rango de acción de nuestra empresa y así poder conseguir mejores ingresos y establecer nuevos negocios, además de incrementar nuestro acervo de información.

Es aquí donde el concepto de seguridad en la información se convierte en una prioridad, teniendo como objetivo el proveer una adecuada protección a la información durante su generación, procesamiento, almacenamiento y transferencia, así como brindar una protección contra posibles alteraciones en el contenido de la información y contra el acceso a la misma por personas no autorizadas que provocarían un daño importante a nuestros intereses.

Por esto es necesario recordar cuales son los factores de que trata la seguridad en la información, es decir, entender cuales son las posibles amenazas que ocasionan los ataques, quienes son capaces de realizarlos y definiendo las causas que los provocan. El ***capítulo 1*** describe cada uno de estos puntos, proporcionando definiciones que permitan a cualquier persona, iniciada en el tema de seguridad en la información o no, comprenda de que trata la seguridad en la información, que aspectos comprenden y quienes o cuales son sus actores.

Una vez establecido de qué trata la seguridad en la información, el ***capítulo 2*** nos proporciona los pasos a seguir para la realización de un análisis en materia de seguridad en la información qué tiene por objeto el recabar la información de qué tipo de organización se trata y cómo está constituida, qué clase y que importancia tiene la información, los riesgos a la seguridad, la identificación de las medidas de seguridad y los niveles de acceso a la ***información***. Proporciona además una descripción de los diferentes ataques y amenazas, naturales o de interacción humana, físicas como lógicas, que afectan a nuestros sistemas de información.

¿Cómo puede ser posible que una inversión de miles de dólares no garantice un nivel de seguridad adecuado? La respuesta es: a pesar de tener el equipo más sofisticado, los programas de cómputo más avanzados, las mejores instalaciones y servicios de comunicación, el aspecto que más se descuida es el humano, el cual involucra la ética laboral de las personas y su forma de desenvolverse en su puesto.

Está comprobado que más del 50 % de los ataques en materia de seguridad de la información se producen desde el interior de la propia organización. ¿A qué se debe esto?

Ninguna persona está exenta de fallas, de verse envuelto en una filtración de información con el fin de obtener algún beneficio, o de tener un descuido que ocasiona que una persona reciba un correo electrónico que no debía recibir, o de que un extraño mande un archivo desde la terminal del empleado que no asistió a trabajar, o que tuvo acceso a niveles de información que no le correspondían según su jerarquía dentro de la empresa.

Esto es una falta de seguridad que debería ser penalizada, pero para que esto sea una realidad, es necesario establecer un compromiso con cada uno de los integrantes de nuestra empresa o grupo de trabajo en donde es imprescindible primero se establezcan las normas o políticas que regularán toda actividad de carácter físico, lógico y moral dentro de su ambiente laboral.

Teniendo conocimiento de los resultados del análisis propuesto, en el ***capítulo 3*** se establecerán las políticas de seguridad en la información, proporcionando su definición, sus fundamentos y su alcance, así como un análisis y gestión de riesgos que implican la acción de definir las políticas de seguridad en la información, tanto en el aspecto monetario como en el laboral, estableciendo su estructura jerárquica ligada a la estructura jerárquica de la empresa y los niveles a los cuales se aplicaran junto con los procedimientos definidos para cada tipo de política de seguridad, así como su diseño identificando sus recursos y proporcionando una metodología para su desarrollo.

Estas políticas de seguridad de la información no son las mismas para todas las organizaciones pues sus actividades pueden variar de una a otra organización así como sus intereses y sus necesidades respecto a seguridad informática se refiere. Por consiguiente, al igual que las políticas empresariales que conforman a cada organización y que rigen su conducta laboral y que son únicas para dicha empresa, éstas deberán ser elaboradas de acuerdo al tipo de actividades que se realicen en la organización y la constitución jerárquica de sus miembros, además de ser flexibles con el tiempo y estar en constante evolución para ser actuales a la realidad de carácter empresarial.

Existe una problemática para la seguridad, a lo largo de los últimos años los problemas de seguridad que se vienen observando en las empresas y organismos han sido una constante recurrente. La situación real suele ser que en las empresas y organismos el negocio y la imagen se anteponen a la seguridad. La organización crece e implementa soluciones de seguridad de acuerdo a necesidades puntuales, no hay definida una estrategia, ni normas ni procedimientos, es decir, lo habitual es que no se contemple expresamente la seguridad.

Por esto realizar un plan de implementación que introduzca esta idea a la organización, detallado en el ***capítulo 4,*** que genere una conciencia de las consecuencias de su falta y que sea respetada por todos los miembros, desde niveles directivos hasta los empleados comunes, incluyendo a personas ajenas que realicen una interacción laboral o personal con los miembros de la organización, tomando la estrategia de seguridad que mas se adecue a los objetivos que se deseen alcanzar, siguiendo los lineamientos establecidos por las políticas de seguridad previamente definidas.

Por último el ***capítulo 5*** enumera algunas de las técnicas a utilizar para establecer la seguridad en la información, seguridad que no depende de una sola de estas herramientas, sino de la aplicación correcta de varias de estas. El conocer o mostrar algunas aplicaciones existentes de seguridad, tanto de hardware como de software, que proporcionarían los niveles adecuados de seguridad requeridos por la organización, basándonos en los resultados del análisis y apoyados en las políticas de seguridad definidas por cada organización para cumplir óptimamente con el compromiso de la seguridad en la información, nos proporcionara una ayuda para establecer un nivel de seguridad adecuado a nuestras necesidades, evitando gastos innecesarios y pérdidas de tiempo.

ÍNDICE

CAPÍTULO I

ANTECEDENTES Y PRINCIPIOS DE SEGURIDAD

1.1 La Seguridad en la Información.

El concepto de Seguridad en su definición se maneja con cierto grado de incertidumbre teniendo distinto significado para distintas persona. Esto tiene la peligrosa consecuencia de que la función de seguridad puede ser etiquetada como inadecuada o negligente.

"La Seguridad es hoy en día una profesión compleja de funciones especializadas"[1]. Como se sabe, los problemas nunca se resuelven y la "solución" estará dada por su transformación en problemas diferentes, más pequeños y aceptables.

En los problemas aparecen tres figuras:

1. El poseedor del valor: **Protector**
2. Un aspirante a poseedor: **Competidor-Agresor**
3. Un elemento a proteger: **Valor**

Para estos elementos, la **Seguridad** se definirá como:

"La interrelación dinámica (competencia) entre el agresor y el protector para obtener (o conservar) el valor tratado, enmarcada por la situación global."

Aclaraciones:

1 El protector no siempre es el poseedor de valor.
2 El agresor no siempre es el aspirante a poseedor.
3 Ambas figuras pueden ser delegadas a terceros por el cambio de otro valor, generalmente dinero.
4 El valor puede no ser algo concreto. Por ejemplo se podría querer cuidar el honor, la intimidad, el conocimiento, etc.
5 La situación global que no será lo mismo en México que en algún otro país, en donde sus habitantes no cuentan con las posibilidades socio-económicas para subsistir o la falta de preparación educativa para tener una mejor forma de vida.

Los competidores se pueden subdividir en:

- **Competidor Interno:** es aquel que piensa que el interés de la organización está por encima de sus intereses y, por lo tanto, actúa para sobreponer su interés personal, provocando daños a la organización.

- **Competidor Externo:** es aquel que actúa para arrebatar al poseedor lo que para él significa un valor empresarial o personal (cliente, mercado, información, etc.).

---

[1] "Seguridad: una Introduccion", Dr MANUNTA, Giovanni. Revista de Seguridad Corporativa. *http://www.seguridadcorporativa.org*

"La seguridad es un problema de antagonismo y competencia. Si no existe un competidor-amenaza el problema no es de seguridad".

Actualmente la seguridad se ha convertido en un elemento necesario e indispensable ya que La última de las tres grandes revoluciones de la humanidad, la revolución de la era de la información, ("Tercera Ola"); que sigue a las anteriores revoluciones agrícola e industrial, ha generado grandes evoluciones y cambios, pero nos ha generado un nuevo problema, el de la Seguridad de la Información.

Hoy en día las personas y empresas generan y poseen un volumen de datos que es procesado, almacenado y transmitido. La importancia de esta información para el desarrollo económico y social, no tiene ninguna comparación con la que tuvo en el pasado. De hecho, en la actualidad, las organizaciones consideran que la información es un bien más de su activo y, en muchos casos, prioritaria sobre los restantes.

Gran parte de esos datos que nosotros, o las entidades de nuestra sociedad, manejamos, han sido tratados, sea durante su proceso, o almacenamiento, o transmisión, mediante las llamadas tecnologías de la información, entre las que ocupa un lugar focal la informática. Consiguientemente, la seguridad de las tecnologías de información, y por ende la informática, se convierte en un tema de crucial importancia para el continuo y espectacular progreso de nuestra sociedad, e incluso para su propia supervivencia.

El surgimiento en los últimos años de las redes informáticas y fundamentalmente de Internet, ha sido el factor fundamental que ha hecho que la Seguridad en la Información cobrase una importancia vital en el uso de sistemas informáticos conectados. Desde el momento en que nuestra computadora se conecta a una red de área local o extensa (LAN o WAN) y a Internet, se abren ante nosotros toda una nueva serie de posibilidades, como son la transferencia de datos en cuestión de minutos y el aumento de la productividad de nuestro trabajo, sin embargo éstas traen consigo toda una serie de nuevos y en ocasiones complejos tipos de ataque. Más aun, mientras en una computadora aislada el posible origen de los ataques es bastante restringido, al conectarnos a una red LAN o WAN y a Internet, cualquier usuario de cualquier parte del mundo puede considerar nuestro sistema un objetivo apetecible.

La solución a este problema se dará al satisfacer las necesidades de comprensión de los conceptos de "Seguridad" y "Sistema Informático" en torno a alguien (organismo, instituto, empresa, institución, organización o particular) que gestiona información. Por lo que es necesario aplicar los principios de Seguridad en un contexto informático, siendo necesario el trabajo conjunto de expertos en seguridad y expertos en informática para que exista la Seguridad en la Información.

Un *Sistema Informático* se define como el "conjunto formado por personas, computadoras (hardware y software), papeles, medios de almacenamiento digitales, el entorno donde actúan y sus interacciones"[2], que procesa la Información.

[2] ALDEGANI, Gustavo, Miguel. Seguridad Informatica, MP Ediciones, Argentina, 1997,Página 22.

El término de Seguridad en la Información se refiere a la prevención y a la protección que se le brinda a la información, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional, la trasferencia, modificación, fusión o destrucción no autorizada de la información.

La **Información** es un conjunto de datos que tienen un signado específico más allá de cada uno de éstos y tendrá un sentido particular según cómo y quién lo procese, al respecto **Dato** es la unidad mínima con la que se compone cierta información.

Así **"El objetivo de la Seguridad en la Información será entonces mantener la Integridad, Disponibilidad, Confidencialidad, Control de Acceso, Autenticación y No Repudio de la información manejada por computadora."**

El valor de la información es totalmente relativo, pues constituye un recurso que, en la mayoría de los casos no se valora adecuadamente debido a su intangibilidad, lo que no ocurre con los equipos y la documentación.

Existe información que **debe o puede ser pública**, que puede ser visualizada por cualquier persona y aquella que **debe ser privada**, que solo puede ser visualizada por un grupo selecto de personas que trabajan con ella o que para realizar su trabajo requieren de ella. En este carácter privado se deben maximizar los esfuerzos para preservarla de ese modo, reconociendo las siguientes características en la Información:

1 Es Crítica: es indispensable para garantizar la continuidad operativa de la organización.
2 Es Valiosa: es valorada por el dueño de ésta ya que de ella depende el funcionamiento de la organización.
3 Es Sensitiva: debe ser conocida única y exclusivamente por las personas que la requieren para realizar exitosamente su trabajo dentro de la organización.

1.2. Servicios de Seguridad

Teniendo conocimiento de las características que permiten identificar la información que debe ser protegida, a continuación se debe determinar cuál o cuáles servicios de seguridad son los que ésta requiere para su protección:

La **Integridad** de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificaciones hechas por personas que se infiltran en el sistema.

La **Disponibilidad** de la Información es su capacidad de estar siempre disponible para ser accedida por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La **Confidencialidad** de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En caso de falta de confidencialidad, la Información puede provocar severos daños a su dueño o hasta volverse obsoleta.

El **Control de Acceso** a la Información permite asegurar que solo los usuarios autorizados pueden acceder a ella y el custodio de ésta decidir cuándo y cómo permitir el acceso a la misma.

La **Autenticación** es verificar la identidad de algo o de alguien (persona, sistema, proceso o dispositivo) de manera que permite definir si la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando al emisor de la misma, al receptor de ésta o bien a los dos si fuera necesario con el fin de evitar suplantación de identidades.

Otros aspectos adicionales a considerar pero que incorporan algunos aspectos particulares:

- **Protección a la Réplica:** mediante la cual se asegura que la transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- **No Repudio:** mediante el cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o no la recibió.
- **Consistencia:** se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- **Aislamiento:** permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo, íntimamente ligado a la **Confidencialidad**.
- **Auditoría:** es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuándo las realiza.

Una **Amenaza** algo o alguien que pretende hacer daño y se representa a través de una persona, una circunstancia o evento, un fenómeno natural o una idea maliciosa, las cuales pueden llegar a provocar daño cuando existe una violación de la seguridad. En el entorno informático, se define como cualquier elemento que comprometa al sistema. (**Figura 1.1**)

Figura 1.1 Tipos de Amenazas para la Seguridad en la Información

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de un sistema informático.

a. **La Prevención (antes):** mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
b. **La Detección (durante):** mecanismos orientados a revelar violaciones a la seguridad. Programas de auditoría.
c. **La Recuperación (después):** mecanismos que aplican cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo la recuperación desde las copias de seguridad (backup) realizadas.

Normalmente, las preguntas que se hacen ante un problema de seguridad están relacionadas con medidas defensivas que únicamente retrasan y no solucionan el problema dado. La amenaza o riesgo sigue allí, por lo que las preguntas correctas serían:

- ¿Cuánto tardará la amenaza en superar la "solución" planteada?
- ¿Cómo se hace para detectarla e identificarla a tiempo?
- ¿Cómo se hace para neutralizarla?

En busca de una respuesta, definiremos a **Riesgo** como "la proximidad o posibilidad 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:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

El **Daño** es el resultado de la amenaza; también es el resultado de la no-acción, o acción defectuosa, del protector. Puede producirse porque el protector no supo identificar adecuadamente la amenaza, si lo hizo, se impusieron ciertos intereses personales u organizacionales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza y para la figura del protector.

El protector será el encargado de detectar cada una de las **Vulnerabilidades** (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo. También será el encargado de aplicar las **Contramedidas** (técnicas de protección) adecuadas.

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, por lo que 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 Sistema Fiable en vez de seguro.

Para que un sistema se fiable debe garantizar las características de Integridad, Operatividad, Privacidad, Control y Autenticidad. Es necesario conocer "que es lo que queremos proteger", "de quien lo queremos proteger","como se puede lograr"; para concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución o anulación de los riesgos.

Las amenazas de la seguridad provienen de diversas fuentes, entre ellas se encuentran:

1. **De humanos:** la amenaza surge por ignorancia en el manejo de la información, por descuido, por negligencia, por inconformidad.
2. **Errores de Hardware:** se da la amenaza por fallas físicas que presente cualquier elemento de los dispositivos que conforman a la computadora. Los más comunes son fallos en el suministro de energía, ruido electromagnético, distorsión, alto voltaje, etc.
3. **Error de la Red:** se presenta una amenaza cuando no se calcula bien el flujo de la información que se va a circular por el canal de comunicación, es decir, un atacante podría saturar el canal de comunicación provocando la no disponibilidad de la red o la desconexión del mismo.
4. **Problemas de tipo lógico:** la amenaza se hace presente cuando un diseño bien elaborado de un mecanismo de seguridad, se implementa mal o no cumple con las especificaciones del diseño.
5. **Desastres:** la amenaza de este tipo surge de las fuerzas de la naturaleza tales como las inundaciones, los terremotos, el fuego, el viento. Dichos desastres hacen surgir amenazas directas, pues repercuten indiscutiblemente en el funcionamiento físico de las computadoras, redes, instalaciones, líneas de comunicación, etc.

1.3. Clasificación de Amenazas y Ataques

Para cualquier de los elementos descritos existen multitud de amenazas y ataques que se los pueden clasificar en:

1. **Ataques Pasivos**: el atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que esta siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico. Generalmente se emplean para:

    - Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados.
    - Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
    - Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los periodos de actividad.

2. **Ataques Activos**: estos ataques implican algún tipo de modificación del flujo de datos trasmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:

    - **Interrupción**: si hacen que un objeto del sistema se pierda, quede inutilizable o no disponible.
    - **Intercepción**: si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
    - **Modificación**: si además de conseguir el acceso consigue modificar el objeto.
    - **Fabricación**: se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.
    - **Destrucción**: es una modificación que inutiliza el objeto.

Se llama **Intruso** o Atacante a la persona que accede (o intente acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

En la actualidad, los Intrusos se caracterizan desde el punto de vista del nivel de conocimientos:

1. **Clase A**: el 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban.
2. **Clase B**: es el 12% son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistemas operativos usa la victima, testean las vulnerabilidades del mismo e ingresan por ellas.
3. **Clase C**: es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

4. **Clase D**: es el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

Para llegar desde la base hasta el ultimo nivel se tarda desde 4 a 6 años, por nivel de conocimiento que se requiere asimilar. Es practica, conocer, programar, mucha tarea y mucho trabajo.

Seleccionar las medidas de seguridad a implantar requiere considerar el equilibrio entre los intereses referidos a la seguridad, los requerimientos operacionales y la "amigabilidad" para el usuario.

La solución no es el colocar una computadora a 20 metros bajo tierra en un recinto de hormigón, aislada informáticamente de otras computadoras y alimentada por un sistema autónomo de triple reemplazo. Su utilidad tiende a nula.

La Seguridad y la Utilidad de una computadora son inversamente proporcionales; es decir que incrementar la seguridad en un sistema informático, su operatividad desciende y viceversa.

$$\textbf{Operatividad} = \frac{1}{\textit{Seguridad}}$$

Esta función se vuelve exponencial al acercarse al 100% de seguridad. Los costos se disparan (tendientes al infinito) por los complejos estudios que se deberán realizar para mantener este grado de seguridad.

Siempre se mantendrá la incertidumbre propia del comportamiento humano, que puede permitir a un atacante violar el sistema, haciendo que los costos hayan sido, sí bien no inútiles, excesivos.

CAPÍTULO II

ANÁLISIS Y DETERMINACIÓN DE REQUERIMIENTOS

2.1 Concepto y objetivo de la organización

Desde el punto de vista empresarial, puede definirse la organización como la aplicación de un conjunto de técnicas conducentes para obtener una empresa estructurada en forma tal, que con la correspondiente división de actividades y la debida coordinación de estas, se obtenga la máxima rentabilidad. La organización es la base de la labor del manager que tiende a adecuar los recursos previstos en la planificación para conseguir sus objetivos.

La organización tiende a estructurar la empresa creando órganos con funciones distintas, pero coordinados todos ellos entre sí para obtener el último fin de la empresa, que es el beneficio y el progreso. Establece la estructura de la empresa, determina relaciones, describe puestos de trabajo, califica estos puestos, etc.

La organización constituye, esencialmente, una estructura. El organigrama es la estructura que refleja una organización. Para establecer el organigrama de la empresa debemos asentarnos sobre pasos firmes y seguir una serie de normas:

- Toda organización debe modelarse sobre los objetivos de la empresa. La organización debe adaptarse a los objetivos y no los objetivos a la organización. Nunca debemos copiar el organigrama a otra empresa, en todo caso adaptarlo a nuestras peculiaridades.
- La organización debe adaptarse a los hombres de que disponga la empresa o de los que pueda disponer.
- Una organización es una entidad inamovible pero nunca estática. Debe adaptarse constantemente al cambio, tanto interno como externo, y debe ser revisable periódicamente.
- La posición del hombre en el organigrama no es inamovible.

El organigrama presenta todas las partes que constituyen a la empresa, dejando en claro sus divisiones y dependencias. La división se puede definir como una estructura de organizaciones montadas sobre unidades completas de gestiones rentable, dependiendo de un mando único superior. Cada unidad es, en cierto modo, una empresa, una integración funcional elemental bajo el mando único del jefe de la división. Las diferentes divisiones de la empresa desempeñan un papel vital para el crecimiento y desarrollo de la misma, pero siempre atendiendo a los objetivos que se ha fijado la organización. Para lograrlos, es necesario que exista una comunicación y coordinación estrecha entre cada una de las partes que la constituyen.

Las sociedades avanzadas de finales del pasado y principios del presente siglo son denominadas frecuentemente sociedades de la información, pues el volumen de datos que es procesado, almacenado y transmitido es inconmensurablemente mayor que es cualquier época pretérita.

Además, no sólo el volumen, sino la importancia de esta información para el desarrollo económico y social, no tiene ningún parangón con la que tuvo en el pasado. De hecho, en la

actualidad, las organizaciones consideran que la información es un bien más de su activo y, en muchos casos, prioritaria sobre los restantes.

Pero gran parte de esos datos que nosotros, o las entidades de nuestra sociedad, manejamos, han sido tratados, sea durante su proceso, o almacenamiento, o transmisión, mediante las llamadas tecnologías de la información, entre las que ocupa un lugar focal la informática. Consiguientemente, la seguridad de las tecnologías de información, y por ende la informática, se convierte en un tema de crucial importancia para el continuo y espectacular progreso de nuestra sociedad, e incluso para su propia supervivencia.

Por otro lado, la eclosión en los últimos años de las redes informáticas y fundamentalmente de Internet, ha sido el factor fundamental que ha hecho que la Seguridad en la Información cobrase una importancia vital en el uso de sistemas informáticos conectados. Desde el momento en que nuestra computadora se conecta a una red de área local o extensa (LAN o WAN) y a Internet, se abren ante nosotros toda una nueva serie de posibilidades, como son la transferencia de datos en cuestión de minutos y el aumento de la productividad de nuestro trabajo, sin embargo éstas traen consigo toda una serie de nuevos y en ocasiones complejos tipos de ataque. Más aun, mientras en una computadora aislado el posible origen de los ataques es bastante restringido, al conectarnos a una red LAN o WAN y a Internet, cualquier usuario de cualquier parte del mundo puede considerar nuestro sistema un objetivo apetecible.

Existe un acuerdo y conciencia general sobre la importancia de la Seguridad de los Sistemas de Información (SSI). La SSI está relacionada con la disponibilidad, confidencialidad e integridad de la información tratada por los computadoras y las redes de comunicación.

2.1.2 Información y Sistema Informático

Entendemos por información el conjunto de datos que sirven para tomar una decisión. En consecuencia, su necesidad es evidente tanto en la planificación estratégica a largo plazo como en la fijación de estándares para la planificación a corto. La información también es necesaria para el estudio de las desviaciones y de los efectos de las acciones correctoras; es un componente vital para el Control.

En cuanto a su implantación, se puede hablar de:

- Subsistema formalizado: Normas, procedimientos e información de negocio.
- Subsistema no formalizado: Flujos de información que no pasan por el sistema de información formalizado (rumores, charlas informales, llamadas telefónicas, etc.).

El sistema informático es un subconjunto del subsistema formalizado, con distinto grado de cobertura. Por otra parte, se puede ver el sistema informático como el conjunto de los recursos técnicos (máquinas y utensilios), financieros (ingresos, gastos y patrimonio) y humanos (plantilla de informáticos y personal auxiliar), cuyo objetivo consiste en el almacenamiento, procesamiento y transmisión de la información de la empresa.

2.1.3 Aspectos clave en la Seguridad de los Sistemas de Información (SSI)

Debido a la difusión de las tecnologías de la información, la mayoría de las organizaciones actuales están expuestas a una serie de riesgos derivados de una protección inadecuada o inapropiada de la información o de sus sistemas de tratamiento. Apuntaremos sólo dos ejemplos de esta vulnerabilidad creciente. Primero, con la gran expansión del uso de computadoras personales se ha magnificado el problema de la SSI, debido sobre todo a la carencia de controles de seguridad básicos en este tipo de sistemas. En segundo lugar, la evolución hacia entornos con acceso global y múltiple, con un aumento de la conectividad entre organizaciones distintas, plantea retos importantes a la gestión de la seguridad.

Los riesgos fundamentales asociados con la incorrecta protección de la información son:

- Revelación a personas no autorizadas
- Inexactitud de los datos
- Inaccesibilidad de la información cuando se necesita

Estos aspectos se relacionan con las tres características que debe cubrir un SI seguro: *confidencialidad, integridad y disponibilidad.* Así pues, preservar estas tres características de la información constituye el objetivo de la seguridad.

Los problemas técnicos, las amenazas ambientales, las condiciones de instalación desfavorables, los usuarios, la situación política y social, son otros tantos factores susceptibles de poner en peligro el buen funcionamiento de los SI. Las amenazas a los SI van desde desastres naturales tales como inundaciones, accidentes o incendios, hasta abusos deliberados como fraudes, robos, virus, con un origen tanto interno como externo.

Aunque se pueda pensar que el problema de la seguridad de los SI está sobredimensionado, muchos intereses no son nunca detectados, o se ocultan por los gestores porque muestran fallos o debilidades de los procedimientos de seguridad, existiendo una natural resistencia en informar de los mismos a personas ajenas.

2.2 Evaluación de Seguridad de un Sistema de Información

2.2.1 Importancia de la Información

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

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

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

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

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

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

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

Para continuar es muy importante conocer el significado de dos palabras, que son riesgo y seguridad.

Riesgo

Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

Seguridad

Cualidad o estado de seguro. Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo. Ejemplo: Seguridad Social Conjunto de organismos, medios, medidas, etc., de la administración estatal para prevenir o remediar los posibles riesgos, problemas y necesidades de los trabajadores, como enfermedad, accidentes laborales, incapacidad, maternidad o jubilación; se financia con aportaciones del Estado, trabajadores y empresarios. Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

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

2.2.2 Identificación de riesgos a la seguridad

¡Debe ser difícil lograr confidencialidad, integridad y disponibilidad, cuando no se tiene claro qué es lo que se quiere proteger y contra qué se quiere proteger!

Desgraciadamente, ese es el caso en muchas compañías e instituciones. No existen análisis de riesgos que permitan identificar los activos con que se cuenta, su valía, y los riesgos de cualquier tipo que pudieran afectarlos. Desde luego, tampoco se tienen estimados de lo que costaría recuperarse de un incidente. Sin esta información, el aventurarse a elegir mecanismos de protección, se convierte en un juego sin sentido en el que se suelen comprar cañones para matar moscas (resulta más caro protegerse que dejar que ocurra un problema y recuperarse), se adquieren soluciones contra riesgos que no existen, o se pasan por alto riesgos críticos que posteriormente resultan en compromisos del sistema.

La implantación sensata de una estrategia de seguridad debe comenzar con la identificación de los riesgos potenciales. Este proceso debe ser desarrollado formalmente por un grupo de personas de todas las áreas de la compañía, con objeto de obtener una visión completa del valor de los activos y las consecuencias de que se vea comprometida su confidencialidad, integridad o disponibilidad. Una buena manera para obtener dicha información es el dar respuestas serias a las siguientes preguntas:

- **¿Qué podría pasar?** Buscando identificar los activos existentes (software, hardware, datos, personas, etc.) y los eventos amenazantes.
- **¿Si pasara qué tan malo sería?** Buscando cuantificar el impacto de las amenazas en todos los ámbitos (operativo, financiero, mercadológico, etc.).
- **¿Qué tan frecuentemente podría pasar?** Con objeto de identificar la frecuencia de ocurrencia potencial de los eventos amenazantes.
- **¿Qué tan correctas son las respuestas a las tres preguntas anteriores?**

La respuesta cuidadosa y estudiada a estas preguntas, permitirá tener un excelente nivel de conocimiento sobre los activos con que se cuenta y lo que representan para la empresa, así como conocer cual sería el impacto en caso de que sufran algún incidente de seguridad.

2.2.3 Identificación de medidas de seguridad

Una buena identificación de riesgos, permitirá una adecuada selección de mecanismos de protección. Del mismo modo, una mala identificación de riesgos puede conducir a una mala selección de mecanismos, provocando una falsa sensación de seguridad, la cual podría enfatizar la severidad de las consecuencias de un incidente. La identificación y selección de medidas de seguridad dependen entonces completamente del éxito de la identificación de riesgos. El proceso de identificación de mecanismos de seguridad puede realizarse dando cuidadosas respuestas a las preguntas:

- **¿Qué puede hacerse?** Buscando identificar las acciones que ayudan a mitigar los riesgos ya identificados (mecanismos, procedimientos, entrenamiento).
- **¿Cuánto cuesta hacerlo?** Identificando el costo financiero, operativo, etc. que implica ejecutar dichas acciones.
- **¿Los beneficios superan a los costos?** Buscando que el costo de protegerse de una amenaza sea menor al costo de recuperarse de una ocurrencia de la misma.

La respuesta a estas preguntas permitirán identificar varias alternativas distintas para mitigar el impacto de los riesgos identificados. Dependiendo de las implicaciones de cada alternativa y la situación única de cada compañía, deberán elegirse los mecanismos suficientes necesarios para lograr los niveles de confidencialidad, integridad y disponibilidad requeridos.

2.3 Ataques de Seguridad

Una **Amenaza** se representa a través de una persona, circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño cuando existe una violación a la seguridad.

Un **Ataque de la Seguridad** es la realización de una amenaza. Las amenazas están en cualquier parte de nuestro entorno informático y cuando se presenta una oportunidad de realizar la violación, automáticamente se esta llevando a cabo un ataque.

Cualquier ataque necesita, para efectuarse, tres elementos: motivación, capacidad y oportunidad. Si el ataque es sobre los limites físicos de una organización, se necesita además tener ciertas características especiales de personalidad.

Los ataques tienen varios objetivos incluyendo el fraude, la extorsión, el robo de información, la venganza o simplemente el desafió de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso o por atacantes externos que acceden remotamente o interceptan el trafico de red.

Por lo anterior, las amenazas pueden clasificarse en:

Amenazas de tipo Pasivo: Recibe este nombre debido a que el atacante no altera en ningún momento la información, es decir, únicamente la observa., escucha, obtiene o monitorea mientras está siendo trasmitida.

Como amenazas de tipo pasivo tenemos:

- **Intercepción de datos:** consiste en el conocimiento de la información cuando existe una liberación de los contenidos del mensaje. La *Intercepción* se da cuando una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la *confidencialidad* La entidad no autorizada podría ser una persona o un programa. Ejemplos de este ataque son tener acceso a una línea para hacerse de datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de los paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).(**Figura 2.1**)

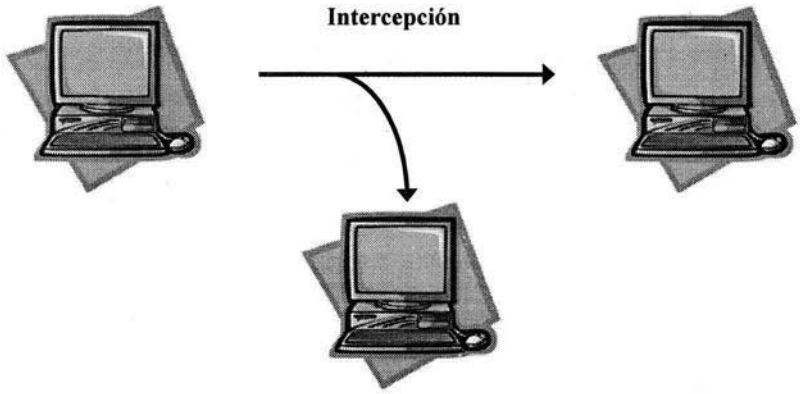

Figura 2.1 Intercepción de Datos

- **Análisis de Tráfico:** consiste en la observación de todo el trafico que pasa por la red.

La información que puede obtenerse a través de estos tipos de ataques puede consistir en :

a) **Obtención del origen y destinatario** de la comunicación, esto se logra cuando el intruso lee las cabeceras de los paquetes que continuamente está monitoreando. Con ello se determina la localización y la identidad de los anfitriones (emisor, receptor).
b) **Control del volumen de trafico** intercambiando entre las entidades monitoreadas, de esta forma se obtienen todos los datos necesarios para percatarse de la actividad o inactividad inusuales, se conoce la frecuencia y longitud de los mensajes.
c) **Control de horas habituales** de intercambio de datos entre las entidades de la comunicación, con ello se extraen los datos acerca de los periodos de actividad. El intruso conoce la frecuencia con la que se trasmiten los mensajes.

Las amenazas y ataques de tipo pasivo son muy difíciles de detectar e interceptar, debido a que no provocan ninguna alteración de los datos.

Amenazas de tipo Activo: se nombran así debido a que implican algún tipo de modificación del flujo de datos trasmitido (modificación de la corriente de datos) o la creación de un falso flujo de datos (creación de una corriente falsa).

Como amenazas de tipo activo tenemos:

- **Interrupción o destrucción:** un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son

la destrucción de un elemento de hardware, como un disco duro. Cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos. (**Figura 2.2**)

Figura 2.2 Interrupción de Datos

- **Modificación:** una entidad no autorizada no solo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido del mensajes que esta siendo transferidos por la red **(Figura 2.3)**

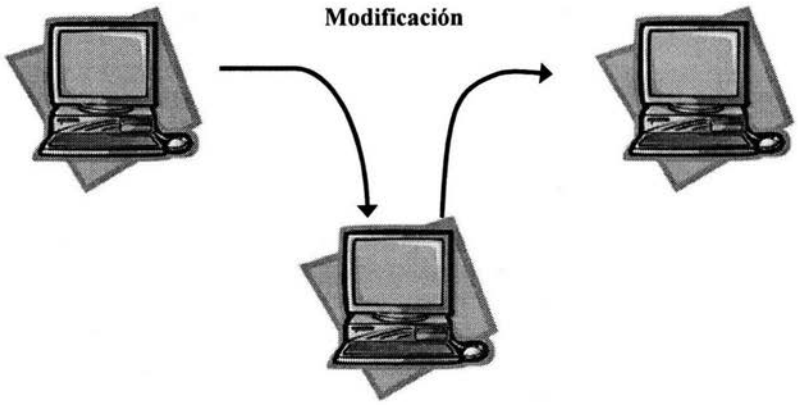

Figura 2.3 Modificación de Datos

- **Suplantación:** una entidad no autorizada inserta objetos falsificados en el sistema. Este ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.**(Figura 2.4)**

Figura 2.4 Suplantación

Las amenazas de la seguridad provienen de diversas fuentes, entre ellas se encuentran:

1. **De humanos:** la amenaza surge por ignorancia en el manejo de la información, por descuido, por negligencia, por inconformidad (cuando el empleado es despedido).
2. **Errores de Hardware:** se da la amenaza por fallas físicas que presente cualquier elemento de los dispositivos que conforman a la computadora. Los más comunes son fallos en el suministro de energía, ruido electromagnético, distorsión, alto voltaje, etc.
3. **Error de la Red:** se presenta una amenaza cuando no se calcula bien el flujo de la información que se va a circular por el canal de comunicación, es decir, un atacante podría saturar el canal de comunicación provocando la no disponibilidad de la red o la desconexión del mismo.
4. **Problemas de tipo lógico:** la amenaza se hace presente cuando un diseño bien elaborado de un mecanismo de seguridad, se implementa mal o no cumple con las especificaciones del diseño.
5. **Desastres:** la amenaza de este tipo surge de las fuerzas de la naturaleza tales como las inundaciones, los terremotos, el fuego, el viento. Dichos desastres hacen surgir amenazas directas, pues repercuten indiscutiblemente en el funcionamiento físico de las computadoras, redes, instalaciones, líneas de comunicación, etc.

2.4 Controles de Seguridad

Un entorno operativo seguro exige la garantía de que sólo pueda acceder a una determinada información aquellos que están autorizados para ello, que la información se procese correctamente y que está disponible cuando se necesita.

Para aplicar controles adecuados, es preciso comprender primero quién o qué es lo que amenaza dicho entorno, así como conocer los riesgos asociados a dichas amenazas si llegan a materializarse.

La información se ve sometida a distintas amenazas que pueden clasificarse en *intencionadas, no intencionadas y naturales.*

Las amenazas intencionadas las ejercen usuarios no autorizados que acceden de forma indebida a los datos o información sensible. Los usuarios no autorizados pueden ser externos o pertenecientes a la propia organización y se pueden clasificar como curiosos o maliciosos. Los curiosos normalmente ojean un poco y no siempre entran con unas pretensiones concretas, ni saben lo que van a encontrar. Los maliciosos entran a los sistemas para apropiarse de datos o información por intereses económicos, o bien con ánimo de dañar o destruir recursos. El acceso no autorizado de usuarios ya sea curioso o malicioso significa siempre una violación de la confidencialidad y con frecuencia acarrea violaciones de la integridad y de la disponibilidad.

Las amenazas no intencionadas provienen típicamente de empleados con poca formación o negligentes que no han seguido los pasos para proteger sus contraseñas, asegurar adecuadamente sus computadoras o actualizar con la frecuencia debida el programa antivirus. Las amenazas no intencionadas también implican a veces a los programadores o personal de proceso de datos cuando no se siguen las normas y procedimientos de seguridad establecidos, cuando existen. Este entorno operativo es especialmente sensible ya que sencillos errores en un programa pueden afectar a la integridad de la aplicación global y de cualquier otra aplicación con la que comparta información en común.

Las amenazas naturales incluyen fallos de equipos y calamidades tales como incendios, inundaciones y terremotos que pueden causar la pérdida de equipos y datos. Las amenazas naturales suelen afectar a la disponibilidad de los recursos y de la información. (Véase **Tabla 2.1)**

Los riesgos asociados a la pérdida de la confidencialidad, integridad o disponibilidad son de diverso tipo y casi siempre implican daños económicos incluyendo responsabilidad contractual, falsos datos financieros, mayores costes, pérdidas de activos, pérdida de negocios, descrédito y pérdida de imagen pública.

Amenaza		Problema	Riesgo
Usuario no autorizado		Confidencialidad	Acceso no autorizado
	(curioso)	Integridad	Divulgación no autorizada Observación no autorizada Monitorización no autorizada Copias no autorizadas Sustracción de información
Usuario no autorizado		Confidencialidad	Acceso indebido, copia o sustracción de datos
	(malicioso)	Integridad	Alteración de datos, falsificación, fraude
		Disponibilidad	Destrucción, pérdida, repudio del servicio
Usuario autorizado		Integridad	Pérdida o alteración de información
		Disponibilidad	Daños, denegación o alteración de servicio
Catástrofe natural		Disponibilidad	Destrucción, daños, averías, pérdida de servicio

Tabla 2.1 Matriz de Amenazas / Cualidad / Riesgo

Las amenazas pueden ser de los tipos siguientes:

a) Amenazas de fuerza mayor
b) Fallos de organización
c) Fallos humanos
d) Fallos técnicos
e) Actos malintencionados

Algunas de las amenazas más frecuentes están relacionadas con el incumplimiento de las medidas de seguridad y con la administración incorrecta de los sistemas y la comisión de errores en su configuración y operación.

El incumplimiento de las medidas de seguridad, como consecuencia de actos negligentes o falta de controles adecuados, originan daños que podrían haber sido evitados o por lo menos minimizados. Según las responsabilidades del usuario y la importancia de la norma incumplida, los daños podrían llegar a ser de gravedad.
Algunos ejemplos típicos son:

- Mantener accesibles puertas de emergencia en locales protegidos por sistemas de control de acceso.
- Guardar la llave del armario de los soportes físicos con información confidencial en un sitio de fácil acceso.
- Dejar escritas en un papel, cerca de la estación de trabajo, las contraseñas y claves de acceso.
- No disponer de archivo de respaldo en el momento en que se produce la pérdida de datos

La administración incorrecta del sistema ya sea por negligencia o por ignorancia, y los errores en la configuración de los parámetros y opciones de los programas, condicionan también su seguridad.

Algunos ejemplos típicos son:

- Instalar de forma inadecuada los nuevos paquetes software
- No analizar los archivos de eventos.
- No disponer de un sistema de auditorías.
- Ser excesivamente permisivo en la adjudicación de autorizaciones de acceso.
- No tener un control exhaustivo de los nombres de usuario, permitiendo su repetición.
- Utilizar de forma inadecuada, o no utilizar, las herramientas de seguridad disponibles en los Sistemas Operativos.
- No controlar los puntos de acceso a las redes.

2.5 Seguridad Física

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, hackers, virus, etc; la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

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

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

Así, la Seguridad Física 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"[3]. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

El objetivo de la Seguridad Física es el de evitar riesgos potenciales de ataque, pérdida, robo o daño a los Sistemas de Información de la empresa, accidentales o intencionados, que puedan ocasionar la interrupción, total o parcial, de las actividades de negocio.

2.5.1 Tipos de Desastre

Cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto también es valido para el edificio en el que nos encontramos. Es por ello que siempre se recomiendan pautas de aplicación general y no procedimientos especifico. Este tipo de seguridad esta enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que es encuentra ubicado el centro.

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

1. Desastres naturales, incendios accidentales, tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

Para sacar ideas de cómo obtener la máxima seguridad en un sistema informático no hace falta recurrir a las películas de espionajes, además de que resultaría extremadamente caro. En ocasiones basta con recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas sigue siendo técnica validas en cualquier entorno.

---

[3] HUERTA, Antonio Villalón. "Seguridad en Unix y Redes", Octubre de 2002. *http://www.kriptopolis.com*

Los peligros más importantes que se corren un centro de procesamiento de información son:

- 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 seguridad. Es considerado el enemigo numero uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Desafortunadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos (como son el agua y espumas químicas). El dióxido de carbono resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputo.

Para reducir el riesgo de un incendio a los que se encuentra sometido un centro de computo, se debe contemplar:

1. El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
2. El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
3. Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo
4. Debe construirse un "piso falso" instalado sobre el piso real, con materiales incombustibles y resistente al fuego.
5. No debe estar permitido fumar en el área de proceso.
6. Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
7. El piso y el techo en el recinto del centro de computo y del almacenamiento de los medios magnéticos deben ser impermeables.

Es necesario proteger los equipos de computo instalándolos en áreas en las cuales el acceso a lo mismos solo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18° C y el límite de humedad no debe superar el 65% para evitar el deterioro.

- Los centros de computo deben estar provistos de equipo para la extinción de incendios con relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

El personal designado para usar extinguidores de fuego debe ser entrenado en el uso.

Si hay un sistema de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con el proceso automático.

Implementar paredes protectoras de fuego alrededor de las áreas que se desean proteger del incendio que podría originarse en las áreas adyacentes.

Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere lenta y costosa operación de limpieza.

Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel.

