ELABORACIÓN DE UNA GUIA PRÁCTICA DE SEGURIDAD INFORMATICA

GISELA IMBETH TAMARA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
PROGRAMA INGENIERÍA DE SISTEMAS
CARTAGENA
2005

ELABORACIÓN DE UNA GUIA PRÁCTICA DE SEGURIDAD INFORMATICA

GISELA IMBETH TAMARA

Trabajo de grado, presentado como requisito para optar titulo de Ingeniería de Sistemas

DIRECTOR
Magíster GIOVANNY R. VASQUEZ MENDOZA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
PROGRAMA INGENIERÍA DE SISTEMAS
CARTAGENA
2005

Cartagena, Noviembre de 2005

Señores
Comité Programa Ingeniería de Sistemas
L. C.

Por medio de la presente me comunico con ustedes que he avalado el trabajo de Grado titulado, **ELABORACIÓN DE UNA GUIA PRÁCTICA DE SEGURIDAD INFORMATICA,** presentado por la estudiante **GISELA IMBETH TAMARA**, para optar titulo de Ingeniera de Sistemas.

Atentamente,

_____

GIOVANNY R. VÁSQUEZ MENDOZA.

Cartagena, Noviembre de 2005

Señores
Comité Programa Ingeniería de Sistemas
L. C.

Por medio de la presente me comunico con ustedes la elaboración de mi trabajo de grado titulado, **ELABORACIÓN DE UNA GUIA PRÁCTICA DE SEGURIDAD INFORMATICA**, como requisito para optar el titulo de Ingeniero de Sistemas

Atentamente,

_____

GISELA IMBETH TAMARA
COD 9505502

Nota de aceptación

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

_____

Cartagena, Diciembre del 2005

RESUMEN

Para comenzar el análisis de la seguridad informática se deberá conocer las características de lo que se pretende proteger: la información.
Así definimos, Dato, como la unidad mínima con la que compone la información.

Hay información que debe o puede ser publica: puede ser visualizada por cualquier persona (por ejemplo: índice de analfabetismo de un país); y aquella que puede ser privada solo puede ser visualizado por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos) En esta última debemos maximizar nuestros esfuerzos para preservarla de este modo reconociendo las siguientes características en la información: critica, es indispensable garantizar la continuidad operativa; valiosa, es un activo con valor de si misma y sensitiva, debe ser conocida por las personas que la procesan y solo por ellas.

La integridad hace que el usuario confíe en que el sistema le esta proporcionando información correcta. Mantener la integridad de la información supone garantizar que esta no se ha falseado, esto es, que no se han realizado modificaciones inadecuadas, de forma que cuando el usuario acceda a ella sea completa y exacta. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La disponibilidad establece que los usuarios habilitados para ello podrán acceder a la información cuando lo requieran. El sistema deberá además responder dentro de unos márgenes de tiempo adecuados.

La confidencialidad de la información esta relacionada con la prevención del acceso no autorizado a la misma. El objetivo básico es salvaguardar los datos ante operaciones de lectura por parte de usuarios, ya sean personas o programas, no habilitados para ello.

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

La autenticidad permite definir que la información requerida es valida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores pero que se incorporan algunos aspectos particulares:

Protección de la replica: mediante la cual se asegura que una transacción sola 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 la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

Consistencia: se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.

Aislamiento: este aspecto, íntimamente relacionado con la confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.

Auditoria: es la capacidad de determinar que acciones o procesos se están llevando a cabo en el sistema, así como quien y cuando las realiza.

Cabe definir la amenaza, en el entorno informático, como cualquier elemento que comprometa al sistema.

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

a) La prevención: mecanismos que aumentan la seguridad de un sistema durante su funcionamiento normal.
b) La detección: mecanismos orientados a revelar violaciones a la seguridad.
c) La recuperación: mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar este a su funcionamiento normal.

Se llama intruso o atacante a la persona que accede (o intenta acceder) sin autorización a un sistema ajeno, ya sea en forma intencional o no.

Según Julio C. Ardita[1] clasifica a los intrusos de la siguiente manera:

Clase A: el 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, están jugando, son pequeños grupos que se juntan y dicen vamos a probar.

Clase B: es el 12% son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo que esta usando es victima, testean las vulnerabilidades del mismo e ingresan por ellas.

Clase C: es el 5%. Es personal que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar

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

En un sistema informático hay tres elementos básicos a proteger: el hardware, el software y los datos.

El hardware que es el conjunto de elementos tangibles como: CPU, cables, CD-ROM, cintas, componentes de comunicación.