Suministrar información, del centro de computo, al departamento local de bomberos, antes de que ellos sean llamados en una emergencia. Hacer que este departamento este consciente de las particularidades y vulnerabilidades del sistema, por excesivas cantidades de agua y la conveniencia de una salida para el humo, es importante. Además, ellos pueden ofrecer excelentes consejos como precauciones para prevenir incendios.

- Inundaciones

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenajes ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajara por las escaleras.

- Condiciones climatológicas

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 combustibles para la emergencia.

- Terremotos

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensible 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.

- Señales de Radar

La influencia de las señales o rayos de radar sobre el funcionamiento de una computadora ha sido exhaustivamente estudiada desde hace varios años. Los resultados de las investigaciones más recientes son que las señales muy fuertes de radar pueden interferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor. Ello podría ocurrir solo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana.

- Instalaciones Eléctricas

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta es una de las principales áreas a considerar en la seguridad física. 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.

- Picos y Ruidos Electromagnéticos.

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También esta el ruido que interfiere el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos y favorece a la interferencia electrónica.

- 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 son construidos con los cables instalados para ahorrar tiempo y gastos posteriores, minimizando los riesgos de un corte, rozadura u otro daño accidental.

Algunos de los riesgos más comunes para el cableado son:

1. Interferencia: modificaciones generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren problemas de alteración de los datos que viajan a través de él por acción de campos eléctricos, que si sufren los cables metálicos.
2. Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
3. Daños en el cable: los daños normales con el uso pueden dañar la cubierta que preserva la integridad de los datos trasmitidos o dañar en propio cable, lo que ocasiona que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

1. Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de acceso adecuados 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.
2. Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

No hace falta penetrar en los cables físicamente para obtener los datos que trasportan.

- Pisos de Placas Extraíbles.

Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser alojados en el espacio que se dispone en los pisos extraíbles debajo del mismo.

- Sistema de Aire Acondicionado

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado que se dedique al cuarto de computadoras y equipos de procesos de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

- Emisiones Electromagnéticas.

Desde hace tiempo se sospecha que las emisiones de muy baja frecuencia que generan algunos periféricos son dañinas para el ser humano.

Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente para las personas.
Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

- La Salud Mental.

La carga física del trabajo adopta modalidades diferentes en los puestos informatizados. De hecho disminuye los desplazamientos de los trabajadores y las tareas requieren un menor esfuerzo muscular dinámico, pero aumenta, al mismo tiempo, la carga estática de acuerdo con las posturas inadecuadas asumidas.

Por su parte, la estandarización y racionalización que tiende a acompañar la aplicación de las PC´s en las tareas de ingreso a datos, puede llevar a la transformación del trabajo en una rutina inflexible que inhibe la iniciativa personal, promueve sensaciones de hastió y monotonía y conduce a una pérdida de significado del trabajo.

El estrés informático está convirtiéndose en una nueva enfermedad profesional relacionada con el trabajo, provocada por la carga mental y psíquica inherente a la operación con los nuevos equipos.

Los efectos del estrés pueden encuadrarse dentro de varias categorías:

1. Los efectos fisiológicos inmediatos, caracterizados por el incremento de la presión arterial, el aumento de la frecuencia cardiaca, etc.
2. Los efectos psicológicos inmediatos hacen referencia a la tensión, irritabilidad, cólera, agresividad, etc. Estos sentimientos pueden, a su vez, inducir ciertos efectos en el comportamiento tales como el consumo de alcohol y psicofármacos, el hábito de fumar, etc.
3. También existen consecuencias médicas a largo plazo, tales como enfermedades coronarias, hipertensión arterial, úlceras pépticas, agotamiento; mientras que las consecuencias psicológicas a largo plazo pueden señalar neurosis, insomnio, estados crónicos de ansiedad y/o depresión, etc.
4. La apatía, sensaciones generales de insatisfacción ante la vida, la pérdida de la propia estima, etc., alteran profundamente la vida personal, familiar y social del trabajador llevándolo, eventualmente, al aislamiento, al ausentismo laboral y la pérdida de la solidaridad social.

2.5.2 Acciones Hostiles.

- Robo.

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una maquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraible y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

- Fraude.

Cada año, millones de dólares son sustraídos de empresas y, en muchas 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.

- Sabotaje.

El peligro más temido en los centros de cómputo, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

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

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.
Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

2.5.3 Conductas dirigidas a causar daños físicos

El primer grupo comprende todo tipo de conductas destinadas a la destrucción «física» del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc. En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

2.5.4 Conductas dirigidas a causar daños lógicos

El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

Este tipo de daño a un sistema se puede alcanzar de diversas formas. Desde la más simple que podemos imaginar, como desenchufar la computadora de la electricidad mientras sé esta trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

Estos programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada. Sin pretender realizar una clasificación rigurosa de estos métodos de destrucción lógica, podemos distinguir:

- Personas

No podernos engañarnos: la mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno (o algunos) de los riesgos lógicos de los que hablaremos a continuación, especialmente agujeros del software.

Pero con demasiada frecuencia se suele olvidar que los piratas "clásicos" no son los únicos que amenazan nuestros equipos: es especialmente preocupante que mientras que hoy en día cualquier administrador mínimamente preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su software, restringiendo servicios, utilizando cifrado de datos...), pocos administradores tienen en cuenta factores como la ingeniería social o él basureo a la hora de diseñar una política de seguridad.

Aquí se describen brevemente los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes

grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican -o destruyen-, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los crackers realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y activos en caso contrario, y el personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

- Personal

Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento...) puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas y sus debilidades), lo normal es que más que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad: un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de archivos; y en el primer caso, el "atacante" ni siquiera ha de tener acceso lógico (<ni físico!) a los equipos, ni conocer nada sobre seguridad. Hemos de recordar siempre que decir "No lo hice a propósito" no va a servir para recuperar datos perdidos ni para restaurar un hardware dañado o robado.

- Basureo

La técnica del basureo (en inglés, scavenging) está relacionada tanto con los usuarios como con la seguridad física de los sistemas, de la que hemos hablado en el anteriormente; consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo. Él basureo puede ser físico, como buscar en cubos de basura (trashing, traducido también por basureo) listados de impresión o copias de documentos, o lógico, como analizar buffers de impresoras, memoria liberada por procesos, o bloques de un disco que el sistema acaba de marcar como libres, en busca de información.

Aunque esta técnica no es muy utilizada en la mayoría de entornos, hemos de pensar que si un usuario tira a la basura documentos que proporcionen información sobre nuestro sistema, cualquier potencial atacante puede aprovechar esa información para conseguir acceder al equipo; algo tan simple como una factura en la que se especifiquen números de teléfono o nombres (reales o de entrada al sistema) de usuarios puede convertirse en una valiosa información para un atacante. Además, en ocasiones ni siquiera es necesario andar revolviendo por los cubos de basura en busca de información comprometedora: la carencia

de nociones básicas sobre seguridad informática hace posible que los usuarios dejen al alcance de cualquiera información vital de cara a mantener un sistema seguro.

Como hemos dicho él basureo no es un ataque habitual en organizaciones "normales", simplemente porque los datos con los que están trabajan no suelen ser de alta confidencialidad. De cualquier forma, si deseamos evitar problemas lo más inmediato es utilizar una máquina trituradora de papel (su precio no suele ser prohibitivo, y la inversión quizás valga la pena) para destruir toda la documentación antes de arrojarla a la basura; incluso nos puede interesar contratar los servicios de compañías dedicadas exclusivamente a la destrucción de estos soportes. En el caso de sistemas de almacenamiento lógico (discos, CD-ROMs, cintas...) también es importante una correcta inutilización de los mismos para que un potencial atacante no pueda extraer información comprometedora; no suele ser suficiente el simple borrado del medio o un leve daño físico (por ejemplo, partir un CD-ROM), ya que como comentaremos al hablar de recuperación de datos existen empresas capaces de extraer hasta el último bit de un medio borrado o dañado. Lo más efectivo sería un borrado seguro, seguido de una destrucción física importante que haga imposible la reconstrucción del medio.

- Ex-empleados

Otro gran grupo de personas potencialmente interesadas en atacar nuestro sistema son los antiguos empleados del mismo, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia). Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo: amparados en excusas como "No me han pagado lo que me deben" o "Es una gran universidad, se lo pueden permitir" pueden insertar troyanos, bombas lógicas, virus o simplemente conectarse al sistema como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso meses después de abandonar la universidad o empresa), conseguir el privilegio necesario, y dañarlo de la forma que deseen, incluso chantajeando a sus ex-compañeros o ex-jefes.

- Curiosos

Junto con los crackers, los curiosos son los atacantes más habituales de sistemas y en redes. Recordemos que los equipos están trabajando en entornos donde se forma a futuros profesionales de la informática y las telecomunicaciones (gente que a priori tiene interés por las nuevas tecnologías), y recordemos también que las personas suelen ser curiosas por naturaleza; esta combinación produce una avalancha de estudiantes o personal intentando conseguir mayor privilegio del que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. Y en la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.

- Crackers

Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Por un lado, son redes generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas; por otro, el gran número y variedad de sistemas conectados a estas redes provoca, casi por simple probabilidad, que al menos algunos de sus equipos (cuando no la mayoría) sean vulnerables a problemas conocidos de antemano. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple exploit los equipos que presentan vulnerabilidades; esto convierte a las redes de las de empresas, o a las de ISPs en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos, desde los más novatos (y a veces más peligrosos) hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otros organismos, con el consiguiente deterioro de imagen (y a veces de presupuesto) que supone para una universidad ser, sin desearlo, un apoyo a los piratas que atacan sistemas teóricamente más protegidos, como los militares.

- Terroristas

Por "terroristas" no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él. Por ejemplo, alguien puede intentar borrar las bases de datos de un partido político enemigo o destruir los sistemas de archivos de un servidor que alberga páginas web de algún grupo religioso; típicos ataques son la destrucción de sistemas de prácticas o la modificación de páginas web de algún departamento o de ciertos profesores, generalmente por parte de alumnos descontentos.

- Intrusos remunerados.

Este es el grupo de atacantes de un sistema más peligroso, aunque por fortuna el menos habitual en redes normales; suele afectar más a las grandes - muy grandes - empresas o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía...) o simplemente para dañar la imagen de la entidad afectada.
Esta tercera parte suele ser una empresa de la competencia o un organismo de inteligencia, es decir, una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad: se suele pagar bien a los mejores piratas, y por si esto fuera poco los atacantes van a tener todos los medios necesarios a su alcance.
Aunque como hemos dicho los intrusos remunerados son los menos comunes en la mayoría de situaciones, en ciertas circunstancias pueden aprovechar nuestras redes como plataforma para atacar otros organismos; una excelente lectura sobre esta situación es [Sto89], en la que el experto en seguridad Cliff Stoll describe cómo piratas pagados por el KGB soviético

utilizaron redes y sistemas Unix dedicados a I+D para acceder a organismos de defensa e inteligencia estadounidenses.

2.6 Seguridad Lógica.

La mayoría de los daños que puede sufrir un centro de computo no será sobre los medios físicos sino contra la información almacenada y procesada. La Seguridad Física, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. El activo más importante que se posee es la **información,** y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estás técnicas las brinda la Seguridad Lógica.

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

Los objetivos que se plantea son:

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

Bajo la etiqueta de `amenazas lógicas' encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (*software* malicioso, también conocido como *malware*) o simplemente por error (*bugs* o agujeros)

- Software incorrecto.

Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones. Una situación no contemplada a la hora de diseñar el sistema de red del *kernel* o un error accediendo a memoria en un archivo *setuidado* pueden comprometer local o remotamente a cualquier otro sistema operativo.
A estos errores de programación se les denomina *bugs*, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, *exploits*. Estos representan la amenaza más común contra cualquier sistema operativo, ya que cualquiera puede conseguir un *exploit* y utilizarlo contra nuestra máquina sin ni siquiera saber cómo funciona y sin unos conocimientos mínimos de los sistemas operativos; incluso hay *exploits* que dañan

seriamente la integridad de un sistema (negaciones de servicio o incluso acceso `root` remoto) y están preparados para ser utilizados desde MS-DOS, con lo que cualquier pirata novato (comúnmente, se les denomina *Script Kiddies*) puede utilizarlos contra un servidor y conseguir un control total de una máquina de varios millones de pesetas desde su PC sin saber nada del sistema atacado; incluso hay situaciones en las que se analizan los *logs* de estos ataques y se descubre que el pirata incluso intenta ejecutar órdenes de MS-DOS.

- Herramientas de seguridad

Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos. Herramientas como NESSUS, SAINT o SATAN pasan de ser útiles a ser peligrosas cuando las utilizan *crackers* que buscan información sobre las vulnerabilidades de un *host* o de una red completa.

La conveniencia de diseñar y distribuir libremente herramientas que puedan facilitar un ataque es un tema peliagudo; incluso expertos reconocidos como Alec Muffet (autor del adivinador de contraseñas `Crack`) han recibido enormes críticas por diseñar determinadas herramientas de seguridad para Unix. Tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas por parte de los atacantes: esta política, denominada *Security through obscurity*, se ha demostrado inservible en múltiples ocasiones. Si como administradores no utilizamos herramientas de seguridad que muestren las debilidades de nuestros sistemas (para corregirlas), tenemos que estar seguro que un atacante no va a dudar en utilizar tales herramientas (para explotar las debilidades encontradas); por tanto, hemos de agradecer a los diseñadores de tales programas el esfuerzo que han realizado (y nos han ahorrado) en pro de sistemas más seguros.

- Puertas traseras

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un *software* de gestión de bases de datos en el que para acceder a una tabla se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una única clave "especial", con el objetivo de perder menos tiempo al depurar el sistema.

Algunos programadores pueden dejar estos atajos en las versiones definitivas de su *software* para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer, lo que obviamente supone un grave peligro para la integridad de nuestro sistema.

- Bombas lógicas (time bombs)

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos archivos, la ejecución bajo un determinado UID o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa: si las activa el *root*, o el programa que contiene la bomba está situado a su nombre, los efectos obviamente pueden ser fatales.

En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.

Ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los archivos de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa. Otra modalidad que actúa sobre los programas de aplicación es el llamado «cáncer de rutinas» («cáncer routine»). En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos. Una variante perfeccionada de la anterior modalidad es él «virus informático» que es un programa capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión.

- Canales cubiertos

Según la definición de los canales cubiertos (o canales ocultos, según otras traducciones) son canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; dicho de otra forma, un proceso transmite información a otros (locales o remotos) que no están autorizados a leer dicha información.

Los canales cubiertos no son una amenaza demasiado habitual en redes de I+D, ya que suele ser mucho más fácil para un atacante aprovechar cualquier otro mecanismo de ataque lógico; sin embargo, es posible su existencia, y en este caso su detección suele ser difícil: algo tan simple como el puerto *finger* abierto en una máquina puede ser utilizado a modo de *covert channel* por un pirata con algo de experiencia.

- Virus

Un virus es una secuencia de código que se inserta en un archivo ejecutable (denominado *huésped*), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Todo el mundo conoce los efectos de los virus en algunos sistemas operativos de sobremesa; sin embargo, en Unix los virus no suelen ser un problema de seguridad grave, ya que lo que pueda hacer un virus lo puede hacer más fácilmente cualquier otro mecanismo lógico (que será el que hay que tener en cuenta a la hora de diseñar una política de seguridad)

Aunque los virus existentes para entornos Unix son más una curiosidad que una amenaza real, en sistemas sobre plataformas IBM-PC o compatibles (recordemos que hay muchos sistemas Unix que operan en estas plataformas, como Linux, FreeBSD, NetBSD, Minix, Solaris...) ciertos virus, especialmente los de *boot*, pueden tener efectos nocivos, como dañar el sector de arranque; aunque se trata de daños menores comparados con los efectos de otras amenazas, hay que tenerlos en cuenta.

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

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

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

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

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

12 de diciembre de 1987. El virus de Navidad. Una tarjeta navideña digital enviada por medio de un BBS de IBM atasco las instalaciones en los EE.UU. por 90 minutos. Cuando se ejecutaba el virus este tomaba los Adress Book del usuario y se retransmitía automáticamente, además que luego colgaba al equipo anfitrión.

Esto causo un desbordamiento de datos en la red.

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

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

4 de noviembre de 1988 Un virus invade miles de computadoras basadas en Unix en universidades e instalaciones de investigación militares, donde las velocidades fueron reducidas y en otros casos paradas. También el virus se propagó a escala internacional.
Se estableció que la infección no fue realizada por un virus sino por un programa gusano, diseñado para reproducirse así mismo indefinidamente y no para eliminar datos. El programa se difundió a través de un corrector de errores para correo electrónico, que se movió principalmente en Internet (Arpanet) y contamino miles de computadoras en todo el mundo contando 6000 computadoras en centros militares en los EE.UU. , incluyendo la NASA, la Fuerza Aérea, el MIT, las universidades de Berkeley, Illinois, Boston, Stanford, Harvard, Princeton, Columbia y otras. En general se determino que la infección se propago en las computadoras VAX de DEC (digital equipament corp) y las fabricadas por Sun Microsystems, que empleaban Unix.

Se halla al culpable Robert Morris, estudiante de 23 años, que declara haber cometido un error al propagar el gusano. Morris era el hijo de un experto en seguridad informática del gobierno.

El caso fue investigado por el FBI. Posiblemente se sentencie a Morris por 5 años de prisión y una multa de 250000 USD.

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

Y los últimos pero recordados vaccina, hacker, cpw543, natas, antiexe, etc.

- Gusanos

Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que conecta para dañarlos. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fué precisamente

el *Internet Worm*, un gusano que en 1988 causó perdidas millonarias al infectar y detener más de 6000 máquinas conectadas a la red.

Hemos de pensar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema: mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra red completa (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

- Caballos de Troya

Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente.

En la práctica totalidad de los ataques, cuando un intruso consigue el privilegio necesario en el sistema instala troyanos para ocultar su presencia o para asegurarse la entrada en caso de ser descubierto: por ejemplo, es típico utilizar lo que se denomina un rootkit, que no es más que un conjunto de versiones troyanas de ciertas utilidades (netstat, ps, who...), para conseguir que cuando el administrador las ejecute no vea la información relativa al atacante, como sus procesos o su conexión al sistema; otro programa que se suele suplantar es login, por ejemplo para que al recibir un cierto nombre de usuario y contraseña proporcione acceso al sistema sin necesidad de consultar los registros del sistema.

- Programas conejo o bacterias.

Bajo este nombre se conoce a los programas que no hacen nada útil, sino que simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio. Por sí mismos no hacen ningún daño, sino que lo que realmente perjudica es el gran número de copias suyas en el sistema, que en algunas situaciones pueden llegar a provocar la parada total de la máquina.

Hemos de pensar hay ciertos programas que pueden actuar como conejos sin proponérselo; ejemplos típicos se suelen encontrar en los sistemas Unix destinados a prácticas en las que se enseña a programar al alumnado: es muy común que un bucle que por error se convierte en infinito contenga entre sus instrucciones algunas de reserva de memoria, lo que implica que si el sistema no presenta una correcta política de cuotas para procesos de usuario pueda venirse abajo o degradar enormemente sus prestaciones. El hecho de que el autor suela ser fácilmente localizable no debe ser ninguna excusa para descuidar esta política: no podemos culpar a un usuario por un simple error, y además el daño ya se ha producido.

- Técnicas salami

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de pesos se roban unos céntimos, nadie va a darse cuenta de ello; si esto se automatiza para, por ejemplo, descontar un peso de cada nómina pagada en la universidad o de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una cantidad ínfima.

Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad medios es posible que haya computadoras dedicados a contabilidad, facturación de un departamento o gestión de nóminas del personal, comentamos esta potencial amenaza contra el *software* encargado de estas tareas

CAPÍTULO III

IDENTIFICACIÓN Y ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD

3.1 Fundamentos de las políticas de seguridad

Al ser las políticas de seguridad parte esencial en la estructura normativa de la dependencia, reviste especial importancia el conocer y comprender los principios básicos acerca de las políticas, estar consciente del reto que plantea el construirlas y del compromiso de llevarlas a cabo, así como mantener su vigencia.

3.1.1 ¿Qué es una política de seguridad?

Una Política de Seguridad se define como la especificación de los requerimientos para el control de acceso a la información, aplicaciones y servicios de seguridad informática de una organización. Estos requerimientos a su vez definen cuáles rubros pueden ser accesados: información, servicios, aplicaciones, con qué permisos: lectura, modificación, eliminación, transferencia , cuándo y por quién.

Dentro de las funciones de las entidades informáticas, las políticas de seguridad se deben enfocar inicialmente a la protección de la información recabada, procesada y distribuida mediante sus recursos; sin embargo, también se deben emitir políticas para todos los rubros, incluyendo facilidades, aplicaciones, instalaciones y equipos.

La política de seguridad es una declaración de intenciones de alto nivel que cubre la seguridad de los Sistemas de Información 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 distintas medidas a tomar para proteger la seguridad del sistema, las funciones y responsabilidades de los distintos componentes de la organización y los mecanismos para controlar su correcto funcionamiento.

Son los directivos, junto con los expertos en tecnologías de la información, quienes deben definir los requisitos de seguridad, identificando y priorizando la importancia de los distintos elementos de la actividad realizada, con lo que los procesos más importantes recibirán más protección. La seguridad debe considerarse como parte de la operativa habitual, no como un extra añadido.

El compromiso de la Dirección con la Seguridad de los Sistemas de Información debe tomar la forma de una política de seguridad de los Sistemas de Información formalmente acordada y documentada. Dicha política tiene que ser consistente con las prácticas de seguridad de otros departamentos, puesto que muchas amenazas (incendio, inundación) son comunes a otras actividades de la organización.

Algunas reglas básicas a la hora de establecer una política de seguridad.

- Toda política de seguridad debe ser holística, es decir, debe cubrir todos los aspectos relacionados con el sistema.

- Debe proteger el sistema en todos los niveles: físico, humano, lógico y logístico.

- Debe tener en cuenta no sólo los distintos componentes del sistema, tales como el hardware, software, entorno físico y usuarios, sino también la interacción entre los mismos.

- Debe tener en cuenta el entorno del sistema, esto es, el tipo de compañía o entidad con que tratamos (comercial, bancaria, educativa, etc.) De esta consideración surge la segunda regla básica:

La política de seguridad debe adecuarse a nuestras necesidades y recursos, el valor que se le da a los recursos y a la información, el uso que se hace del sistema en todos los departamentos.

- Deben evaluarse los riesgos, el valor del sistema protegido y el coste de atacarlo. Las medidas de seguridad tomadas deben ser proporcionales a estos valores.

Toda política de seguridad debe basarse fundamentalmente en el sentido común. Es necesario:

a) Un conocimiento del sistema a proteger y de su entorno.

b) Un conocimiento y experiencia en la evaluación de riesgos y el establecimiento de medidas de seguridad.

c) Un conocimiento de la naturaleza humana, de los usuarios y de sus posibles motivaciones.

A la hora de establecer una política de seguridad debemos responder a las siguientes tres preguntas:

- ¿ Qué necesitamos proteger?
- ¿ De qué necesitamos protegerlo?
- ¿ Cómo vamos a protegerlo?

Esto nos lleva a los siguientes pasos básicos:

1. *Determinar los recursos a proteger y su valor.*

2. *Analizar las vulnerabilidades y amenazas de nuestro sistema, su probabilidad y su coste.*

3. *Definir las medidas a establecer para proteger el sistema.* Estas medidas deben ser proporcionales a lo definido en los pasos 1 y 2 y establecerse a todos los niveles: físico, lógico, humano y logístico, además debe definirse una estrategia a seguir en caso de fallo.

4. *Monitorizar el cumplimiento de la política y revisarla y mejorarla cada vez que se detecte un problema.*

Los pasos 1 y 2 se denominan **Análisis de riesgos**, mientras los pasos 3 y 4 se designan **Gestión de riesgos**. *La **política de seguridad** es el conjunto de medidas establecidas en el paso 3.*

3.1.2 Análisis y Gestión de Riesgos

El objetivo de la Seguridad en los Sistemas de Información es mantener la confidencialidad, integridad y disponibilidad de la información. Una violación de la seguridad es cualquier suceso que compromete estos objetivos. *El Análisis y Gestión de Riesgos* es un método formal para investigar los riesgos de un SI y recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

En toda evaluación de riesgos deben tenerse en cuenta tres costes o valores fundamentales:

- ***Cr***: *Valor de nuestro sistema informático*, esto es, de los recursos y la información a proteger.
- ***Ca***: *Coste de los medios necesarios* que requeriría un criptoanalista para romper las medidas de seguridad establecidas en nuestro sistema.
- ***Cs***. *Coste de las medidas de seguridad necesarias* para salvaguardar los bienes informáticos.

Para que la política de seguridad de nuestro sistema sea lógica debe cumplirse la siguiente relación:

$$Ca > Cr > Cs$$

El que ***Ca sea mayor que Cr*** significa que ***el ataque a nuestro sistema debe ser más costoso que su valor.*** Así, los beneficios obtenidos de romper nuestras medidas de seguridad no deben compensar el coste de desarrollar el ataque.

El que ***Cr sea mayor que Cs*** significa ***que no debe costar más proteger la información que la información protegida***. Si esto ocurriese, nos resultaría más conveniente no proteger nuestro sistema y volver a obtener la información en caso de pérdida.

3.1.3 Evaluación del valor del sistema informático (Cr)

Al evaluar el sistema informático al cual se desea brindar seguridad, su valor puede desglosarse en dos partes fundamentales:

- El valor intrínseco del producto a proteger.

- Los costes derivados de su pérdida.

Valor intrínseco

Es la parte más sencilla de valorar, puesto que en la mayoría de los casos podemos establecer unos valores objetivos y medibles de nuestros recursos e información. Se trata de enumerar los recursos incluidos en el sistema informático y de establecer su valor.

Por ejemplo, un servidor de un departamento donde trabajan varios grupos de investigación podría valorarse del siguiente modo:

- Valor del hardware. La computadora y de sus periféricos.
- Valor del software. Programas y aplicaciones.
- Valor de los resultados de investigación, patentes, etc., almacenados.
- Coste del esfuerzo y material invertido para obtener los datos.
- Valor de la información personal que contiene.

Costes derivados

Son bastante más difíciles de enumerar y cuantificar que los anteriores. Dependiendo del tipo de sistema con que tratemos pueden ser muy distintos, o su valor e importancia relativa pueden variar enormemente. En términos generales podemos incluir los siguientes conceptos:

- Valor de sustituir el hardware.
- Valor de sustituir el software.
- Valor de los resultados.
- Coste de reproducir los experimentos significativos.
- Coste de regenerar la información personal.

Para comprender la variabilidad de este tipo de costes consideremos un par de casos:

Si la información perdida incluye los datos de planificación y el desarrollo de una campaña publicitaria en un entorno muy competitivo, p.e. el de las bebidas refrescantes, el valor de los datos perdidos y las consecuencias para la compañía pueden superar con mucho el coste de las horas invertidas o de los recursos utilizados.

Existe un valor intangible muy superior al valor material en este tipo de información. Además en este caso puede entrar en juego el prestigio de la compañía. Este factor tiene un valor incalculable de cara a su imagen y a su capacidad de ventas. Si se conoce que los datos han sido robados puede suponer un golpe muy duro para las ventas de la compañía.

De hecho ésta es la razón por la que muchas compañías comerciales no comunican los ataques a sus sistemas.

El factor prestigio también tiene una importancia capital en las entidades bancarias o en las entidades públicas y sobretodo las de defensa. Imaginemos como reaccionaríamos ante un banco en el que tenemos una cuenta y de la que conocemos que han sido robados los datos personales y financieros de todos sus clientes.

Otro ejemplo de la dificultad de valorar ciertas pérdidas puede ser el relativo a los datos personales. ¿Qué valor le otorgamos a nuestros datos personales, expedientes académicos, datos sanitarios, información sobre nuestras cuentas o los datos de nuestros seguros, nuestra siniestralidad, morosidad, etc.?

Aparte de afectar a nuestro prestigio personal, impedir que abramos una cuenta bancaria o que concertemos un seguro, pueden servir a otros para suplantarnos, y otorgarles impunidad para cometer crímenes o realizar gastos imputándonoslos a nosotros.

En resumen, aunque en principio pueda parecer fácil la valoración de los bienes protegidos, pueden existir numerosos costes ocultos inherentes a su pérdida o compromiso que sólo un análisis detallado puede revelar y que a menudo requieren una valoración por alguien con experiencia en seguridad en conjunción con expertos especializados en el tratamiento de los bienes protegidos.

3.1.4 Cuantificación de los riesgos

Cuando se han identificado los riesgos debe estimarse la probabilidad de que ocurra cada uno de ellos. Esto puede ser más sencillo si se consideran ocurrencias anuales.

La cuantificación de riesgos es un trabajo pesado. Algunas estimaciones se pueden obtener de terceros, por ejemplo las compañías de seguros. Si algo sucede en forma regular, la estimación puede basarse en los registros históricos. Las organizaciones industriales pueden haber recopilado estadísticas o reportes que se han publicado. También es posible hacer estimaciones con base en cálculos serios extrapolados de la experiencia. Por ejemplo:

- La compañía de luz puede proporcionar una estimación oficial de la probabilidad de que un edificio en particular sufra una interrupción del servicio durante el próximo año. También es posible que pueda cuantificar el riesgo de que la interrupción dure unos cuantos segundos o que dure minutos u horas.

- La compañía de seguros puede proporcionar información actuarial sobre la probabilidad de muerte del personal clave según su edad y estado de salud.

- Los registros personales pueden utilizarse para calcular la probabilidad de la salida de empleados clave en el área de cómputo.

- La experiencia y la extrapolación inteligente pueden permitir apreciar la probabilidad de que se descubra que los programas de un cierto proveedor contengan errores serios durante el próximo año (tal vez 100%).

Si se espera que algo suceda más de una vez al año hay que anotar cuántas veces se espera que suceda. Si se espera que ocurra un terremoto serio una vez cada cien años se pone 1% en la lista, pero si se espera descubrir tres errores serios en sendmail durante el próximo año se anota 300%.

Se deben revisar los riesgos

El análisis de riesgos no debe hacerse sólo una vez y después olvidarse, sino que es necesario actualizarlo periódicamente. Además, la parte relativa a la evaluación de amenazas debe repetirse cada vez que la operación y la estructura cambian en forma significativa. Si ocurre una reorganización, se hace una mudanza a otro edificio, se cambian proveedores o suceden otros cambios importantes se tienen que volver a evaluar las amenazas y las pérdidas potenciales.

3.1.5 Análisis de costo-beneficio

Al terminar el análisis de riesgos es necesario asignar un costo a cada riesgo, y determinar el costo de defenderse. A esto se le llama análisis de costo-beneficio.

Costo de las pérdidas

Calcular las pérdidas puede ser muy difícil. En forma simple se toma en cuenta el costo de reparar o sustituir un ítem. Una evaluación más sofisticada puede tomar en cuenta el costo de no disponer del equipo, de la capacitación adicional requerida, de los procedimientos adicionales que resulten de la pérdida, el costó de la reputación de la empresa e incluso el costo a los clientes. En general, la inclusión de más factores en el análisis de costos implicará más trabajo, pero mejorará su precisión.

Para la mayor parte de los propósitos no se requiere asignar un valor exacto a cada riesgo posible. Normalmente es suficiente un rango de costos para cada ítem. Por ejemplo la pérdida de una docena de disquetes en blanco se puede clasificar como "menor que 500 dólares", mientras que un incendio destructivo en la sala de cómputo puede clasificarse como "mayor que 1000000 de dólares". Algunos ítems se pueden clasificar como "irreparables / insustituibles", por ejemplo la base de datos de contabilidad completa o la muerte de un empleado clave.

Puede ser conveniente asignar estos costos con una escala de pérdida más fina que simplemente "pérdida / no pérdida". Por ejemplo, si se quiere asignar costos separados a cada una de las siguientes categorías (no se han ordenado por importancia):

- Interrupción de corto plazo (menos de 7 a 10 días)
- Interrupción de mediano plazo (una o dos semanas)
- Interrupción de largo plazo (más de dos semanas)

- Destrucción o pérdida permanente
- Pérdida o daño parcial accidental
- Pérdida o daño parcial intencional
- Divulgación no autorizada interna
- Divulgación no autorizada a algunos extraños
- Divulgación completa a extraños, competidores y a la prensa
- Costo de reemplazo o, recuperación

Costo de prevención

Para terminar hay que calcular el costo de prevenir cada tipo de pérdida.

Por ejemplo, el costo de recuperarse de una falla momentánea de potencia puede ser sólo el tiempo de inactividad del personal además del tiempo necesario para reiniciar el equipo. Pero el costo de la prevención puede ser la adquisición de un sistema de potencia ininterrumpida.

El costo debe amortizarse a lo largo de la vida esperada de las opciones, según sea apropiado. La obtención de estos costos puede revelar costos secundarios o ingresos que también deben tomarse en cuenta. Por ejemplo, la instalación de un sistema contra incendios mejor puede hacer que disminuyan las primas del seguro contra incendios y además representar un beneficio fiscal adicional por depreciación de capital. Pero gastar dinero en un nuevo sistema contra incendios significa que el dinero no estará disponible para otras cosas, tales como capacitación de personal, o incluso para invertirlo.

Ejemplos de costo-beneficio

Supóngase, por ejemplo que existe una probabilidad de 0.5 % de que una sola interrupción de potencia dure más de unos cuantos segundos en un año. La pérdida esperada por tener al personal sin hacer nada es 25 000 dólares y el costo de recuperación (manejar la reiniciación y la revisión de discos) es de 10 000 dólares, más el tiempo perdido y costos de personal. Esto indica que la pérdida esperada y el costo de recuperación es de (25 000 + 10 000) x 0.005 = $175. Si el costo de un sistema de potencia ininterrumpida que pueda satisfacer sus necesidades es de 150 000 dólares y tiene una vida esperada de diez años, entonces el costo de evitar el riesgo es de 15 000 dólares por año. Claramente, invertir en un sistema de potencia ininterrumpida no conviene.

Supóngase, como segundo ejemplo, que la divulgación de la contraseña de cualquier empleado pudiera dar como resultado que un extraño lograra acceso a información privada con valor de 1000 000 de dólares. No hay recuperación posible, porque se perdería la clasificación de secreto comercial, la cual no se recupera si se pierde.
Hay 50 empleados que usan su red mientras viajan, y la probabilidad de que uno de ellos accidentalmente revele su contraseña (por ejemplo, por "husmeo" en Internet) es 2%.

Así, la probabilidad de que se pierda por lo menos una contraseña en un año dado es de 63.6%. t, es decir, 1 - (1.0- 0.02) 50. La pérdida esperada es (1000 000 + 0) x 0.636 = $636 000. Si el costo de evitar este riesgo es comprar una tarjeta que contenga una contraseña descartable de 75 dólares para cada empleado, más 20 000 del programa, y el sistema servirá durante cinco años, entonces el costo de evitar el riesgo es (50 * 75 + 20 000) / 5 = $4750 al año. Es muy claro que se debería comprar ese sistema.

Cómo sumar las cifras

Al término del proceso se debe tener una matriz multidimensional que consista de activos, riesgos y posibles pérdidas. Para cada pérdida hay, que tener una probabilidad, la pérdida estimada y la cantidad de dinero que se requiere para defenderse de esa pérdida. Si se quiere ser preciso es necesario incluir la probabilidad de que la defensa falle.

El proceso de determinar si cada defensa debe emplearse o no es ahora directo. Se hace multiplicando cada pérdida esperada por la probabilidad de que ocurra como resultado de cada amenaza. Los resultados se ponen en orden descendente y se compara el costo del suceso con el costo de su defensa.

Esta comparación tiene como resultado una lista en orden de prioridad de lo que se debe hacer. La lista puede ser sorprendente. El objetivo debe ser evitar pérdidas caras y probables antes de preocuparse de pérdidas menos probables y poco cuantiosas. En muchos ambientes, los incendios y la pérdida de personal clave son mucho más probables y dañinos que los virus o los intrusos que usen la red.

Es sorprendente que los intrusos y los virus parecen acaparar la atención y los presupuestos de los administradores. Esto no es eficiente, ni mejora la confianza que se tenga en el sistema en su conjunto.

No es posible eliminar los riesgos

Se pueden identificar y reducir los riesgos, pero no se pueden eliminar por completo.

Por ejemplo, se puede adquirir un sistema de potencia ininterrumpida para reducir el riesgo de que una interrupción de potencia dañe los datos. Pero esta unidad puede fallar cuando se necesite. La interrupción puede durar más que la duración de las baterías. El personal de limpieza puede haber desconectado la unidad para conectar su pulidora.

Un análisis cuidadoso de riesgos permitirá identificar estos riesgos secundarios e incorporarlos a los planes. Por ejemplo, se puede comprar otra unidad de potencia ininterrumpida. Pero claro, ambas podrían fallar al mismo tiempo. Puede suceder una interacción entre ellas que no se tomó en cuenta cuando se instalaron. La probabilidad de que se interrumpa la potencia disminuye a medida que se adquieren más unidades de respaldo, pero nunca llega a cero.

El análisis de riesgos ayuda a protegerse de riesgos humanos y naturales. Por ejemplo, puede ayudar a protegerse de intrusos identificando los: riesgos y las medidas de protección. Pero tal como sucede con las fallas de potencia, no se puede eliminar la posibilidad de que alguien penetre en una computadora.

Esto es fundamental para la seguridad informática: no importa qué tanto se asegure una computadora si el enemigo tiene suficiente tiempo, recursos, motivación y dinero para lograr penetrarla.

Hasta los sistemas que están certificados según el "Libro Naranja" del Departamento de Defensa de Estados Unidos son susceptibles de penetración. Una razón es que a veces los sistemas no están bien administrados. Otra es que algunos usuarios pueden aceptar sobornos para violar la seguridad. Los controles de acceso no sirven si no se administran bien. Tal como una cerradura no sirve para nada si el vigilante es quien está robando equipo a las 2 a.m.

Con frecuencia la gente es el eslabón más débil de un sistema de seguridad. El sistema más seguro del mundo está totalmente abierto si el administrador coopera con quienes quieren penetrar. Las personas se pueden comprometer con dinero, amenazas o argumentos ideológicos. También pueden equivocarse, por ejemplo, enviando correo electrónico que contenga contraseñas a una persona equivocada.

En realidad es más barato y fácil comprometer a una persona que a las salvaguardas tecnológicas.

Para decidir qué hacer se deben estudiar las cifras que se han obtenido sobre prevención y, recuperación, y analizar cómo se pueden atender los ítems de más alta prioridad. Para lograrlo hay que sumar el costo de recuperación a las pérdidas promedio, y multiplicar ese resultado por la probabilidad de que suceda el evento. Se debe comparar, el resultado con el costo de prevención. Si el costo de prevención es menor que el de la defensa del riesgo es recomendable invertir en la estrategia de prevención si se cuenta con los recursos para hacerlo. Si el costo de prevención es mayor que el de la defensa no debe hacerse nada hasta que se hayan atendido otras amenazas.

Cómo convencer a los directivos

La seguridad no es gratuita. Las medidas más complicadas de seguridad son más caras. Los sistemas más seguros son más difíciles de usar, aunque esto no tiene porque ser así.

La seguridad puede estorbar a los usuarios "avanzados" que muchas veces quieren llevar a cabo operaciones difíciles y a veces peligrosas sin autenticación o responsabilidad. Estos usuarios avanzados pueden ser muy poderosos dentro de una organización.

Al terminar el análisis de riesgos y el de costo-beneficio se debe convencer a los directivos de la organización que es necesario actuar. Normalmente se formularía una política que se adoptaría oficialmente. Con frecuencia, ésta es una marcha cuesta arriba. Afortunadamente no hay razón para que esto suceda.

El objetivo del análisis de riesgos y de costo-beneficio es asignar prioridades a las acciones y al gasto en seguridad. Si el plan de negocios sugiere que no se acepte ningún riesgo mayor a 10 000 al año, sin seguro, se puede emplear el análisis realizado para determinar cuánto hay que gastar para lograr este objetivo. El análisis es también una guía sobre qué debe hacerse primero, qué debe hacerse después y para identificar lo que puede dejarse para muchos años después.

Otro beneficio del análisis de riesgos es que ayuda a justificar ante los directivos las necesidades de recursos adicionales para la seguridad. Una gran cantidad de administradores y directores no sabe mucho sobre computadoras, pero entiende lo que es un riesgo y los análisis de costo-beneficio. Si se puede demostrar que una organización se enfrenta a un riesgo que podría ascender a 20 000000 de dólares al año (incluyendo las pérdidas y los costos de recuperación de lo que se tiene), esta estimación ayudará a convencer a la administración de que asigne dinero para aumentar el personal y los recursos.

Por otra parte, si se llega a decir a la administración vagamente "Es muy probable que suframos varias penetraciones desde Internet después de la próxima recomendación del CERT", es poco probable que se logre algo más que una leve preocupación (si acaso)

3.1.6 Problemas en la definición de políticas

Las Políticas de Seguridad son difíciles de aceptar por algunos administradores, debido generalmente a que en el pasado han existido problemas con su desarrollo. Los administradores se han enfrentado a grandes presiones para instalar alguna suerte de sistemas de protección en sus organizaciones, especialmente después de la ocurrencia de un incidente o violación a los sistemas. Además, si el establecimiento de políticas hace más lento el proceso de instalación de protecciones, la estructura demandante de servicios ejerce también grandes presiones para saltar este paso.

Los administradores también asocian las políticas de seguridad con burocracia. En efecto, el término "Política de Seguridad" evoca imágenes de la organización de la seguridad a

nivel corporativo generando textos, haciendo ir al personal a aburridas reuniones y en general, haciéndole la vida difícil a quienes sólo tratan de hacer su trabajo. Este punto de vista es desafortunado dado que la organización de la seguridad a nivel corporativo juega un papel importantísimo en la protección de la información, además de que las políticas definidas deben ser parte del trabajo diario de todo el personal.

En muchas ocasiones la documentación se elabora y se guarda sin que nadie lea su contenido. Esta situación tan típica minimiza el gran esfuerzo de la organización de seguridad y el espíritu y propósito de las políticas.

3.1.7 Consideraciones para realizar políticas

Crear políticas es, por definición, especificar las necesidades de control de acceso a la información. En particular, las políticas deberán reflejar los objetivos de la Institución con respecto a la relativa importancia de cada rubro a proteger y la manera en que esa información contribuye a la misión de cada Institución. Por su parte, las normas, procedimientos, prácticas y estándares, deberán acoplar esas necesidades con los recursos técnicos existentes en la Institución e incidirán en su caso en la modernización de los esquemas técnicos de seguridad.

Una manera formal de iniciar la generación de políticas, es el atacar tópicos básicos con fundamento en aspectos generales, aplicables al entorno de responsabilidad de todas las Instituciones. Este paso deberá enriquecerse con aspectos específicos a cada entorno en particular.

3.2 Estructura jerárquica de las políticas de seguridad en la información

Identificar la ubicación jerárquica de las Políticas de Seguridad dentro de la Dependencia, permite por un lado, hacia arriba, mantener la congruencia con los objetivos institucionales, y por otro, hacia abajo, normar los procedimientos de operación en observancia a las Políticas de Seguridad definidas.

Es evidente que entre más alto sea el nivel jerárquico de los enunciados regulatorios, las modificaciones serán mínimas, pero serán más generales y legislativamente más robustos, mientras que los niveles inferiores estarán más apegados a soluciones muy concretas, por lo que su modificación puede ser más frecuente.

A continuación en la fig. 3.1 se presenta la estructura jerárquica por bloques que comprende todos los niveles en que un enunciado regulatorio es definido.

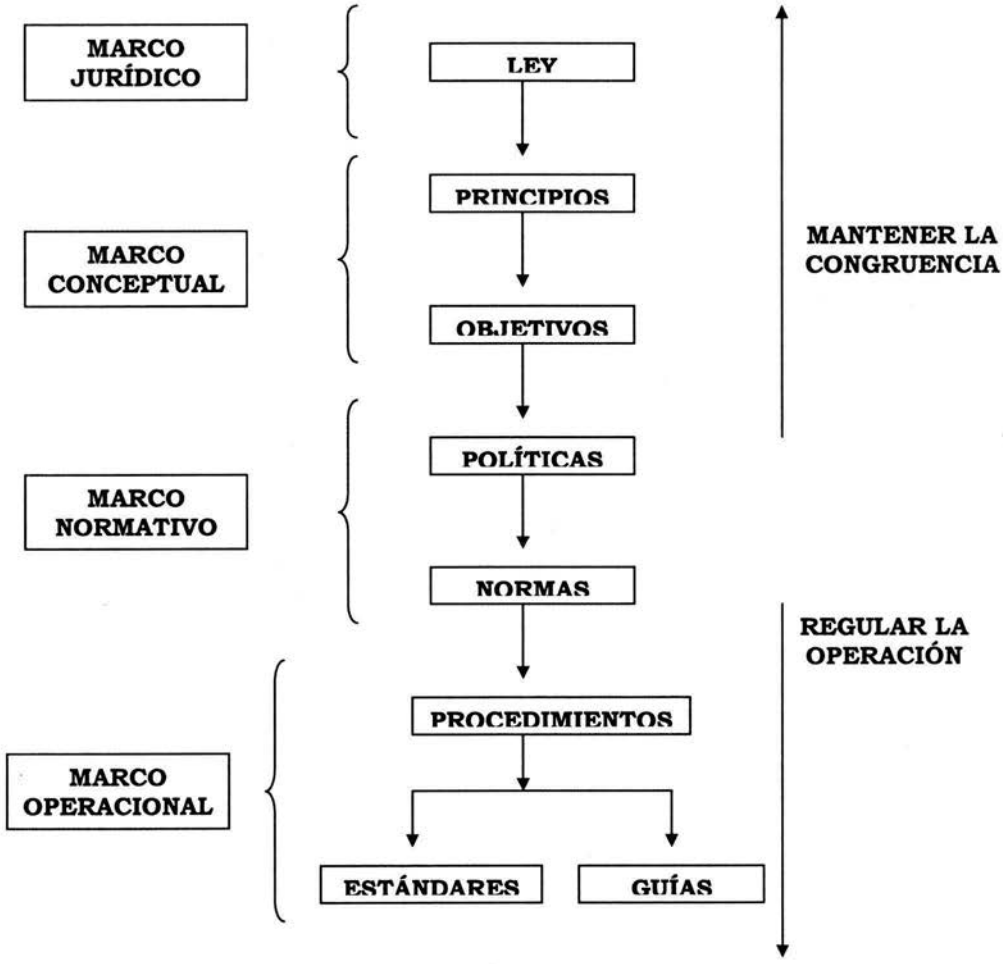

Fig. 3.1 Estructura jerárquica de las políticas de seguridad en la información

Descripción de la estructura:

Marco Jurídico.- Define la Ley o Leyes que dan origen a la creación por decreto de la Institución o Dependencia, la cual mantendrá su vigencia o espíritu mientras encuentre el sustento jurídico que permite su existencia.

Ley.- Sustenta la existencia legítima de la Institución.

Marco Conceptual.- Es el espíritu institucional dentro del que se engloban los valores y metas de la Institución, en concordancia con la naturaleza de la ley que la origina.

- Principios.- Esencia moral y ética de la Institución.
- Objetivo.- Propósito de la Institución.

Marco Normativo.- Es el conjunto de preceptos que regulan la conducta institucional con el fin de llevar a buen término sus objetivos.

- Políticas.- Forma en que se cumple con el objetivo .
- Normas.- Regla específica que debe cumplirse; su omisión causará la sanción respectiva.

Marco Operacional.- Es el conjunto de elementos de orden que definen la operación de los esquemas de manejo de información.

- Procedimientos.- Son instrucciones precisas para el desarrollo de actividades.
- Estándares.- Procedimientos apegados estrictamente a la norma.
- Guías.- Procedimientos dirigidos u orientados, susceptibles de ser comentados o interpretados.

Como se observa, los procedimientos pueden ser estándares o guías; cuando sólo se recomienda la manera de hacer alguna tarea específica, se emite una guía, misma que no es obligatoria, sino una sugerencia de acción; por otro lado, un estándar es mucho más riguroso, y es de observancia obligatoria; cuando las guías son adoptadas y probadas en su efectividad, pueden pasar a ser estándares.

Vulnerabilidad, amenazas y contramedidas

Hay tres conceptos que entran en discusión cuando hablamos de la seguridad de un sistema informático: vulnerabilidad o inseguridad (vulnerability), amenazas (threat) y contramedidas (countermesures)

Vulnerabilidad

Punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático.

Amenaza

Posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, etc.), o un suceso natural o de otra índole (fuego, inundación, etc.) Representan los posibles atacantes o factores que pretenden aprovechar las debilidades del sistema.

Contramedida

Técnicas de protección del sistema contra las amenazas.

La seguridad informática se encarga no sólo de la identificación de las amenazas sino también de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades.

Una máxima de la seguridad informática es que: "No existe ningún sistema completamente seguro". Existen sistemas más o menos seguros, y más o menos vulnerables, pero la seguridad nunca es absoluta.

3.3 Políticas de seguridad

Cuando se habla de un documento de Políticas de Seguridad, no se trata de un documento general, ya que por definición debe responder a las necesidades y características de la Institución que incorpora las políticas; se refiere a un documento dinámico, es decir, que requiere de constante revisión para mantenerlo vigente, no por exaltarlo o por ocio, sino por cuestiones de legítima seguridad, sobre todo en ámbitos tan cambiantes como lo es la Internet, donde la vigencia de las soluciones técnicas y administrativas es de primordial importancia para mantener nuestros sistemas confiables.

Es por lo anterior que se denominará inicial al documento, además, debe ser objeto de "mantenimiento" periódico, de revisión y mejora constante, y será compromiso de los responsables de la implantación de Políticas de Seguridad, lograr el éxito en esta empresa.

3.3.1 Estructura de las políticas de seguridad

Dependiendo de la amplitud de las situaciones que pretenda abarcar una política, la misma puede ser clasificada en los siguientes niveles jerárquicos:

Niveles de Políticas:

- Política general: Visión de seguridad respecto a todo el servicio de Internet.
- Política específica a un tema: Se orienta a tópicos que tienen un interés específico.
- Política particular a una aplicación: Se enfoca a decisiones tomadas por la administración para proteger aplicaciones o sistemas particulares.

Partiendo de las políticas generales, el grado de detalle y complejidad requerido aumenta conforme se avanza hacia las políticas particulares. Así mismo, entre más detallada y compleja es una política, se requiere actualizarla más frecuentemente y es más complicado el proceso de implantación de la misma.

Por otro lado, **de acuerdo al recurso al que está dirigida una política, ésta puede ser clasificada en los siguientes tipos básicos:**

- **Orientada a los recursos lógicos**: Cuando el recurso tiene que ver con las técnicas empleadas para generar, explotar o intercomunicar tanto aplicaciones como los datos asociados a las mismas.
- **Orientada a la gestión**: Cuando el recurso tiene que ver con aspectos administrativos, de personal o con la misma estructura organizacional de la Dependencia.
- **Orientada a los recursos físicos**: Cuando se trate de bienes materiales como instalaciones y equipos.
- **Orientada a la respuesta ante incidentes**: Cuando se trate de los recursos empleados durante y después de una contingencia.

3.3.2 Lista de verificación para la redacción de políticas de seguridad

El estilo con el que se redacte una política debe tomar en cuenta la cultura organizacional de la Dependencia.

La redacción de cualquier política debe ser lo suficientemente clara como para evitar confusiones y no generar nuevos problemas. Por esta razón se debe considerar que sea comprendida por la mayoría de los empleados de la Institución.

Con el propósito de verificar que el contenido de una política sea el apropiado, a continuación se propone una lista de seis puntos que normalmente deben estar incluidos en su enunciado.

1. Qué es lo que se pretende proteger.
2. Sobre quién recae la responsabilidad.
3. En dónde se aplica dentro de la Dependencia (alcance).
4. Cómo se verificará su cumplimiento (monitoreo).
5. A partir de cuándo tendrá efecto la política (vigencia).
6. Por qué se creó la política.

Aunque es importante considerar los seis puntos durante la redacción de una política, los tres primeros siempre deberán estar reflejados en el enunciado final de la política, mientras que los tres últimos se pueden tomar como optativos.

3.3.3 Procedimientos y políticas de seguridad

El objetivo de desarrollar una política de seguridad informática, es definir las expectativas de una institución respecto al uso adecuado del equipo y de la red, así como los procedimientos precisos para prevenir y responder a los incidentes de seguridad.

Las nuevas políticas de seguridad para una empresa deben ajustarse a las mismas políticas, normas, regulaciones y leyes que ya existen en la organización.

3.3.4 Esquema de seguridad

Como primer punto, es necesario hacer énfasis en que el apoyo por parte de la gente con el poder de decisión dentro de la empresa o institución es fundamental para el éxito de un esquema de seguridad, ya que sin él algunos elementos del esquema no podrán aplicarse, como podría ser el caso de las políticas y procedimientos.

Los usuarios deben conocer el uso adecuado de los sistemas de cómputo y saber cómo protegerse a sí mismos de accesos no autorizados. Debe crearse una cultura de seguridad, haciendo ver a la gente involucrada los peligros a los que se está expuesto en un ambiente tan hostil como el que ha generado la evolución de las actuales redes de computadoras.

El primer paso a considerar en un esquema de seguridad, que muchas veces no recibe suficiente atención, el cual no es uno de los objetivos de esta tesis, es la seguridad física, las medidas que se usan para proteger las instalaciones en las que reside un sistema de cómputo: llaves, candados, tarjetas de acceso, puertas, ventanas, alarmas, vigilancia, etc.

No se puede pasar por alto la importancia de la seguridad física, ya que es parte de un modelo general de seguridad de todo sistema informático.

El siguiente cuadro (ver **cuadro 3.1**) presenta el esquema que se describe en este capítulo para mantener la seguridad en un sistema de computo en el ámbito general basado en las políticas de seguridad y procedimientos que cualquier institución pueda tener.

Cuadro 3.1: Esquema de seguridad para un sistema de cómputo

3.4 Políticas y procedimientos de seguridad

Políticas de seguridad son los documentos que describen la forma adecuada para hacer uso de los recursos de un sistema de cómputo, las responsabilidades, derechos y acciones que tanto usuarios como administradores tienen y deben hacer ante un incidente de seguridad.

Mientras las políticas indican el "qué", los procedimientos indican el "cómo". Estos últimos son los que nos permiten llevar a cabo las políticas. Ejemplos que requieren la creación de un procedimiento son:

- Otorgar una cuenta
- Dar de alta a un usuario
- Conectar una computadora a la red
- Localizar una computadora
- Actualizar el sistema operativo
- Instalar software localmente o vía red
- Actualizar software crítico
- Exportar sistemas de archivos
- Respaldar y restaurar información
- Manejar un incidente de seguridad

Las políticas son parte fundamental de cualquier esquema de seguridad eficiente. A los administradores les aminora los riesgos, y les permite actuar de manera rápida y acertada en caso de haber una emergencia de cómputo. A los usuarios, les indica la manera adecuada de usar un sistema, indicando lo que puede hacerse y lo que debe evitarse en el sistema. El tener un esquema de políticas facilita grandemente la introducción de nuevo personal, teniendo ya una base escrita y clara para capacitación, dan una imagen profesional a la organización y facilitan una auditoria.

Los principales puntos que deben contener las políticas de seguridad son:

- Ámbito de aplicación
- Análisis de riesgos
- Enunciados de políticas
- Sanciones
- Sección de uso ético de los recursos de cómputo
- Sección de procedimientos para el manejo de incidentes

Para que las políticas se puedan llevar a cabo deberán tener las siguientes características:

- Apoyadas por los directivos
- Únicas
- Claras (explícitas)
- Concisas (breves)

- Bien estructuradas
- Servir de referencia
- Escritas
- Revisadas por abogados
- Dadas a conocer
- Entendidas por los usuarios
- Firmadas por los usuarios
- Mantenerse actualizadas

A continuación se describen algunas de las políticas que se pueden aplicar en el ámbito general en cualquier institución o empresa.

3.4.1 Políticas de responsabilidades del usuario

Para la creación de políticas, en donde el usuario es el principal actor, se deben considerar algunos de los siguientes aspectos, con los cuales queden establecidos los lineamientos a seguir.

- Guías respecto al uso de recursos de red en caso de que los usuarios estén restringidos y cuáles son las restricciones.
- Lo que constituye abuso en los términos del uso de los recursos de red que afectan el desempeño del sistema y la red.
- ¿Podrán los usuarios compartir sus cuentas o permitir a otros utilizarlas?
- ¿Deberían los usuarios revelar sus contraseñas de manera temporal para permitir a quienes trabajan en un proyecto el acceso a sus cuentas?
- Con qué frecuencia deberían cambiar sus contraseñas los usuarios y cualesquiera otras restricciones de contraseña o requerimientos
- ¿Son responsables los usuarios de brindar respaldo de sus datos o es responsabilidad del sistema?
- Consecuencias para los usuarios que divulgan información que podría ser propietaria.
- Una declaración sobre la privacidad de correo electrónico.
- Una política sobre comunicaciones electrónicas como falsificación de correo.

La lista de políticas descritas a continuación, es dirigida principalmente a todos y cada uno de los usuarios que conforman un sistema.

1. La cuenta de usuario es personal e intransferible, por lo cual no se permite que éste comparta su cuenta y contraseña con persona alguna, aún si está acredita la confianza del usuario.

2. Para reforzar la seguridad de la información de la cuenta, el usuario bajo su criterio deberá hacer respaldos de su información dependiendo de la importancia y frecuencia del cambio de la misma.

3. Está estrictamente prohibido ejecutar programas que intenten adivinar las contraseñas.

4. Está estrictamente prohibido hacer uso de programas que exploten alguna vulnerabilidad para proporcionar privilegios no otorgados explícitamente por el administrador.

5. La contraseña del usuario no debe de ser obvia.

6. Está estrictamente prohibido copiar software que no le haya sido autorizado.

7. El usuario tiene la obligación de abandonar la sesión de trabajo, si ésta no es utilizada por un tiempo considerado.

8. La contraseña debe de ser cambiada de inmediato si el usuario detecta o asume que ésta ha sido identificada por descuido o por otro medio.

9. Está estrictamente prohibido crear nombres de archivos que hagan referencia a los comandos propios del sistema.

10. Ninguna cuenta de usuario podrá ser usada para propósitos ilegales.

11. Cuando el usuario deje de tener alguna relación oficial con la institución o la cuenta deje de ser utilizada por un tiempo definido por los administradores, ésta debe ser removida.

12. Cuando el usuario deje de laborar o de tener una relación con el instituto, éste debe notificarlo al administrador de sistemas para proceder y tomar las medidas pertinentes con su información y cuenta de acceso.

13. Nadie puede ver, copiar, alterar o destruir la información de un usuario sin el consentimiento explícito del afectado.

14. Está estrictamente prohibido crear cuentas (si se cuenta con privilegios para hacerlo) sin autorización del administrador.

15. Está estrictamente prohibido crear sistemas de archivos en áreas de los sistemas no autorizadas.

3.4.2 Política de responsabilidades de los administradores del sistema

Cuando ocurren los ataques a la seguridad de la red, el administrador del sistema podrá examinar los directorios y archivos privados del usuario para el diagnóstico del problema hasta cierto límite estipulado por la política del sistema o red. Las preguntas clave para diseñar las políticas de este tipo son:

- ¿Quién debe tener privilegios de administrador? - Debe utilizarse el principio del mínimo privilegio: Proporcionar sólo los privilegios suficientes para ejecutar las tareas necesarias
- ¿Cuáles son los derechos y responsabilidades de los administradores?
- ¿Pueden monitorear o leer los archivos de los usuarios?
- ¿Tienen derecho a examinar el tráfico de una máquina en específico?
- ¿Tienen derecho a examinar el tráfico de toda la red?
- ¿A qué grado pueden hacer uso de sus privilegios?
- ¿Qué tanto deberán respetar la privacía de los usuarios?
- ¿Cómo deben resguardar su contraseña?
- ¿Cómo debe manejarse la información sensitiva?
- Debe evitarse que los usuarios almacenen información valiosa en sistemas poco seguros.

Así como los usuarios, los administradores también deberán estar sujetos a normas para proporcionar una seguridad más eficaz en el tratamiento de la información. Políticas como las que se describen a continuación son las que deberá seguir toda persona que se dedica a la administración de un sistema de cómputo.

16. La contraseña del administrador (o contraseña de *root)* debe ser cambiada de inmediato si éste detecta o asume que ha sido identificada por descuido o por otro medio.

17. Tiene la obligación de validar que los nombres de archivos no hagan referencia a los comandos propios del sistema.

18. El administrador debe auditar periódicamente los sistemas y los servicios de red, para verificar que no existen archivos no autorizados, configuraciones inválidas o permisos extra que pongan en riesgo la seguridad de la información.

19. El administrador no podrá remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche ser de algún intruso utilizando una cuenta ajena.

20. El administrador debe hacer respaldos periódicamente del Sistema Operativo de las máquinas que tengan a su cargo.

21. Es responsabilidad del administrador revisar periódicamente las bitácoras de los sistemas a su cargó.

Dentro de las políticas de un administrador están también las "Políticas sobre el sistema y servicios de red", no se hace una separación de éstas con las del administrador ya que, también son su responsabilidad, por ello deberá de configurar los sistemas y generar las cuentas asignando sus respectivas contraseñas como se puntualiza en la siguiente lista.

22. La configuración de los sistemas debe ser estándar a todos los equipos y revisada periódicamente.

23. Se debe proveer la instalación de un sistema de contraseñas cuyo mecanismo impida reutilizar los mismos y obligue al usuario al cambio periódico y la elección de contraseñas únicas y robustas.

24. Se debe normar el uso de los recursos del sistema y de la red, restricción de directorios, permisos y programas para ser ejecutados por los usuarios.

25. No está permitido hacer uso de huecos en la seguridad, programas o accesos no autorizados que alteren la seguridad, consistencia o que dañen cualquier sistema de cómputo.

26. En caso de que los sistemas se encuentren comprometidos por algún hacker o por cualquier amenaza a la seguridad del sistema y si así se requiere por los encargados, el usuario tiene la obligación de cambiar su contraseña y colaborar en lo que sea necesario. Si por alguna razón se percata de cualquier hueco, falla de seguridad o inconsistencia en cualquier sistema de cómputo, está obligado a reportarlo a los administradores del mismo.

27. Está prohibido a los usuarios tener acceso remoto a computadoras y equipo de red que no se le hayan designado explícitamente.

28. Está prohibido el uso remoto de servicio que permita averiguar direcciones de otros usuarios sobre la Red y permitan contar a los demás sobre la Red más detalles sobre uno mismo, como el finger.

3.4.3 Políticas de respaldo

Tanto el personal del área administrativa como los usuarios de los sistemas deberán hacer periódicamente los respaldos de la información que están generando, y para ello tendrán que respetar las políticas de respaldo, las cuales siempre estarán orientadas al resguardo de los archivos más importantes relacionados con el sistema operativo empleado.

29. Respaldar información vital para el funcionamiento correcto del sistema operativo.

30. Los administradores delimitarán las responsabilidades de sus subordinados y determinarán quién está autorizado a consultar o modificar dicha información tomando las medidas de seguridad pertinentes.

31. Se deberá tener el respaldo diario de las modificaciones efectuadas, manteniendo una rotación de los dispositivos de respaldo y guardando respaldos históricos semanalmente.

32. La información necesaria pero no indispensable, deberá ser respaldada con una frecuencia mínima de una semana, manteniendo una rotación de los dispositivos de respaldo y guardando respaldos históricos mensualmente.

33. El respaldo de la información ocasional o eventual (por ejemplo, herramientas de seguridad y administración) queda a criterio de los administradores.

34. Los archivos magnéticos de información, de carácter histórico quedarán documentados como activos del área de seguridad y estarán debidamente resguardados.

Algo de suma importancia que debe estar siempre presente dentro de un esquema de seguridad y que tiene plena relación con los respaldos, es la integración de un plan de contingencias que incluye tanto a los administradores como a los usuarios de soporte técnico, en el cual se incluyan por lo menos algunos de los siguientes puntos:

35. Continuar con la operación utilizando procedimientos alternos.

36. Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.

37. Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.

38. Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.

39. Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.

3.4.4 Política de cuenta y contraseña

Política de cuenta: Establece qué es una cuenta de usuario de un sistema de cómputo, cómo está conformada, a quién puede serle otorgada, quién es el encargado de asignarlas, cómo deben ser creadas y comunicadas, etc. Algunas políticas son:

40. Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos.

41. Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.

42. El nombre de usuario de una cuenta deberá estar conformado de acuerdo a la nomenclatura especificada en la estandarización y reorganización de las cuentas.

Políticas de contraseñas: Son una de las políticas más importantes, ya que por lo general, las contraseñas constituyen la primera y tal vez la única manera de autenticación. Éstas establecen quién asignará la contraseña, qué longitud debe tener, a qué formato deberá apegarse, cómo será comunicada, etc. Algunas políticas son:

43. La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el usuario. Todas las contraseñas deberán contar con al menos ocho caracteres.

44. Todas las contraseñas elegidas deben ser difíciles de adivinar. No deben ser utilizadas palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.

45. Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otras que cambien de manera predecible y sean fáciles de adivinar.

46. Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.

47. Las contraseñas deben renovarse periódicamente (cada X tiempo; pero en ninguna circunstancia exceder un período de 2 años)

48. Se deben eliminar del sistema todas aquéllas contraseñas inutilizadas en cuanto pierdan su vigencia.

3.4.5 Política de acceso a los recursos

Puede hacerse una lista de los usuarios que requieren ingresar a los recursos de la red. La mayoría de los usuarios de la red se divide en grupos ya sea por departamentos o por jerarquías, dependiendo de la aplicación. También se deberán incluir una clase de usuarios llamada usuarios externos, estos son los usuarios que pueden tener acceso a la red desde cualquier parte, como las estaciones individuales de trabajo u otras redes. Las preguntas clave para diseñar esta política serían:

- ¿Quién debe poder usar los recursos? - Sólo personal autorizado: programadores, proveedores, administradores, secretarias, investigadores, etc.

- ¿Con qué tipo de privilegio puede acceder a los recursos? – Lectura, escritura, creación, modificación, supresión, exportación, ejecución, etc., si no se determina además de quién, con qué tipo de privilegio(s) puede acceder al sistema se corre el riesgo de proporcionar acceso a un área en particular pero con todos los derechos para hacer o deshacer sin medida.

- ¿Quién debe poder proporcionar acceso al sistema? - Si no se tiene control sobre quién está dando acceso al sistema, tampoco se podrá tener control sobre quién lo utiliza.

En términos generales, este tipo de políticas especifican cómo deben los usuarios acceder al sistema, desde dónde y de qué manera pueden autenticarse. Algunas políticas para el acceso a los recursos son:

49. Todos los usuarios deberán acceder al sistema utilizando algún programa que permita una comunicación segura y codificada.

50. Está prohibido acceder al sistema con una cuenta diferente de la propia, aún con la autorización del dueño de dicha cuenta.

51. Si un usuario está fuera del sitio de trabajo, debe conectarse a una máquina pública del sitio y, únicamente desde ésta hacer la conexión a la máquina deseada.

52. Al momento de ingresar al sistema, cada usuario deberá ser notificado de la fecha, hora y dirección desde la que se conectó al sistema por última vez, lo cual le permitirá al usuario detectar fácilmente si se ha hecho uso no autorizado del sistema y reportarlo al administrador.

3.4.6 Política de uso correcto de los recursos

El siguiente paso será el de proveer guías para el uso aceptable de los recursos. Las guías dependerán de la clase de usuario y por consiguiente de sus normas. La política que se desarrolle se llamará política de uso aceptable (PUA) para la red. Si el acceso a un recurso se restringe, deberá considerarse el nivel de acceso que tendrán las diferentes clases de usuarios. Las preguntas clave para el diseño de este tipo de políticas son:

- ¿Se permite irrumpir en cuentas ajenas?
- ¿Se permite adivinar contraseñas?
- ¿Se permite interrumpir el servicio?
- ¿Puede leerse un archivo ajeno cuyos permisos ante el sistema incluyen el de lectura para todos?
- ¿Puede modificarse un archivo ajeno cuyos permisos ante el sistema incluyen el de escritura para todos?
- ¿Pueden los usuarios compartir sus cuentas?

- ¿Puede copiarse el software que no lo permita en su licencia? La respuesta a todas estas preguntas debe ser negativa.

Existen dos enfoques o filosofías para la redacción de políticas: *enfoque permisivo* (todo lo que no esté explícitamente prohibido está permitido) y *enfoque prohibitivo* (todo lo que no esté explícitamente permitido está prohibido). Cuál de estas elegir dependerá del tipo de organización y el nivel de seguridad que ésta requiera.

Tras haber aclarado estos últimos puntos, se puede proceder a mencionar algunas políticas de uso adecuado.

53. Está terminantemente prohibido ejecutar programas que intenten adivinar las contraseñas alojadas en las tablas de usuarios de máquinas locales o remotas.

54. La cuenta de un usuario es personal e intransferible, por lo cual no se permite que se comparta su cuenta ni su contraseña con persona alguna, aún si ésta acredita la confianza del usuario.

55. Está estrictamente prohibido hacer uso de herramientas propias de delincuentes informáticos, tales como programas que rastrean puntos vulnerables en sistemas de cómputo propios o ajenos

56. Está estrictamente prohibido hacer uso de programas que exploten alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el administrador

57. No se permite bajo ninguna circunstancia el uso de cualquiera de las computadoras con propósitos de ocio o lucro.

3.4.7 Políticas de seguridad física

Como no es el tema principal de este trabajo la seguridad física, sólo se mencionarán algunas políticas de este punto, las cuales son:

58. Mantener las computadoras alejadas del fuego, humo, polvo y temperaturas extremas.

59. Colocarlas fuera del alcance de fuentes de calor, vibraciones, insectos, ruido eléctrico (balastras, equipo industrial, etc.), agua, etc.

60. Mantener las computadoras alejadas de comida y bebida.

61. No desatender las sesiones de trabajo activas.

Listas de verificación de seguridad (checklist)

Las listas de verificación, son un conjunto de registros referentes a lo que se debe comprobar en el funcionamiento del sistema. Algunos ejemplos de los puntos a verificar de acuerdo a las actividades en las listas son:

De planeación

- Identificar lo que se necesita proteger
- Establecer prioridades de seguridad
- Planes de emergencia
- Educar y concienciar a los usuarios

De usuarios y contraseñas

- Asegurarse que cada usuario tenga una cuenta individual
- Asegurarse que todos tengan una contraseña
- Tener una buena contraseña
- Si se cuenta con un programa para adivinar contraseñas, correrlo una vez
- Considerar programas para generar contraseñas
- Nunca transmitir contraseñas electrónicamente
- Asegurarse que el archivo de contraseñas no sea leído por usuarios desconocidos

Del usuario ROOT o ADMINISTRADOR

- Entrar al sistema con cuenta de usuario para entrar a *root o administrador*, debe ser autorizado por el personal encargado del sistema, y estos últimos deberán otorgar los permisos correspondientes para el acceso a la información.

Del sistema de archivos

- Realizar búsquedas de archivos que permitan ejecutar aplicaciones o comandos con diferentes privilegios a los de la sesión iniciada.
- Buscar archivos que no deban tener permisos de escritura para otros usuarios o grupos de trabajo que no pertenezca a la sesión iniciada.
- Periódicamente revisar todos los archivos de arranque de los sistemas y los archivos de configuración para detectar modificaciones y/o cambios en ellos
- Si se realizan copias de seguridad de directorios o archivos críticos, usar alguna herramienta de comparación para detectar modificaciones no autorizadas

De cuentas

- Desactivar y borrar cuentas inactivas
- Asegurarse que cada cuenta tenga su propia contraseña
- Nunca usar teclas de función programables en una terminal para almacenar información de login o contraseña

- Concienciar a los usuarios de pulsar la tecla ESCAPE antes de ingresar su login y su password, a fin de prevenir los "Caballos de Troya".

De datos

- Realizar respaldos regularmente
- Asegurarse de que los respaldos estén sean fiables
- ¿Están las copias de seguridad bien resguardadas?
- Crear PDF's o SD empacados
- Asegurarse que todos los archivos del sistema tengan los permisos apropiados

De archivos log

- Verificar el archivo de bitácora del sistema, para mostrar desde donde se accedió al sistema y en que modo de usuario, así como verificar los intento fallidos por entrar al sistema.
- Checar los logs de auditoria
- Checar los logs de las cuentas

De amenazas originadas por software

- Nunca instalar software desconocido
- Si es posible, no usar archivos que almacenan comandos con permisos de ejecución activados
- Buscar archivos ocultos y directorios login con permisos de escritura para otros
- No poner en la ruta de búsqueda de archivo, carpeta o unidad caracteres no validos (“,”,$,%,.,#, etc)
- Periódicamente verificar los archivos de inicio del sistema y la configuración de archivos por posibles modificaciones sin autorización
- Asegurarse que ningún comando permita un escape dentro de un archivo de comandos.

De redes y comunicaciones

- Buscar y examinar los archivos que especifican los sistemas y usuarios que pueden acceder como el usuario propietario de dicho directorio (para ver sí esta permitido su contenido)
- Guardar la lista de los servidores seguros
- Deshabilitar servicios de red que no se estén usando
- Verificar que los servicios *ftp y tftp* sean seguros
- Verificar que el servicio *FTP anonymous* sea seguro
- Considerar usar fibras ópticas como medio de transporte de información en la red
- Limitar el acceso físico a cables de red, ruteadores, repetidores y terminadores.
- Los usuarios deben tener diferentes contraseñas sobre diferentes segmentos de la red.

- Vigilar regularmente la actividad sobre los *gateways.*

De seguridad física

- Tener censores de humo y fuego en el cuarto de computadoras.
- Tener medios de extinción de fuego adecuados en el cuarto de computadoras.
- Entrenar a los usuarios sobre qué hacer cuando se disparan las alarmas.
- Instalar y limpiar regularmente filtros de aire en el cuarto de computadoras.
- Instalar UPS, filtros de línea, protectores gaseosos al menos en el cuarto de computadoras.
- Tener planes de recuperación de desastres.

3.4.8Políticas de listas de verificación

Una lista de verificación deberá de cubrir los siguientes requisitos:

62. Deberán estar documentadas.

63. Se clasificarán por categorías de verificación, como se hizo en la lista descrita en este punto.

64. Tendrán una secuencia dentro del proceso de verificación de las políticas.

65. Analizarán puntos considerados como críticos y de posible riesgo; además de los procedimientos rutinarios(cuentas inactivas, dormidas, etc.)

66. Toda lista de verificación, generara su correspondiente reporte de resultados.

3.4.9 Auditoría

La palabra auditar significa "examinar con la intención de verificar". Una auditoría en seguridad es un intento para verificar que día con día la operación del ambiente de cómputo esté acorde con la información de las políticas sobre seguridad. Las políticas sobre seguridad deberán ser la base para una auditoría.

Es importante identificar el objetivo y los límites de lo que se intenta auditar. Una auditoría deberá cubrir cada sección de las políticas sobre seguridad. Las áreas más comunes para una auditoría incluyen:

- Seguridad física
- Servidores
- Servicios de red
- Firewalls

Además de identificar las áreas sobre las que deberá operar, también deberá contener las siguientes características.

Políticas de auditoría

67. La auditoria será un proceso de verificación, no de corrección.

68. Su aplicación debe ser periódica, y en caso de riesgo su utilización deberá ser a la brevedad.

69. Estará sujeta a reforzar y verificar la utilidad de las políticas.

70. Dará como resultado un reporte del estado de seguridad del sistema operativo

71. El reporte de auditoría, así como sus copias serán almacenadas utilizando algún tipo de seguridad efectiva (asignar contraseña al documento)

72. Deberán mantener un mejoramiento constante.

73. Contará con una definición clara de objetivos y límites de la auditoría.

74. Deberá ser un proceso automatizado.

Las herramientas para la auditoría en seguridad pueden ser comerciales o de dominio público. Algunas son útiles para auditorías, mientras que otras ayudan en la seguridad llevada por los sistemas y por la red. En general las herramientas para auditoría se clasifican en:

- Herramientas de auditoria basada en servidores
- Herramientas de auditoria para redes amplias
- Herramientas para el análisis de tráfico en red
- Herramientas para el manejo de la seguridad
- Herramientas para la seguridad del perímetro y cortafuegos
- Herramientas para codificación
- Herramientas para la verificación

Un buen principio para llevar a cabo una auditoria es entrevistando a un porcentaje de los usuarios y del personal técnico y de administración. Estas entrevistas sirven para entender

la manera en que el personal cree que trabaja la seguridad, y cómo están implementando las políticas de la misma.

Por ejemplo, en las entrevistas de usuarios se puede preguntar con qué frecuencia cambian sus contraseñas y si entienden las reglas de cómo debe estar compuesta una contraseña; al hacerlo se tendrá una idea de la forma en que el usuario entiende las políticas sobre seguridad. Al entrevistar a varios usuarios, se verá si entienden las políticas publicadas y si éstas están siendo cumplidas como parte de la responsabilidad de su trabajo. Se recomienda para la realización adecuada del reporte de auditoria que los usuarios tengan un entrenamiento en el cual adquieran conciencia de la importancia de la seguridad en la red.

Una entrevista similar puede ser hecha al personal de administración, preguntándoles si se les comunicó de la renuncia de un empleado o de una baja temporal, permitiendo así la desactivación de la cuenta del usuario. Cuando las entrevistas se hayan realizado, se tendrá una perspectiva de lo que se encontrará cuando se audite a los servidores y a las redes.

Como se mencionó anteriormente, se han definido cuatro áreas a examinar durante una auditoria. Éstas son físicas, servidores, redes y firewalls. A grandes rasgos se describen los aspectos que deben auditarse en cada una de estas áreas.

3.5 Diseño de una política de seguridad

Al diseñar un esquema de políticas de seguridad, conviene dividir el trabajo en varias y diferentes políticas específicas a un campo: cuentas, contraseñas, control de acceso, uso adecuado, respaldos, correo electrónico, auditoría del sistema, seguridad física, personal, etc.

Antes de construir una barrera de protección, como preparación para conectar una red con el resto del mundo, es importante que se entienda con exactitud qué recursos de la red y servicios se desean proteger y contra qué, para lo cual, primero deben identificarse los recursos.

3.5.1 Identificación de recursos

Los recursos del sistema que deben ser considerados al estimar las amenazas a la seguridad general, y desarrollar políticas para su protección son:

- Hardware: procesadores, tarjetas, teclados, terminales, líneas de comunicación, ruteadores, etc.
- Software: programas fuente, programas objeto, utilerías, programas de comunicación, sistemas operativos, etc.
- Datos: durante la ejecución, almacenados en línea, bitácoras de auditoría, bases de datos, en tránsito sobre medios de comunicación, etc.
- Personal: usuarios, administradores.
- Documentación: sobre programas, hardware, sistemas, procedimientos administrativos locales.

- Accesorios: reportes, cintas, información grabada.

3.5.2 Metodología del desarrollo

Un esquema de políticas de seguridad debe llevar ciertos pasos, para garantizar su funcionalidad y permanencia en la institución. Nuestra propuesta es seguir los pasos que detallamos a continuación:

- *Preparación:* La recopilación de todo tipo de material relacionado con cuestiones de seguridad en la organización: Manuales de procedimientos. planes de contingencia, cartas compromiso, etc.

- *Redacción:* Escribir las políticas de una manera clara, concisa y estructurada. Requiere de la labor de un equipo en el que participen abogados, directivos, usuarios y administradores.

- *Edición:* Reproducir las políticas de manera formal para ser sometidas a revisión y aprobación.

- *Aprobación:* Probablemente la parte más difícil del proceso, puesto que es común que la gente afectada por las políticas se muestre renuente a aceptarlas. En esta etapa es fundamental contar con el apoyo de los directivos.

- *Difusión:* Dar a conocer las políticas a todo el personal de la organización mediante proyecciones de video, páginas Web, correo electrónico, cartas compromiso, memos, pancartas, etc.

- *Revisión:* Las políticas son sometidas periódicamente a revisión por un comité, que discutirá los comentarios emitidos por las personas involucradas.

- *Aplicación:* Es peor tener políticas y no aplicarlas que carecer de ellas. Una política que no puede implementarse o hacerse cumplir, no tiene ninguna utilidad. Debe predicarse con el ejemplo.

- *Actualización:* Además de la revisión correspondiente y debidamente programada, En el momento requerido las políticas deberán ser revisadas y actualizadas, respondiendo a los cambios en las circunstancias. El momento ideal es justo después de que ocurra un incidente de seguridad.

Al desarrollar las políticas de seguridad informática se considera indispensable y se recomienda tomar en cuenta diferentes escenarios como los que se describen a continuación:

Tarde o temprano, todas las políticas serán violadas. ¿Qué puede llevar a que una política sea violada?

- Negligencia
- Error accidental
- Desconocimiento de la misma
- Falta de entendimiento de la misma

¿Qué debemos hacer si una política es violada?

- Investigar quién llevó a cabo esta violación
- Investigar cómo y por qué ocurrió esta violación
- Aplicar una acción correctiva (disciplinaria)

¿Qué sucede si un usuario local viola las políticas de un sitio remoto?

- Debe haber acciones a seguir bien definidas con respecto a los usuarios locales
- Debe estarse bien protegido en contra de posibles acciones desde el sitio remoto
- ¿Cómo reaccionar ante un incidente de seguridad? Hay dos estrategias básicas:

Proteger y preservar

Su principal objetivo es proteger y preservar los servicios del sitio, y restablecerlos lo más rápido posible. Para ello se realizan acciones drásticas, tales como dar de baja los servicios, desconectar el sistema de la red, apagarlos, etc.

Lo utilizamos cuando:

- Los activos están bien protegidos
- Se corre un gran riesgo debido a la intrusión
- No existe la posibilidad o disposición para enjuiciar
- Se desconoce la base del intruso
- Los usuarios son poco sofisticados y su trabajo es vulnerable
- Los recursos de los usuarios son minados.

La metodología de esta primera estrategia es proteger de manera inmediata la red y restaurarla a su estado normal para que los usuarios puedan seguir utilizándola. Para ello, quizá se tenga que interferir en forma activa con las acciones del intruso y evitar mayor acceso.

Perseguir y enjuiciar

Su objetivo principal es permitir que los intrusos continúen con sus actividades en el sistema hasta que pueda identificarse a los responsables sin lugar a ambigüedades

Lo utilizamos cuando:

- Los recursos están bien protegidos

- Se dispone de respaldos confiables
- El riesgo para los activos es mayor que el daño de ésta y futuras intrusiones
- El ataque proviene de un sitio con el que guardamos cierta relación, y ocurre con cierta frecuencia e intensidad
- El sitio posee cierta atracción para los intrusos
- El sitio está dispuesto a correr el riesgo a que se exponen los activos al permitir que el ataque continúe
- Puede controlarse el acceso al intruso
- Se cuenta con herramientas de seguridad confiables
- El personal técnico conoce a profundidad el sistema operativo y sus utilerías, tanto como para poder rastrear al intruso
- Existe disposición para la persecución por parte de los directivos
- Existen leyes al respecto
- En el sitio existe alguien que conozca sobre cuestiones legales

El segundo enfoque adopta la estrategia de que la mejor opción es permitir a los intrusos seguir con sus acciones mientras se observan sus actividades, las cuales están siendo registradas.

Una forma posible de vigilar a los intrusos sin causar daño al sistema es construir un *"Jarrón de miel (Honey pot)"*. Un *Jarrón de miel*, en este caso, define un medio simulado con datos falsos para que lo utilice el intruso, para que sus actividades puedan ser observadas.

3.6 Leyes para la seguridad en red

Para ofrecer un sistema de red seguro se deberá aplicar una serie de leyes de seguridad, cuantas más medidas se tomen, mayor será la protección y menor el riesgo. Enseguida se enumeran, 6 leyes que deben ser consideradas para obtener un nivel adecuado de seguridad:

1. **Elegir un administrador de red.** Esta medida de prevención quizás sea la más importante. Una de las cosas que se debe tener en cuenta en el momento de establecer una red, es quién se encargará de controlar su funcionamiento y su seguridad. Por ello, se recomienda elegir un administrador de redes que conozca perfectamente sus procesos, conexiones, y accesos. Una buena persona para realizar esta tarea debe conocer a fondo el sistema operativo con el que trabaja, y las funciones de sus aplicaciones. Pero eso no es suficiente, debe ser una persona honesta y ética, con alto sentido de responsabilidad y de lealtad.

2. **Seguridad física.** Cualquier *hacker* en el mundo, o cualquier persona que quiera atacar una red sabe que la manera más eficaz de hacerlo es desde adentro del sistema, o teniendo contacto con el mismo. Por ello, la seguridad física abarca un conjunto de medidas que pueden variar desde darle acceso a las salas de computo, al equipo físico en sí donde sólo el administrador del sistema y su personal autorizado, o el mismo operador de la terminal controla la información disponible y su acceso a la computadora. Una medida razonable sería utilizar determinados planes de acción

para brindar seguridad, no solo en el acceso informático, sino también en el control del acceso a las instalaciones de la organización, desde la entrada misma, como el acceso a departamentos específicos de la misma.

3. **Vigilar las actividades del sistema.** Ésta garantiza un buen control de cualquier sistema incluyendo la red. Vigilar las actividades que se producen en el sistema y sus procesos, es una medida muy importante, ya que es difícil que un intruso ataque la primera vez que entra. Con esta medida de prevención podrían atraparse a la mayoría de los atacantes si se cuenta con mecanismos o procedimientos que vigilen y registren las entradas de las personas a la red y sus actividades. El hacer un censado de las personas que accesan al sistema y el tipo de información que consultan, ayudaría a identificar y corroborar si se realiza una actividad que no corresponde a su rubro, a que hora se realizo y de que lugar se realizo. Otras acciones podrían que auxiliar son el cambiar las contraseñas en determinado tiempo, dar de baja contraseñas que ya no estén en uso o que pertenezcan a personas que no laboren en la organización, instalar software de control, etc.