El software: es la parte lógica de nuestro computador, sin este no tendría vida nuestra maquina: el sistema operativo, aplicaciones, utilidades.

Los datos: son el conjunto de información lógica que maneja el software y el

[1] ARDITA, Julio Cesar. Director de Cybsec S.A. Security System y es-hacker. http://www.cybec.com

hardware: base de datos, documentos y archivos.

También podemos hacer referencia de un cuarto elemento llamado fungible que son los que se gastan con el uso continuo: papel, tonner, tinta, cintas magnéticas, disquetes.

De los cuatro los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, del software o de los elementos fungibles, estos pueden adquirirse nuevamente desde de su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar: hemos de pasar obligatoriamente por un sistema de copia de seguridad, y aun así es difícil de devolver los datos a su forma de anterior al daño.

Con demasiada frecuencia se cree que los piratas son los únicos que amenazan nuestro sistema, siendo poco los administradores que consideran todos los demás riesgos.

En la actualidad existen en el mercado ciertos tipos de antivirus, firewalls o cortafuegos**.**

Estos dispositivos los hay de tipo de lógico o físico, otros costosos, y también podemos encontrar en el mercado de la Web, cortafuegos gratuitos.

Podemos definir a los cortafuegos o firewall que son un software o dispositivo que están destinados a garantizar la seguridad en sus comunicaciones vía Internet al bloquear las entradas sin autorización a su computadora y restringir la salida de información. Con respecto, a los cortafuegos los mejores son los físicos (hardware), y con un precio elevado.

Algunos firewalls que podemos encontrar son: Zone Alarm, Agnitum Outpost Free, Kerio Personal Firewall, Sygate Personal Firewall.

La criptografía busca definir y analizar lo que entendemos por seguridad computacional, estudiando los algoritmos, técnicas y protocolos, datos transmitidos electrónicamente, así como su integridad y autenticidad.

Por ejemplo la encriptación de datos permite garantizar que solo el destinario del mensaje puede comprender su significado, y las firmas digitales permiten asegurar que el mensaje proviene de un remitente específico y que su contenido no ha sido modificado.

Es importante que el lector se familiarice con nuestro vocabulario, por eso he elaborado un glosario en el cual de una manera fácil nos explica ciertas palabras para que la guía sea de gran ayuda.

Espero que esta guía sirva de mucho a las personas que les interese aprender los conceptos de seguridad.

Los resultados de la investigación nos dieron a conocer como es que funciona el proceso de la seguridad computacional, las políticas que se deben tener en cuenta. También cuales son las nuevas tecnologías y herramientas que se usan, las aplicaciones criptográficas que se usaban y las que hoy día se manejan.
Se cumplió con los objetivos trazados, porque metodológicamente se fue haciendo cada capitulo paso a paso, sin dejar un detalle por fuera.

La seguridad computacional es muy importante porque debido a que sin importar que un profesional tenga o no información en el campo de la

informática, tiene una responsabilidad directa, como profesional con la seguridad informática.

GLOSARIO

Auditoria: proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el alcance al que se cumplen los procedimientos o requisitos contra los que se compara la evidencia.

Backup: copia de seguridad, se hace para prevenir una posible pérdida de información.

Bugs: Un error de software o computer bug, que significa bicho de computadora, es el resultado de una falla de programación introducida en el proceso de creación de programas de computadora.

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

Cookies: ficheros de texto codificado que la mayoría de los servidores web de Internet envían y registran en un archivo del disco duro de cada usuario que visita el web, se utiliza para registrar el paso del usuario y controlar sus preferencias y establecer un perfil personalizado del los usuarios.

Crackers: Hackers tentados por el reverso tenebroso. Expertos en informática que utilizan sus conocimientos para realizar acciones más o menos deplorables, como reventar programas o penetrar en ordenadores ajenos para robar o destruir datos.

Freeware: programas que se pueden emplear gratuitamente. Creados por programadores que no buscan lucrase con ellos.

Hackers: Un hacker (del inglés hack, recortar), también conocidos como sombreros blancos es el neologismo utilizado para referirse a un experto en varias o algunas ramas relacionadas con la computación y telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz.

Linux: sistema operativo derivado del UNÍX que manteniendo casi todas las ventajas que este ofrece, puede ser ejecutado en computadoras personales. Fue desarrollado originalmente por el estudiante finlandés de informática Linus Torvalds, quien publicó su código fuente en 1990, en la forma de código abierto.

Número IP o **Dirección IP**: dirección numérica con la que se identifica una máquina conectada a Internet, consta de varios grupos de dos o tres números separados por puntos.