4. **Conocer el software**. Cada aplicación instalada debería ser revisada con la máxima seguridad. El administrador del sistema debería saber a qué tipo de programas están instalados o van a ser instalados en su equipo, cual es su función principal, sus requerimientos y posibles efectos que tengan en el hardware por su desempeño, como son los puertos de TCP y UDP a que tienen acceso las aplicaciones, con cuáles cuentas de usuarios interactúa el software, y los permisos de directorio que requiere. Se debe contar con información de origen de los programas, es decir, quien lo fabrica, de que módulos esta compuesto, si es del tipo firmware, freeware o si hay que comprar las licencias correspondientes, para evitar en primer lugar sanciones económicas por parte de autoridades de control de software y en segundo lugar, la implantación de programas que trabajen en background y que realicen procesos que atenten contra la seguridad en la información.

5. **Herramientas de seguridad**. Además de considerar las cuatro leyes anteriores, se puede considerar el uso de cortafuegos, el software de detección de instrucciones, y los *proxys*. Estas herramientas de seguridad son bastante importantes pero no pueden aplicarse solas, deben ser un complemento del análisis e identificación de amenazas tratado en el Capítulo 2 y que es la base para una seguridad aceptable en la información. Las herramientas a utilizar son determinadas por las amenazas a las que nos encontramos expuestos, a los requerimientos identificados, al nivel de seguridad requerido y a los resultados de la valoración de bienes.

6. **Auditoría de seguridad.** La seguridad de los sistemas de redes es relativa ya que día a día alguien está tratando de descubrir una nueva forma de invadirlos. Por ello, es importante probar regularmente la seguridad de la red. Si no se tienen los medios para realizar estas pruebas, una alternativa sería contratar un auditor para examinar y probar el sistema, mediante diversas acciones como podrían ser ataques al servidor de correo, el DNS, el dominio, la web, y/o los servidores de FTP, entre otras, según lo que se quiera probar.

En resumen, es importante aplicar simultáneamente todas estas medidas, o al menos la mayoría de ellas, ya que una sola no será lo suficientemente efectiva, porque todas pertenecen a un conjunto de leyes complementarias para garantizar seguridad y confiabilidad.

3.7 Tipos de medidas de seguridad o contramedidas

Los sistemas informáticos pueden diseñarse de acuerdo con criterios de economía, de eficiencia y de eficacia, etc., porque son claramente medibles y se asocian a parámetros que, maximizando unos y minimizando otros, se puede tender hacia diseños óptimos.

Diseñar sistemas mediante criterios de seguridad es más complejo, pues las amenazas son en muchos casos poco cuantificables y muy variadas. La aplicación de medidas para proteger el sistema supone un análisis y cuantificación previa de los riesgos o vulnerabilidades del sistema.

En muchos casos las medidas de seguridad llevan un costo aparejado que obliga a subordinar algunas de las ventajas del sistema. Por ejemplo, la velocidad de las transacciones. Con relación a esto, también se hace obvio que a mayores y más restrictivas medidas de seguridad, menos amigable es el sistema. Se hace menos cómodo para los usuarios ya que limita su actuación y establece unas reglas más estrictas que a veces dificultan el manejo del sistema. Por ejemplo, el uso de una política adecuada de passwords, con cambios de las mismas.

Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales: lógicas, físicas, administrativas y legales.

CAPÍTULO IV

IMPLANTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

4.1 La Problemática de la Seguridad

A lo largo de los últimos años los problemas de seguridad que se vienen observando en las empresas y organismos han sido una constante recurrente; se pueden diferenciar en tres grandes grupos:

a) Problemas estructurales

- Habitualmente la estructura de la organización no se hace pensando en la seguridad por lo que no hay una definición formal de las funciones ni responsabilidades relativas a seguridad.
- No suelen existir canales de comunicación adecuados para tratar incidentes de seguridad, predominando los canales de tipo informal y el boca a boca.
- Exceptuando determinados ambientes como la banca o la defensa, no suelen existir recursos específicos dedicados a seguridad, y cuando existen suelen dedicarse a la seguridad física (puertas, alarmas, dispositivos antiincendios, etc.) por ser más fácilmente justificable su adquisición.

b) Problemas en el planteamiento

- Los planteamientos de seguridad suelen adolecer de coherencia ya que no suelen ser ni suelen estar adaptados a las necesidades de la empresa.
- Habitualmente las directrices no son homogéneas en toda la organización.
- Como consecuencia de la falta de definición de funciones, nadie quiere responsabilizarse de los riesgos asumidos en la organización y nadie quiere adoptar medidas que puedan dificultar el proceso de negocio.
- No se definen normas ni procedimientos salvo cuando su ausencia puede afectar al propio negocio (por ejemplo la existencia de copias de seguridad) o tras un incidente grave de seguridad.
- Al no existir beneficios inmediatos, resulta difícil justificar gastos y recursos.

c) El problema tecnológico

A pesar de la opinión generalizada, la tecnología no es la panacea:

- Las herramientas son un soporte, pero si no hay una base con ideas sólidas no solucionan los problemas.
- Las herramientas existentes, de por sí, no cubren todas las necesidades.
- La sensación de falsa seguridad provocada por la excesiva confianza en las soluciones tecnológicas induce a bajar la guardia.

Resumiendo, **la situación real suele ser que en las empresas y organismos el negocio y la imagen se anteponen a la seguridad**. La organización crece e implementa soluciones de seguridad de acuerdo a necesidades puntuales, no hay definida una estrategia, ni normas ni procedimientos, es decir, lo habitual es que no se contemple expresamente la seguridad.

Motivo por lo cual el presente trabajo busca subsanar estos aspectos y para ello se ha venido desarrollando en los capítulos anteriores.

4.2 Planificando la Seguridad

La forma adecuada para plantear la planificación de la seguridad en una organización debe partir siempre de la definición de una política de seguridad que defina el **QUÉ** se quiere hacer en materia de seguridad en la organización para a partir de ella decidir mediante un adecuado plan de implementación el **CÓMO** se alcanzarán en la práctica los objetivos fijados.

La Política de Seguridad engloba pues los objetivos, conductas, normas y métodos de actuación y distribución de responsabilidades y actuará como documento de requisitos para la implementación de los mecanismos de seguridad. La política debe contemplar al menos la definición de funciones de seguridad, la realización de un análisis de riesgos, la definición de normativa y procedimientos, la definición de planes de contingencia ante desastres y la definición del plan de auditoria.

A partir de la Política de Seguridad define el **Plan de Implementación**, que es muy dependiente de las decisiones tomadas en ella, en el que se contemplará: el estudio de soluciones, la selección de herramientas, la asignación de recursos y el estudio de viabilidad.

Hay dos cuestiones fundamentales que deberán tenerse en cuenta para implantar con éxito una política de seguridad: Es necesario que la política sea aprobada para que esté respaldada por la autoridad correspondiente que asegure su cumplimiento y la asignación de recursos; y es necesario que se realicen revisiones periódicas que la mantengan siempre actualizada y acorde con la situación real del entorno.

La Política de Seguridad y el Plan de Implementación (y la implantación propiamente dicha) están íntimamente relacionados:

La Política de Seguridad define el Plan de Implementación ya que la implementación debe ser *un fiel reflejo* de los procedimientos y normas establecidas en la política.

El **Plan de Seguridad** debe estar revisado para adaptarse a las nuevas necesidades del entorno, los servicios que vayan apareciendo y a las aportaciones que usuarios, administradores, etc. vayan proponiendo en función de su experiencia. La revisión es esencial para evitar la obsolescencia de la política debido al propio crecimiento y evolución de la organización. Los plazos de revisión deben estar fijados y permitir además revisiones extraordinarias en función de determinados eventos (por ejemplo, incidentes)

El Plan de Implementación debe ser auditado para asegurar la adecuación con las normas.

El Plan de Implementación debe realimentar a la Política de Seguridad. La experiencia, los problemas de implantación, las limitaciones y los avances tecnológicos, etc. permitirán que

la política pueda adecuarse a la realidad, evitando la inoperancia por ser demasiado utópica y la mejora cuando el progreso lo permita.

Un enfoque como el propuesto asegurará la adecuación del nivel de seguridad implantado con las necesidades de la organización y el correcto seguimiento y control de los riesgos.

4.3 Estrategia de Seguridad.

Para establecer una estrategia adecuada es conveniente pensar una política de protección en los distintos niveles que ésta debe abarcar y que no son ni más ni menos que los estudiados hasta ahora: Hardware, Software, Humana y la interacción que existen entre estos factores.

En cada caso considerado, el plan de seguridad debe incluir una estrategia **Proactiva** 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 Proactiva, 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.

Como ya se había mencionado, 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 que acciones se toleran y cuáles no y en la medida que se sigan por el propio cuerpo directivo, de sistemas y de seguridad la implantación resultará en un proceso menos complicado.

4.4 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 este apoyo, las medidas que se tomen no tendrán la fuerza necesaria.*

Se deberá tener en cuenta que la implementación de Políticas de Seguridad, trae aparejados varios tipos de problemas que afectan el funcionamiento de la organización. La implementación de un sistema de seguridad conlleva a incrementar la complejidad en la operatoria de la organización, tanto técnica como administrativamente.

Por esto, será necesario sopesar 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 Política de Seguridad en la Información 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.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.
- Definición de violaciones y las consecuencias de falta de 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 permiten dar indicaciones sobre la clase de sanciones que se puedan imponer. Pero, no debe especificar con exactitud que pasará o cuando algo sucederá; ya que no es una sentencia obligatoria de la ley.
- Explicaciones comprensibles (libre tecnicismo y términos legales pero sin sacrificar su precisión) sobre él porque de las decisiones tomadas.
- Finalmente, como documento dinámico de la organización, debe seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta y rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc.

Una proposición de una forma de realizar una Política de Seguridad en la Información puede apreciarse en el siguiente **figura 4.1**

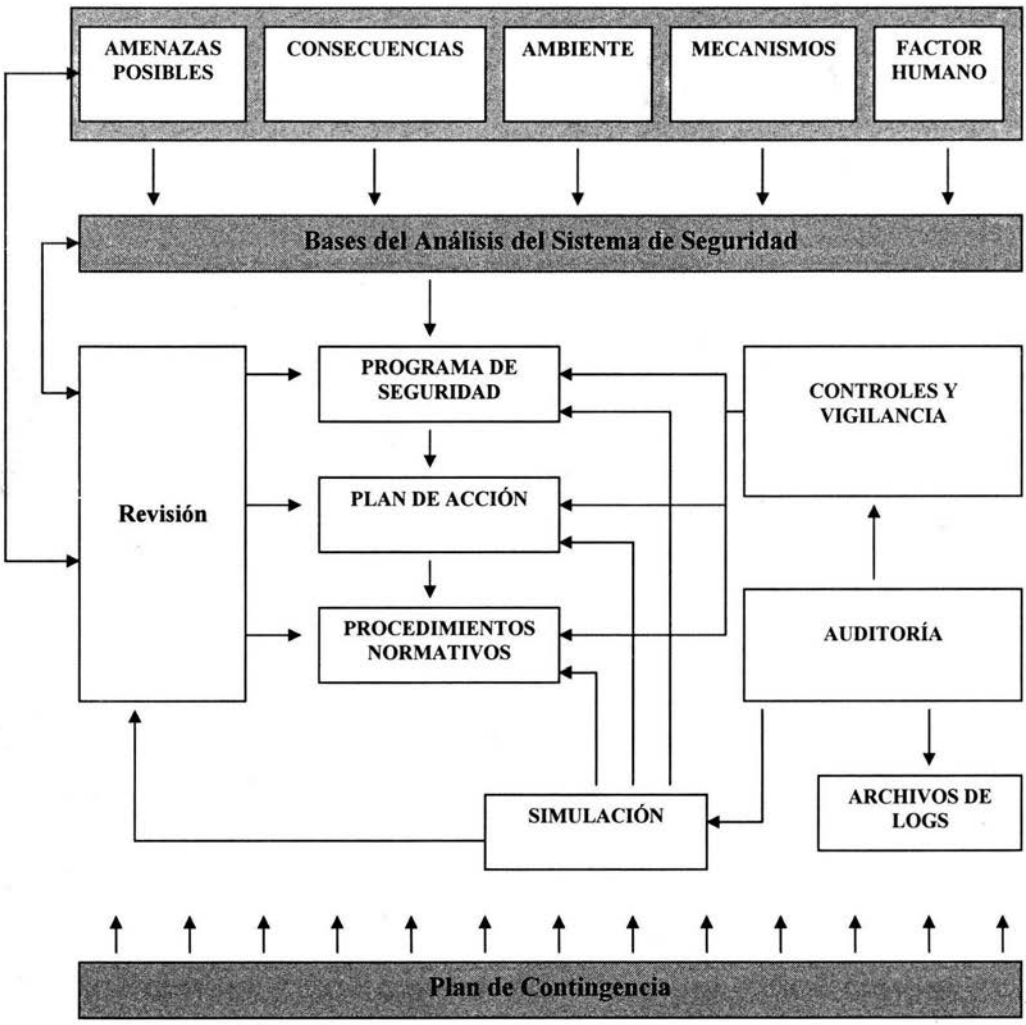

Figura 4.1 : Realización de una Política de Seguridad en la Información

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 Logs 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 realimentación 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 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 mucho mayores que implican mayores costos para lograr, en la mayoría de los casos, un menor grado de seguridad

"Construya la seguridad desde el principio. La máxima de que es más caro añadir después de la implementación es cierta". [4]

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.

4.4.1 Auditoría y Control

Se considera que la Auditoria son los "ojos y oídos" de la dirección, que generalmente no puede, no sabe realizar las verificaciones y evaluaciones.

La Auditoria consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, que 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.

[4] Encuesta de Seguridad Informática 2001". Marzo de 2001. Ernst & Young

4.4.2 Plan de Contingencia

Pese a todas las medidas de seguridad puede ocurrir un desastre. De hecho los expertos es seguridad afirman "sutilmente" que hay que definir un plan de recuperación de desastres "para cuando falle el sistema", no "por si falla el sistema"[5]

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 de 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 a la capacidad de seguir trabajando en un plazo mínimo después de que 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.*

4.5 Etapas para Implantar un Sistema de Seguridad en Marcha

Para hacer que el plan entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguiente 8 pasos:

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

[5] ARDITA, Julio Cesar. Director de Cybsec S.A. Security System.

Como se ha visto la implantación de las políticas de seguridad no es nada sencillo, es necesario el compromiso y participación de toda la organización, que tendrá que estar completamente convencida de que las políticas son necesarias para el optimo desempeño de sus funciones.

Desgraciadamente en México no hay una cultura en materia de seguridad en la información, debido a que la legislación no le da la importancia que esta representa, por lo que nosotros como empresa u organización debemos de elaborar los planes que introduzca esta idea a la organización, y que a la vez generen una conciencia de las consecuencias de su falta y que sea respetada por todos los miembros, desde niveles directivos hasta los empleados comunes, incluyendo a personas ajenas que realicen una interacción laboral o personal con los miembros de la organización.

Para lograrlo se puede seguir varios lineamientos establecidos en otros países y que pueden servir para la implementación de nuestras propias políticas de seguridad en la información.

Un ejemplo de estos, son las **"GUÍAS PARA LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y REDES"** desarrolladas por la OCDE (Organización de la Cooperación y Desarrollo Económicos)[6] por primera vez en 1992 y que han sido actualizadas de acuerdo a los cambios en el ambiente general de la tecnología de la información y las comunicaciones, así como en el uso de los sistemas de información y redes.

Estos cambios continuos ofrecen grandes ventajas, pero hacen necesario que los gobiernos, los negocios, otras organizaciones y los usuarios que desarrollan, poseen, proporcionan, administran estos servicios y usan sistemas de información y redes (participantes) pongan mayor atención en los aspectos relacionados con la seguridad.

El ambiente en el que predominaba en el pasado, en el que los sistemas operaban de manera aislada o en redes propietarias, ha sido sustituido por las computadoras personales que cada vez tienen mayor capacidad de proceso, la convergencia de las tecnologías y la difusión masiva del uso del Internet.

Hoy en día los participantes se encuentran cada vez más interconectados y estas conexiones se extienden más allá de las fronteras nacionales. Al mismo tiempo, el Internet forma parte de la infraestructura de operación de sectores estratégicos como los de energía, transporte y finanzas y desempeña un papel muy importante en la forma en cómo las compañías hacen sus negocios, cómo los gobiernos proporcionan sus servicios a los ciudadanos y a las empresas y cómo los ciudadanos se comunican e intercambian información de manera individual. La naturaleza y el tipo de tecnologías que constituyen la infraestructura de información y comunicaciones también han cambiado de manera significativa.

---

[6] Organization for Economic Cooperation and Development, www.oecd.org (Mundial), http://rtn.net.mx/oecd (México)

El número y el tipo de aparatos que integran la infraestructura de acceso se ha multiplicado para incluir dispositivos de tecnología fija, inalámbrica y móvil, y una proporción creciente de los accesos están conectados de manera permanente. Como consecuencia de todos estos cambios la naturaleza, volumen y sensibilidad de la información que se intercambia a través de esta infraestructura se ha incrementado de manera muy significativa.

Como resultado de la creciente conectividad, los sistemas de información y las redes son más vulnerables ya que están expuestos a un número creciente así como un rango de variedad mayor de amenazas y vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en el tema de seguridad. Por estas razones, estas guías aplican para todos los participantes de la nueva sociedad de la información y sugieren la necesidad de tener una mayor conciencia y entendimiento de los aspectos de seguridad, así como de desarrollar una "cultura de seguridad".

Estas guías responden a un ambiente de seguridad cada vez más cambiante mediante la promoción del desarrollo de una cultura de seguridad esto es, un enfoque hacia la seguridad en el desarrollo de sistemas de información y redes, así como la adopción de nuevas formas de pensamiento y comportamiento cuando se usan y sé interactúa mediante sistemas de información y redes. Estas guías marcan un rompimiento con los tiempos en que los aspectos de seguridad al desarrollar redes y sistemas se consideraban como un elemento a posteriori. La operación de los sistemas de información, redes y servicios afines debe ser confiable y segura ya que los participantes se han vuelto cada vez más dependientes de éstos. Sólo un enfoque que tome en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines puede proveer una seguridad efectiva.

Cada participante es un actor importante para garantizar la seguridad. Cada participante de acuerdo al papel que desempeña deberá estar consciente de los riesgos de la seguridad y de las medidas preventivas correspondientes, deberá asumir la responsabilidad correspondiente y tomar las medidas que permitan fortalecer la seguridad de los sistemas de información y las redes.

La promoción de una cultura de seguridad requiere tanto de un liderazgo fuerte como de una participación amplia para asegurar que se le otorgue un carácter de prioritario a la planeación y administración de la seguridad, así como del entendimiento de la necesidad de seguridad para todos los participantes. Los temas de seguridad deberán ser tópicos de preocupación y responsabilidad para todos los niveles de gobierno, negocios y todos los participantes. Las guías proponen adoptar y promover una cultura de seguridad para toda la sociedad. Esto permitirá que los participantes consideren la seguridad en el diseño y uso de los sistemas de información y de las redes. Las guías proponen que todos los participantes adopten y promuevan una cultura de seguridad como una manera de pensar sobre este tema, así como de evaluar y actuar en relación a los sistemas de información y redes.

Los propósitos de estos lineamientos son:

- Promover una cultura de seguridad entre todos los participantes como un medio de proteger los sistemas de información y las redes.

- Incrementar la conscientización sobre el riesgo de los sistemas de información y las redes; Las políticas, prácticas, medidas y procedimientos disponibles para poder enfrentar estos riesgos, así como la necesidad de adoptarlos e implementarlos.

- Promover entre todos los participantes una confianza mayor en los sistemas de información y las redes, la forma en la que operan y se usan.
- Crear un marco general de referencia que ayude a los participantes en el entendimiento de los aspectos de seguridad y respeto de valores éticos en el desarrollo e implementación de políticas coherentes, prácticas, medidas y procedimientos para la seguridad de sistemas de información y redes.

- Promover entre todos los participantes cuando sea apropiado, la cooperación y el intercambio de información sobre el desarrollo e implementación de políticas de seguridad, prácticas, medidas y procedimientos.

- Promover la consideración del tema de seguridad como un objetivo importante a lograr por parte de todos los participantes involucrados en el desarrollo e implementación de estándares.

Los siguientes nueve principios son complementarios y deben ser leídos de manera integral. Éstos le competen a todos los participantes de todos los niveles, tanto los del ámbito político como operacional. De acuerdo con estos lineamientos, la responsabilidad de ellos varía de acuerdo con los papeles que desempeñen.

Todos se verán beneficiados por la conscientización, educación, intercambio de información y capacitación que conlleven a la adopción de un mejor entendimiento de la seguridad y las prácticas que se requieren. Los esfuerzos para fortalecer la seguridad de los sistemas de información y de las redes deben ser consistentes con los valores de una sociedad democrática, en particular con la necesidad de contar con flujos de información libres y abiertos, y los principios básicos de protección de la privacidad personal.

Además de las Guías de Seguridad, la OCDE ha desarrollado recomendaciones complementarias concernientes a los lineamientos de otros aspectos importantes de la sociedad de la información mundial. Esto se relaciona con la privacidad (en 1980 las Guías OCDE de Protección a la Privacidad y de los flujos entre fronteras de Datos Personales) y criptografía (la OCDE en 1997 Guía de las Políticas de Criptografía) Las guías de seguridad deben ser leídas de manera conjuntas con ésta.

1) Conscientización

Los participantes deben estar conscientes de la necesidad de contar con sistemas de información y redes seguros, y qué es lo que pueden hacer para promover y fortalecer la seguridad.

La conscientización de los riesgos y de los mecanismos disponibles para salvaguardarla, es el primer paso en la defensa de la seguridad de los sistemas de información y redes.

Éstos pueden ser afectados tanto por riesgos internos como externos. Los participantes deben entender que las fallas de seguridad pueden repercutir en daños significativos a los sistemas y a las redes que están bajo su control. Deben estar conscientes del daño potencial que esto puede provocar a otros derivados de la interconectividad y la interdependencia. Los participantes deben estar conscientes de: las configuraciones y actualizaciones disponibles para sus sistemas, su lugar dentro de las redes, las mejores prácticas que pueden implementar para fortalecer la seguridad y las necesidades de otros participantes.

2) Responsabilidad

Todos los participantes son responsables de la seguridad de los sistemas de información y redes.

Los participantes que dependen de sistemas de información y redes interconectados de manera local y global deben comprender su responsabilidad en salvaguardar la seguridad de éstos. Deben de responder ante esta responsabilidad de una manera apropiada a su papel individual.

Los participantes deben revisar sus propias políticas, prácticas, medidas y procedimientos de manera regular y evaluar si éstos son apropiados en relación con su entorno. Aquellos que desarrollan y diseñan o proveen productos o servicios deben considerar la seguridad de los sistemas y redes y distribuir a los usuarios de manera oportuna información apropiada incluyendo actualizaciones para que éstos entiendan mejor la funcionalidad de la seguridad de sus productos y servicios y la responsabilidad de ellos con relación a este tema.

3) Respuesta

Los participantes deben actuar de manera oportuna y cooperativa para prevenir, detectar y responder a incidentes que afecten la seguridad. Al reconocer la interconectividad de los sistemas de información y de las redes, así como el riesgo potencial de un daño que se extienda con rapidez y tenga una alcance amplio, los participantes deben actuar de manera oportuna y cooperativa para enfrentar los incidentes que afecten la seguridad.

Cuando sea apropiado deben compartir información sobre los riesgos y vulnerabilidades e implementar procedimientos para una cooperación rápida y efectiva que permita prevenir, detectar y responder a incidentes que afecten la seguridad. Cuando sea permitido, esto puede implicar el intercambio de información y cooperación transfronteriza.

4) Ética

Los participantes deben respetar los intereses legítimos de los otros. Debido a la permeabilidad de los sistemas de información y las redes en nuestras sociedades, los participantes necesitan reconocer que sus acciones o la falta de éstas, pueden dañar a otros. Es crucial mantener una conducta ética y los participantes deben hacer esfuerzos por desarrollar y adoptar las mejores prácticas y promover conductas que reconozcan la necesidad de salvaguardar la seguridad y respetar los intereses legítimos de otros.

5) Democracia

La seguridad de los sistemas de información y redes debe ser compatible con los valores esenciales de una sociedad democrática.

La seguridad debe ser implementada de manera consistente con los valores reconocidos por las sociedades democráticas, incluyendo la libertad de intercambio de pensamiento e ideas, así como el libre flujo de información, la confidencialidad de la información y la comunicación y la protección apropiada de información personal, apertura y transparencia.

6) Evaluación del riesgo

Los participantes deben llevar a cabo evaluaciones de riesgo. La evaluación del riesgo identifica las amenazas y vulnerabilidades y debe ser lo suficientemente amplia para incluir los factores internos y externos fundamentales como tecnología, factores físicos y humanos, políticas y servicios de terceros que tengan implicaciones en la seguridad.

La evaluación del riesgo permite determinar los niveles aceptables de seguridad y ayudar en la selección de controles apropiados para administrar el riesgo de daños potenciales a los sistemas de información y redes, en relación a la naturaleza e importancia de la información que debe ser protegida. Debido a la creciente interconectividad de los sistemas de información, la evaluación del riesgo debe incluir consideraciones acerca del daño potencial que puede ser provocado por otros o que puede ocasionarse a otros.

7) Diseño e implementación de seguridad

Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas de información y redes.

Los sistemas, las redes y las políticas deben ser diseñadas, implementados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo está en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial hacia amenazas o vulnerabilidades que se hayan identificado. Las salvaguardas y mecanismos técnicos y no técnicos son necesarios y deben ser proporcionales al valor de la información de los sistemas de información y redes de la organización.

La seguridad debe ser un elemento fundamental de todos los productos, servicios, sistemas y redes; y una parte integral del diseño y arquitectura de los sistemas. Para los usuarios finales el diseño e implementación de la seguridad radica fundamentalmente en la selección y configuración de los productos y servicios para sus sistemas.

8) Administración de la Seguridad

Los participantes deben adoptar una visión integral de la administración de la seguridad.

La administración de la seguridad debe estar basada en la evaluación del riesgo y ser dinámica, debe comprender todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones. Debe incluir posibles respuestas anticipadas a riesgos emergentes y considerar la prevención, detección y respuesta a incidentes que afecten la seguridad, recuperación de sistemas, mantenimiento permanente, revisión y auditoria.

Las políticas de seguridad de los sistemas de información, redes, así como las prácticas, medidas y procedimientos deben estar coordinadas e integradas para crear un sistema coherente de seguridad. Los requerimientos en la administración de la seguridad dependen de los niveles de participación, del papel que desempeñan los participantes, del riesgo implicado y de los requerimientos del sistema.

9) Reevaluación

Los participantes deben revisar y reevaluar la seguridad de sus sistemas de información y redes y hacer las modificaciones pertinentes a sus políticas, prácticas, medidas y procedimientos de seguridad. De manera constante se descubren nuevas amenazas y vulnerabilidades. Los participantes deben revisar y evaluar, modificar todos los aspectos de la seguridad de manera continua, a fin de poder enfrentar los riesgos que se encuentran en evolución permanente.

Así mismo, la OCDE recomienda reconociendo:

- Que los sistemas de información y redes son cada vez más usado y de un valor creciente para los gobiernos, las empresas y otras organizaciones, así como los usuarios individuales;

- Que la creciente importancia del papel de los sistemas de información y redes y la creciente dependencia en ellos para asegurar la estabilidad y eficiencia de las economías nacionales y del comercio internacional, y de la vida social, cultural y política, hacen evidente la necesidad de desarrollar esfuerzos especiales para proteger y promover la confianza en ellos;

- Que los sistemas de información y redes y su proliferación en todo el mundo han estado acompañados de nuevos y crecientes riesgos;

- Que los datos e información almacenados y transmitidos a través de los sistemas de información y redes están sujetos a amenazas de accesos, usos, apropiación y alteración no autorizados, transmisión de código dañino, caída o destrucción del servicio, y requieren de mecanismos adecuados para salvaguardarlos:

- Que existe la necesidad de incrementar la conscientización sobre los riesgos a los sistemas de información y redes, y de las políticas, prácticas, medidas y procedimientos disponibles para responder a éstos, y que promover un comportamiento adecuado como un paso esencial para el desarrollo de una cultura de seguridad;

- Que hay una necesidad de revisar las políticas, prácticas, medidas y procedimientos con los que se cuentan en la actualidad para ayudar a asegurar que éstos sean capaces de responder a los retos cambiantes de las amenazas que enfrentan los sistemas de información y redes;

- Que es del interés común promover la seguridad de los sistemas de información y redes mediante una cultura de seguridad que promueva la coordinación y cooperación internacional para enfrentar los riesgos para las economías nacionales, el comercio internacional y la vida social, cultural y política provocados por el daño potencial de fallas en la seguridad.

Reconociendo también:

- Que las Guías para la Seguridad de los Sistemas de Información y Redes hacia una Cultura de Seguridad son recomendaciones de carácter voluntario y no afectan los derechos de la soberanía de las naciones;

- Que estas guías por ningún motivo sugieren que exista una solución única para la seguridad o qué políticas, prácticas, medidas y procedimientos son apropiados para una situación particular, sino más bien, buscan proveer un marco de principios para promover una mejor comprensión de cómo los participantes pueden beneficiarse y contribuir al desarrollo de una cultura de seguridad;

Recomienda estas Guías para la Seguridad de los Sistemas de Información y Redes hacia una cultura de Seguridad a gobiernos, empresas, otras organizaciones y usuarios individuales que desarrollen, posean, provean, administren o proporcionen servicio y usen sistemas de información y redes.

Recomienda a los Países Miembros:

- Establecer nuevas o modificar las políticas, prácticas, medidas y procedimientos con que cuenten para reflejar y tomar en cuenta el contenido de las Guías para la Seguridad de los Sistemas de Información y Redes hacia una Cultura de Seguridad mediante la adopción y promoción de una cultura de seguridad como proponen estas guías;

- Desarrollar esfuerzos para consultar, coordinar y cooperar a nivel nacional e internacional a efecto de poder implantar estas guías;

- Dar a conocer las guías al sector público y privado, incluyendo las organizaciones de los gobiernos, los negocios y otras y usuarios individuales para promover una cultura de seguridad y hacer que todas las partes involucradas respondan a este

llamado, desarrollen las acciones necesarias para implementar estas guías de una manera adecuada a sus papeles individuales;

- Poner a disposición de países no miembros estas guías en el tiempo y forma adecuados; Revisar estas guías cada cinco años para promover la cooperación internacional en aspectos relacionados con la seguridad de los sistemas de información y las redes;

- Instruye al Comité de Política de Información, Computación y Comunicaciones de la OCDE para promover la implantación de estas guías.

Las guías de seguridad se concluyeron por primera vez en 1992, y fueron revisadas en 1997. La revisión actual fue iniciada en el 2001 por el Grupo de Trabajo sobre Seguridad de la Información y Privacidad (GTSIP) en cumplimiento a un mandato del Comité de Políticas para la Información, Computación y Comunicaciones (CPICC) y acelerada por los eventos trágicos del 11 septiembre del 2002.

La redacción fue elaborada por el grupo experto de GTSIP, quienes se reunieron en: Washington DC el 10 y 11 de diciembre de 2001, Sydney el 12 y 13 de febrero de 2002,

París el 4 y 6 de marzo de 2002. El GTSIP se reunió en PARIS el 5 y 6 de marzo del 2002, el 22 y 23 de abril, así como el 25 y 26 de junio de 2002.

Es necesario que se establezca el compromiso de la organización a revisar periódicamente sus niveles de seguridad y la realización de al menos una vez al año un nuevo análisis para conocer la eficiencia de sus políticas de seguridad. Dependiendo del resultado se definirían las acciones que puedan tomar los directivos para su modificación y mejoramiento.

Seguridad y confidencialidad

Las organizaciones enfrentan una gran variedad de riesgos para la seguridad y la confidencialidad, y son plenamente responsables del mantenimiento de todos los aspectos de seguridad y confidencialidad de los datos y la información. Los posibles conflictos entre la difusión de datos y la seguridad y la confidencialidad de los mismos deben abordarse al comienzo del proceso de adquisición y desarrollo de sistemas.

La empresa que automatiza los módulos de aplicaciones considerará varios factores de implementación referidos a la seguridad y a la confidencialidad en todo el sistema que superan los límites de las aplicaciones.

Dos factores convierten al tema en una inquietud preeminente actual: la naturaleza intrínsecamente sensible de los datos de los clientes y el uso creciente de la computación en red, en particular Internet, para el procesamiento de información para atención de solicitudes. Con frecuencia, estos dos elementos en combinación llegaron a la primera plana en los últimos años.

Convencer a los administradores de la importancia de la seguridad y aumentar la conciencia sobre la seguridad en los empleados y el personal administrativo, así como diseñar, implementar y supervisar políticas de seguridad, son funciones del administrador del sistema que trabaja en estrecha colaboración con el comité de sistemas de información, el nivel alto de administración, y el asesor jurídico de la organización.

La terminología utilizada en las áreas de "seguridad", "resguardo" y "protección de datos" dista mucho de ser uniforme y con frecuencia es confusa. No obstante, se pueden agrupar todos los temas en cuatro áreas:

- Integridad: la prevención de la modificación no autorizada de información.
- Acceso: la prevención del ingreso no autorizado a los recursos de información.
- Protección física: la protección de datos y equipos para el procesamiento de datos contra el daño intencional o accidental.
- Confidencialidad: evitar la divulgación no autorizada de información.

Ninguno de los temas relacionados con la seguridad de los sistemas y la confidencialidad es exclusivo. Sin embargo, la combinación de algunos de estos aspectos justifica la consideración especial en el caso de los sistemas de información particular. Entre las muchas características de los datos sobre salud algunas son muy particulares:

a) Los sistemas de información almacenan datos identificados sobre la condición económica y/o social de las personas y parte de la información es sumamente confidencial.

b) Debido a la naturaleza del equipo de trabajo y las frecuentes actividades interdisciplinarias en la información, muchos profesionales necesitan datos individuales confidenciales y el control y la autorización para el acceso se tornan problemas especiales.

c) Los datos individuales registrados desempeñan una función esencial en la prestación de servicios públicos o particulares y pueden incluso ser críticos para el individuo. La disponibilidad de tales datos, incluso en línea, y su calidad merecen especial atención y el equilibrio entre el acceso y el control de la integridad es un problema grave en estas circunstancias.

d) Se está otorgando acceso remoto a registros personales y otros datos relacionados con la atención a un número cada vez mayor de proveedores de servicios, contribuyentes, controladores y trabajadores administrativos. El reto es proporcionar simultáneamente niveles necesarios de acceso y asegurar la protección para sistemas internos, confidencialidad, autenticación significativa de usuarios y la capacidad de auditar la utilización de los sistemas.

e) Los datos de los individuos son importantes para la investigación, así como el análisis estadístico de grupos de personas, es importante para la planificación y el mejoramiento del ejercicio de diferentes actividades personales y de interés social. La confidencialidad, uno de los aspectos de la seguridad de los datos, incluye el equilibrio de la demanda de información sobre atención de solicitudes de datos y los derechos de privacidad de las personas y el establecimiento de principios justos de privacidad para los datos individuales: límites de uso de registros de información por parte de las autoridades de públicas y particulares, la policía y los investigadores.

f) La noción de propiedad del o de los registros concuerda con el énfasis creciente en el individuo como el elemento fundamental de la atención y solicitud de su información. Cada vez más, la tendencia es promover la personas como el propietario de los datos plasmados en el registro de datos. Sin embargo, son insuficientes o inexistentes los instrumentos legales para hacer cumplir esta perspectiva. En la mayoría de los países del continente la institución es la propietaria legal de los registros de datos creado en esa entidad, de la misma manera que la institución es titular de otros "registros empresariales" creados. Y mientras la mayoría de las organizaciones independientes, los grupos de usuarios, los consultores y las afiliaciones alientan a los proveedores, los contribuyentes y los empleadores a fomentar la propiedad entre sus miembros, en este momento la realidad es que no existen reglas claras.

Cada organización debe determinar el nivel de seguridad y confidencialidad para diferentes categorías de información, y el acceso a cada categoría de información apropiado según el cargo y la función laboral del usuario. Una manera eficaz de abordar las preguntas en torno a la seguridad y la confidencialidad incluye las siguientes definiciones:

- ¿Quién tiene acceso a los datos o la información?
- Definición de datos o conjuntos de información a los que tiene acceso un profesional particular.
- Establecimiento de mecanismos para educar y obligar (mediante acciones disciplinarias) al individuo que tiene acceso a la información a mantener el carácter confidencial.
- Reglas para la divulgación de información relacionada con la condición socioeconómica de las personas.
- Establecimiento de barreras físicas y elementos de disuasión para los sistemas con el fin de proteger los datos y el equipo de procesamiento de datos contra la entrada no autorizada, la corrupción, el desastre, el hurto y el daño intencional o no intencional.

Muchas características bajo el tema general de la seguridad merecen la consideración de las empresas. La seguridad puede aplicarse a nivel de los equipos informáticos o software y una arquitectura de acceso remoto seguro puede combinar una variedad de tecnologías: "firewalls", autenticación, redes virtuales privadas, filtros, prevención de fallas de seguridad de software, cifrado, contraseñas, etc., pero las características de seguridad que repercuten directamente en la confidencialidad y en la protección del uso de los datos electrónicos de personas se clasifican en cinco categorías básicas:

1. ***Seguridad física.*** Los problemas más comunes comprenden iluminación, fluctuaciones de potencia, inundaciones, incendios, carga eléctrica estática y condiciones ambientales inadecuadas. El robo de equipos y medios de datos es menos común pero puede ser desastroso. Un plan de contingencia para la recuperación y la copia de seguridad de datos en caso de desastres y equipo redundante son maneras de abordar problemas de esta naturaleza.
2. ***Autenticación.*** Se trata del método más básico. Implica un usuario que envía un código de identificación de usuario, junto con una contraseña, a la red que el usuario interroga. El sistema de seguridad de la red compara la identidad con la contraseña y "autentica" al usuario en el caso de una coincidencia, o niega el acceso del usuario si no hay coincidencia. Se pueden definir diferentes niveles de acceso para el mismo registro.
3. ***Cifrado.*** El cifrado es el método de codificar un mensaje, un campo, formas, datos o toda una red, con el uso de claves alfanuméricas que mezclan desordenadamente los datos para que solo los individuos que poseen la clave apropiada puedan descifrar y leer la información. El resultado final es datos asegurados. La clave de cifrado puede ser una cadena de dígitos que tienen una relación matemática con una clave de descifrado correspondiente, de manera que una se utiliza para cifrar, otra para descifrar o la misma clave puede utilizarse para cifrar y descifrar.
4. ***Firma digital.*** Se trata de una marca de identificación proporcionada por el remitente/compositor en cada transacción de comunicaciones para demostrar que realmente envió el mensaje. Las firmas digitales reúnen las siguientes condiciones: son imposibles de imitar fraudulentamente, son auténticas, no alterables y no

reutilizables. Potencialmente tienen mayor autoridad legal que las firmas manuscritas.

5. ***Control de acceso.*** Es una forma compleja de seguridad de amplia aplicación en todos los sectores de una organización. Los sistemas para el control de acceso funcionan al permitir a la empresa definir varias funciones. Los ejemplos de las funciones son directivos, gerentes, especialistas de consulta, secretarias, administradores de departamentos, empleados, etc. Diferentes funciones tienen acceso permitido a diferentes niveles de datos, más allá del requisito sencillo de autenticación. Los métodos para el control de acceso tienen el potencial excelente de proteger datos confidenciales de clientes.

Estas categorías presentan muchas características, algunas sutiles, otras obvias (**Cuadro 4.1**)

La empresa que automatiza la seguridad en una red debe investigar a fondo los elementos específicos de los proveedores que suministran la seguridad electrónica.

Sin embargo, el factor humano es el eslabón más débil en la prevención de la seguridad y las fallas de confidencialidad en cualquier entorno. La mayoría de los episodios de fallas de seguridad en los sistemas y acceso no autorizado a registros confidenciales se relacionan con la falta de procedimientos o procedimientos mal ejecutados o supervisados y el uso con mala intención o el daño de los sistemas por miembros, empleados descontentos, actividad fraudulenta o criminal, y espionaje.

Recientemente, los expertos en seguridad han formulado advertencias a las organizaciones sobre el riesgo incrementado de ataques externos y los peligros implícitos en bajar archivos ejecutables (Java applets, Active X) y recomiendan que nunca debe permitirse la ejecución de un código en el que no se tiene confianza en la red institucional.

Se debe definir un plan de recuperación para compensar los efectos de un desastre impredecible o la pérdida de datos. Tal operación de contingencia puede expresarse en un documento que delinee los pasos necesarios para recuperación, incluida una lista de las operaciones críticas, financieras o de otro tipo, que deben reanudarse de inmediato y una lista de todos los elementos de software (aplicaciones y archivos de datos) necesarios para llevar a cabo las operaciones críticas de la organización.
El documento debe incluir también las listas de equipos, las consideraciones sobre la prestación de servicios de los proveedores, las especificaciones de las interconexiones de comunicaciones y las personas a quienes dirigirse. En muchos países se ha introducido la intervención del gobierno y las limitaciones legales, especialmente en países de Europa.

Un conjunto de recomendaciones en torno al tema de la seguridad fue desarrollado por el Gobierno de los Estados Unidos y dirigido al mejoramiento de las medidas de seguridad en las organizaciones

Requisito	Implementación
Certificación. Cadena de confiable de gestión confidencial entre socios. Plan de contingencia (todas las características de implementación enumeradas deben ponerse en vigencia)	Aplicaciones y análisis de la sensitividad de los datos. Plan para copia de seguridad de datos. Plan de recuperación para casos de desastres. Plan de operación en modalidad de emergencia. Puesta a prueba y revisión.
Mecanismo formal para el procesamiento de registros. Control de acceso a la información (todas las características de implementación enumeradas deben ponerse en vigencia).	Autorización de acceso. Determinación de acceso. Modificación de acceso.
Auditoría interna. Seguridad de personal (todas las características de implementación enumeradas deben ponerse en vigencia).	Asegure la supervisión del personal de mantenimiento por parte de persona autorizada y con conocimientos. Mantenimiento de registro de las autorizaciones de acceso. Personal de operaciones, y en algunos casos, de mantenimiento con autorización adecuada de acceso. Procedimiento de aprobación de personal. Política/procedimiento de seguridad del personal. Capacitación en seguridad de los usuarios del sistema, incluido el personal de mantenimiento.
Gestión de la configuración de seguridad (todas las características de implementación enumeradas deben ponerse en vigencia).	Documentación. Evaluación de instalación y mantenimiento y prueba de las características de seguridad en los equipos y el software. Inventario. Prueba de seguridad. Control de virus.
Procedimientos para incidentes de seguridad (todas las características de implementación enumeradas deben ponerse en vigencia).	Procedimientos para informes. Procedimientos para respuesta. Proceso para gestión de seguridad (todas las características de implementación enumeradas deben ponerse en vigencia). Análisis de riesgos. Gestión de riesgos. Política de sanciones. Política de seguridad.
Procedimientos de terminación (todas las características de implementación enumeradas deben ponerse en vigencia).	Cambio de los candados con combinación. Remoción de las listas de acceso. Remoción de la(s) cuenta(s) de usuario(s). Retorno de llaves, insignias o tarjetas que permiten el acceso.
Capacitación (todas las características de implementación enumeradas deben ponerse en vigencia).	Capacitación de todo el personal para crear conciencia Recordatorios periódicos de seguridad. Instrucción a los usuarios en lo que respecta a la protección contra virus. Instrucción a los usuarios en lo que respecta a la importancia de supervisar "log-ins" satisfactorios o no y cómo informar las discrepancias. Capacitación de los usuarios para el manejo de contraseñas.

Cuadro 4.1. Procedimientos administrativos para proteger la integridad, confidencialidad y disponibilidad de los datos

CHECKLIST PARA IDENTIFICAR LAS NECESIDADES DE SERVICIOS EN SEGURIDAD Y AUDÍTORIA DE SISTEMAS[7]

Nombre del Cliente (Empresa): _____

1. Talento Humano asignado a la Función de Sistemas de Información.

1.1 Cantidad de personas en el área de Sistemas: _____

1.2 Perfil del personal de sistemas.

Perfil	Cantidad
Tecnólogos en Sistemas	
Ingenieros de Sistemas	
Especialistas en Telecomunicaciones.	
Otros (Indique)	

2. Plataformas de Hardware y Software utilizadas.

Plataforma	Descripción
Sistemas Operacionales	
Motores de Bases de Datos	
Otras Herramientas de Desarrollo	
Software de Red.	
Equipos Activos de la Red	
Internet	
Intranet	
Extranet	
Servidores de Correo Electrónico	
Firewalls	
Servidores de Archivo	
Mainframes	
Minicomputares	
Microcomputadores	
E-business	
Business Intelligence	
Data Warehouse	
Otras (indique)	

[7] Auditoría Integral y Seguridad de Sistemas de Información. www.audisis.com/docs/checklist.doc

3. Sistemas de Información ERPs (Enterprise Resource Planning) que utiliza la empresa.

No	Nombre del ERP	Módulos Componentes

4. Portafolio de Aplicaciones o Módulos de Sistemas de Información ERPs que están en producción y su importancia para la empresa.

No	Nombre de la Aplicación	Importancia Para la Empresa (1)	Herramienta de Desarrollo Utilizada	Poseen Programas Fuentes ? (2)

5. Portafolio de Aplicaciones o Módulos de Sistemas de Información ERPs que están en desarrollo o implantación y su importancia para la empresa.

No	Nombre de la Aplicación	Importancia Para la Empresa (1)	Herramienta de Desarrollo Utilizada	Poseen Programas Fuentes ? (2)

(1) Importancia para los objetivos de la empresa. Utilice un numero entre 1 y 5 (1: la menor importancia; 5: la mayor importancia).

(2) Conteste SI o NO.

6. Las actividades de procesamiento de datos que se realizan en la empresa.

No	*Descripción*	**Marque con X**
1	Grabación (captura de Datos)	2 ( )
2	Control de Entradas y Salidas.	2 ( )
3	Producción de información (Procesamiento y actualización de archivos).	2 ( )
4	Help Desk.	2 ( )
5	Soporte a usuarios de microcomputadores y LANs.	2 ( )
6	Mantenimiento de hardware.	2 ( )
7	Administración de bases de datos (DBA)	2 ( )
8	Administración de la Seguridad lógica (controles de acceso)	2 ( )
9	Planeación estratégica de sistemas.	2 ( )
10	Administración de contratos de terceras partes.	2 ( )
11	Definición e implementación de políticas de seguridad corporativas.	2 ( )
12	Análisis y Diseño de Sistemas.	2 ( )
13	Construcción de Programas (Elaboración de programas de computador).	2 ( )
14	Mantenimiento de Software Aplicativo	2 ( )
15	Administración de Telecomunicaciones.	2 ( )
16	Quality Assurance.	2 ( )
17	Otras.	2 ( )

7. **Servicios de procesamiento de datos que son contratados con terceros.**

No	*Descripción*	**Marque con X**
1	Mantenimiento de hardware.	2 ( )
2	Administración de los Centros de Procesamiento de Datos	2 ( )
3	Grabación de Datos	2 ( )
4	Planeación estratégica de sistemas.	2 ( )
5	Interventoría de proyectos de sistemas.	2 ( )
6	Planeación de Contingencias en Sistemas de Información.	2 ( )
7	Análisis y Diseño de Sistemas.	2 ( )
8	Programación de aplicaciones.	2 ( )
9	Mantenimiento de Software Aplicativo	2 ( )
10	Administración y soporte técnico en Telecomunicaciones.	2 ( )
11	Quality Assurance (Aseguramiento de calidad).	2 ( )
12	Seguridad en Sistemas de Información.	
13	Otras (indíquelas).	2 ( )

8. Módulos Componentes del Sistema de Información Comercial (Diligenciar únicamente en empresas de servicios públicos)

No	*Descripción*	**Marque con X**
1	Facturación.	
2	Recaudos	
3	Solicitudes de Servicios	
4	Atención al Suscriptor	
5	Medidores	
6	Financiación de servicios y de deuda	
7	Control de Perdidas y Fraudes	
8	Cartera	
9	Enlace Financiero	
10	Seguridad y Administración del sistema	
11	Estadísticas	
12	Auditoria de Sistemas	
13	Administración de Parámetros Generales	
14	Facturación en sitio	
15	Otros (especifique)	

9. Servicios de Control Interno y Seguridad de Sistemas que Ud. Solicita (que son de su interés.)

No	*Descripción*	**Marque con X**
1	Asesoría para implantación de estándar COBIT (Control Objectives for Information and Related Technology).	
2	Diseño e implantación de Controles en operaciones de negocio que se soportan en Sistemas de Información (Aplicaciones de Computador).	
3	Diseño e implantación del Plan de Acción de Prevención y Mitigación de Riesgos (Mapas de Riesgo).	
4	Diseño e implantación de controles en el Desarrollo de Sistemas (especifique)	
5	Aseguramiento de Calidad del Software	
6	Aseguramiento de Calidad de Bases de Datos	
7	Elaboración e Implantación del Plan de Continuidad (Contingencias) en Sistemas de Información.	
8	Ejecución de pruebas de software	
9	Asesoría para implantar AUDICONTROL (Metodología Asistida por computador para Diseño de Controles y Administración de Riesgos en Sistemas de Información).	
10	Capacitación en Controles y Seguridad en Sistemas de Información.	
11	Definición de Políticas, Estándares y Procedimientos de Seguridad en Tecnología de Información	
12	Otros (Especifique)	

10. Servicios de Auditoria de Sistemas que Ud. Solicita (que son de su interés).

No	*Descripción*	**Marque con X**
1	Auditoria a la Organización y Funcionamiento de la Informática de la Empresa (Auditoria de Controles Generales de Sistemas de Información)	
2	Auditoría de Sistemas ERPs y Aplicaciones en Producción	
3	Auditoria al Sistema de Información Comercial (Únicamente para empresas de Servicios Públicos)	
4	Auditoría al Desarrollo de Sistemas (especifique)	
5	Auditoria al Plan de Contingencias de Sistemas de Información (Continuidad del Negocio)	
6	Desarrollo de Software de Auditoria (Especifique)	
7	Organización e Implantación de la Auditoría de Sistemas.	
8	Asesoría para la adquisición de Software de Auditoría	
9	Capacitación en Auditoría de Sistemas.	
10	Asesoría para implantar el enfoque de Auditoría de Sistemas Orientada al Riesgo.	
12	Asesoría para implantar AUDAP (Metodología Asistida por Computador para auditoría orientada al riesgo en Operaciones de Negocio Automatizadas).	
13	Asesoría para implantar el software IDEA (Interactive Data Extraction and Analysis).	
14	Otros – Especifique	

11. Periodicidad de los servicios de auditoria de Sistemas solicitados.

No	*Descripción*	**Marque con X**
1	Por una sola vez (trabajo puntual).	
2	Por periodos Anuales	
3	Asesoría Permanente	
4	Otro – Especifique	

Nombre del funcionario encuestado:_____

Cargo: _____

Tel: _____

Fecha: _____.

CAPÍTULO V

IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes (seguridad física por ejemplo) otras no lo son tanto e incluso algunas pueden ocasionar una sensación de falsa seguridad.

Muchas de las vulnerabilidades estudiadas son el resultado de alguna implementación incorrecta de tecnologías, otras son consecuencia de la falta de planeamiento de las mismas pero, como ya se ha mencionado, la mayoría de los agujeros de seguridad son ocasionados por los usuarios de dichos sistemas y es responsabilidad del administrador detectarlos y encontrar la mejor manera de cerrarlos.

Ninguna de las técnicas expuestas a continuación representarán el 100% de la seguridad deseada ya que no existe la seguridad total, y aunque muchas parezcan la panacea, más bien será la suma de varias de ellas las que convertirán un sistema interconectado en uno confiable.

5.1 Administración de la Seguridad

Es posible dividir las tareas de administración de seguridad en tres grandes grupos:

- **Autenticación:** se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.
- **Autorización:** es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.
- **Auditoría:** se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su "voluntad de hacer algo" que permita detener un posible ataque antes de que éste suceda (proactividad). Tema que ya se abordó en el presente trabajo de tesis, ahora se trata de la implementación de las políticas, para lo cual se cuenta con algunos métodos de protección, entre los que más comúnmente son empleados se encuentran los siguientes:

1. **Sistemas de detección de intrusos:** son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.
2. **Sistemas orientados a conexión de red:** monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el

rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuego (Firewalls) y los Wrappers.

3. **Sistemas de análisis de vulnerabilidades:** analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "desventaja"de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.
4. **Sistemas de protección a la integridad de la información:** sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest (MD5) o Secure Hash Algorithm (SHA), o bien sistemas que utilizan varios de ellos como PGP, Tripwire y DozeCrypt.
5. **Sistemas de protección a la privacidad de la información:** herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas se puede citar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los Certificados Digitales.

5.2 Penetration Test , Ethical Hacking o Prueba de Vulnerabilidad

*"El **Penetration Test** es el conjunto de metodologías y técnicas, para realizar una evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de accesos, a cualquier entorno informático, de un intruso potencial desde diferentes puntos de entrada que existan, tanto internos como remotos"*[8]

El objetivo general del Penetration Test es acceder a los equipos informáticos de la organización tratada e intentar obtener los privilegios del administrador del sistema, logrando así realizar cualquier tarea sobre dichos equipos. También se podrá definir otros objetivos secundarios que permitan realizar pruebas puntuales sobre algunos ámbitos particulares de la empresa.

El **Penetration Test** se compone de dos grandes fases de testeo:

1. **Penetration Test Externo:** el objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del Firewall y consisten en penetrar la Zona Desmilitarizada para luego acceder a la red interna . Se compone de un elevado número de pruebas, entre las que se puede nombrar:

    - Pruebas de usuario y la "fuerza" de sus passwords.
    - Captura de tráfico.
    - Detección de conexiones externas y sus rangos de direcciones.
    - Detección de protocolos utilizados.

[8] ARDITA, Julio Cesar. "prueba de Vulnerabilidad". 1996-2001 CYBSEC S.A. http: //www.cybsec.com

- Scanning de puertos TCP, UDP e ICMP.
- Intentos de acceso vía accesos remotos, módems, Internet, etc.
- Análisis de la seguridad de las conexiones con proveedores, trabajadores remotos o entidades externas a la organización.
- Pruebas de vulnerabilidades existentes y conocidas en el momento de realización del Test.
- Pruebas de ataques de Denegación de Servicio.

2. **Penetration Test Interno:** este tipo de pruebas trata de demostrar cuál es el nivel de seguridad interno. Se deberá establecer que puede hacer un Insider y hasta donde será capaz de penetrar en el sistema siendo usuario con privilegios bajos. Este Test también se compone de numerosas pruebas:

   - Análisis de protocolos internos y sus vulnerabilidades.
   - Autenticación de usuarios.
   - Verificación de permisos y recursos compartidos
   - Test de los servidores principales (WWW, DNS, FTP, SMTP, etc.).
   - Test de vulnerabilidad sobre las aplicaciones propietarias.
   - Nivel de detección de la intrusión de los sistemas.
   - Análisis de la seguridad de las estaciones de trabajo.
   - Seguridad de la red.
   - Verificación de reglas de acceso.
   - Ataques de Denegación de Servicio.

Para proteger nuestro sistema y partiendo de el análisis realizado para la identificación de riesgos y amenazas, se ha diseñado una política de seguridad que incluya responsabilidades y reglas para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan.

Para ello establecimos una serie de mecanismos de seguridad que se dividen en 4 grandes grupos, mecanismos de prevención, de detección, de recuperación y de auditoría.

a) **Mecanismos de prevención**

Garantizan la seguridad del sistema durante su uso habitual. Podemos destacar los mecanismos ya mencionados en autentificación, autorización, confidencialidad, integridad de la información, no repudio y disponibilidad.

Los disquetes, CD-ROM's, y otros medios *removibles* que entran y salen de nuestro sistema deberán ser tenidos en cuenta, así como los medios no electrónicos como impresos, faxes, teletipos, pantallas, con que las personas tratan la información.

Para todos ellos las soluciones serán fundamentalmente organizativas. Hoy la inmensa mayoría de las computadoras está conectado a una red, y de éstos, la inmensa mayoría utiliza *TCP/IP* como lenguaje de comunicación. TCP/IP es el conjunto de protocolos de comunicación estándar de Internet, por lo que toda computadora conectada a Internet entiende TCP/IP.

Mediante este protocolo, una máquina puede establecer múltiples conexiones simultáneas por lo que se denominan *puertos,* un concepto similar a los canales del televisor, los cuales vienen en un único cable. Existen puertos dedicados a tareas específicas, como por ejemplo, el puerto 80, dedicado a dar servicio de páginas Web. Para atender las peticiones a estos puertos existen diversos programas, llamados *demonios,* que se encargan de responder a esas peticiones. Los demonios son programas, por lo que no son perfectos. Es posible enviar peticiones extrañas a un demonio asociado a un puerto y conseguir efectos como la parada del equipo, tomar el control del equipo, conseguir contraseñas, etc. Esta suele ser la labor de los hacker.

Un elemento especialmente interesante que nos permite delimitar claramente quien entra y qué hace es el cortafuegos *(firewall).* Este elemento se utiliza para controlar el acceso desde cualquier sitio hacia el interior de nuestra red que es el entorno de nuestro interés por proteger, más sin embargo no brinda ninguna protección de ataques internos. Se basa, fundamentalmente, en el filtrado de paquetes IP. Este sistema está, generalmente, implementado como una tabla de condiciones y acciones, reglas que efectúan un filtrado de paquetes basándose en el origen y destino del paquete, así como el servicio TCP/IP que utiliza (Web, correo).

Un cortafuegos moderno, además del filtrado de paquetes implementa toda una serie de mecanismos adicionales de seguridad que nos defienden de ataques de denegación de servicio, de ataques *spoofing* (cuando alguien modifica sus paquetes IP para simular que se encuentra en una zona diferente a la dirección IP real)

Otro elemento que aporta un alto grado de seguridad es el denominado *proxy de aplicaciones.* Su funcionamiento también es muy simple. Consiste en una especie de embudo por la que hacemos pasar los servicios TCP/IP de todo un grupo de máquinas para limitarlos. Obtenemos una serie de ventajas entre las cuales está como que el exterior tan solo ve una máquina trabajando fuera (con la consiguiente simplificación de nuestras reglas de cortafuegos) y que podemos limitar los servicios según nuestras necesidades (por ejemplo permitir FTP en descarga pero no en envío).

A la vez se pueden añadir técnicas de NAT (Traducción de direcciones de red) que nos permiten ocultar al exterior las verdaderas direcciones de nuestras máquinas. Un ejemplo muy habitual es transformar la dirección de nuestro proxy.

b) **Mecanismos de detección**

Un grupo de tecnologías se encargan de detectar intentos de ataques o ataques propiamente dichos. Aportan unas ciertas medidas de monitorización y detección de actividad sospechosa, que pueden ser más o menos "inteligentes". Desde el simple registro de los paquetes que llegan al sistema, pasando por los que analizan las franjas horarias, las direcciones que nos "scanean", ..., hasta aquellos que simulan servicios que no existen para tentar a los atacantes y así descubrirlos. Los propios cortafuegos implementan muchas de estas técnicas.

Otro tipo de tecnologías son las de análisis de riesgos. Estas se encargan de detectar problemas de seguridad en nuestros sistemas. Los hay de muchos tipos:

Herramientas que realizan un barrido en nuestros sistemas comprobando agujeros de seguridad conocidos en el sistema:

Son los ***analizadores de vulnerabilidades***: herramientas que se encargan de advertir de todos los servicios que nuestro sistema está ofertando a la red ya que en muchas ocasiones son más de los necesarios.

Los ***scanner de puertos*** son herramientas que hacen una "foto" del sistema en su origen, y que permiten comprobar que todo sigue igual con el paso del tiempo, y no se han producido modificaciones al software básico.

Estas "fotos" se basan en algoritmos ***hash*** sobre los archivos clave del sistema, herramientas que actúan sobre las contraseñas del sistema. Se encargan de detectar la vulnerabilidad de estas contraseñas.

Otro tipo de tecnologías se encarga de los fallos hardware, la monitorización, las alertas, acciones ante fallos, etc. Todo un abanico de herramientas de gestión de infraestructuras que permiten detectar fallos, en muchas ocasiones, antes de que produzcan daños al sistema. Y no solo fallos, también se encargan de detectar los niveles de saturación de los elementos críticos antes de que se produzcan problemas en el servicio.

Por último un elemento imprescindible de detección en una red es el ***antivirus***, programa, o conjunto de programas, encargados de mantener una computadora y/o una red libres de virus. Se deberán colocar antivirus en todos los puntos de entrada/salida de información de nuestro sistema.

c) **De recuperación**

Nos permiten recuperar el estado habitual del sistema tras una falla o ataque. Fundamentalmente son herramientas basadas en las copias de seguridad.

d) **De auditoría**

Nos permiten determinar las causas de los problemas antes, durante y después de que suceda. Fundamentalmente son registros de los sucesos que se van produciendo en el sistema: usuarios que entran, acciones que realizan, tiempos en los que se hacen las cosas...

5.3 HoneyPots – HoneyNets

Estas "Trampas de Red" son sistemas que se activan con la finalidad específica de que los expertos en seguridad puedan observar en secreto la actividad de los Hackers/Crackers en su habitad natural.

Consiste en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los Honeynets dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos.

5.4 Firewalls

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información.

El firewall podrá únicamente autorizar el paso del trafico, y el mismo podrá ser inmune a la penetración. desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

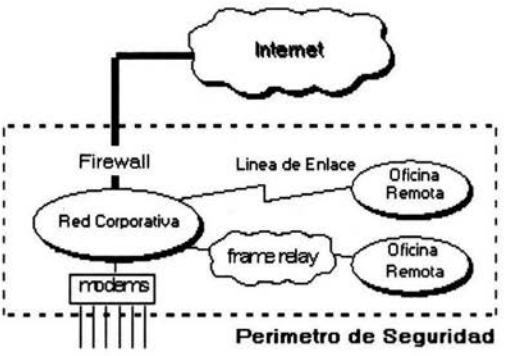

Figura 5.1 : La Política de Seguridad Crea un Perímetro de Defensa.

Esto es importante, ya que debemos notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información (**Figura 5.1**).

Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

5.4.1 Beneficios de un firewall en Internet

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa , este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del trafico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.

Figura 5.2: Beneficios De Un Firewall De Internet.

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs) (Ver **Figura.5.2)**

Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Finalmente, el firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando - únicamente el acceso al Internet esta perdido - .

La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significa dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente.

5.4.2 Limitaciones de un firewall

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

Por ejemplo, si existe una conexión dial-out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet.(**Figura 5.3**) Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un Firewall Proxy server (FPS) lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque. Los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.

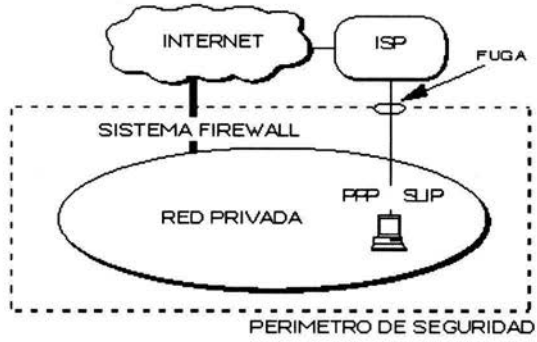

Figura 5.3 Conexión Circunvecina al Firewall de Internet.

El firewall no puede protegerse de las amenazas a que está sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquetes o tarjetas PCMCIA y substraigan estas del edificio.

El firewall no puede proteger contra los ataques de la "Ingeniería Social", por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor del corporativo o que le permita el acceso "temporal" a la red.

Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software. Obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el.

La solución real esta en que la organización debe ser consciente en instalar software antiviral en cada despacho para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentes datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo mas fácil el acceso de un intruso al sistema.

Como nosotros podemos ver, el desempeño de los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles por los ataques con transferencia de datos.

5.4.3 Bases para el diseño decisivo del firewall

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

- Posturas sobre la política del Firewall.
- La política interna propia de la organización para la seguridad total.
- El costo financiero del Proyecto "Firewall".
- Los componentes o la construcción de secciones del Firewall.

5.4.4 Políticas del firewall.

Las posturas del sistema firewall describen la filosofía fundamental de la seguridad en la organización. Estas son dos posturas diametralmente opuestas que la política de un firewall de Internet puede tomar:

- "No todo lo específicamente permitido esta prohibido"
- "Ni todo lo específicamente prohibido esta permitido"

La primera postura asume que un firewall puede obstruir todo el trafico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso.

Esta propuesta es recomendada únicamente a un limitado numero de servicios soportados cuidadosamente seleccionados en un servidor. La desventaja es que el punto de vista de "seguridad" es mas importante que - facilitar el uso - de los servicios y estas limitantes numeran las opciones disponibles para los usuarios de la comunidad. Esta propuesta se basa en una filosofía conservadora donde se desconocen las causas acerca de los que tienen la habilidad para conocerlas.

La segunda postura asume que el firewall puede desplazar todo el trafico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso. Esta propuesta crea ambientes mas flexibles al disponer mas servicios para los usuarios de la comunidad. La desventaja de esta postura se basa en la importancia de "facilitar el uso" que la propia - seguridad - del sistema. También además, el administrador de la red esta en su lugar de incrementar la seguridad en el sistema conforme crece la red. Desigual a la primer propuesta, esta postura esta basada en la generalidad de conocer las causas acerca de los que no tienen la habilidad para conocerlas

5.5 Edificando obstáculos: ruteador filtra-paquetes

Este ruteador toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos.(**Figura 5.4)** El ruteador examina cada datagrama para determinar si este corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP, ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interfase de entrada del paquete, y la interfase de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

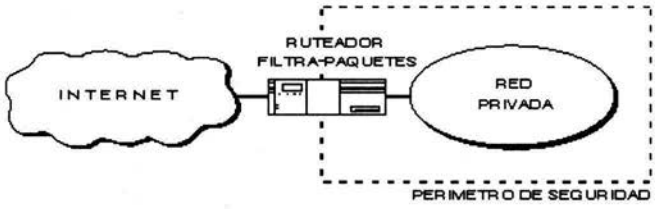

Figura 5.4: Ruteador Filtra-Paquetes.

5.5.1 Servicio dependiente del filtrado

Las reglas acerca del filtrado de paquetes a través de un ruteador para rehusar/permitir el trafico esta basado en un servicio en especifico, desde entonces muchos servicios vierten su información en numerosos puertos TCP/UDP conocidos.

Por ejemplo, un servidor Telnet esta a la espera para conexiones remotas en el puerto 23 TCP y un servidor SMTP espera las conexiones de entrada en el puerto 25 TCP. Para bloquear todas las entradas de conexión Telnet, el ruteador simplemente descarta todos los paquetes que contengan el valor del puerto destino TCP igual a 23. Para restringir las conexiones Telnet a un limitado numero de servidores internos, el ruteador podrá rehusar el paso a todos aquellos paquetes que contengan el puerto destino TCP igual a 23 y que no contengan la dirección destino IP de uno de los servidores permitidos.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un ruteador filtra-paquetes para perfeccionar su funcionamiento serian:

- Permitir la entrada de sesiones Telnet únicamente a una lista especifica de servidores internos.
- Permitir la entrada de sesiones FTP únicamente a los servidores internos especificados.
- Permitir todas las salidas para sesiones Telnet.
- Permitir todas las salidas para sesiones FTP.
- Rehusar todo el trafico UDP.

5.5.2 Servicio independiente del filtrado

Este tipo de ataques ciertamente son difíciles de identificar usando la información básica de los encabezados debido a que estos son independientes al tipo de servicio. Los ruteadores pueden ser configurados para protegerse de este tipo de ataques pero son mas difíciles de especificar desde entonces las reglas para el filtrado requieren de información adicional que pueda ser estudiada y examinada por la tabla de ruteo, inspeccionando las opciones especificas IP, revisando fragmentos especiales de edición, etc. Algunos ejemplos de este tipo de ataques incluye:

Agresiones Originadas Por El Direccionamiento IP.

Para este tipo de ataque, el intruso trasmite paquetes desde afuera pretendiendo pasar como servidor interno

- Los paquetes poseen una dirección fuente IP falsa de un servidor interno del sistema
- El agresor espera que usando este impostor se pueda penetrar al sistema para emplearlo seguramente como dirección fuente donde los paquetes que trasmita sean autentificados y los del otro servidor sean descartados dentro del sistema. Los ataques por seudo-fuentes pueden ser frustrados si descartamos la dirección fuente de cada paquete con una dirección fuente "interno" si el paquete arriva en una de las interfaces del ruteador "externo".

Agresiones Originadas En El Ruteador.

En un ataque de ruteo, la estación de origen especifica la ruta que un paquete deberá de tomar cuando cruce a través del Internet. Este tipo de ataques son diseñados para cuantificar las derivaciones de seguridad y encauzan al paquete por un inesperado camino a su destino. Los ataques originados en el ruteador pueden ser frustrados simplemente descartando todos los paquetes que contengan fuentes de ruteo opcionales.

Agresiones Por Fragmentación.

Por este tipo de ataques, los intrusos utilizan las características de fragmentación para crear fragmentos extremadamente pequeños y obligan a la información del encabezado TCP a

separarse en paquetes. Estos pequeños fragmentos son diseñados para evitar las reglas definidas por el filtrado de un ruteador examinando los primeros fragmentos y el resto pasa sin ser visto. Aunque si bien únicamente es explotado por sencillos decodificadores , una agresión pequeñísima puede ser frustrada si se descartan todos los paquetes donde el tipo de protocolo es TCP y la fragmentación de compensación IP es igual a 1.

5.5.3 Beneficios del ruteador filtra-paquetes

La mayoría de sistemas firewall son desplegados usando únicamente ruteadores filtra-paquetes. Otros que tienen tiempo planean los filtros y configuran el ruteador, sea este pequeño o no , el costoso para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto. Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del ruteador moderando el trafico y definiendo menos filtros. Finalmente, el ruteador de filtrado es por lo general transparente a los usuarios finales y a las aplicaciones por lo que no se requiere de entrenamiento especializado o software especifico que tenga que ser instalado en cada uno de los servidores.

5.5.4 Limitaciones del ruteador filtra-paquetes

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo. Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo mas difícil su administración y comprensión. Finalmente, estas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas en el ruteador. Potencialmente se puede dejar una localidad abierta sin probar su vulnerabilidad.

Cualquier paquete que pasa directamente a través de un ruteador puede ser posiblemente usado como parte inicial un ataque dirigido de datos. Haciendo memoria este tipo de ataques ocurren cuando los datos aparentemente inocuos se desplazan por el ruteador a un servidor interno. Los datos contienen instrucciones ocultas que pueden causar que el servidor modifique su control de acceso y seguridad relacionando sus archivos facilitando al intruso el acceso al sistema.

Generalmente, los paquetes entorno al ruteador disminuyen conforme el numero de filtros utilizados se incrementa. Los ruteadores son optimizados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes para la interfase apropiada de la transmisión. Si esta autorizado el filtro, no únicamente podrá el ruteador tomar la decisión de desplazar cada paquete, pero también sucede aun aplicando todas las reglas de filtrado. Esto puede consumir ciclos de CPU e impactar el perfecto funcionamiento del sistema.

El filtrado de paquetes IP no puede ser capaz de proveer el suficiente control sobre el trafico. Un ruteador Filtra-Paquetes puede permitir o negar un servicio en particular, pero no es capaz de comprender el contexto/dato del servicio. Por ejemplo, un administrador de red necesita filtrar el trafico de una capa de aplicación - limitando el acceso a un subconjunto de comandos disponibles por FTP o Telnet, bloquear la importación de Mail o Newsgroups concerniente a tópicos específicos. Este tipo de control es muy perfeccionado a las capas altas por los servicios de un servidor Proxy y en Gateways a Nivel-aplicación.

5.6 Edificando obstáculos: gateways a nivel-aplicación

Los gateways nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes. Mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de proposito-especial (un servicio Proxy) para cada aplicación deseada. Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrán desplazarse a través del firewall.

Aun cuando, el código Proxy puede ser configurado para soportar únicamente las características especificas de una aplicación que el administrador de red considere aceptable mientras niega todas las otras.

Un aumento de seguridad de este tipo incrementa nuestros costos en términos del tipo de gateway seleccionado, los servicios de aplicaciones del Proxy, el tiempo y los conocimientos requeridos para configurar el gateway, y un decrecimiento en el nivel de los servicios que podrán obtener nuestros usuarios, dando como resultado un sistema carente de transparencia en el manejo de los usuarios en un ambiente "amigable". Como en todos los casos el administrador de redes debe de balancear las necesidades propias en seguridad de la organización con la demanda de "fácil de usar" demandado por la comunidad de usuarios.

Es importante notar que los usuarios tienen acceso por un servidor Proxy, pero ellos jamás podrán seccionar en el Gateway a nivel-aplicación. Si se permite a los usuarios seccionar en el sistema de firewall, la seguridad es amenazada desde el momento en que un intruso puede potencialmente ejecutar muchas actividades que comprometen la efectividad del sistema.

Por ejemplo, el intruso podría obtener el acceso de root, instalar un caballo de Troya para colectar las contraseñas, y modificar la configuración de los archivos de seguridad en el filrewall.

5.6.1 Servidor de defensa

Un ruteador filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, diferente a esto el Gateway a nivel-aplicación deja que la información circule entre los sistemas pero no permite el intercambio directo de paquetes. El principal riesgo de permitir que los paquetes se intercambien dentro y fuera del sistema se debe a que el

servidor residente en los sistemas de protección de la red podrá ser asegurado contra cualquier amenaza representada por los servicios permitidos.

Un Gateway a nivel-aplicación por lo regular es descrito como un "servidor de defensa" porque es un sistema diseñado específicamente blindado y protegido contra cualquier ataque. Hay varias características de diseño que son usadas para hacer mas seguro un servidor de defensa:

La plataforma de Hardware del servidor de defensa ejecuta una versión "segura" de su sistema operativo. Por ejemplo, si el servidor de defensa es una plataforma UNIX, se ejecutara una versión segura del sistema operativo UNIX que es diseñado específicamente para proteger los sistemas operativos vulnerables y garantizar la integridad del firewall.

Únicamente los servicios que el administrador de redes considera esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no esta instalado, este puede ser atacado. Generalmente, un conjunto limitado de aplicaciones Proxy tales como Telnet, DNS, FTP, SMTP, y autenticación de usuarios son instalados en este servidor.

El servidor de defensa podrá requerir de una autenticación adicional para que el usuario accese a los servicios Proxy. Por ejemplo, el servidor de defensa es ideal para colocar un sistema fuerte de supervisión de autorización (tal como la tecnología "una-sola vez" de contraseña donde una tarjeta inteligente generaba un código de acceso único por medios criptográficos). Adicionalmente, cada servicio Proxy podrá requerir de autorización propia después que el usuario tenga acceso a su sesión.

Cada Proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, es porque simplemente no esta disponible para el usuario.

Cada Proxy esta configurado para dejar acceder únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características/comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida.

Cada Proxy mantiene la información detallada y auditada de todos los registros del trafico, cada conexión , y la duración de cada conexión. El registro de audición es un herramienta esencial para descubrir y finalizar el ataque de un intruso.

Cada Proxy es un programa pequeño y sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisar y analizar posibles intrusos y fugas de seguridad. Por ejemplo, una típica aplicación - UNIX mail - puede tener alrededor de 20,000 líneas de código cuando un correo Proxy puede contener menos de mil.

Cada Proxy es independiente de todas las demás aplicaciones Proxy en el servidor de defensa. Si se sucitara un problema con la operación de cualquier Proxy, o si se descubriera un sistema vulnerable, este puede desinstalarse sin afectar la operación de las demás aplicaciones. Aun, si la población de usuarios requiere el soporte de un nuevo servicio, el

administrador de redes puede fácilmente instalar el servicio Proxy requerido en el servidor de defensa.

Un Proxy generalmente funciona sin acceso al disco lo único que hace es leer su archivo de configuración inicial . desde que la aplicación Proxy no ejecuta su acceso al disco para soporte, un intruso podrá encontrar mas dificultades para instalar caballos de Troya perjudiciales y otro tipo de archivos peligrosos en el servidor de defensa.
Cada Proxy corre como un usuario no-previlegiado en un directorio privado y seguro del servidor de defensa.

Ejemplo: telnet proxy

Obsérvese la **Figura 5.5.** Aquí se ilustra la operación de un Telnet Proxy en un servidor de defensa. Para este ejemplo, un cliente externo ejecuta una sesión Telnet hacia un servidor integrado dentro del sistema de seguridad por el Gateway a nivel-aplicación.

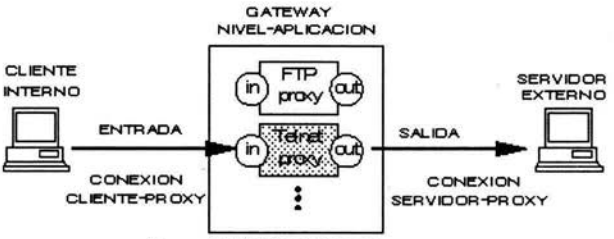

Figura 5.5 Telnet Proxy.

El Telnet Proxy nunca permite al usuario remoto que se registre o tenga acceso directo al servidor interno. El cliente externo ejecuta un telnet al servidor de defensa donde es autorizado por la tecnología "una-sola vez" de contraseña. Después de ser autentificado, el cliente obtiene acceso a la interfase de usuario del Telnet Proxy. Este únicamente permite un subconjunto de comandos Telnet y además determina cual de los servidores son disponibles para el acceso vía Telnet.

Los usuarios externos especifican el servidor de destino y el Telnet Proxy una vez hecha la conexión, los comandos internos son desplazados hacia el cliente externo. El cliente externo cree que el Telnet Proxy es el servidor interno real, mientras el servidor interno cree que el Telnet proxy es un cliente externo.

La autenticación puede basarse en "algo conocido por los usuarios" (como una contraseña) o "algo que tengan" que posean físicamente (como una tarjeta electrónica) cualquiera de las dos. Ambas técnicas están sujetas a plagio, pero usando una combinación de ambos métodos se incrementa la probabilidad del uso correcto de la autenticación. En el ejemplo de Telnet, el Proxy transmite un requerimiento de registro y el usuario, con la ayuda de su tarjeta electrónica, obtendrá una respuesta de validación por un numero. Típicamente, se le

entrega al usuario su tarjeta desactivada para que el introduzca un PIN y se le regresa la tarjeta, basada en parte como llave "secreta" de encriptación y con un reloj interno propio, una vez que se establece la sesión se obtiene un valor de respuesta encriptado.

5.6.2 Beneficios del gateway a nivel-aplicación

Son muchos los beneficios desplegados en un gateway a nivel-aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede accesar a los servicios. Aun cuando, el administrador de la red tenga el completo control acerca de que servicios que son permitidos desde la carencia de un servicio proxy para uno en particular significa que el servicio esta completamente bloqueado. Los gateways a nivel-aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información detallada de registro. Finalmente, las reglas de filtrado para un gateway de este tipo son mucho mas fáciles de configurar y probar que en un ruteador filtra-paquetes.

5.6.3 Limitaciones del gateway a nivel-aplicación

Probablemente una de las grandes limitaciones de un gateway a nivel-aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accese a los servicios Proxy. Por ejemplo, el acceso de Telnet vía gateway a nivel-aplicación demanda modificar la conducta del usuario desde el momento en que se requiere de dos pasos para hacer una conexión mejor que un paso. Como siempre, el software especializado podrá ser instalado en un sistema terminado para hacer las aplicaciones del gateway transparentes al permitir a los usuarios especificar el servidor de destino, mejor que el propio, en un comando de telnet.

5.7 Edificando obstáculos: gateway a nivel-circuito

Un Gateway a nivel-circuito es en si una función que puede ser perfeccionada en un Gateway a nivel-aplicación (**Figura 5.6**). A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

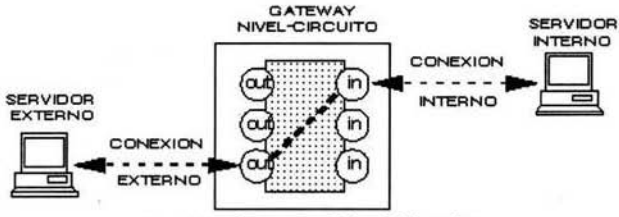

Figura 5.6: Gateway Nivel-Circuito.

Tal como se menciono anteriormente, este gateway simplemente trasmite la conexión a través del firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El gateway a nivel-circuito acciona como una cable copiando los bytes antes y después entre la conexión interna y la conexión externa. De cualquier modo, la conexión del sistema externo actúa como si fuera originada por el sistema de firewall tratando de beneficiar el encubrir la información sobre la protección de la red.

El Gateway a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un Gateway "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.
Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización de los ataques externos.

5.8 Acces Control Lists (ACL)

Las Listas de Control de Accesos proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

En la práctica, rara vez se almacena la matriz puesto que es grande y rala. La mayoría de los dominios no tienen acceso alguno a la mayoría de los objetos, por lo que el almacenamiento de una enorme matriz casi vacía es un desperdicio de espacio en disco. Sin embargo, existen dos métodos prácticos, que guardan la matriz por renglones o por columnas, pero sólo los elementos no vacíos. Los dos puntos de vista son distintos, aunque no lo parezcan.

La primera técnica asocia a cada objeto una lista (ordenada) con todos los dominios que pueden tener acceso al objeto y la forma de dicho acceso. Esta lista se llama Lista de Control de Acceso (ACL).

El propietario de un objeto puede modificar su ACL en cualquier momento, lo que hace fácil prohibir accesos antes permitidos. El único problema es que probable que la modificación de la ACL no afecte a los usuarios que utilicen en ese momento al objeto (por ej. alguien que tenga abierto el archivo).

La otras forma de dividir la matriz es por renglones. Al utilizar este método, se le asocia a cada proceso una lista de objetos a los cuales puede tener acceso, junto con una indicación con las operaciones permitidas en cada uno; en otras palabras, su dominio. Esta lista se llama Lista de Posibilidades y los elementos individuales se llaman Posibilidades.

Cada posibilidad tiene una campo Tipo, el cual indica el tipo del objeto; un campo Derechos, un mapa de bits que indica las operaciones básicas permitidas en este tipo de objeto; así como un campo objeto, un apuntador al propio objeto (por ej. su número de nodo-i). Las listas de posibilidades son a su vez objetos que se les puede apuntar desde otras listas de posibilidades, lo que facilita la existencia de subdominios compartidos. Con frecuencia, se hace referencia a las posibilidades mediante su posición en la lista. Un proceso podría decir: "Lee 1 k del archivo que apunta a la posibilidad 2". Esta forma de direccionamiento es análogo al uso de los descriptores de archivos en UNIX. (**Tabla 5.1**)

	Tipo	Derechos	Objeto
0	Archivo	R - -	Apuntador al Archivo3
1	Archivo	R W X	Apuntador al Archivo4
2	Archivo	R W -	Apuntador al Archivo5
3	Impresora	- W -	Apuntador a la impresora1

Tabla 5.1 Matriz de ACL

Es evidente que las listas de posibilidades, o listas-c, deben ser protegidas del manejo indebido por parte del usuario. Se han propuesto tres métodos para su protección. La primera necesita una arquitectura marcada, un diseño en hardware en el que cada palabra de memoria tiene un bit adicional que indica si la palabra tiene una posibilidad o no. El bit de marca no se utiliza para instrucciones aritméticas, de comparación u otras similares y solo puede ser modificado por programas que se ejecuten en modo núcleo.

La segunda vía es mantener la lista de posibilidades dentro del sistema operativo y hacer que los procesos hagan referencia a las posibilidades por su número, como se mencionó antes.

La tercera vía es mantener la lista en el espacio del usuario, pero cada posibilidad cifrada con una clave secreta desconocida para el usuario.

Además de los derechos específicos dependientes del objeto, como la lectura y la ejecución, las posibilidades tienen por lo general derechos genéricos aplicables a todos los objetos. Los siguientes son ejemplos de derechos genéricos:

- Copiar posibilidad: crear una nueva posibilidad para el mismo objeto.
- Copiar objeto: crear un duplicado del objeto con una nueva posibilidad.
- Eliminar posibilidad: eliminar un dato dentro de la lista-c sin afectar al objeto.
- Destruir objeto: eliminar en forma permanente un objeto y una posibilidad.

Muchos sistemas con posibilidades se organizan como una colección de módulos, con módulos administradores de tipos para cada tipo de objeto. Las solicitudes para llevar a cabo operaciones en un archivo se envían al administrador de archivo, mientras que las solicitudes para realizar algo con un buzón van hacia el administrador del buzón. Estas solicitudes van acompañadas por la posibilidad correspondiente. Aquí surge un problema, puesto que el módulo administrador de tipos es un programa común y corriente. El propietario de la posibilidad de un archivo puede desarrollar solo alguna de las operaciones en el archivo pero no puede penetrar a su representación interna (por ej. su nodo-i). Es esencial que el módulo administrador de tipos pueda hacer más cosas con la posibilidad que un proceso ordinario.