Plan de contingencia: definición de acciones a realizar, recursos a utilizar y personal a emplear caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización.

Política de seguridad: conjunto de reglas para el establecimiento de servicios de seguridad.

Proxy: software que permite a varios ordenadores acceder a Internet a través de una única conexión física y puede permitir acceder a páginas Web, correo electrónico, etc., y también, servidor de comunicaciones, responsable de canalizar el tráfico entre una red privada e Internet, que contiene un cortafuegos.

Riesgo: posibilidad de que se produzca un impacto dado en la organización.

Servicio de seguridad: servicio suministrado por uno o más niveles de un sistema abierto de comunicación, que garantiza la seguridad del sistema y de las transferencias de datos, tales como confidencialidad, autenticación, integridad, no repudio, control de acceso y disponibilidad.

Shareware: programas que se pueden emplear gratuitamente durante un tiempo de prueba y que, una vez transcurrido el plazo, el usuario debe pagar una cantidad para seguir utilizándolos.

Uníx: es un sistema operativo originario de Bell. Es el primer sistema operativo en lenguaje C. Evolucionó como un gran producto libre (freeware) con muchas extensiones e ideas proporcionadas por una gran variedad de versiones de Unix por diferentes empresas, universidades e individuos. En parte porque no era propiedad de ninguna compañía de computación y en parte porque está escrito en un lenguaje estándar y tiene muchas ideas populares.

Virus: programa que “infecta” un ordenador, capaz de propagarse de un fichero a otro del ordenador, y que causa efectos indeseables y daños irreparables.

CONTENIDO

1. EL PROCESO DE LA SEGURIDAD INFORMÁTICA

Un proceso es un conjunto de actividades o eventos que se realizan o suceden con un determinado fin. Este término tiene significados diferentes según la rama de la ciencia o la técnica en que se utilice[2].
Sistema por el cual un conjunto de recursos y actividades interrelacionadas transforman elementos de entrada en elementos de salida.[3] De su diseño y documentación depende el éxito de la gestión. Conjunto de las fases, momento o etapas sucesivas de un fenómeno, tarea u operación.[4]

La seguridad informática es un proceso y no una actividad particular que desarrolla cualquier persona u organización.

Al hablar de seguridad hay que inv0olucrar muchos aspectos que no solo están relacionados con herramientas tecnológicas. Abordar el tema de seguridad no solo implica una solución de hardware y software, también involucra un conocimiento sobre el riesgo que significa no dar confiabilidad a la información, lo que en ocasiones tiene que ver con un desconocimiento de parte de los administradores de sistemas sobre el tema.

El problema hay que enfrentarlo con tecnología, pero también debe involucrar a los tomadores de decisiones, que son finalmente quienes

[2] http://es.wikipedia.org/wiki/Proceso
[3] www.ripit.granma.inf.cu/PerfecEmp/Paginas/Glosario.asp
[4] www.policia.gov.co/inicio/portal/portal.nsf/paginas/GlosarioInstitucional

deciden las inversiones, ellos deben comprender claramente la problemática para destinar los recursos necesarios para garantizar la confiabilidad, disponibilidad e integridad de los datos.

La seguridad informática no siempre es reconocida como una necesidad, en muchos casos la seguridad, se ve como un valor adicional que no ofrece ningún beneficio tangible e inmediato. Esto tiene implicaciones en las cuales la seguridad se implementa después de que un servicio informático entra en funcionamiento y esto lo hace mucho más impactante y costoso. La idea de que la seguridad puede ser por medio de un paquete independiente del servicio es algo que también impera en los niveles administrativos, aunque en algún caso esto es aplicable, la seguridad debe ir vinculada estrechamente a las políticas, riesgo, tecnologías, protección, etc. Y estos aspectos deben ser diseñados de acuerdo con las características de la organización.

1.1. PROPIEDADES DE LA INFORMACIÓN QUE PROTEGE LA SEGURIDAD INFORMÁTICA:

La Seguridad Informática debe tener en cuenta las siguientes propiedades:

- Confidencialidad: cuando la información que se tiene no pueda estar disponible a personas ajenas a quien tiene derecho a hacerlo.
- Integridad: cuando la información no puede ser modificada, a menos de la persona que lo envía.
- Disponibilidad: Se define como el "grado en el que una información está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede

acceder a un Sistema de Información en un periodo de tiempo considerado aceptable

- Autentificación o no repudio: cuando se conoce a la persona que envía la información (un ejemplo de esta son las firmas digitales).