Una última observación acerca de los sistemas con lista de posibilidades es que la revocación del acceso a un objeto es un poco difícil. Al sistema le cuesta trabajo determinar todas las posibilidades existentes para cierto objeto y eliminarlas. Una forma de enfrentar este problema es hacer que cada posibilidad apunte hacia un objeto indirecto, en vez de apuntar a un objeto en si. Si el objeto indirecto apunta hacia el objeto real, el sistema siempre puede romper esa conexión, con lo que invalida las posibilidades.

Cada objeto contiene un enorme número aleatorio, también presente en la posibilidad. Cuando una posibilidad se presenta para su uso, se comparan los dos números. Se permita la operación solo en el caso de que estos números coincidan. El propietario de un objeto puede solicitar el cambio del número aleatorio en dicho objeto, lo cual invalida las posibilidades existentes.

5.9 Wrappers

Un Wrapper es un programa que controla el acceso a un segundo programa. El Wrapper literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad. Los Wrappers son usados dentro de la seguridad en sistemas UNIXs. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los Wrappers son ampliamente utilizados, y han llegado a formar parte de herramientas de seguridad por las siguientes razones:

- Debido a que la seguridad lógica esta concentrada en un solo programa, los Wrappers son fáciles y simples de validar.
- Debido a que el programa protegido se mantiene como un a entidad separada, éste puede ser actualizado sin necesidad de cambiar el Wrapper
- Debido a que los Wrappers llaman al programa protegido mediante llamadas estandar al sistema, se puede usar solo Wrapper para controlar el acceso a diversos programas que se necesiten proteger.
- Permite un control de acceso exhaustivo de los servicios de comunicaciones, además de buena capacidad de auditorias de petición a dichos servicios, ya sean autorizados o no.

El paquete Wrapper más ampliamente utilizado es el TCP_Wrappers, el cual es un conjunto de utilidades de distribución libre, escrito por Wietse Venema (co-autor de SATAN, con Dan Farmer, y considerado el padre de los sistemas Firewalls) en 1990.

Consiste en un programa que es ejecutado cuando llega una petición a un puerto específico. Este, una vez comprobada la dirección de origen de la petición, la verifica contra las reglas almacenadas, y en función de ellas, decide o no dar paso al servicio. Adicionalmente, registra estas actividades del sistema, su petición y su resolución.

Algunas configuraciones avanzadas de este programa, permiten también ejecutar comandos en el propio sistema operativo, en función de la resolución de la petición. Usando Wrappers se puede controlar el acceso a cada máquina y los servicios accedidos. Así, estos controles son el complemento perfecto de un Firewall y la instalación de uno no está supeditada a la del otro.

5.10 Sistema de Detección de Intrusos.

La seguridad en un sistema podríamos clasificarla de dos modos: activa y preventiva. La seguridad activa de un sistema consiste en protegerlo todo lo posible ante potenciales intentos de abuso del mismo. Un firewall es un buen ejemplo de seguridad activa, trata de filtrar el acceso a ciertos servicios en determinadas conexiones para evitar el intento de forzamiento desde alguno de ellos.

Por otro lado, la seguridad preventiva es aquella que implantamos en nuestro sistema para que nos informe si en el está teniendo lugar una incidencia de seguridad. No pretende proteger el sistema, pretende alertarnos de que algo extraño esta sucediendo en el. Un buen ejemplo de seguridad preventiva es un sistema de detección de intrusos.

Un sistema de detección de intrusos es aquel que nos permite recabar información de distintas fuentes del sistema en el que se implanta para alertar de un posible intrusión en nuestras redes o máquinas. La alerta puede ser del hecho de que existe un intento de intrusión, como del modo en el que este se está realizando y en algunos casos por parte de quién esta siendo efectuado. Podemos considerar un sistema de detección de intrusos como un control de auditoría que nos permitirá tomar decisiones a la hora de realizar una auditoría de seguridad de nuestro sistema.

Un sistema de detección de intrusos surge como una medida preventiva, nunca como una medida para asegurar nuestros sistemas, ayudan al administrador de dicho sistema a permanecer al tanto de cualquier intención aviesa contra el sistema que administra.

5.10.1 Tipos de sistemas de detección de intrusos

Llegados a este punto es interesante clasificar de algún modo los distintos sistemas de detección de intrusos.

Una primera clasificación puede ser entre sistemas en tiempo real y aquellos que no lo son. Los sistemas en tiempo real permanecerán constantemente chequeando el sistema buscando alguna señal de un incidente de seguridad e inmediatamente provocarán una alarma. Por contra, los sistemas de detección de intrusos que no son de este tipo se usan generalmente cuando existe la creencia de que estamos ante un incidente de seguridad y se usan para recabar información del tipo y alcance de esta incidencia, generalmente sobre registros o información del sistema.

Una clasificación más rigurosa la podemos realizar según los medios que utilizan los sistemas de detección de intrusos para monitorizar las incidencias. Tenemos según esta clasificación cuatro tipos de sistemas:

- Basados en el host. Estos sistemas recaban información del sistema para realizar un análisis de las posibles incidencias pero siempre desde el punto de vista del propio sistema y con sus recursos.
- Basados en la red. Sistemas que observan el tráfico de red buscando algún indicio de un ataque conocido. Generalmente un interfaz en modo promíscuo buscando datos sobre una red. (Suelen pertenecer también al tipo de tiempo real).
- Basados en la aplicación. Estos recaban datos de una aplicación activa en el sistema (por ejemplo los logs u otra) y buscan evidencias en estos datos. La diferencia con los basados en host es que estos los propios recursos son detectores de intrusos y en el caso de aplicación los datos han de ser filtrados para ser tratados como alarmas.
- Basados en el objetivo. Estos monitores se basan en salvaguardar la integridad del objetivo que podría ser cualquier recurso del sistema (por ejemplo el sistema de archivos).
- Ya por último y para terminar esta taxonomía podemos diferenciar los sistemas de detección de intrusos según el tipo de análisis que realiza:
- Detección de uso inadecuado. En estos casos el sistema busca un patrón de un ataque bien definido.
- Detección de alguna anomalía. Se busca sobre el sistema alguna anomalía que pueda hacer creer que hay un incidente de seguridad, pero que puede no ser provocada por esto.

5.10.2 Arquitectura de un sistema de detección de intrusos

Prácticamente todos los sistemas de detección de intrusos tienen ciertas partes bien definidas las cuales se listan a continuación:

- **Fuentes de recogida de datos** de aplicaciones. Punto de recogida de datos para análisis actual o posterior que bien puede ser una red, el sistema o elementos que residen en el propio sistema.
-
- **Reglas.** Estas reglas en muchos casos son las que caracterizan las violaciones que pueden ser cometidas y contra las que se contrastan los datos obtenidos en el punto anterior.
- **Filtro.** Esta parte se encarga de contrastar las reglas contra los datos obtenidos.

- **Detectores de anomalías.** En los casos de análisis por anomalías son aquellos que detectan eventos extraños en el sistema o los recursos monitorizados.

- **Generador de informes o alarmas.** Una vez que se han procesado los datos contra las reglas por el filtro y si existe alguna situación que haga creer que se ha vulnerado o intentado vulnerar la seguridad del sistema, esta parte del detector de intrusos informa al administrador de este hecho (mediante correo, mensajes a móviles, avisos acústicos, etc...).

En la **Figura 5.7** podemos ver gráficamente como se puede diseccionar la arquitectura de un sistema de detección de intrusos.

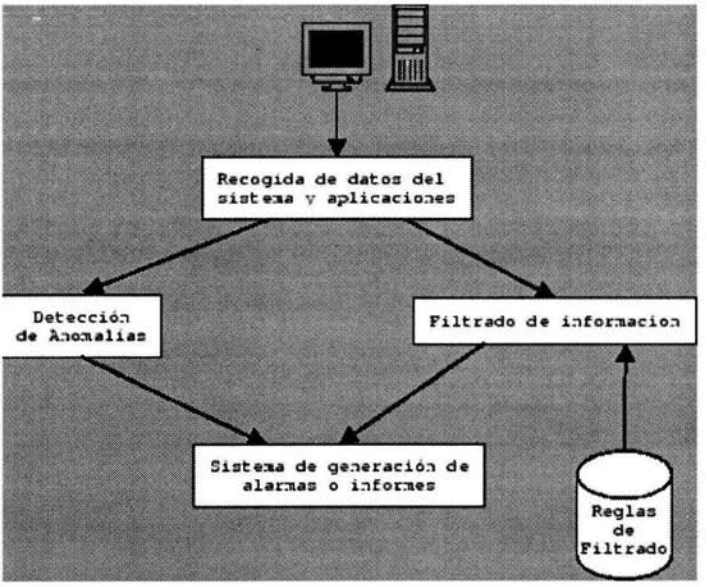

Figura 5.7: **Arquitectura de un sistema de detección de intrusos**

5.11 Call Back

Este procedimiento es utilizado para verificar la autenticidad de una llamada vía modem. El usuario llama, se autentifica contra el sistema, se desconecta y luego el servidor se conecta al número que en teoría pertenece al usuario.

La ventaja reside en que si un intruso desea hacerse pasar por el usuario, la llamada se devolverá al usuario legal y no al del intruso, siendo este desconectado. Como precaución adicional, el usuario deberá verificar que la llamada-retorno proceda del número a donde llamo previamente.

5.12 Sistemas Anti Sniffers

Esta técnica consiste en detectar Sniffers en el sistema. Generalmente estos programas se basan en verificar en estado de la placa de red, para detectar el modo en el cual está actuando y el tráfico de datos en ella.

5.13 Seguridad en protocolos y servicios

NETBIOS

Los puertos 137-139 en TCP y UDP son empleados en las redes Microsoft para la autentificación de usuarios y la compartición de recursos. Como primera medida debe minimizarse la cantidad de recursos compartidos y luego evitarse permitir el acceso global a esos dispositivos, ya que es posible el acceso de intrusos desde cualquier lugar de la red.

ICMP

A fin de prevenir los ataques basados en bombas ICMP, se deberán filtrar todos los paquetes de redirección y los paquetes inalcanzables.

FINGER

Típicamente el servicio Finger (puerto 79 en TCO) ha sido una de las principales fuentes de problemas. Este protocolo proporciona información detallada de los usuarios de una estación de trabajo, estén o no conectados en el momento de acceder al servicio.

La información suministrada suele ser de mucha utilidad para un atacante: datos del usuario, hábitos de conexión, cuentas inactivas. Está claro que esto es fácilmente aprovechable por un intruso para practicar ingeniería social contra esos usuarios.

Es básico deshabilitar este servicio, restringir su acceso a unos cuantos equipos de la red local o utilizar versiones de Finger que permiten especificar la información que se muestra al acceder al servicio.

POP

El servicio POP (puertos 109 y 110 en TCP) utilizado para que los usuarios puedan acceder a su correo sin necesidad de montar sistemas de archivos compartidos. Se trata de un servicio que se podría considerar peligroso, por lo que debemos deshabilitarlo a no ser que sea estrictamente necesario ofrecerlo; en ese caso debemos restringir al máximo los lugares y usuarios desde los que se pueden acceder.

Mediante POP se genera un transito peligroso de contraseñas a través de la red. Se ofrece tres modelos distintos de autenticación: uno basado en Kerberos, apenas utilizado, otro basado en un protocolo desafió-respuesta, y otro basado en un simple nombre de usuario con su password correspondiente.

Este último es el más usado en todo tipo de entornos, es un excelente objetivo para un intruso con un Sniffer. Los usuarios suelen configurar sus clientes para que chequen el buzón de correo cada pocos minutos, con lo que a intervalos muy cortos envían su clave a un puerto conocido de una máquina conocida; al realizar toda esta comunicación en texto claro, un atacante no tiene más que interceptar la sesión POP para averiguar nombres de usuario y claves (a parte de poder leer el correo).

NNTP

El servicio NNTP (puerto 119 en TCP) se utiliza para intercambiar mensajes de noticias entre servidores de News. Los diferentes demonios encargados de esta tarea suelen discriminar conexiones en función de la dirección o el nombre de la maquina cliente para decidir si ofrece el servicio a un determinado host, y si es así, concretar de que forma puede acceder a él(solo lectura, sólo ciertos grupos, etc.).

De esta forma, los servidores NNTP son muy vulnerables a cualquier ataque que permita falsear la identidad de la máquina origen, como el IP Spoofing.

Los problemas relacionados con las News no suelen ser excesivamente graves desde el punto de vista estrictamente técnico, pero en ocasiones si lo son aplicando una visión global. Por ejemplo, habría que evaluar el daño que le supone a la imagen de la organización el que un atacante envíe mensajes insultantes o pornográficos utilizando el nombre o los recursos de la misma.

NTP

NTP (puerto 123 en UDP y TCP) es un protocolo para sincronizar relojes de máquinas de una forma muy precisa; a pesar de su sofisticación no fue diseñado con una idea de robustez ante ataques, por lo que puede convertirse en una gran fuente de problemas si no está correctamente configurado.

Su principal problema se ofrece a la hora de determinar cuando sucedió determinado evento. Otro problema surge cuando ciertas tareas no se lleguen a ejecutar o que se ejecuten

varias veces , o que se ejecuten cuando no han de hacerlo, si el reloj tiene problemas; esto es especialmente peligroso para tareas que depende la seguridad, como los backups.

No obstante, muy pocos sistemas necesitan la precisión de NTP, por lo que es habitual tener este servicio deshabilitado.

TFTP

TFTP es un protocolo de transferencia de archivos (puerto 69 basado en UDP) que no proporciona ninguna seguridad. Por tanto en la mayoría de sistemas es deseable (obligatorio) que este servicio esté desactivado. Al utilizar este servicio en ningún momento se solicita un nombre de usuario o una clave, lo que da una idea de los graves problemas de seguridad que ofrece el servicio.

FTP

Un problema básico y grave de FTP (puerto 21 en TCP) es que ha sido diseñado para ofrecer la máxima velocidad en la conexión, pero no para ofrecer la seguridad; todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto claro, con lo que un atacante no tiene más que capturar todo el tráfico y conseguir así un acceso válido al servidor. Incluso puede ser una amenaza a la privacidad de los datos el hecho de que ese atacante también pueda capturar y reproducir (y modificar) los archivos transferidos.

Para solucionar este problema es conveniente dar acceso FTP a pocos usuarios bien identificados y que necesiten utilizarlo, concientizándolos de la utilidad de aplicaciones que cifren todo el tráfico de información (como SSH por ejemplo).

TELNET

El protocolo TELNET (TCP, puerto 23) permite utilizar una maquina como terminal virtual de otra a través de la red, de forma que se crea un canal virtual de comunicaciones similar (pero mucho más inseguro) a utilizar una terminal físicamente conectada a un servidor.

TELNET es el clásico servicio que hasta hace años no se solía deshabilitar nunca; lo más normal es que este servicio esté disponible para que los usuarios puedan trabajar remotamente, al menos desde un conjunto de máquinas determinado.

Evidentemente, reducir al mínimo imprescindiblemente el conjunto de sistemas desde donde es posible la conexión es una primera medida de seguridad; no obstante, no suele ser suficiente.

TELNET no utiliza ningún tipo de cifrado, por lo que todo el tráfico entre equipos se realiza en texto claro. Cualquier intruso con un Sniffer puede capturar el login y el password utilizados en una conexión otorgando a cualquiera que lea esos datos un acceso total a la máquina destino. Es muy recomendable no utilizar TELNET para conexiones

remotas, sino sustituirlo por aplicaciones equivalentes pero que utilizan cifrado para transferencia de datos (SSH o SSL-Telnet por ejemplo).

SMTP

La mala configuración del servicio SMTP (puerto 25 en TCP) utilizado para transferir correo electrónico entre equipos remotos suele ser causante del Mail Bombing y el Spam redirigido.

Por lo general se recibirá correo de un numero indeterminado de máquinas, y no se podrá bloquear el acceso SMTP. No obstante, en este caso podemos aplicar unas medidas de seguridad simples, como realizar una consulta inversa a DNS para asegurarnos de que solo máquinas registradas envían correo o no permitir que el sistema reenvíe correo que no provenga de direcciones registradas bajo su dominio.

Servidores WWW

Los problemas de seguridad relacionados con el protocolo http se dividen en tres grandes grupos en función de los datos a los que pueden afectar:

- **Seguridad en el servidor:** es necesario garantizar que la información almacenada en la máquina servidora no pueda ser modificada sin autorización, que permanezca disponible y que solo pueda ser accedida por los usuarios a los que les esté legítimamente permitido
- **Seguridad en la red:** cuando un usuario conecta a un servidor web se produce un intercambio de información entre ambos; es vital garantizar que los datos que recibe el cliente desde el servidor sean los mismos que se están enviando (que no sufran modificaciones de terceros), y también garantizar que la información que el usuario envía hacia el servidor no sea capturada, destruida o modificada por un atacante.
- **Seguridad en la cliente:** es necesario garantizar al usuario que descarga páginas de un servidor no va a perjudicar a la seguridad de su equipo. Se debe evitar Applets maliciosos, programas con virus o simples cuelgues al acceder a las páginas de la organización.

Asegurar el servidor implica medidas excepcionales dedicadas al servidor Web y su entorno de trabajo.

Sea cual sea el servidor utilizado, es necesario minimizar al número de usuarios en la máquina y minimizar el número de servicios ofrecidos en ella; aunque lo normal es que una máquina dedicada a cualquier tarea, sea también el servidor Web, es recomendable que dicho servidor sea dedicado solo a esa tarea.

Los problemas relacionados con servidores Web suelen proceder de errores de programación en los CGIs ubicados en el servidor, La capacidad del CGI para comunicarse con el resto del sistema que alberga las páginas es lo que le otorga su potencia, pero

también lo que causa mayores problemas de seguridad: un fallo en estos programas suele permitir a cualquier "visitante" ejecutar órdenes en el sistema.
Una medida de seguridad básica es ejecutar el demonio servidor bajo la identidad de un usuario con privilegios mínimos para que todo funcione correctamente, pero nunca como Administrador, Root o cuanta del sistema.
Para garantizar la seguridad de los datos que circulan entre un cliente y el servidor es casi obligatorio cifrar dichos datos (mediante SSL o utilizando Certificados Digitales por ejemplo)

5.13.1 Criptografía

Es el conjunto de técnicas que permiten transformar un trozo de información, de tal forma que quienes deseen recuperarlo sin estar en posesión de otra pieza de información (clave), se enfrentarán a un problema intratable.

Conviene recordar que "intratable" no significa lo mismo que "insoluble"; puesto que el número de posibles claves ha de ser finito, la fuerza bruta siempre nos permitirá recuperar el mensaje original, al margen de que seamos luego incapaces de reconocerlo. En cualquier caso, desde un punto de vista práctico la casualidad deberá ser descartada, ya que las probabilidades de que se descifre por la fuerza bruta un mensaje en tiempo razonable es inferior a la de que le caiga a usted en este preciso instante un meteorito sobre la cabeza.

Pero, ¿qué es exactamente un problema intratable? Sencillamente aquel que para ser resuelto de forma satisfactoria requiere una cantidad de recursos computacionales (tiempo y memoria) más allá de las posibilidades del atacante. De hecho, si tuviéramos claves de 256 bits y la Física actual no se equivoca, no hay suficiente materia ni energía en el Universo para construir una computadora que recorra todas las posibles combinaciones.

Sin embargo, existe un último e inquietante detalle para tener en cuenta: la definición anterior necesita para ser operativa que el contrincante carezca de "atajos" para resolver nuestro problema en teoría intratable. Por desgracia, y para satisfacción de muchos paranoicos, prácticamente para ninguno de los problemas que plantean los algoritmos criptográficos actuales se ha demostrado que no pueda existir algún atajo..."[9]

Vamos a describir los principales tipos de tecnologías empleados para cifrar información y sus diversas implementaciones.

a) ***Algoritmos hash de una dirección***. Un algoritmo *hash de una dirección* funciona de este modo: se introduce un documento en el algoritmo y se genera un *hash* que es un pequeño trozo de información que representa al mensaje original. La característica fundamental de estos algoritmos es que tan solo funcionan en una dirección, es decir, no se puede obtener el documento original a partir del *hash.* Y un determinado *hash* tan sólo se puede obtener de un determinado documento origen.

[9] Lucena López M. Números primos y criptografía. Kriptópolis 8 Julio 2000.
http://www.kriptopolis.com/luc/20000708.html

Ejemplos de algoritmos:

- MD4 y MD5 (Message Digest) 128 bits.
- SHA (Secure Hash Algorithm) 160 bits.

Un subconjunto de estos algoritmos es el que utiliza una clave (conjunto de bits) como parte de la función. Un ejemplo de algoritmo de este tipo es: MAC (Message Authentication Code).

Algoritmos hash de una dirección con clave: A modo de ejemplo describimos en esta imagen el proceso de Autentificación en un entorno NT ó UNIX tradicionales. La línea negra determina lo que viaja por la red. Claramente se observa que no viaja nunca la información de la contraseña. Además, el servidor no conoce la contraseña.

b) ***Algoritmos de clave privada (simétricos)*** Un algoritmo de *clave privada* funciona de este modo: el emisor introduce un documento en el algoritmo así como la clave privada (trozo de información conocido sólo por el emisor y el receptor), se obtiene el mismo documento pero cifrado, es decir, ininteligible. El receptor recoge el documento cifrado y lo introduce de nuevo en el algoritmo así como la clave privada obteniendo el documento origen. (**Figura 5.8**)

Ejemplos de algoritmos:

- DES y triple DES.
- RC2 y RC4.
- IDEA.
- SkipJack.

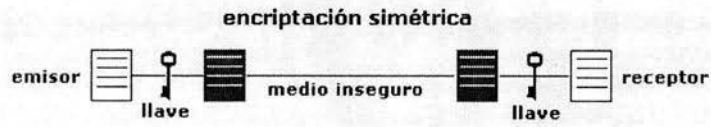

Figura 5.8: **Encriptación Simétrica**

La característica principal de este algoritmo es que existe *una única clave* que solo conocen los interlocutores, y que sirve tanto para cifrar como para descifrar. Es muy rápido.

c) ***Algoritmos de clave pública (asimétricos).*** Un algoritmo de *clave asimétrica* se basa en la existencia de una pareja de claves: la clave privada, conocida solo por el propietario de la pareja, y la clave pública, que el emisor reparte a quienes él desee. Ambas claves se generan en un mismo proceso y forman una pareja que depende una de la otra. Funciona de este modo: el emisor introduce un documento en el algoritmo así como su clave privada, se obtiene el mismo documento pero cifrado, es decir, ininteligible. El receptor recoge el documento cifrado y lo introduce de nuevo en el algoritmo así como la clave pública del emisor, obteniendo el documento origen. Del mismo modo el algoritmo funciona de forma inversa. Es decir, lo cifrado por el receptor con la clave pública del emisor, sólo puede ser descifrado por éste, con su clave privada. (**Figura 5.9**)

Ejemplos de algoritmos:

- RSA (Rivest-Shamir-Adleman).
- Diffie - Hellman.

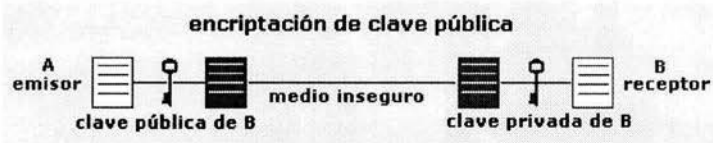

Figura 5.9: **Encriptación Pública.**

5.13.2 Usos de las tecnologías de encriptación

Estas tecnologías tienen múltiples utilidades entre las que destacaremos las siguientes.

Firma digital

Para garantizar la integridad de un documento así como validar su autor utilizamos el mecanismo de firma digital, que utiliza tecnología de clave pública. Para firmar debemos introducir el documento en un algoritmo hash de modo que obtenemos el resumen cifrado (hash) del documento.

Recordemos el esquema básico de una firma digital básica (**Figura 5.10**):

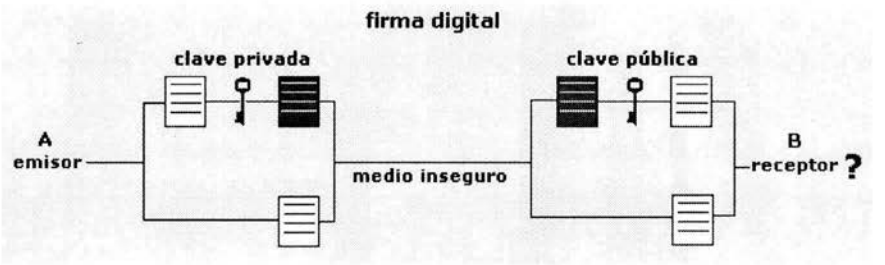

Figura 5.10: Esquema básico de una firma digital básica.

El proceso de firma digital consta de dos partes bien diferenciadas:

1. Proceso de Firma: en el que el emisor encripta el documento con su llave privada, enviando al destinatario tanto el documento en claro como el encriptado.

2. Proceso de Verificación de la Firma: el receptor desencripta el documento cifrado con la clave pública de A y comprueba que coincide con el documento original, lo que atestigua de forma total que el emisor del mismo ha sido efectivamente A.

El método de la firma digital no sólo proporciona autenticidad al mensaje enviado por A, si no que también asegura el no repudio, ya que sólo el dueño de una llave privada puede encriptar un documento de tal forma que se pueda desencriptar con su llave pública, lo que garantiza que ha sido A y no otro el que ha enviado dicho documento.

Así mismo proporciona Integridad de datos, ya que si el documento fuera accedido y modificado en el camino el resumen del documento cambiaría también.

Este resumen lo introducimos a su vez en un algoritmo de clave pública junto con la clave privada del emisor obteniendo el hash cifrado. Ese hash se adjunta al documento garantizando la integridad del documento y su propietario.

Cuando el documento firmado llega a alguien que pretende validarlo debe realizar este proceso. Introduce la firma del documento así como la clave pública del emisor en el algoritmo de clave pública para obtener el hash del documento. Por otro lado introduce los datos del documento en el algoritmo hash para obtener el resumen (hash) que deberá ser igual en ambos casos para garantizar la validez del documento.

Funciones hash.

Si imaginamos el envío de un documento extenso que queremos firmar digitalmente, nos daremos cuenta de que cifrar el documento entero es una pérdida de tiempo, ya que los medios de encriptación de llave pública son lentos, pués precisan un grán proceso de cómputo.

Para solventar éste aspecto aparecen las funciones hash, que son unas funciones matemáticas que realizan un resumen del documento a firmar. Su forma de operar es comprimir el documento en un único bloque de longitud fija, bloque cuyo contenido es ilegible y no tiene ningún sentido real. Tanto es así que por definición las funciones hash son irreversibles, es decir, que a partir de un bloque comprimido no se puede obtener el bloque sin comprimir, y si no es así no es una función hash. Estas funciones son además de dominio público.

A un mensaje resumido mediante una función hash y encriptado con una llave privada es lo que en la vida real se denomina firma digital.

El esquema de firma digital mediante una función hash es el siguiente (**Figura 5.11**):

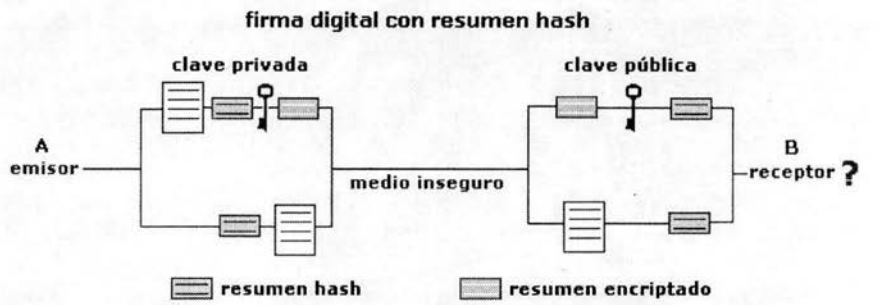

Figura 5.11: Esquema básico de una firma digital básica

Y su mecanismo es el siguiente:

1. El emisor aplica una función hash conocida al documento, con lo que obtiene un resumen hash del mismo.
2. Encripta dicho resumen con su clave privada.
3. Envía al receptor el documento original plano y el resumen hash encriptado.
4. El receptor B aplica la función hash al resumen sin encriptar y desencripta el resumen encriptado con la llave pública de A.
5. Si ambos coinciden está seguro de que ha sido A el que le ha enviado el documento. Si no coinciden, está seguro de que no ha sido A o de que el envío ha sido interceptado durante el medio de envío y modificado.

El caso de que ambos resúmenes no coincidan contempla también la posibilidad de que el mensaje haya sido alterado en su viaje de A a B, lo que conlleva igualmente el rechazo del documento por no válido.

Las funciones hash y la firma digital son elementos indispensables para el establecimiento de canales seguros de comunicación, basados en los Certificados Digitales.

Para que una función pueda considerarse como función hash debe cumplir:

- Debe transformar un texto de longitud variable en un bloque de longitud fija, que generalmente es pequeña (algunas son de 16 bits).
- Debe ser cómoda de usar e implementar.
- Debe ser irreversible, es decir, no se puede obtener el texto original del resumen hash.
- Debe ser imposible encontrar dos mensajes diferentes cuya firma digital mediante la función hash sea la misma (no-colisión).
- Si se desea además mantener un intercambio de información con Confidencialidad, basta con cifrar el documento a enviar con la clave pública del receptor.

Las funciones hash más conocidas y usadas son:

MD2, abreviatura de *Message Digest 2*, diseñado para computadoras con procesador de 8 bits. Todavía se usa, pero no es recomendable, debido a su lentitud de proceso.

MD4, abreviatura de *Message Digest 4*, desarrollado por Ron Rivest, uno de los fundadores de RSA Data Security Inc. y padre del sistema asimétrico RSA. Aunque se considera un sistema inseguro, es importante porque ha servido de base para la creación de otras funciones hash. Un sistema de ataque desarrollado por Hans Dobbertin posibilita el crear mensajes aleatorios con los mismos valores de hash (colisiones), por lo que ya no se usa. De hecho, existe un algoritmo que encuentra una colisión en segundos.

MD5, abreviatura de *Message Digest 5*, también obra de Ron Rivest, que se creó para dar seguridad a MD4, y que ha sido ámpliamante usado en diversos campos, como autenticador de mensajes en el protocolo SSL y como firmador de mensajes en el programa de correo PGP. Si embargo, fué reventado en 1996 por el mismo investigador que lo hizo con MD4, el señor Dobbertin, que consiguió crear colisiones en el sistema MD5, aunque por medio de ataques parciales. Pero lo peor es que también consiguió realizar ataques que comprometían la no-colisión, por lo que se podían obtener mensajes con igual hash que otro determinado. A pesar de todo esto, MD5 se sigue usando bastante en la actualidad.

SHA-1, *Secure Hash Algorithm*, desarrollado como parte integrante del Secure Hash Standar (SHS) y el Digital Signature Standar (DSS) por la Agencia de Seguridad Nacional Norteamericana, NSA. Sus creadores afirman que la base de este sistema es similar a la de MD4 de Rivest, y ha sido mejorado debido a ataques nunca desvelados. La versión actual se considera segura (por lo menos hasta que se demuestre lo contrario) y es muy utilizada algoritmo de firma, como en el programa PGP en sus nuevas claves DH/DSS (Diffie-Hellman/Digital Signature Standar). Destacar también que en la actualidad se están estudiando versiones de SHA con longitudes de clave de 256, 384 y 512 bits.

RIPEMD-160, desarrollada por un grupo de investigadores europeos, entre los que se encuentra Hans Dobbertin (el reventador de MD4-MD5) y otros investigadores incluidos en el proyecto RIPE (RACE Integrity Primitives Evaluation). Su primera versión adolecía de las mismas debilidades que MD4, produciendo colisiones, pero las versiones mejoradas actuales son consideradas seguras. Maneja claves muy robustas, normalmente de 160 bits, aunque exiten versiones de 128 y se están planteando nuevas de 256 y 320 bits. Es muy rápido, no está patentado y su código fuente es abierto, de libre acceso.

Certificados

Para realizar intercambios de información seguros es preciso que, además de cifrar la información mediante mecanismos de clave pública, algo ó alguien nos garantice que las claves públicas de nuestros interlocutores sean verdaderas. Para esto utilizamos los llamados certificados digitales, algo así como el DNI digital.

Un certificado digital contiene, fundamentalmente, los datos de un usuario (o entidad) y su clave pública (ligada a su clave privada). Esta información viene avalada por una entidad tercera que garantiza la validez de su contenido: es la *entidad certificadora.* Ésta valida el contenido firmando digitalmente todo el certificado, de modo que cualquiera que quiera validar su contenido solo deberá comprobar la firma del certificado.

Tipos de certificados y su utilidad:

1. Personales:
    1. Firma digital
    2. Cifrado de correo electrónico (S/MIME)
    3. Firma de formularios
    4. SSL
    5. Soluciones de Single-Sign-On (identificación única)

- De servidor:
    6. SSL
    7. Time stamp
    8. VPN's

Comunicación segura con un servidor

SSL (*Secure Sockets Layer*) creado por Netscape, y **TLS** (*Transport Layer Security*) abierto y basado en SSL, son dos protocolos que aportan una capa de seguridad para garantizar la autenticidad, integridad y confidencialidad en una comunicación. SSL es el protocolo que utilizamos con el navegador cuando nos conectamos a los llamados sitios seguros.

Mediante SSL es posible autenticar al servidor y al cliente. Si solo interesa autenticar al servidor, éste entregará su certificado al cliente. Si además es preciso autenticar al cliente, el servidor solicitará un certificado al cliente. Aspectos técnicos de la seguridad en la información sanitaria

Comunicación segura en sistemas financieros

SET, *Secure Electronic Transaction*, es un standard abierto creado por VISA y Mastercard para facilitar las transacciones comerciales y los pagos sobre Internet.

El protocolo SET utiliza criptografía basada en certificados. El sistema es similar a SSL pero con la ventaja de disponer de una encriptación mucho más fuerte, además de exigir la certificación de todas las entidades que intervienen en una transacción comercial: el titular de la tarjeta de crédito, el comercio, la pasarela de pagos y las entidades financieras emisora y adquiriente.

SGC, *Server Gated Crypto*, es una extensión de SSL también para el entorno financiero muy similar a SET.

Cifrado de correo y archivos

Dos entes especialmente sensibles son los archivos y los correos electrónicos. Ambos son documentos con información que de algún modo debemos proteger.

PGP (*Pretty Good Privacy*) es un sistema de clave pública para encriptar correo, archivos y hasta tráfico TCP/IP desarrollado a principio de los 90 por Phill Zimmerman. Su uso se ha extendido ampliamente debido a su facilidad para gestionar las claves públicas y privadas.

S/MIME es otro sistema más moderno de securizar mediante tecnología de clave pública el formato de correo **MIME** (*Multipurpose Internet Mail Extensions*).

Smart Cards (Tarjetas inteligentes)

Las llamadas tarjetas inteligentes son un dispositivo de seguridad del tamaño de una tarjeta de crédito que ofrece funciones de almacenamiento y procesamiento seguro de información. La diferencia con las tarjetas normales estriba en que éstas tienen una banda magnética en la que existe cierta información, mientras que las tarjetas inteligentes disponen de un chip empotrado en la propia tarjeta.

Las tarjetas aportan las siguientes características de seguridad:

- Almacenamiento resistente a ataques para claves privadas y otra información sensible.
- Aislamiento de los procesos de autentificación, firmado digital e intercambio de claves de otros elementos del sistema que no tienen porqué conocerlos.
- Portabilidad de las credenciales digitales y otras informaciones.
- Doble seguridad: algo poseído (la tarjeta) y algo conocido (el PIN de identificación). Su funcionalidad es la misma que aportan los certificados digitales, teniendo en cuenta que puede almacenar también la clave privada.

Redes privadas virtuales (VPN's)

Para proteger la información que viaja a través de redes públicas ó poco seguras se emplea la tecnología de *Redes Privadas Virtuales.* Existen diferentes aproximaciones tecnológicas para solucionar este problema pero todas ellas consisten en crear un 'túnel' entre dos extremos que se comunican. El túnel se crea encriptando la información en el origen y desencriptándola en el destino. Existe un gran número de protocolos empleados para crear túneles, vamos a mencionar las tecnologías más utilizadas:

- **PPTP**: (*Point to Point Tunneling Protocol*) diseñado para autenticar y encriptar (además de comprimir) una comunicación entre dos extremos, en base a un identificador y una contraseña.

- **L2F**: (*Layer 2 Fordwarding*). Ofrece la misma funcionalidad que PPTP.

- **L2TP**: (*Layer 2 Transfer Protocol*) es una combinación de PPTP y L2F que mejora sus funcionalidades.

- **IPSec**: Añade a los anteriores la capacidad de garantizar la integridad de los paquetes enviados por la red. Limitado a tráfico IP.

PKI

PKI (*Public Key Infraestructure*) es un conjunto de tecnologías que se aprovechan de los algoritmos de encriptación de clave pública, de clave privada y hash.

Nace de la necesidad que surge en una comunicación entre dos extremos de garantizar, la autenticidad, integridad y confidencialidad de los comunicantes y del contenido de la transmisión. Esto se realiza mediante la intervención de un tercero confiado por ambos.

Una PKI está compuesta por una serie de entidades: Usuarios, Autoridad de Registro, Autoridad de certificación, Servidores de tiempo y Repositorio de la información.

a) **Autoridad de registro**

La *Autoridad de Registro (RA)* es una entidad autorizada por la *Autoridad de Certificación (CA)* para auxiliarla en el proceso de asegurar que los usuarios satisfacen todos los requisitos para que se le expida un certificado, es decir, se encarga de *dar fe* ante la CA de la validez de los datos que le envía. Estas son sus funciones:

- Recibe solicitudes de certificación y mantiene una base de datos con ellas. Las solicitudes pueden ser de dos tipos:

    1. **De firma de certificado** *(CSR, Certificate Signing Request)*. En este caso el solicitante ha creado, con un software, la pareja de claves privada-pública y, junto a sus datos identificativos, entrega a la RA su clave pública para ser firmada.
    2. **De creación de certificado completo**. El solicitante solo entrega sus datos identificativos y recibirá el certificado y su clave privada asociada.

- Recibe solicitudes de revocación de certificados previas a la expiración de éstos

- Recibe solicitudes de renovación de certificados ante su expiración. La RA debe advertir a sus clientes de la necesidad de renovación de sus certificados antes de que se creen situaciones de denegación de servicio.

- Debe decidir la validación o deniego de todas estas solicitudes.

- Debe mantener una base de datos con todas las solicitudes.

- Generalmente es parte de su responsabilidad la publicación en el repositorio correspondiente de los certificados y de las listas de certificados revocados.

b) **Autoridad de certificación**

La *Autoridad de Certificación (CA)* es una entidad de prestigio y confianza que *da fe* de que una clave pública pertenece realmente a la entidad que consta en el certificado. Éstas son sus funciones:

- Recibe las peticiones de la RA y genera los certificados. En función del tipo de solicitud realiza esto de dos formas:

    1. Si el solicitante entrega la clave pública, junto con los datos asociados, tan solo los firma digitalmente con su clave privada.
    2. Si el solicitante solo entrega los datos identificativos, la CA crea la pareja de claves pública-privada y después firma la pública junto con el resto de datos.

- Entrega los certificados y, en su caso, las claves privadas a la RA.

- Genera las *Listas de Certificados Revocados (CRL)* para que se publiquen en el repositorio. En la CRL están los números de serie de los certificados revocados, todos ellos firmados por la CA para garantizar su validez.

- Debe mantener una base de datos con todos los certificados y claves emitidas.

- Son las encargadas de definir las *Políticas de Certificación (CPS, certification practice statements),* que son las reglas que definen los procedimientos a seguir en los procesos de certificación.

Al conjunto de CA's que se rigen por una misma CPS se denomina *Dominio de Certificación.* Dentro de un dominio todos los usuarios de certificados se pueden validar unos a otros, pero fuera de él no. Para evitar esto los CA's se certifican unas a otras en base a dos modelos diferentes:

El modelo *jerárquico,* en el que existen dos tipos de CA's. Las *CA raíz* que generan sus propios certificados y se encuentran en el punto más alto de la jerarquía, y las *CA subordinadas,* que obtienen sus certificados de sus CA padres.

El modelo de *certificación cruzada* de CA's, en el que las CA's se certifican unas a otras de forma bilateral.

c) **Repositorio de información pública**

El *repositorio* es un servicio de red que permite el almacenamiento y la distribución de los certificados (y CRL's) de una PKI. Es un servicio público, es decir, debe estar accesible por todo el mundo de modo que cualquiera pueda validar los certificados de la CA. El estándar de facto que se utiliza como repositorio es un directorio (X.500) compatible LDAP que almacena la información en forma de árbol. Este tipo de repositorio tiene numerosas ventajas:

- Las aplicaciones pueden acceder a los certificados y CRL's de forma transparente al usuario utilizando el estándar LDAP.
- Esta tecnología es escalable en cuanto a número de certificados que pueden almacenar (millones), tiempos de respuesta en accesos, búsquedas eficaces, distribución del directorio.
- Como valor añadido los directorios pueden almacenar numerosa información de la organización además de los certificados: direcciones de correo de los usuarios, teléfonos.

d) **Servidores de tiempo**

Son servicios de red generados por una tercera parte confiable que permiten asociar a los procesos digitales una fecha y hora. Los servidores de tiempo son claves en todos los procesos en los que el momento de realización de la transacción es de vital importancia como periodos de validez, caducidad, garantías.

5.14 VPN (Redes Privadas Virtuales)

Una RED se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones).

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de los famosos firewalls y las VPN

5.14.1 ¿Por qué una VPN?

Cuando deseo enlazar mis oficinas centrales con alguna sucursal u oficina remota tengo tres opciones:

- ***Modem***: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuadas.

- ***Línea Privada***: Tendría que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo necesito enlazar mi oficina central con una sucursal que se encuentra a 200 Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

- ***VPN***: Los costos son bajos porque solo realizo llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

5.14.2¿Que es una VPN?

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. (ver **Figura 5.12** siguiente)

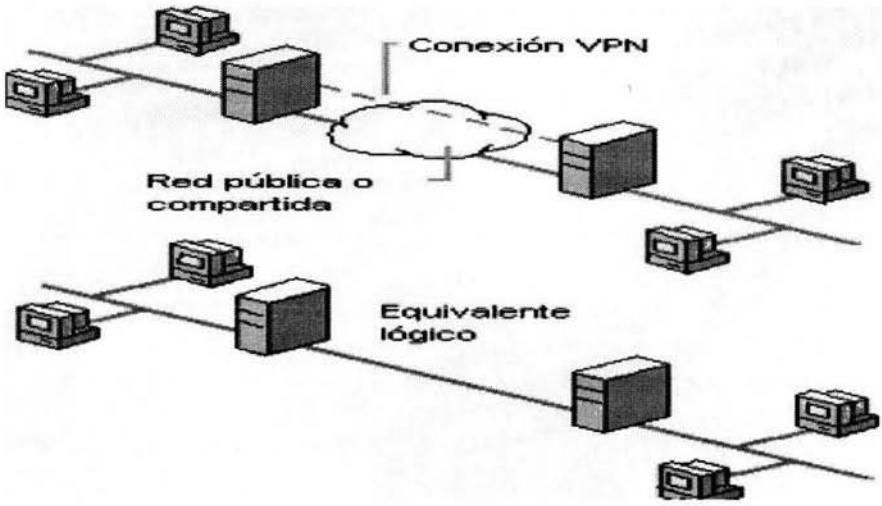

Figura 5.12: **Red Privada Virtual (VPN)**

Figura 5.13: **Tráfico de datos en una Red Privada Virtual (VPN)**

En la figura anterior (**Figura 5.13**) se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de Internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado y lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Las VPN pueden enlazar mis oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, Ipsec, Frame Relay, ATM como lo muestra la **Figura 5.14** siguiente.

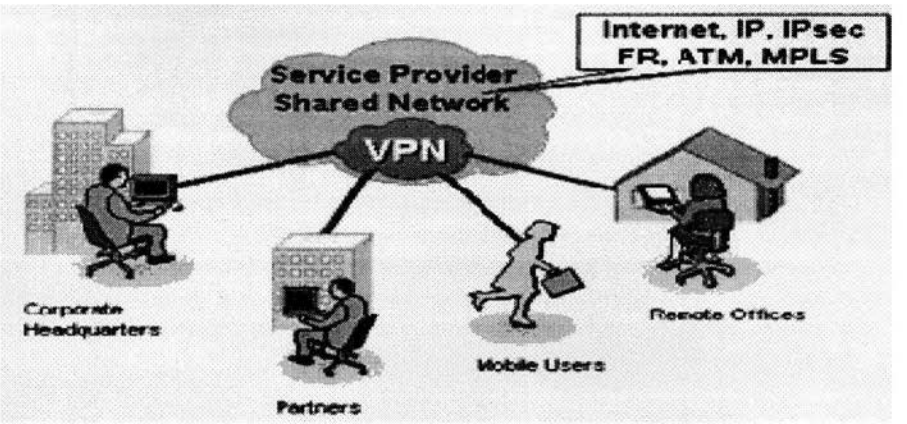

Figura 5.14: Enlaces en una Red Privada Virtual (VPN)

Tecnología de túnel

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños. (**Figura 5.15**)

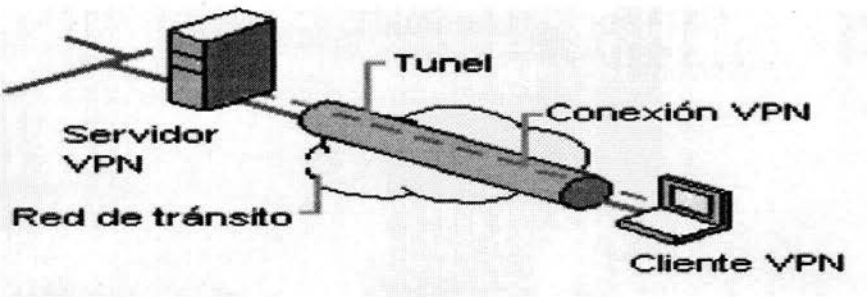

Figura 5.15: Tecnología de tuneleo en una Red Privada Virtual (VPN)

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de transito se envían los datos sin problemas.

5.14.3 Requerimientos básicos de una VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples
- Identificación de usuario

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

a) **Administración de direcciones**

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

b) **Codificación de datos**

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

c) **Administración de claves**

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

d) **Soporte a protocolos múltiples**

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet(IP), el intercambio de paquete de internet(IPX) entre otros.

5.14.4 Herramientas de una VPN

- VPN Gateway : Dispositivos con un software y hardware especial para proveer de capacidad a la VPN

- Software: Esta sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN.

- Firewall

- Router

5.14.5 Ventajas de una VPN

- Dentro de las ventajas más significativas podremos mencionar la integridad, confidencialidad y seguridad de los datos.
- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente. Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

5.15 Seguridad en la Web

Dado el gran auge que hoy en día tiene Internet, su uso se ha masificado enormemente. Desde páginas meramente informativas hasta sitios interactivos usando tecnologías nuevas. Empresas de diversa índole ya usan la Internet para comunicarse y el problema principal que surgió es la confiabilidad en que lo que se esta comunicando no sea visto por personas que puedan hacer mal uso de dicha información.

Por ejemplo, las tiendas comerciales ya están dando la posibilidad de realizar compras por la Web, pero el principal talón de Aquiles lo constituye la inseguridad que causa dar un número de tarjeta de crédito para pagar la compra.

O cosas tan simples como cuando uno envía un mail y no querer que nadie lo lea sino el destinatario. A raíz de todo esto surgieron tecnologías que persiguen mejorar la seguridad de todas estas comunicaciones.

5.15.1 Seguridad en la transmisión

La seguridad de este tipo se basa en el hecho de poder encriptar los mensajes que se envían por a red entre un servidor y un cliente y que solo ellos puedan descifrar los contenidos a partir de una clave común conocida solo por los dos.

Para llevar a cabo esta seguridad se crearon diversos protocolos basados en esta idea:

- **SSH**: Usado exclusivamente en reemplazo de telnet

- **SSL**: Usado principalmente en comunicaciones de hipertexto pero con posibilidad de uso en otros protocolos
- **TSL**: Es del mismo estilo del anterior.
- **HTTPS**: Usado exclusivamente para comunicaciones de hipertexto

SSH (Secure Shell)

Este protocolo fue diseñado para dar seguridad al acceso a computadores en forma remota. Cumple la misma función que telnet o rlogin pero además, usando criptografía, logra seguridad con los datos. A diferencia de telnet u otro servicio similar, SSH utiliza el puerto 22 para la comunicación y la forma de efectuar su trabajo es muy similar al efectuado por SSL.

Para su uso se requiere que por parte del servidor exista un demonio que mantenga continuamente en el puerto 22 el servicio de comunicación segura, el sshd. El cliente debe ser un software tipo TeraTerm o Putty que permita la hacer pedidos a este puerto 22 de forma cifrada.

La forma en que se entabla una comunicación es en base la misma para todos los protocolos seguros:

- El cliente envía una señal al servidor pidiéndole comunicación por el puerto 22.
- El servidor acepta la comunicación en el caso de poder mantenerla bajo encriptación mediante un algoritmo definido y le envía la llave publica al cliente para que pueda descifrar los mensajes.
- El cliente recibe la llave teniendo la posibilidad de guardar la llave para futuras comunicaciones o destruirla después de la sesión actual.

Se recomienda que si se esta en un computador propio, la clave sea guardada, en otro caso, destruirla

SSH es un servicio de arquitectura cliente-servidor que permite conectarse desde una estación a otra a través de la red para ejecutar programas de forma remota. Dado que exista un servidor de SSH, los clientes pueden autenticarse en este e invocar comandos que se ejecutan en el servidor. SSH puede sustituir a programas como telnet, rsh, rlogin y rcp.

Estos tienen como desventaja fundamental su gran vulnerabilidad debido a que la información intercambiada se trasmite de la misma forma en que se envía, pudiendo ser accedida por ``clientes" no autorizados. En cambio SSH provee varios mecanismos para encriptar lo trasmitido a través de canales inseguros. Con SSH también se pueden mover archivos desde un extremo a otro de la conexión así como establecer conexiones gráficas X seguras.

SSH prosee las siguientes ventajas:

- Autenticación potente. Cierra la mayoría de los huecos de seguridad. Brinda nuevos métodos de autenticación tales como: archivo .rhosts más autenticación RSA7.1 basada en host, y autenticación RSA pura.

- Incremento de la privacidad. Toda la comunicación es trasparente y automáticamente encriptada. La encriptación comienza antes de la autenticación y esto permite que los passwords no se trasmitan claramente. La encriptación también permite protegerse de los paquetes falsos.

- Sesiones X Window seguras.

- Cualquier conexión TCP/IP puede ser redireccionada a través de un canal de encriptación SSH en ambas direcciones.

- No es necesaria ninguna adecuación para los usuarios, todo ocurre automáticamente. Los antiguos archivos .rhosts pueden funcionar con una autenticación potente si se instalan los archivos de llaves por host.

- Nunca se confía en la red. Se tiene la menor confianza posible en el lado remoto de la conexión y en los servidores de nombre de dominio. La autenticación RSA pura no cree en nada más que en la llave privada.

- Automáticamente se ejecuta rsh si no existiera un servidor de SSH en la máquina remota con la cual se desea establecer la conexión.

- Compresión opcional de los datos trasmitidos utilizando gzip. Particularmente para las conexiones X puede resultar ventajoso si el ancho de banda es limitado.

- Sustitución total de rsh, rlogin, rcp.

OpenSSH es el nombre de una implementación libre con código abierto (OpenSource) de la última versión libre del SSH. Esta es la que brindan las distribuciones de Linux incluyendo a Red Hat. OpenSSH contiene varias utilidades y programas:

- ssh: es el comando que permite invocar el cliente SSH para conectarse a la máquina servidora o ejecutar comandos en ella. También se puede llamar slogin. Sustituye a telnet, rsh y rlogin.

- sshd: es el daemon servidor de SSH. Siempre está escuchando las solicitudes de los clientes y cuando uno se conecta realiza la autenticación y comienza a servir al cliente mientras dure la conexión.

- scp: permite copiar archivos de una máquina a otra a través de un canal SSH. Sustituye a rcp.

- sftp y sftp-server: constituyen las partes cliente y servidora del servicio FTP con las facilidades del SSH incorporadas.

- ssh-keygen: permite generar llaves para autenticación RSA y DSA tanto basada en hosts como en usuarios.

SSH posee dos versiones en su protocolo de comunicación: la 1 y la 2. Esta es determinada por el cliente. Las diferencias fundamentales están en la forma de encriptación y autenticación. A continuación se mencionan en el orden en que ocurren los tipos de autenticación que trata de emplear el cliente para cada versión:

- Versión 1

    a) Autenticación basada en archivos .rhosts.

    b) Autenticación basada en archivos .rhosts combinada con autenticación RSA basada en host.

    c) Autenticación RSA pura.

    d) Autenticación basada en passwords.

- Versión 2

    a) Autenticación basada en llave pública.

    b) Autenticación basada en passwords

SSL (Secure Socket Layer) y TLS(Transport Layer Secure)

El protocolo SSL fue desarrollado por Netscape para permitir confidencialidad y autenticación en Internet. SSL es una capa por debajo de HTTP y tal como lo indica su nombre esta a nivel de socket por lo que permite ser usado no tan solo para proteger documentos de hipertexto sino también servicios como FTP, SMTP, TELNET entre otros.
La idea que persigue SSL es encriptar la comunicación entre servidor y cliente mediante el uso de llaves y algoritmos de encriptación.
El protocolo TLS esta basado en SSL y son similares en el modo de operar. Es importante señalar que ambos protocolos se ejecutan sobre una capa de transporte definida, pero no determinada. Esto indica que pueden ser utilizados para cualquier tipo de comunicaciones.
La capa de transporte más usada es TCP cobre la cual pueden implementar seguridad en HTTP.
Como punto de diferencia se puede mencionar que existen protocolos implementados sobre la capa de red, por ejemplo sobre IP. Tal es el caso de IPSec.

¿De qué están compuestos?

Estos protocolos se componen de dos capas: el ***Record Protocol*** y el ***Handshake Protocol.***

El *Record Protocol* es la capa inmediatamente superior a TCP y proporciona una comunicación segura. Principalmente esta capa toma los mensajes y los codifica con algoritmos de encriptación de llave simétrica como DES, RC4 aplicándole una MAC (Message Authentication Code) para verificar la integridad , logrando así encapsular la seguridad para niveles superiores.

El *Handshake protocol* es la capa superior a la anterior y es usada para gestionar la conexión inicial.

¿Cómo funcionan?

En resumidas cuentas, después que se solicita una comunicación segura, servidor y el cliente se deben poner de acuerdo en como se comunicaran (SSL Handshake) para luego comenzar la comunicación encriptada. Luego de terminada la transacción, SSL termina.

Solicitud de SSL:
Típicamente este proceso ocurre en el momento que un cliente accede a un servidor seguro, identificado con "https://...". pero como se mencionó, no necesariamente es usado para HTTP. La comunicación se establecerá por un puerto distinto al utilizado por el servicio normalmente. Luego de esta petición, se procede al SSL Handshake.

SSL Handshake:
En este momento, servidor y cliente se ponen de acuerdo en varios parámetros de la comunicación. Se puede dividir el proceso en distintos pasos:

- . *Client Hello*: El cliente se presenta. Le pide al servidor que se presente (certifique quien es)y le comunica que algoritmos de encriptación soporta y le envía un número

aleatorio para el caso que el servidor no pueda certificar su validez y que aun así se pueda realizar la comunicación segura.

- *Server Hello*: El servidor se presenta. Le responde al cliente con su identificador digital encriptado, su llave pública, el algoritmo que se usará, y otro número aleatorio. El algoritmo usado será el más poderoso que soporte tanto el servidor como el cliente. Aceptación del cliente: El cliente recibe el identificador digital del servidor, lo desencripta usando la llave pública también recibida y verifica que dicha identificación proviene de una empresa certificadora segura. Luego se procede a realizar verificaciones del certificado (identificador) por medio de fechas, URL del servidor, etc. Finalmente el cliente genera una llave aleatoria usando la llave pública del servidor y el algoritmo seleccionado y se la envía al servidor.
- *Verificación*: Ahora tanto el cliente y el servidor conocen la llave aleatoria (El cliente la generó y el servidor la recibió y desencriptó con su llave privada). Para asegurar que nada ha cambiado, ambas partes se envían las llaves. Si coinciden, el Handshake concluye y comienza la transacción.

- *Intercambio de Datos:* Desde este momento los mensajes son encriptados con la llave conocida por el servidor y el cliente y luego son enviados para que en el otro extremo sean desencriptados y leídos.
- *Terminación de SSL:* Cuando el cliente abandona el servidor, se le informa que terminara la sesión segura para luego terminar con SSL.

S/MIME

No hay nada más fácil que leer los correos de otras personas, ya que viajan de forma transparente por la Red.

Un correo electrónico normal es como una tarjeta postal sin sobre, que la puede leer todo el que tenga interés. Por consiguiente, la mejor manera de preservar la intimidad en los mensajes de correo electrónico es recurrir a las técnicas de cifrado.

Por medio de potentes técnicas criptográficas, el contenido del mensaje puede ser enviado cifrado, permitiendo así que sólo el destinatario legítimo del correo sea capaz de leerlo. Con este mecanismo se garantiza la confidencialidad del correo. Sin embargo, los modernos sistemas de seguridad para el correo electrónico, como Safeguard Sign & Crypt y otros, no se limitan a cifrar el contenido de los mensajes intercambiados, sino que también añaden otros servicios, como la integridad, que garantiza que el contenido del mensaje no ha sido alterado por el camino; la autentificación, que asegura la identidad del remitente del correo, de manera que podemos estar seguros de que fue escrito por quien lo envió y no ha sido falsificado; y el no repudio, que nos protege frente a que posteriormente el que envió el correo (o lo recibió de nosotros) alegue posteriormente no haberlo enviado (o recibido si era el destinatario). Estos últimos servicios se prestan mediante las firmas digitales.

S/MIME (*Secure/Multipurpose Internet Mail Extensions*) es una especificación para correo electrónico seguro. Este estándar fue diseñado para añadir seguridad en los mensajes de correo electrónico en formato MIME. Los servicios de seguridad que proporciona están

basados en la privacidad (utilizando cifrado) y en la autentificación (a través de la firma digital).

Fue diseñado para que fuese interoperable (dos o más paquetes de software que implementen S/MIME pueden comunicarse de forma segura). Es el formato de intercambio de información firmada y/o cifrada a través de Internet, que ha ganado gran aceptación por parte de las empresas de seguridad.

La protección de correos basados en mensajes MIME se hace normalmente mediante la utilización de S/MIME (definida en in IETF RFC 2633 "S/MIME Version 3 Message Specification), que su vez depende de Cryptographic Message Syntax (CMS) definida en IETF RFC 2630. CMS es una extensión de PKC#7, que define una sintaxis y métodos para el intercambio de mensajes criptográficos.JDspMIME proporciona CMS y S/MIME v3 no incluido en el JDK, integrado con la extensión estándar JavaMail (incluida en el J2EE), para la protección de correo electrónico y comunicaciones HTTP seguras.

Características

- *Fácil integración en sus aplicaciones.* Está diseñado para ser integrado rápidamente en sus aplicaciones. jDspMIME acelera y asegura el intercambio de mensajes s/MIME entre aplicaciones a través de una API sencillo para s/mime, JavaMail y CMS.

- Firma digital y encriptación segura. jDspMIME soporta: Cifrado RSA y DSA. IDEA, Tirple DES, y encriptación RC2 (40 y 128 bit). CMS (SignedData y EnvelopedData).

SOCKS

SOCKS es una abreviación de *SOCK-et-S.* Los socks son un protocolo de red para conexiones de TCP/IP que permite dirigir el trafico de una red de "igual manera" que un servidor proxy.

El lenguaje sock fue escrito hace mucho tiempo y actualmente es desarrollado por el equipo de NEC laboratories. Este lenguaje inicialmente estaba dirigido como uso de firewall pero actualmente se utiliza como Proxy Server, soluciones VPN y también por supuesto como firewall.

La función de este protocolo es probar los paquetes entrantes y los salientes ocultando las direcciones IP de nuestra red. Actualmente existen dos versión de socks la 4 y la 5. Este tipo de lenguaje se puede descifrar pero requiere mucho tiempo.

La versión 5 destaca de la 4 porque es mas robusta ya que agrega un método de autentificación y que hace que el modelo de seguridad de nuestras aplicaciones sea mejor.

Las dos versiones de socks, tienen tres funciones generales:

1. Realizan la petición de la conexión desde el cliente pasando por el servidor SOCKS hasta la red exterior.
2. Habilitan un circuito de tipo proxy entre el cliente y el servidor SOCKS.
3. Reenvían los datos de la aplicación entre la red interior y la exterior

El servidor sock se instala entre la red interna y la red externa. Si un usuario de la red interna quiere acceder a los recursos de la red externa SOCKS lo permite. También bloquea el intento de usuarios externos a los recursos de la red interna sin ninguna autorización.

Cuando un cliente de la red interna quiere conectarse a la red externa se conecta primero al servidor que tiene implementado socks, el servidor con socks hace una petición a la maquina deseada y le manda la información que el cliente necesita. El puerto que generalmente es usado en los servidores para ofrecer este servicio es el 1080.

La máquina externa solo conoce la dirección del servidor que tiene implementado socks.

Por este motivo se puede ocultar nuestra dirección IP en IRC, FTP y Web. Entre otras muchas cosas que soportan socks.

Existe la forma de utilizar un scanner de puertos que se puedan poner un rango de IP y scannear el puerto 1080. Entre muchísimas direcciones IP para encontrar servidores con socks.

Para win9x tenemos útiles como: ts v.1 socks 5 scanner y Socks Scan V 2.0, son fáciles de encontrar. Para poder instalar socks en nuestro PC tanto para *ix como win9x. tenemos el: Windsock. Para Windows, lógicamente, también tiene versión JAVA

CONCLUSIONES

La presente tesis **Diseño y Desarrollo de una Metodología para la Determinación y el Establecimiento de Normas de Seguridad Informática** busca ser una guía de ayuda para todas las personas interesadas en la seguridad en la información, sin importar el nivel de conocimientos que posean sobre el tema, mostrando los aspectos importantes que deben ser considerados desde el desarrollo hasta la implementación de las medidas de seguridad que sean mas adecuadas a las necesidades y circunstancias que rodean a los participantes, apoyándose en el análisis y evaluación de su costos y requerimientos, diferentes para cada tipo de organización y a partir de los cuales se llevara a cabo su desarrollo e implementación, sin olvidar el aspecto ético vital para definir las responsabilidades de cada quien y el papel que interpretan en la seguridad de la información en la actualidad.

Como hemos visto, la **Información** nos proporciona los conocimientos necesarios para tomar una decisión o seguir una serie de pasos con el fin de obtener un beneficio o cubrir una necesidad, a la vez de proporcionarnos una retribución por la oportuna acción que hayamos tomado; es un recurso valioso para todas las personas, organizaciones y empresas sin importar su actividad.

Los eventos mundiales recientes han generado un mayor sentido de urgencia que antes con respecto a la necesidad de tener mayor **seguridad en la información**, tanto física como de otro tipo.

Las personas, las empresas y organizaciones pueden haber reforzado las medidas de seguridad en la información , pero nunca se sabe cuándo o cómo puede estar expuesto a una **amenaza** que provocaría un ataque que afectaría directa o indirectamente nuestros intereses.

El conocer y entender a qué amenazas estamos expuestos, cuáles son, cómo dañan y quienes las llevan a cabo es vital para la creación de medidas de prevención, de reacción y de restauración de nuestra información.

A fin de brindar la más completa protección a los recursos valiosos para las organizaciones e individuos, se requiere un sistema exhaustivo de seguridad en la información y la implementación de **políticas de seguridad** que respalden todas las acciones a tomar, tanto a nivel empresa-organización, como a nivel individuo, para aplicar las medidas que la institución requiera para implementar, mejorar o reestructurar su seguridad en la información, de acuerdo a sus necesidades y apoyándose en los lineamientos legales que le rijan.

Para lograrlo, es vital realizar un **análisis completo para identificar los riesgos, amenazas, requerimientos y carencias** de la estructura operativa y jerárquica de la organización y que son directamente responsables de la falta o la mala seguridad en la información presente en su actividad diaria.

El implementar un software de seguridad no es siempre la mejor solución. Sin embargo, al **implementar las políticas de seguridad en la información** permitirán el **desarrollo e implementación de un plan proactivo** que indique cómo sobrevivir a los múltiples

escenarios y que también preparará a las organizaciones en el manejo de las amenazas inesperadas que podría afrontar en el futuro.

Si la empresa ya ha invertido tiempo y dinero en la construcción de una infraestructura para la tecnología de la información que soporte su compañía, esa infraestructura de TI podría resultar ser una gran debilidad si se ve comprometida. Para las organizaciones que funcionan en la era de la informática interconectada y la comunicación electrónica, las políticas de información bien documentadas que se comunican, entienden e implementan en toda la empresa, son herramientas comerciales esenciales en el entorno actual.

Imaginemos que sucedería si ...

- La información esencial fuera robada, se perdiera, estuviera en peligro, fuera alterada o borrada.
- Los sistemas de correo electrónico no funcionaran durante un día o más. ¿Cuánto costaría esta improductividad?
- Los clientes no pudieran enviar órdenes de compra a través de la red durante un prolongado periodo de tiempo.

Prepararse para múltiples escenarios parece ser la tendencia creciente. Durante los próximos años se espera que los ejecutivos corporativos se interesen cada vez más directamente en la prevención de desastres físicos, ciberterrorismo y espionaje de libre competencia para la seguridad.

Implementar una política de seguridad completa le da valor intrínseco a las empresas. También mejorará la credibilidad y reputación de la empresa y aumenta la confianza de los accionistas principales, lo que le dará a la empresa una ventaja estratégica.

Para desarrollar una política de seguridad informática para cualquier organismo o institución es necesario:

- ***Identificar y evaluar los activos***: ¿Qué activos deben protegerse y cómo protegerlos de forma que permitan la prosperidad de la empresa?.

- ***Identificar las amenazas:*** ¿Cuáles son las causas de los potenciales problemas de seguridad? Considerar la posibilidad de violaciones a la seguridad y el impacto que tendrían si ocurrieran.

  Estas amenazas pueden ser externas y/o internas:

Amenazas externas: Se originan fuera de la organización y son los virus, gusanos, caballos de Troya, intentos de ataques de los hackers, retaliaciones de ex-empleados o espionaje industrial.

Amenazas internas: Son las amenazas que provienen del interior de la empresa y que pueden ser muy costosas porque el infractor tiene mayor conocimiento, acceso y perspicacia para saber donde reside la información sensible e importante. Las amenazas internas también incluyen el uso indebido del acceso a aplicaciones o bases de datos por parte de los empleados, así como los problemas que podrían ocasionar los empleados al enviar y revisar el material ofensivo a través de las redes de comunicación.

- ***Evaluar los riesgos:*** Éste puede ser uno de los componentes más desafiantes del desarrollo de una política de seguridad. Debe calcularse la probabilidad de que ocurran ciertos sucesos y determinar cuáles tiene el potencial para causar mucho daño. El costo puede ser más que monetario - se debe asignar un valor a la pérdida de datos, la privacidad, responsabilidad legal, atención pública indeseada, la pérdida de clientes o de la confianza de los inversionistas y los costos asociados con las soluciones para las violaciones a la seguridad.

- ***Asignar las responsabilidades:*** Seleccionar un equipo de desarrollo que ayude a identificar las amenazas potenciales en todas las áreas de la empresa. Sería ideal la participación de un representante por cada departamento de la compañía. Entre los principales integrantes del equipo deberán estar: el administrador de redes, un asesor jurídico, un ejecutivo superior y representantes de los departamentos de Recursos Humanos y Relaciones Públicas.

- ***Establecer políticas de seguridad en la información:*** Crear una política que apunte a los documentos asociados; parámetros y procedimientos, normas, así como los contratos de empleados. Estos documentos deben tener información específica relacionada con las plataformas informáticas, las plataformas tecnológicas, las responsabilidades del usuario y la estructura organizacional. De esta forma, si se hacen cambios futuros, es más fácil cambiar los documentos subyacentes que la política en sí misma.

- ***Implementar una política en toda la organización:*** La política que se escoja debe establecer claramente las responsabilidades en cuanto a la seguridad y reconocer quién es el propietario de los sistemas y datos específicos. También puede requerir que todos los empleados firmen la declaración; si la firman, debe comunicarse claramente. Éstas son las tres partes esenciales de cumplimiento que debe incluir la política:

    1. **Cumplimiento**: Indica un procedimiento para garantizar el cumplimiento y las consecuencias potenciales por incumplimiento.
    2. **Funcionarios de seguridad**: Nombre individuos que sean directamente responsables de la seguridad de la información. No debe ser la misma persona que supervisa, implementa o revisa la seguridad para que no haya conflicto de intereses.
    3. **Financiación**: Se debe asegurar que a cada departamento se le haya asignado los fondos necesarios para poder cumplir adecuadamente con la política de seguridad de la compañía.

- ***Administrar el programa de seguridad:*** Establecer los procedimientos internos para implementar estos requerimientos y hacer obligatorio su cumplimiento.

A través del proceso de elaboración de una *política de seguridad*, es importante asegurarse de que la política tenga las siguientes *características*:

- *Se pueda implementar y hacer cumplir*
- *Sea concisa y fácil de entender*

Una vez que la política se aprueba totalmente, debe hacerse asequible a todos los empleados porque, en última instancia, ellos son responsables de su éxito. Las políticas deben revisarse anualmente o al menos cada dos años para reflejar los cambios en la organización o cultura.
Se debe mencionar que no debe haber dos políticas de seguridad iguales puesto que cada empresa es diferente y los detalles de la política dependen de las necesidades exclusivas de cada una. Sin embargo, el equipo responsable de la seguridad de la organización puede comenzar con un sistema general de políticas de seguridad y luego personalizarlo de acuerdo con sus requerimientos específicos, limitaciones de financiamiento e infraestructura existente.

Una política completa de seguridad de la información es un recurso valioso que amerita la dedicación de tiempo y esfuerzo. La política que adopte su empresa brinda una base sólida para respaldar el plan general de seguridad. Y una base sólida sirve para respaldar una organización sólida.

GLOSARIO

A

Algoritmo Hash
Las funciones de comprobación aleatoria son similares a las de cifrado (de hecho, algunas de ellas son funciones de cifrado con ligeras modificaciones). La mayoría de estas funciones toma un bloque de datos y lo somete reiteradamente a una sencilla función de desordenación (scramling) para alterar sus elementos. Si esta operación se repite un cierto número de veces, no existe forma práctica conocida de predecir el resultado. Es imposible modificar un documento de un modo determinado y estar seguro de que la función de comprobación aleatoria producirá el mismo resultado.

Este tipo de firma utiliza una función de comprobación aleatoria criptográficamente segura, como *Message digest 5* (MD-5) o *Secure Hash Algorithm* (SHA), para producir un valor de comprobación aleatoria a partir de un archivo. El procedimiento de comprobación aleatoria encadena su clave secreta. El destinatario también tiene un a copia de la clave secreta y la utiliza para evaluar la firma.

B

Boot
El sector de Boot es el primer sector absoluto (Track 0, head 0, sector 1) de una unidad de disco, ya sea diskette o disco duro en una PC, y está compuesto por los primeros 512 bytes. En ellos se almacenan los archivos "ocultos" (hidden files) del sistema de Inicio del Sistema Operativo, tanto en el MS-DOS como en Windows 95/98, Millenium, NT o 2000.

Bugs
Término aplicado a los errores descubiertos al ejecutar cualquier programa informático. Utilizado por vez primera por Grace Murrat Hopper en 1945, una de las pioneras de la programación moderna, al descubrir cómo un insecto -bug- había dañado un circuito de la computadora.

C

Cracker
Persona que se introduce sin la autorización pertinente en una computadora de otra persona o en el sistema de redes de una institución o empresa con el fin de romper las barreras de seguridad establecidas. Puede tener distintas finalidades. A veces, el cracker persigue su propio beneficio y, en otras ocasiones, simplemente se siente retado por el desafío que la intrusión significa ya que pone en evidencia la fragilidad de los sistemas informáticos de algunas webs de Internet. La gran diferencia con el hacker es que éste último no realiza el acto por maldad, mientras que el cracker siempre quiere ocasionar algún tipo de daño u obtener algún tipo de contrapartida a su favor.

Conexión SLIP
Protocolo Internet de Línea en serie, Conexión de acceso telefónico a Internet que usa el protocolo TCP/IP.

Conexión PPP
Point to Point Protocol (Protocolo Punto a Punto). Protocolo de Internet para establecer enlace entre dos puntos.

Convert Channel
"Covert Channels" es un concepto originado en el Libro Naranja. Una definición basada en NSCS-TG-030 "A Guide to Undestanding Covert Channel Analysis of Trusted Systems" (Noviembre, 1993) parte de "Rainbow

Series". Pagina 5: Definición 4 - Covert channels son canales que "usan entidades no visibles normalmente como objetos de datos para transformar información de un tipo a otro".

Cookies
Vocablo inglés que significa galleta. Son los datos que entrega el programa servidor de HTTP al navegador WWW para que éste lo guarde. Normalmente, se trata de información sobre la conexión o los datos requeridos por el usuario. De esta manera, puede saberse qué hizo el internauta en la última visita.

D

DNS
Siglas de Domain Name System (Sistema de Nombres de Dominio). Es un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de estos. El estilo de los nombres de "hosts" utilizado en la Red es llamado "nombre de dominio". Algunos de los dominios mas importantes son: .COM (comercial-empresas), .EDU (educación, centros docentes), . NET (operación de la red), .ORG (organización sin ánimo de lucro), etc. La mayoría de los países tienen un dominio propio. Por ejemplo: .ES (España), .US (Estados Unidos de América), .UK (Reino Unido).

Dominio
Equivalente alfanumérico de la dirección de IP numérica de una página web. El dominio tiene varios niveles separados por puntos. Paradójicamente, el nivel superior, o Top Level Domain,es la última parte del dominio y señala el país o la naturaleza de la página web (.mx indica México y .com denota un ente comercial).

E

Exploits
En Internet se llama Exploits a los programas u otras cosas con algún bug (error, fallo, etc) que pueden ser vulnerables, o sea que pueden ser "explotables" (explotados). Existen páginas Webs llenas de Exploits para que la gente (Hackers y demás) sepa de los fallos y puedan sacar de provecho de ello.

F

Finger
Programa que muestra información acerca de un usuario concreto conectado a un sistema local o remoto en un determinado momento y sobre lo que ese internauta está haciendo. Los datos que normalmente se muestran son, por ejemplo, el nombre y el apellido o la hora de la última conexión.

FTP
Siglas inglesas que corresponden a File Transfer Protocol, traducido literalmente al español como Protocolo de Transferencia de Archivos. Se trata de un servicio que permite recibir y enviar archivos entre las computadoras conectados que sean servidores FTP. La diferencia entre FTP y WWW es que el primer servicio no sirve para navegar.

G

Gateway
Sistema de información que se transfiere entre sistemas o redes que son incompatibles.

H

Hacker
Se conoce con este nombre a aquellos usuarios de la Red que se infiltran en sistemas informáticos protegidos. Por lo general, el único objetivo que motiva su actuación es dejar constancia de que han penetrado en el sistema, informando a veces de los fallos de seguridad que les han permitido entrar. Actualmente, el término se identifica con el de pirata informático, es decir, delincuente informático que opera a través de la Red. Aunque la diferencia es que el hacker busca entrar en el sistema y demostrar que es superior a su administrador, mientras que el pirata informático busca su propio lucro o, incluso, destrozar el sistema.

Hardware
Se utiliza este vocablo inglés para denominar al conjunto de componentes físicos que forman una computadora, incluyendo los periféricos.

I

ICMP
'Internet Control Message Protocol'. En español, Protocolo de Control de Mensajes en Internet. Es el protocolo que usa el IP para informar de errores y excepciones, aunque también incluye algunos mensajes informativos.

ISP´s
Internet Service Provider. Proveedor de Servicios de Internet.

IPX
Es un protocolo de intercambio de paquetes conmutados.

K

Kernel
Es la parte central del sistema operativo de una computadora que provee los servicios básicos. O sea, se ocupa de que el software y el hardware puedan trabajar unidos. Otra de sus funciones es la de administrar la memoria de la computadora.

L

LAN
La 'Local Area Network' es una red de ámbito local. Con este término se hace referencia a la conexión entre computadoras en un espacio limitado como puede ser un edificio, normalmente se usa en ámbitos de oficina. Una de las ventajas es que permite compartir recursos e intercambiar los archivos que forman la red.

Last/Lastb
Last: bitácora del sistema, indica desde donde y modo de sistema en que se realiza una conexión del ultimo usuario o terminal firmada.
Lastb: bitácora del sistema, indica desde donde y modo de sistema en que se realiza una conexión del ultimo usuario o terminal firmada, pero muestra los intentos fallidos para entrar al sistema.

Login
Nombre de usuario con el que se inicia una sesión en una computadora.

Logs
Es una bitácora en donde queda registrado los eventos importantes

M

Malware
Con este nombre se conoce a todo el software diseñado para causar algún daño o realizar alguna actividad ilegal. Aunque hoy en día se mezclan cada vez más entre sí, los principales tipos son:

- Virus: Lo más conocido, en realidad representan poco peligro porque la gente es consciente de su existencia y hay antivirus hace mucho tiempo.
- Adware: Se dedican a mostrar anuncios mientras estamos en Internet.
- Spyware: Pensados para registrar lo que hacemos con la computadora, qué páginas se visitan, a que horas, incluso todo lo que se teclea.
- Troyanos: Su misión es abrir una puerta para que otra persona pueda tomar el control de nuestro PC, convirtiéndolo en un zombie
- Gusanos: Están diseñados para consumir recursos, dejando a los PCs inutilizables. Pueden consumir tiempo de CPU, memoria o ancho de banda.

P

Path
Senda o camino que sigue el software para acceder a los datos contenidos en una unidad de almacenamiento.

Pdf
Siglas de 'Portable Document Format'. El PDF es un formato gráfico desarrollado por la empresa Adobe, capaz de reproducir cualquier tipo de documento en forma digital exacta. Así, permite la distribución electrónica de los documentos a través de la Red en forma de archivos PDF, los cuales conservan todas las características gráficas. El programa gratuito 'Acrobat Reader' nos proporciona su visualización.

Rhost
Archivo que especifica el host o sistemas y usuarios que pueden acceder como el usuario propietario de dicho directorio. Archivo de usuarios y servidores fiables, donde se especifican dichos usuarios y servidores.

Root
Raíz. En sistemas de archivos se refiere al directorio raíz. En Unix al usuario principal.

S

Shell Script
Archivos que almacenan comandos con permisos de ejecución. Simple archivo de texto ejecutable compuesto por una serie de comandos shell.

SMTP
Simple Mail Transfer Protocol, protocolo para el traslado de correo electrónico, e-mail, a través de una conexión TCP/IP.

Software
Está formado por aquellos programas de diversos tipos o elementos lógicos, como el sistema operativo, que hacen funcionar una computadora o una red, que se ejecutan en ellos, en contraposición con los elementos físicos de la red o la computadora. El término software está en oposición al de hardware, duro-blando, por lo que se refiere a la intangibilidad de los programas y la realidad física de la computadora.

Spoofing
Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque - al menos la idea - es muy sencilla: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Y como los anillos de confianza basados en estas características tan fácilmente falsificables son aún demasiado abundantes (no tenemos más que pensar en los comandos r-, los accesos NFS, o la protección de servicios de red mediante TCP Wrapper), el spoofing sigue siendo en la actualidad un ataque no trivial, pero factible contra cualquier tipo de organización.

SSH
El cliente Secure Shell. La Secure Shell es un programa que codifica sesiones remotas en estilo Telnet/Rlogin.

SSL
Secure Socket Layer. Es un protocolo que utiliza criptografía para cifrar los datos que se intercambian con un servidor seguro. Proporciona privacidad para datos y mensajes, y permite autenticar los datos enviados. Básicamente se utiliza para transmitir información personal o relacionada con tarjetas de crédito de los usuarios a través de Internet. Las direcciones de páginas Web que utilizan conexiones SSL, comienzan con https: en lugar del estándar http:.

SUID/SGID
Privilegios (de usuario) de administrador para cambiar passwords. Tanto SUID como SGID, son permisos especiales para archivos. El primero define el ID de usuario, 4000 octal o S, el segundo define el ID de grupo 2000 octal o s. Los programas con permisos SGID y SUID son especiales, ya que los permisos de sus propietarios se representan aún cuando los ejecuten otros usuarios. Esto es, si se define el valor root SUID en un programa, este siempre se ejecutará como root, aunque lo utilice un usuario normal. Este es el motivo por el que los archivos de SGID y SUID pueden suponer un riesgo para la seguridad.

T

TCP/IP
Siglas de 'Transmision Control Protocol/Internet Protocol'. Estos dos protocolos de Transmisiones dirigen la manera en la que los equipos y las redes administran el flujo de datos que circula a través de la Red. Consiste en un estándar de comunicaciones muy difundido y de utilización habitual para software de red basado en UNIX con protocolos Token Ring y Ethernet, entre otros. Es compatible con productos de muchas marcas: IBM, Sun, DEC, AT&T, Data General, etc. Este conjunto de protocolos fue desarrollado inicialmente por el Departamento de Defensa de los Estados Unidos.

Telnet
Es el protocolo estándar de Internet que permite al usuario utilizar un servicio de conexión desde una computadora remota y usarlo como si estuviera en una de sus terminales.

TFTP
TFTP es un protocolo para transferir archivos entre distintas máquinas conectadas a través de una red de comunicaciones. Se implementa sobre un servicio de comunicaciones no fiable y no orientado a conexión. Consiste fundamentalmente en la lectura o escritura por parte de un cliente de/a un archivo de un servidor.

Trusted Host

Servidor de confianza. En el mundo del Unix, la confianza se da fácilmente. Digamos que tienes una cuenta en el sistema A, y otra en la máquina B. Para facilitar ir de una a la otra con un mínimo esfuerzo, deseas establecer una relación o unión entre ambas. En el directorio home en A se crea un archivo .rhosts: `echo "B nombre-de-usuario" > ~/.rhosts´ En el directorio home en B creas otro archivo .rhosts: `echo "A nombre-de-usuario" > ~/.rhosts´ (Como alternativa, el root puede establecer una configuración similar en /etc/hosts.equiv, la diferencia está en que entonces sería a nivel del host entero, no sólo a nivel individual.) Ahora, usando cualquiera de los comandos r* sin necesidad de tener que perder el tiempo con verificaciones de passwords. Estos comandos permitirán la autentificación en base a las direcciones, lo que ofrecerá o negará el acceso dependiendo de la dirección IP del solicitante.

U

UDP

UDP es un protocolo sencillo que implementa un nivel de transporte orientado a datagramas:

- NO orientado a conexión.
- NO fiable.

Los datagramas UDP se encapsulan dentro de la parte de datos de un datagrama IP. Una aplicación que utilice UDP para transmitir datos, producirá exactamente un datagrama UDP por cada operación de salida que precise, el cual originará un datagrama IP encapsulándolo. Si ese datagrama IP va a exceder el tamaño máximo de la unidad de datos del nivel de enlace (ej: Trama Ethernet), se fragmentará.

UPS

Unidad de energía ininterrumpida (Uninterruptible Power Supply), una unidad de energía de seguridad para utilizar cuando el suministro principal esta interrumpido. Normalmente son baterias que pueden soportar su red solo de 20 a 30 minutos.

W

WAN

Red informática que se extiende a lo largo de una distancia geográficas.

Worm

Su traducción al español es gusano. El Worm es un programa informático que se autoduplica y autopropaga. A diferencia de los virus, los gusanos suelen estar principalmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Soc & Hupp, de Xerox.

WWW

World Wide Web o Red Mundial. Sistema de servidores de Internet con páginas formateadas en un lenguaje de programación llamado HTML, y que contienen enlaces a otros documentos a los que se acceden mediante hipervínculos. No todos los servidores de Internet forman parte de la WWW.

APÉNDICE

APÉNDICE

INFORMÁTICA : ÉTICA VS COMPETITIVIDAD

Inmersas en un mundo cada vez más competitivo, global y desafiante, las organizaciones se enfrentan a un cambio de paradigma, en el cual, la tecnología de información juega un papel sin lugar a dudas importante.

Hoy en día las empresas se enfrentan a un sin número de problemas y desafíos que deben confrontar en un mundo cada vez más competitivo, global y en donde la única constante es el cambio.

Estos cambios radicales de economías cerradas a mercados globales, de organizaciones jerárquicas a nuevos estilos de estructuras organizacionales, traen como consecuencia diferentes impactos en la sociedad, por un lado, crean los cimientos de la nueva era de la información del siglo XXI y por otro, afectan el estilo de vida de las personas ocasionando complejos dilemas morales y éticos.

En los últimos años el cuestionamiento acerca de la ética se ha incrementado, llegando a ser en los 90´s uno de los principales temas en las agendas de negocios, del mismo modo la tecnología de la información ha tenido un auge en los negocios, principalmente administrando su información y en la mayoría de las veces enfocado con obtener mayor competitividad. En este espacio hablaremos de aquellos efectos donde las organizaciones en su afán de ser competitivas se olvidan de algo tan sencillo pero tan difícil de lograr: la ética en los negocios.

Aquí cabe mencionar la reflexión que hace Esperanza Guisán, donde se cuestiona lo siguiente:

"....Pareciera que nuestro destino no es otro que sucumbir ante un caos moral, una sociedad permisiva hasta limites intolerables dominados por la codicia del dinero fácil, la competitividad, el consumismo y la corrupción."