1.2 FACTORES QUE AFECTAN LOS SISTEMAS DE INFORMACION:

Los principales factores que afectan los sistemas de informáticos son muchos de los cuales podemos mencionar algunos clasificándolos de la siguiente manera. Las amenazas externas, que afectan al hardware la parte física de nuestro sistema, estos son causados por inundaciones, terremotos, incendios, etc.

Otro tipo de amenazas también puede venirse de usuarios o trabajadores infieles, de los cuales se puede extraer información valiosa causando daños al sistema de información, ya sean lógicas con respecto al sistema operativo o programas aplicativos o físicos con respecto al hardware. En este tipo de amenazas cabe resaltar los virus spyware, etc.

1.2.1 Factores que afectan la integridad de los datos:

- Desastres Naturales: inundaciones, incendios tormentas, terremotos, etc.[5]
- Fallas de hardware: discos, controladores, energía, memoria, dispositivos, etc.
- Fallas humanas: accidentes, inexperiencias, estrés, problemas de comunicación, venganza, interés personal.

[5] Tesis “Seguridad Informática: sus implicancias e implementación”, Cáp. 2. Copyright Cristian F. Borghello 2001. www.cfbsoft.com.ar

- Fallas de la red: controladores, tarjetas, componentes, radiación.
- Problemas de software: requerimientos mal definidos, corrupción de archivos, errores de programas o aplicaciones, problemas de almacenamiento, errores de sistema operativo.

1.2.2 Factores que afectan a la seguridad de los datos:

- Autentificación: la forma en que se hace el proceso de acceso a los sistemas. Ejemplo: password, perfiles de usuarios.
- Basados en cables: todos los cables son inseguros y por medio de ellos se puede acceder fácilmente a los datos que circulan de un nodo a otro en una red, para esto se utilizan las técnicas de encriptación. (Mas adelante se aclara en él capitulo de criptografía)
- Físicas: averías en los componentes físicos, robo espionaje industrial, etc.
- Programación: por las aplicaciones mal construidas, los bugs en el software para reducir el riesgo de perder datos.
- Puertas falsas: en la gran mayoría de los softwares existen puertas falsas que permiten alterar o manipular los datos con los cuales estos trabajan. Ejemplo: manipulación de las tablas en las bases de datos.

1.3 LOS RIESGOS EN LOS SISTEMAS DE INFORMACIÓN:

Los riesgos en los sistema de información constituyen la principal forma de hacer frente al problema de la seguridad informática en las organizaciones o personas naturales, esta pasa ha ser una labor de vital

importancia ya no en el ámbito funcional si no ha nivel corporativo. De ella se desprende la planificación de la seguridad de los sistemas informáticos, y por ende las políticas y medidas de seguridad ha implantar como también los objetivos, estrategias, y organización de la seguridad. El análisis de riesgos en los sistemas de información es una acción permanente cíclica y recurrente, es decir, se ha de realizar continuamente debido a los cambios del sistema y de su entorno.

Sus objetivos son identificar, analizar, y eliminar o controlar las fuentes de riesgos antes de que empiecen ha amenazar el funcionamiento continuo y confiable de los sistemas de información.

1.3.1 Etapas de los riesgos: a continuación observaremos, cada una de las etapas que conforman la gestión de riesgos:

- Identificación de riesgos: es la primera etapa a elaborar, aquí se hace una lista de los recursos que cuenta la empresa. Existen recursos tangibles (monitores, computadoras, impresoras, etc) e intangibles (privacidad de los usuarios, claves de los usuarios, imagen publica, etc). Se debe hacer una lista de las amenazas que afecten los recursos, dichas amenazas pueden ser ambientales o naturales como: incendios y terremotos, amenazas extrañas como: fallas estructurales del edificio, relámpagos, epidemias, inundaciones, pérdida del servicio telefónico, etc., amenazas de introducción de virus informáticos y "bugs" en el software. Después de determinar las amenazas es necesario estimar qué tan factible es que suceda cada una de ellas, esta es una tarea difícil por la cantidad de información a recaudar, por ejemplo: informes estadísticos, seguros, daños, etc.

- Análisis de Riesgos: un análisis de riesgo puede ser efectuado en cualquier momento y tiene como objetivo principal cuantificar a las exposiciones existentes a fin de que se establezca a una base para una selección posterior de las medidas de control con un costo apropiado.

- Priorización de riesgos: esta etapa se lleva a cabo una vez concluida la de análisis de riesgos y tiene como objetivo determinar donde se centrara el esfuerzo en nuestro plan de gestión, en función de nuestros recursos y los objetivos de la empresa.