Pero afortunadamente este caos moral que se vislumbra, nos ha puesto a reflexionar y buscar soluciones a estos problemas éticos y morales. Es aquí donde la información juega un papel importante en la sociedad y es responsabilidad de nosotros el de administrar los conocimientos y la información con juicio recto y moral.

Dejemos abierta la reflexión sobre la ética vs. competitividad, citando a Alvin Toffler, en su libro El Cambio del Poder, "Nos encontramos caminando sobre una capa de hielo muy delgada, donde pocos son los que tienen suficiente experiencia respecto al tema ético, jurídico y en última instancia política que surge con la necesidad de imponer limitaciones en los flujos de información..."

A.1 Marco teórico.

Como podemos ver, analizamos dos temas muy diferentes, por un lado la ética que es una disciplina filosófica y por el otro, el concepto de competitividad que está cobijado por la ciencia administrativa. Estos dos campos que no son excluyentes, se mezclan provocando un complejo escenario de fin de siglo, donde nosotros como individuos dentro de una sociedad de negocios tomaremos la decisión de ser solamente competitivos sin valores o competitivos con una serie de valores apoyados en principios éticos.

Ser solamente competitivo sin valores, se refiere a que podemos ser competitivos en el corto plazo sin ser éticos, pero solo nos estaríamos engañando. Para ser competitivos en el largo plazo tenemos que ser primero éticos y en base a esto buscar la competitividad en la empresa.

Antes de continuar, es conveniente aclarar ciertos conceptos, para poder tener un marco de referencia.

A.II La Ética

Al hablar de ética necesariamente tenemos que hablar de filosofía, debido a que pertenece a esta esfera del conocimiento. La acepción más conocida del vocablo "ethos" se presenta con Aristóteles donde se entendía por "ethos": temperamento, carácter, hábito, modo de ser.

Algunas característica de la ética son:

- Es una disciplina filosófica.
- Su objetivo de estudio es la moral.
- Es normativa de la actividad humana en orden del bien.
- Es reflexiva, porque estudia los actos no como son, sino como deberían de ser.
- Es práctica, es decir, se enfoca al campo de acción humano.

La ética se define como: "principios directivos que orientan a las personas en cuanto a la concepción de la vida, el hombre, los juicios, los hechos, y la moral."

Es conveniente diferenciar la ética de la **moral**, *la ética es una disciplina filosófica, la cual tiene como objetivo de estudio la moral, esto no quiere decir que la ética crea la moral, sino solamente reflexiona sobre ella.*

"La moral se refiere a la conducta del hombre que obedece a unos criterios valorativos acerca del bien y el mal, mientras que la ética reflexiona acerca de tales criterios, así como de todo lo referente a la moralidad."

"El término moral procede del latín "mos", que significa costumbre, hábito, en el sentido de conjunto de normas o reglas adquiridas por medio de hábito"

Otro concepto importante es el de **Valor**, este no lo poseen los objetos por si mismo sino que estos lo adquieren gracias a su relación con el hombre como ser social.

Desde el punto de vista metafórico los valores según Emma Godoy, son como estrellas en el ancho firmamento de la libertad, hacia las cuales solo pueden caminar a ellas por senderos infinitos, como el arte, la ciencia y la moral; el arte se dirige hacia la belleza; la ciencia hacia la verdad; la moral hacia el bien y a estos se le denomina Valores.

Por último, veremos los reguladores de la moral los cuales influencian nuestra conducta.

- *Moral Social*, todo lo que la sociedad nos impone (religión, familia, educación, amistades y cultura)
- *Conciencia Moral*, principios morales de que todo ser humano es digno
- *Leyes del Estado*, reglamentos impuestos por un gobierno, para el mejor funcionamiento de la sociedad.

El primero se refiere a todo aquello que se nos impone sin ninguna consecuencia legal en caso de infringirlos, el segundo apunta por los valores personales de cada individuo, y el tercero el que el estado de derecho fomenta.

A.III "Moral" y "Ética"

El lenguaje ordinario no distingue entre los términos "**moral**" y **ética**". Usamos ambos, indistintamente, para referirnos a normas, conductas y comportamientos del ser humano.

Etimológicamente ambos términos se refieren, respectivamente, a mores o ethos, al comportamiento o conducta del ser humano conectado a las costumbres, a los hábitos y al carácter de los individuos.

Decimos, por ejemplo, que tal o cual conducta o comportamiento es moral o inmoral, ético o contrario a la ética, significando que es "bueno" o "malo", de acuerdo con un determinado código o conjunto de normas que consideramos generalmente aceptadas. Y tendemos a suponer en la mayoría de los casos que este código o conjunto de normas puede ser universal, o sea, compartido por todos y cada uno de los miembros de la especie humana con independencia de las diferencias culturales.

Pero desde un punto de vista técnico-filosófico las palabras "**moral**" y "**ética**" no tienen idéntico significado."**Moral**" *es el conjunto de comportamientos y normas que solemos aceptar como válidos*; y "**ética**" *es la reflexión sobre por qué los consideramos válidos y la comparación con otras "morales" que tienen personas diferentes.*

Por eso se suele decir que, hablando con propiedad, *la ética es la filosofía moral o disciplina filosófica que estudia las reglas morales y su fundamentación.* O también: *la teoría (o ciencia) del comportamiento moral de los hombres en sociedad.*

No voy a entrar en este curso en el análisis y descripción de los distintos tipos de éticas que los filósofos han elaborado a lo largo de la historia ni siquiera en la descripción de las éticas contemporáneas. Basta con saber que hay tantas Éticas o filosofías morales como morales propiamente dichas y que no hay acuerdo entre los filósofos sobre cuál sea la mejor manera de fundamentar las reglas morales.

Esta situación plantea un primer problema: ¿debemos usar las palabras "**moral**" y "**ética**" como las usa la mayoría de gente, esto es, como equivalentes, o más bien debemos aceptar la diferencia entre "**moral**" y "**ética**" establecida por los filósofos y atenernos a un punto de vista meramente descriptivo de las filosofías morales existentes o más bien apuntarnos a una determinada corriente (utilitarismo, existencialismo, marxismo, ética discursiva, contractualismo, etc.) de filosofía moral en el mundo contemporáneo?

Tratando de problemas éticos la decisión sobre este punto es importante. Y más en una sociedad en el que no hay que dar por supuesto que todos o la mayoría de las personas desean dedicarse a la filosofía en un sentido técnico o profesional. Es necesario adoptar como criterio el siguiente: usar las palabras "**moral**" y "**ética**" como las usa la mayoría (para evitar, entre otras cosas, la pedantería y la jerga especializada), pero atenerse a algunas precisiones sobre los conceptos que se expresan en estas palabras y que han sido aportadas por la minoría, en este caso, de los filósofos.

A.IV Significado del Término:

El vocablo moral, usado como adjetivo, se emplea en la conversación corriente:

a) Como sinónimo de los psicológico o lo perteneciente al espíritu, por oposición a lo físico o corporal.

b) También la utilizamos en expresiones para referirnos a ciertas formas del conocimiento al cual no podemos exigir la exactitud y rigor de las ciencias físicas y matemáticas.

c) Como opuesto a lo inmoral o amoral, el término moral es sinónimo de bueno, e indica conformidad con un principio ideal o una ley obligatoria.

En este caso una acción moral sería una acción buena.

Este último concepto nos aproxima al valor del término usado como sustantivo, para significar una de las llamadas "ciencias psicológicas", o aquella parte de la filosofía que estudia la regla de conducta que debe seguir el hombre para vivir de acuerdo con su naturaleza. Algunos prefieren el origen griego del vocablo y usan para el caso el término ética. De acuerdo con esto podemos referirnos al término como Ética o Filosofía Moral.

A.V Naturaleza de la ética:

a) La ética dentro de la filosofía. La filosofía se define como "el conocimiento razonado del hombre, del mundo, de Dios y de sus relaciones". La filosofía concluye que el hombre no alcanza la perfección de su naturaleza, y con ello su fin o destino, que es la dicha o felicidad, sino actuando dentro de particulares normas y principios. Del estudio de estas normas y principios, o de aquello que debe ser la conducta del hombre para el cumplimiento y realización de su fin temporal, hace su objeto una rama de la filosofía que hemos denominado ética o moral.

b) Algunas definiciones.

- Moral viene del latín "mores" que significa costumbre, en cuyo caso la moral sería la "ciencia de las costumbres".
- De manera más explicita y precisa puede ser definida la ética como "la ciencia práctica que enseña las reglas que deben seguirse para hacer el bien y evitar el mal".
- Balmes la define como "la ciencia que tiene por objeto la naturaleza y el origen de la moralidad".
- Lahar la define como "la ciencia de las leyes ideales que regulan las acciones humanas y el arte de usarlas correctamente en las diversas situaciones de la vida".
- Pascal la define como "el arte de vivir bien y ser dichoso".
- P. Foulquié la escribe como "el sistema de reglas de conducta que debe seguir el hombre para vivir de acuerdo con su naturaleza.
- Otros han definido la moral como "la ciencia del buen gobierno de la vida".
- E igualmente podemos definirla como "la parte de la filosofía que estudia el orden a que deben ajustarse los actos libres del hombre".

A.VI Objetivo de la ética.

Como ciencia práctica, no es primordialmente hacernos comprender o darnos a conocer una serie de principios morales o normas de conducta, sino, ante todo, dirigir el proceder del hombre en vista de un resultado.

Como disciplina normativa, la moral señala un fin que debe ser alcanzado y los medios que a él conducen. Nuestro fin es conocer la práctica de las virtudes.
El hombre es el único ser de la creación visible capaz de conocer su fin y de encaminarse a él en forma consciente y libre.

En resumen: el objeto de la filosofía moral es la correspondencia de los actos humanos con una norma o regla ideal, emanada de la misma naturaleza del ser racional, y cuyo último fundamento es el G.·. A.. D.·. U.. , autor de la naturaleza.

Es obvio entonces, que el objeto de la Filosofía Moral es muy vasto, ya que no hay acción humana, ejecutada libremente que se independice del imperio de la ética. Todo acto se

relaciona, directa o indirectamente, con las ordenanzas y principios morales, tanto en su ejecución externa como en las intenciones que lo animan.

A.VII Origen y valor de la idea o noción moral.

Una de las disyuntivas del estudio de la filosofía moral es investigar cual es el criterio supremo de certeza, o aquella razón última que nos permite distinguir la verdad del error. La respuesta está en la evidencia razonada u objetiva que nos proporcionan nuestros principios que han prevalecido por milenios.

Se puede afirmar que estas nociones morales tienen sus orígenes en:

a) Como efecto de la educación, del medio familiar o del medio ambiente.
b) Las que son innatas, es decir, que aparecen como atributos inherentes a la mente humana.

Esta disyuntiva ha dado lugar a mucha controversia, afirmamos con la mejor tradición en filosofía, que nuestros principios no tendrían la fuerza obligatoria que les concede la conciencia moral, sino pudieran ser relacionados, en su origen, a una norma absoluta, independiente de la conciencia individual y colectiva, superior a éstas, y que esté por encima de las variaciones que pudieran imponerle el tiempo y el espacio.

Dicha norma absoluta, si la consideramos en su origen supremo, es el G.·. A.. D.·. U.. , fundamento último del orden moral, y es la naturaleza racional del hombre, si buscamos su fundamento inmediato y próximo.

Para todo ser, su bien es obrar de acuerdo con su naturaleza y con su fin, y su mal es lo contrario. Por lo primero se encamina a su fin, por lo segundo se aleja de él.

Queda así establecido que la moralidad o el orden moral y sus implicaciones, son una realidad sentida y vivida, una realidad que se impone a nuestra conciencia y que se arraiga en un absoluto, y no eso que han querido hacer de ella ciertas doctrinas que lo reducen a una imposición del medio, a cierto género de educación, o a determinada doctrina filosófica, objeto de nuestra preferencia.

La filosofía moral basa su obligatoriedad en principios que en su origen responden a un principio supremo que está por encima de cualesquier conciencia individual o colectiva y no puede ser afectada por el tiempo o el espacio.

A.VIII La competitividad.

"Las empresas que triunfan son las que han sabido adaptarse, transformarse rápidamente bajo el rigor de los tiempos, que han sabido encontrar en la madeja de soluciones posibles, el hilo de la supervivencia, es decir de la vida" [10]

El principal problema, en la actualidad, de las empresas, es que subestiman generalmente la información y el conocimiento, sin pensar que son recursos estratégicos y esenciales para la adaptación de los negocios en un entorno competitivo.

Cuando se hace referencia al concepto de competitividad, se refieren de una manera global y duradera de la empresa y no sólo la competitividad de uno de sus productos o servicios en particular, ya que una empresa puede tener un producto muy competitivo y ser globalmente ineficiente.

Al referir una competitividad duradera se hace con la mira hacia el futuro, es decir basándose en el hecho de que si quieres ser competitivo se tiene que ir a la vanguardia en todos sentidos, y al decir en todos los sentidos también incluye el plano ético y moral.

"Una empresa es competitiva cuando es capaz de mantenerse duradera y voluntarista, en un mercado competitivo y evolutivo, obteniendo un margen de autofinanciación suficiente para asegurar su independencia financiera y los medios de su adaptación."[11]

Según Humberto Lesca, hay que tener en cuenta varios criterios para evaluar la capacidad competitiva de las empresas:

- Capacidad de la empresa a tender hacia la calidad total en el servicio prestado al cliente
- Rapidez de reacción de las empresas
- Capacidad de evolución de la empresa
- Capacidad de innovación de la empresa

Otro modelo de estrategia competitiva es el desarrollado por el profesor Michael Porter, de Harvard Bussines School, el cual es el marco teórico más aceptado para el diseño de una estrategia competitiva de una organización.

Este modelo ha sido sustentado y probado en la industria con resultados verdaderamente sorprendentes, él sugiere que para tener una estrategia competitiva se debe tomar en cuenta no sólo las acciones y reacciones de los competidores directos, sino también los roles de tus proveedores, clientes, productos sustitutos, etc.

---

[10] [Fauvet (J.C.), Fourou (J.R.): La passion d'entreprender, De. d'Organisation,1985 p.96]

[11] Information et adaptation de l'entreprise, Humberto Lesca, Gestión 2000, Masson Paris

Porter, define el espacio competitivo como el conjunto de arenas en las cuales un individuo u organización compite. La competencia siempre ocurre con ciertos limites de fronteras a las cuales le llamaremos arenas competitivas.

"La competitividad de una empresa se mide por las habilidades, que posee destacadamente en mayor grado que cualquiera de sus competidores."

En cada industria, enfatiza Porter el estado de competencia depende de cinco fuerzas:

- La amenaza de nuevos competidores
- Intensidad de rivalidad de competidores directos
- Presión por productos sustitutos
- El poder de negociación con los clientes
- El poder de negociación con los proveedores

La dureza de estas fuerzas determina el beneficio potencial en una industria, donde éste se mide en términos de retorno de capital invertido.

Para lograr una ventaja competitiva en una industria en particular, Porter define tres estrategias genéricas:

- Liderazgo en el costo
- Diferenciación
- Enfoque

La competitividad de una empresa, nos la da una serie de factores, tecnológicos, administrativos etc. entonces estaremos de acuerdo que estos dos conceptos, el de competitividad y ética, no son excluyentes, y no hay nada que impida ser competitivo siendo ético.

Otro factor importante que debemos destacar es que el elemento común que se ve involucrado en obtener competitividad es la información, convirtiéndose en un recurso fundamental de la empresa de hoy. Pero el problema que se presenta, es como administrar la información y el conocimiento.

La competitividad implica administrar información y la administración de la información plantea complejos dilemas morales y éticos los cuales son responsabilidad de los administradores enfrentarlos.

"Frente a la complejidad del mundo, solo sobrevivirán las empresas que hayan aumentado su calidad de información" [12]

[12] IBM France (J.-F. David)

A.IX La Ética y los Sistemas de Información

"Quizá es la Tecnología, la dimensión empresarial, que despierta la conciencia ética con más fuerza, en nuestros días" [Florman]

Desde el advenimiento de la computadora en 1940, cada vez más personas están relacionadas en su trabajo con las mismas, desde analistas, programadores, hasta ejecutivos y directores.

Esto nos da una muestra del impacto que ha tenido la tecnología de información en la sociedad y del papel que juega en las empresas, por un lado dando ventajas competitivas y por otro ocasionando problemas de poder.

La tarea ética frente a la empresa es una continua tarea de rehumanización que puede realizarse a través de legislación, siempre empujada por una especial visión ética de la sociedad.

"Es necesario un principio de moralidad nuevo que se base en las características de la organización moderna y este principio consiste en hacer productivo el esfuerzo humano por medio de la organización de tal manera que el esfuerzo personal organizado produzca beneficios sociales."[Peter Drucker]

Estas reflexiones acerca de la ética en la empresa por parte de Peter Drucker, nos lleva a uno de los muchos ángulos que tiene este singular problema: la falta de códigos éticos referente a la administración de la información, específicamente en medios electrónicos.

En EUA los profesionistas de informática cuentan con diferentes códigos de ética para desempeñar su trabajo, el problema que enfrentan ellos es que tienen muchos y diferentes no pudiendo estandarizar un código de ética en esta área en el ámbito nacional.

En México tenemos mucho camino que recorrer en este sentido, ya que apenas es incipiente la formulación de códigos de ética en los trabajos relacionados con el manejo de información.

Algunas situaciones que presentan problemas de ética.

En la actualidad hay muchas situaciones en las cuales se pueden presentar dilemas morales y éticos relacionados con sistemas de información, los más comunes se listan a continuación:

- Usar programas comerciales sin pagarlos
- Usar recursos computacionales de una compañía para propósito personal
- Hacer mal uso de información de la compañía.
- Intromisión no autorizada en los datos de la compañía o en los datos de la maquina de otro empleado.
- Recolectar datos de otra persona sin su autorización.

- Utilizar las computadoras para monitorear el desempeño de los empleados
- Violar la primacía de software y base de datos
- Crear virus
- Mal uso del correo electrónico
- Ciberpornografía.

A.X Encuesta sobre ética vs. competitividad

Para apoyar los argumentos de este artículo, se realizó una encuesta corta de nueve preguntas referentes a tecnología de información, competitividad y ética.

Se encuesto principalmente a personas que de alguna manera tuvieran relación directa con la tecnología de información ya sea desarrollando software, usuarios finales y ejecutivos de empresas.

En primera instancia el 100% de los encuestados utilizan tecnología computacional en su empresa o trabajo para administrar información. Un dato valioso que aporta este estudio es que el 100% de los encuestados creen que la tecnología de información da mayor competitividad a las empresas.

Los encuestados al responder la pregunta ¿En una escala de 1-10, que tan importante considera Usted que esta tecnología contribuye en la competitividad de su negocio? (En donde 1 significa nada importante y 10 mucho muy importante).

Se generó esta tabla de frecuencias donde podemos observar que el 95% de los encuestados considera importante la tecnología de información para la contribución de la competitividad en su negocio.

Escala	Frecuencia	%
1	0	0.00%
2	0	0.00%
3	0	0.00%
4	0	0.00%
5	1	2.50%
6	0	0.00%
7	1	2.50%
8	16	40.00%
9	8	20.00%
10	14	35.00%
Tot.	40	100.00%

La tercera pregunta es referente a seguridad de los sistemas de información:

¿En una escala de 1-10 que tan seguro son sus sistemas de información en cuanto a plagio de información, fraude y accesos? (En donde 1 significa muy mala seguridad y 10 excelente seguridad) contestaron lo siguiente.

Podemos observar aquí que las opiniones, están más dispersas, porque nadie considera una excelente seguridad en sus sistemas de información, es decir , existen aún desconfianza por parte de los encuestados por su información, sin embargo es una área de oportunidad que se deberá afrontar en los próximos años.

Escala	Frecuencia	%
1	3	7.50%
2	1	2.50%
3	2	5.00%
4	4	10.00%
5	6	15.00%
6	3	7.50%
7	5	12.50%
8	10	25.00%
9	6	15.00%
10	0	0.00%
Tot.	40	100.00%

El siguiente resultado a la pregunta número cinco, aunque no representa la realidad, ya es de por sí un avance importante que más del 35% reconozca que tiene software ilegal, ya que el principal problema, que había años atrás es que ellos no reconocían que estaban infringiendo la ley. También debemos considerar, como ya se observó anteriormente , que hay una tendencia a la baja de la piratería en México.

Respuesta	Frec.	%
SI	25	62.50%
NO	13	32.50%
NO SABE	2	5.00%

En la sexta pregunta ¿Conoces alguna asociación mexicana que tenga campañas para la prevención de software ilegal ?, podemos ver un serio desconocimiento por parte de los encuestados hacia asociaciones como ANIPCO u otras que realicen esfuerzos en México.

Respuesta	Frec.	%
SI	6	15.00%
NO	34	85.00%

La pregunta siete ¿En tu empresa tiene algún código de ética para manejar los sistemas de información?

Respuesta	Frec.	%
SI	14	35.00%
NO	23	57.50%
NO SABE	3	7.50%

La pregunta siete junto con la ocho demuestran claramente la incipiente formulación de códigos de ética en nuestro país, ya que el 92.5% desconoce un código de ética realizado por alguna asociación mexicana para manejo de información.

En la pregunta ocho ¿Conoces algún código de ética por alguna asociación mexicana que delinee los procedimientos a seguir sobre el manejo de información ? siendo sus respuestas :

Respuesta	Frec.	%
SI	3	7.50%
NO	37	92.50%

Por último la pregunta nueve hace una reflexión sobre lo siguiente : ¿A largo plazo ser competitivo implica ser ético ?, generando una polémica interesante donde surgen comentarios que se citaran textualmente.

Respuesta	Frec.	%
SI	27	67.50%
NO	13	32.50%

El 67.5% está de acuerdo en que ser competitivo implica ser ético en el largo plazo, tal vez en corto plazo se pueda plagiar información, copiar software sin autorización, accesar máquinas sin permiso, hacer mal uso del correo electrónico pero en el largo plazo, problemas legales, nueva tecnología , nuevos desarrollos, mayores barreras, mayor seguridad en los sistemas, legislación etc. harán que las supuestas ventajas competitivas que se tenían se pulvericen.

A continuación se citan algunos comentarios importantes a la pregunta nueve que dice porqué piensas tu que ser competitivo en el largo plazo implica ser ético.

- Las empresas han comprendido que el éxito depende de la honestidad en que basen sus acciones ya que los clientes están mejor informados y así pueden tomar mejores decisiones
- No se puede competir imitando, plagiando y copiando, se necesita ser original
- El ser ético, es ser profesional completo y te permite entrar a ser más competitivo
- Como en todo las personas poco éticas pueden llegar a ser más competitivas. Debido a que toman caminos más cortos pero menos éticos

- El ser ético es una base firme de un negocio, el no serlo tarde o temprano le dará problemas legales a la compañía
- En la medida que se es ético, en esa medida se da confianza de los servicios prestados
- La confianza que se brinda en el servicio incrementa la competitividad
- El respeto a los bienes ajenos, fructifica en productividad para las empresas
- Porque toda actitud profesional requiere de la ética
- Cuando no hay un control o protección de la información se pudiera crear conflictos de relación entre empresas o individuos que la conforman

"Motivados por un mundo globalizado hemos orientado a las tecnologías a acercarnos más en una paradoja muy semejante al mural de Miguel Ángel en la Capilla Sixtina, estamos frente a frente cuando siempre habíamos coexistido compartiendo el mismo espacio"

De la reflexión anterior podemos observar que actualmente la humanidad vive un momento histórico trascendental, en el cual, transitamos de una economía industrial a otra economía basada en información y conocimiento.

Queda claro que la tecnología de información juega un papel principal en esta nueva era, pero también aceptamos que se presentan complejos dilemas morales y éticos, los cuales representan un desafío que debemos afrontar de una manera decidida y responsable.

La sociedad deberá prepararse cada vez más para afrontar esta transición que se presenta, y cada individuo deberá administrar los conocimientos e información con juicio recto y moral.

Las organizaciones que deseen ser competitivas, ahora en adelante deberán adaptar la tecnología de información para administrar su información, pero siempre cuidando los principios éticos que delineen políticas y procedimientos a seguir con el uso de la información.

La ciencia y tecnología por su parte deberán preocuparse cada vez más por buscar un enfoque humano en sus investigaciones, adecuándose y soportando esta nueva era de la información.

Los Gobiernos, se deberán enfocar en adaptar la legislación incluyendo todas estas nuevas situaciones que se presentan fomentando un estado de derecho y castigando la anarquía en el uso de la información.

En el largo plazo ser competitivo implica ser ético, ya que nadie podrá adaptarse a tantos y tan drásticos cambios copiando, plagiando, en fin violando los principios éticos básicos porque cuando menos se lo espera se verá rebasado por la verdad.

Por último reflexionemos con la siguiente frase de Octavio Paz sobre la ciencia y tecnología que de alguna manera engloba lo que hemos tratado en este espacio.

"La ciencia y tecnología es como la luz y la sombra, puede el hombre llegar a su autodestrucción mediante esta, pero salvarse mediante la misma" [Octavio Paz]

A.XII Ética en las tecnologías de la información y comunicaciones

Al escribir sobre ética relacionada con una actividad o realidad concreta, muchos autores dedican en general bastantes párrafos o páginas simplemente a justificar por qué escriben sobre ética o por qué quieren hacer una lectura ética de un problema concreto. Esto se acentúa cuando se trata de hacer alguna reflexión ética relacionada con la ciencia o con la tecnología, como es el objetivo de estas páginas dedicadas a ética en las tecnologías de la información y las comunicaciones (TIC).

Hablar de disciplinas más explícitamente científicas o técnicas normalmente está de entrada justificado o tiene ya garantizada una carta de ciudadanía que no precisa especial justificación. La ciencia y la técnica tienen un alto prestigio social y venden por sí solas. Sin embargo, escribir, leer o pensar sobre aspectos éticos relacionados con cuestiones técnicas parece que necesita justificación. A veces existe, aunque de manera no muy bien formulada o explicitada, una cierta descalificación o enmienda a la totalidad cuando se quieren plantear de manera racional dimensiones éticas en la reflexión o análisis de las TIC.

Por eso en estas páginas, incluidas en número monográfico consagrado a las nuevas tecnologías de la información y las comunicaciones, dedicaremos una primera sección a presentar algunas reflexiones que pueden calificarse como teóricas en las cuales describimos algunos aspectos sobre el hecho mismo de querer unir la ética a las TIC. La siguiente sección la dedicaremos a algo que puede ser considerado como más práctico, presentando cuestiones y dilemas concretos directamente provocados por la implantación de las TIC.

A.XIII ¿Por qué hacer consideraciones éticas?

Comencemos con las reflexiones teóricas sobre la ética en las TIC. En primer lugar partimos del hecho de que al reflexionar sobre las TIC podemos fijarnos en distintas dimensiones: en lo que éstas tienen de comunicación, en lo que tienen relacionado con la informática o, por último, lo que tienen en cuanto tecnologías o ingenierías del mundo de la telecomunicación. Son distintos acercamientos que suponen diversos enfoques y el análisis de elementos variados.

Si nos fijamos, por ejemplo, en las tareas de un ingeniero de telecomunicación podemos suponer que puede dedicar su actividad profesional a planificar redes de telecomunicación, a programar sistemas basados en microprocesadores, a diseñar sistemas informáticos distribuidos o a desarrollar servicios electrónicos para comunicaciones, por poner algunos ejemplos de actividades. Por su parte, un ingeniero en informática puede centrar su actividad en gestión de sistemas informáticos, en mantenimiento de infraestructuras informáticas, en planificación de trabajos de análisis y programación o en dirección y de proyectos informáticos.

Las actividades aquí señaladas como muestra son bien diversas, y la lista de actividades relacionadas con las TIC podría multiplicarse. Sin embargo, en todos estos supuestos hay una pregunta que para un porcentaje alto de profesionales es común: ¿qué tienen que ver todas estas actividades con la ética? ¿por qué querer hablar de ética? La respuesta que damos es que sí hace falta hablar de ética porque es un deber considerar las dimensiones éticas de las actividades en las que uno está involucrado.

También hay que señalar que la ética quiere aportar, y reivindicar, como propios una serie de elementos que la caracterizan como disciplina con carácter específico. Aportar, porque es algo que presenta la ética cuando se define a sí misma correctamente. Reivindicar, porque a veces parece que a la reflexión ética se niega carta de ciudadanía al compararla con las disciplinas que quieren ser universitarias o con un valor específico.

Apuntamos aquí algunos de estos elementos que son los que entendemos son propios de la ética hoy en día:

- Racionalidad propia. La ética tiene un modo de racionalidad propio.

Hoy en día es un problema el que la racionalidad científico-técnica o la racionalidad económica se presenten como las únicas de cierto valor. La racionalidad científico-técnica tiene valor y el conocimiento experimentable, contrastable, traducible en nuevos artefactos ciertamente es valioso. También la racionalidad económica es cada vez más importante en un mundo de recursos escasos que requiere una utilización cada vez más ajustada e inteligente de los bienes económicos. Sin embargo, esto no quiere decir que las preguntas propias de la ética (el bien posible, la justicia, la finalidad de las acciones, etc.) hayan de ser sistemáticamente desplazadas y rechazadas porque no responden a la racionalidad de los experimentos medibles o porque no se traducen en lucro y beneficios inmediatos. La racionalidad ética, lejos de ser incompatible con la ciencia, la mejora. Muchos científicos han sido pilares básicos de revoluciones humanistas.

- Subjetivismo. La ética no equivale a puro subjetivismo de que "cada uno piense como quiera".

No se trata de meras decisiones personales ni de que cada uno diga y haga lo que se le antoje y llame ético a lo que quiera. La ética no consiste en dialogar sobre "¿a ti qué te parece?". La ética no es algo banal o algo que se queda en el marco de lo opinable, sino que tiene un rigor específico.

- Principios. La ética no se queda en aplicar a una acción unos principios aprendidos de memoria.

Existen unos códigos deontológicos que tienen su valor pero que nunca pueden agotar lo que pretende la ética. La ética no se reduce a un manual de casuísticas. La realidad tiene unos condicionantes éticos que hacen imposible quedarse en una sola aplicación de principios apriorísticos. La realidad marca los principios éticos. Cada realidad posee una lógica interna que tiene una consistencia ética y unos condicionantes éticos.

- Religión Light.

No tiene fundamento la sospecha de que la ética es una religión light, un intento de salvar en contextos no creyentes un valor supuestamente perdido de la religión. En algunos contextos la ética genera todavía una actitud agresiva en contra por esperarse de ella un discurso de carácter apologético y confesional. No es así. Las cuestiones y el lenguaje que emplea están abiertas a toda persona, independientemente de su credo ideológico. La ética no es un problema confesional sino algo dirigido a todo humano en cuanto humano.

- Moralismo. La ética no consiste en adoctrinamientos.

Hablar de ética no es moralizar. No es decir lo que otros tienen que hacer y así vender seguridades evitando pensar. Con frecuencia se espera un "moralista" ante el que hay que tomar las debidas precauciones. El discurso ético no consiste en adoctrinar o trabajar la buena conciencia del lector o sus buenas y pías intenciones.

En conclusión, podemos afirmar que la ética en las TIC significa, en la teoría, atender a cuestiones de finalidad, cuestiones sobre la bondad de hechos y actividades, cuestiones sobre el deber ser de dichas acciones, cuestiones sobre el deber ejecutar o no ejecutar determinadas acciones en el campo de las TIC. Supone admitir como valiosas preguntas que van más allá de lo meramente técnico o instrumental. Son cuestiones muchas veces sobre los beneficiarios de las acciones. Supone tener por cierta la afirmación de que el que algo sea técnicamente posible, el que algo pueda hacerse, no quiere decir que se deba hacer.

A.IV Dilemas éticos en las tecnologías de la información y las comunicaciones

Después de realizar algunas reflexiones más generales sobre la ética y las T.I.C., pasamos a presentar algunas consideraciones que pueden ser más prácticas. De esta manera, en esta sección apuntaremos a algunas cuestiones problemáticas que son directamente influenciadas por las T.I.C (DIDIER & DUBREIL, LADD, MITCHAM, TAVANI & INTRONA). Se trata de cuestiones concretas que aunque no se asocien única y exclusivamente a las T.I.C. sí son influenciadas de manera determinante por la implantación y generalización de las T.I.C.

- Amenazas a la privacidad y a la seguridad de las organizaciones.

Éste es uno de los temas más clásicos en la ética aplicada a la informática o a los sistemas de información. En este milenio que ahora comienza, uno de los elementos nuevos por medio de los cuales la intimidad de las personas estará en peligro será el motivado por el aumento de las técnicas de búsqueda o escarbo en la red (data-mining) o en las bases de datos, que va mucho más allá de las tradicionales búsquedas de información.

- Contenido y cumplimiento de los códigos de ética.

Los profesionales de la informática y las empresas del mundo de las T.I.C. están desarrollando códigos deontológicos para garantizar la conducta ética en sus asociados o en sus organizaciones. Esto supone un constante reto. Elaborar un código de ética es una tarea laboriosa y detallista. Lamentablemente muchas asociaciones profesionales y empresas creen que su tarea termina cuando consiguen presentar en sociedad un código ético propio bien elaborado mostrándose así ante sus propios países y ante la comunidad internacional como organizaciones responsables y preocupadas por la ética. Sin embargo, hoy en día hay también serios intentos de hacer ver a las asociaciones profesionales que es necesario apoyar activa y continuamente a sus asociados en sus deseos de actuar con justicia en su profesión (ROSENBERG).

- Propiedad de los programas informáticos y la asunción de responsabilidades ante su mal funcionamiento.

Los programas informáticos están suponiendo una manera nueva de entender la propiedad intelectual, pues el objeto a proteger por vía legal, el software, es de una naturaleza distinta a lo anteriormente existente.
Las leyes antipiratería defienden los derechos de los productores de software o de los que tienen en su mano la facultad de vender licencias de uso de dichos programas. El problema ético consiste no sólo en buscar una nueva forma de justificar el derecho a una nueva forma de propiedad, el software, sino en analizar también si las leyes de propiedad intelectual son en sí mismas justas o si debiera de haber nuevas maneras de redireccionar dichas leyes para beneficiar más al gran público.

- Decisiones realizadas por computadora por medios de los sistemas expertos y la posibilidad de comprensión de la complejidad de los sistemas.

Desde hace unos años, los sistemas de información no sólo toman decisiones sino que las ejecutan. En algunos casos se demuestra que toman las decisiones mejor que los decisores humanos. El problema que se plantea es si hay que hacer siempre caso a las máquinas. En otros casos, el problema se puede plantear de otra manera: si los sistemas expertos son tan completos, ¿es moral no hacer caso a las máquinas?

Otro problema dentro de este ámbito es el preguntarse qué hacer ante buscadores de Internet que excluyen sistemáticamente, a veces por error y otras veces por diseño, unos sitios (sites) beneficiando a otros. Se trata de cuestiones no solo técnicas sino también políticas.

- Acceso público justo y relaciones entre las computadoras y el poder en nuestra sociedad.

En este apartado el problema consiste en el acceso a la información y en las cuestiones sobre justicia distributiva, igualdad y equidad. Hay que intentar definir con qué criterios podemos hablar de acceso justamente distribuido a la información, o de igualdad o inclusión en las sociedades de la información presentes y futuras.

- Naturaleza de la sociedad y cultura de la información.

Cuando se utiliza la expresión "sociedad / economía basada en el conocimiento" se quiere destacar la interrelación entre las TIC y el conocimiento y el desarrollo económico. De esta manera, el desarrollo de las TIC plantea la pregunta sobre quién tiene responsabilidad en esta sociedad electrónica o en el ciberespacio. Cómo se reparte el poder, cómo se redistribuye la riqueza o cuáles son las clases sociales beneficiadas y perjudicadas son preguntas que se han de plantear de manera nueva (JOHNSON).

- Realidad virtual e inteligencia artificial.

El presentar como problemática a la realidad virtual (RV) no hace principalmente referencia al problema de si la RV representa bien o no a la realidad. Se refiere principalmente al hecho de que en la posible representación tendenciosa de la RV haya una selección y un favorecimiento no justo de ciertos valores o intereses a expensas de otros. Por su parte, la inteligencia artificial supone también unos planteamientos antropológicos (formas de entender la conciencia, cuestionamiento de la libertad, etc.) que tienen en principio consecuencias para la concepción ética del ser humano.

Hemos analizado situaciones en las que valores de distintos tipos son puestos en juego o amenazados de manera explícita por la generalización de las TIC. Podemos afirmar desde aquí que la Ética en las TIC significa, en la práctica, atender a preguntas sobre situaciones concretas que se ven muy afectadas por la introducción de las TIC. Hemos apuntado algunas, pueden señalarse más. Cada elemento aquí apuntado merece un estudio más detallado y ha de ser fruto de reflexión y atención más pormenorizados.

La ética tiene que ver directamente con las TIC. Un verdadero profesional es aquel que ejerce su competencia científico-técnica desde una profunda integridad personal y a la vez siempre consciente de su propia responsabilidad social. No es solo cuestión de comportarse correctamente como individuos, sino una cuestión de justicia social.

BIBLIOGRAFÍA

Libros de Texto:

- ADELGANI, Gustavo. Miguel. *Seguridad Informática.* MP Ediciones. Uruguay .1997

- CORREA, Carlos M. Batto, Hilda N. Zalduendo, Susana Czar de, Nazar Espeche, Felix A. *Derecho Informático.* De Palma. Argentina. 1987.

- D.B. CHAPMAN y E.D. ZWICKY. *Building Internet Firewalls.* O´Reilly & Associates. Cap 3 y 11.

- D.RUSSELL y G.T. GANGEMI. *Computer Security Basics.* O´Reilly & Associates.

- FOLEY Ph.D, Alan. *Mejores prácticas para la implementación de las políticas de accesibilidad.* North Carolina State University .Bob Regan. Macromedia. Octubre 2001

- JOHNSON, D. *Is the Global Information Infraestructure a Democratic Technology?.* Computers and Society. 1997. pp. 20-26.

- LADD, J. *Ethics and Computer World: A New Challenge for Philosophers.* Computers and Society. 1997. pp. 8-13.

- MITCHAM, C. *Computers, Information and Ethics: A Review of Issues and Literature.* Science and Engineering Ethics. 1995. Vol. 1, pp. 113-132.

- NOMBELLA, Juan José. *Seguridad Informática.* Editorial Paraninfo. España. 1996

- OCDE (Organization for Economic Co-operation and Development): *Guidelines for Security of Information Systems and Networks. Towards a Culture of Security.* OCDE Publications. France. 2002. www.oecd.org (Mundial), http://rtn.net.mx/oecd (México)

- OLGUÍN , Heriberto. *Organización y Administración de Centros de Cómputo.* UNAM-FI-DIE-DIC. México 1997.

- P. HALBROOK y J. REYNOLDS. *Site Security Handbook. Request for comments.*

- PARMAR, S.K. *An Introduction to Security.* sunny@seaside.net

- PFLEEGER. C. P. "Security in Computing". Prentice Hall. Second Ed. Cap.10.

- ROSENBERG, R. *Beyond the Code of Ethics. The Responsibility of Professional Societie.* Computers and Society. 1998. pp. 18-25.

- SANZ Ureta, Jokin y Hualde Tapia, Sebastian. Aspectos técnicos de la seguridad en la información. España. 2001

- STALLINGS, William. *Network Security Essentials: Applications and Standars.* EUA. Prentice Hall. 2000.

- STALLINGS, William. *Network and Internetwork Security.* 2° Edición. Prentice Hall. EUA. 1998

- STOLTZ, Kevin. *Todo acerca de redes de computación.* Prentice may. México 2000.

- SUMMER, Rita. *Secure Computing, Threats and Sfeguards.* EUA. McGraw Hill. 1997

- TAVANI, H.T. & INTRONA, L. D. *Computer Ethics: Philosophical Enquiry.* Computers and Society, March. 1999. pp. 4-8.

- TELLES Valdez, Julio. *Derecho Informatico.* 2° Edición. Mc Graw Hill. México. 1996

- TOFFLER, Alvin. *La Tercera Ola.* Editorial Sudamericana. España. 1998

Sitios de Internet:

- *Amenazas, ataques y vulnerabilidades.* http://it.unix.es//sypi/articulo/ataques.htm

- *Amenazas, ataques, vulnerabilidades.* http://spisa.act.uji.es/SPI/TEORIA/Temario/tema1/

- *Amenazas, servicios y mecanismos.* http://www.eic.es/criptonomicon/seguridad.html

- *Amenazas y ataques a la seguridad.* http://ttt.epsg.upv.es/~juamelju/seguridad/paginas/pag_seguridad.htm

- *Archivos de seguridad informática.* www.rediris.es

- BORGUELLO, Cristian F. *Seguridad Informática: Sus implicancias e implementación.* www.cfbsoft.com , 2001.

- CABRERA Martín Álvaro. *Políticas de seguridad.* http://www.iec.csic.es/criptonomicon/articulos/expertos71.html

- *Ética en las tecnologías de la información y comunicaciones ética en las tecnologías de la información y comunicaciones.* http://paginaspersonales.deusto.es/guibert/1anales.html

- *Evaluación de seguridad de un sistema de información.* www.monografías.com/trabajos/seguinfo/seguridad.shtml www_5.ibm.com/es/press/informes/seguridad.html

- EZEQUIEL Canclini, Fernando. *Desarrollo de una política de protección de datos.* http://www.it-cenit.org.ar/Publicac/PeopleBases/Recopilac/Recopilac12.htm

- http://mx.sun.com/backissues/2001-0313/

- http://www.cisco.com/warp/public/44/solutions/network/vpn.shtml

- http://www.digi-sign-p.com/ndsp/Herramientas/jdspmime.htm

- http://www.entarasys.com/la

- http://www.eurologic.es/conceptos/correoseg.htm

- http://www.gibbon.cl/tutoriales/avanzado-html/node34.html

- http://www.htmlweb.net/seguridad/cripto/cripto_1.html

- http://www.iespana.es/webmaster-hackmat/secciones/proxys.htm

- http://www.inaoep.mx/~moises/s.o./política.doc

- http://www.monografias.com

- http://www.3com.com/nsc/500619.html

- *La ética en el manejo de la información - Los Códigos de ética.* http://www.it-cenit.org.ar/Publicac/PeopleBases/Investigac6.htm

- *Las 75 Herramientas de Seguridad Más Usadas.* Texto original de Fyodor, Traducción por ThiOsk para Hackemate. http://www.insecure.org/tools/tools-es.html

- *Seguridad y protección de la información. Introducción a la problemática de la seguridad informática (by Heineken Team)* http://proxy.itvictoria.edu.mx/sinergiax/seguridad/seguridad.html

- VALVERDE, José R. *Definición de una Política de Seguridad.* www.rediris.es/cert

- www.asc.unam.mx
- www.cert.com