- Resolución de riesgos: se decide que hacer frente al riesgo. Se debe adoptar un camino, con la evaluación del costo que pueda tener para seguirlos. Evitar que el riesgo exista.

- Planificación del control de Riesgos: el objetivo de la planificación es obtener una serie de medidas (ejemplos: planes de contingencia, políticas de seguridad, reglas, etc.) para limitar los riesgos que atentan contra los sistemas de información (disminuir su probabilidad de ocurrencia, etc.).

- Monitoreo de riesgos: es una de las etapas en la que se debe estar en la continua ejecución, sirviendo como medio para evaluar los efectos de los mecanismos de seguridad implantados, permitirá ir

mejorando el plan de control de riesgos como también permitirá que se reevalúen las probabilidades de ocurrencia de ciertos riesgos, existiendo la posibilidad de que desaparezcan o aparezcan nuevos riesgos, obligando a las empresas a modificar su plan.

- Plan de Contingencia: se elabora un documento llamado “Plan de Contingencia o Gestión”. El cual proporciona la cohesión que permite al grupo de personas encargadas de la recuperación, actuar como un equipo al adjudicar a cada miembro una lista concreta de responsabilidades y procedimientos a seguir ante el surgimiento del problema. En un plan de contingencia no se incluyen copias de seguridad como parte de su contenido, sin embargo la realización de estas debe ser un requisito previo al plan de contingencia.

1.4 POLÍTICAS DE SEGURIDAD:

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes ha las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan ha llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede

ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

1.4.1 Definición de Políticas de Seguridad Informática**:** una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

1.4.2 Elementos de una Política de Seguridad Informática: las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los

cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

1.5 PROTECCION:

Una vez que se conocen los ataques a los que están expuestos un sistema es necesario conocer los recursos disponibles para protegerlo. Mientras algunas técnicas son evidentes otras pautas no lo son tanto e incluso algunas pueden ocasionar una sensación de falsa seguridad.

Los intrusos utilizan diversas técnicas para quebrar los sistemas de seguridad de una red. Básicamente buscan los puntos débiles del sistema para poder colarse en ella, estas personas cuentan con grandes herramientas como los Scanners, el cracking de passwords, software de análisis de vulnerabilidades y los exploits.

La administración de la seguridad es posible dividirla en tres grupos:

- Autenticación: se refiere a establecer las entidades que pueden tener acceso al universo de recursos de computación que el medio puede ofrecer.
- Autorización: es el hecho de que las entidades autorizadas a tener acceso a los recursos de computo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio-
- Auditoria: 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 este suceda (proactividad). A continuación se citan algunos de los métodos de protección más conmumente empleados.

1. Sistema de detección de intrusos.

2. Sistema orientados a conexión de red.

3. Sistema de análisis de vulnerabilidades.

4. Sistema de protección a la integridad de información.

5. Sistema de protección a la privacidad de la información.

Resumiendo un modelo de seguridad debe estar formado por múltiplex componentes o capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red. Podemos considerar que estas capas son:

1. Política de seguridad de la organización.

2. Auditoria.

3. Sistemas de seguridad a nivel Router-Firewall.

4. Sistemas de detección de intrusos.

5. Plan respuesta a incidentes.

6. Penetración Test.

1.5.1 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 hábitat natural.

1.5.2 Routers y Bridges: los routers son dispositivos electrónicos encargados de establecer comunicación externas y de convertir los protocolos utilizados en las LAN en protocolos de WAN y viceversa.

En cambio si se conectan dos redes del tipo LAN se utilizan Bridges, los cuales son puentes que operan a nivel de enlace.

Los routers toman decisiones en base a un conjunto de datos, regla, filtros y excepciones que le indican que rutas son las mas apropiadas para enviar los paquetes.

1.5.3 Access Control List: (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 puede definirse sobre un Proxy una lista de todos los usuarios (o grupo de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrían definirse otras características como limitaciones de anchos de banda y horarios.

1.5.4 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 UNIX. 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, son fáciles y simples de validar.
- Debido a que el programa protegido se mantiene como una entidad separada, este puede ser actualizado sin necesidad de cambiar el wrapper.
- Debido a que los wrappers llaman al programa protegido mediante llamadas estándar al sistema, se puede usar un solo wrapper para controlar el acceso a diversos programas que se necesiten proteger.
- Permite un control de accesos exhaustivo de los servicios de comunicaciones, además de buena capacidad de Logs y auditorias de peticiones a dichos servicios, ya sean autorizados o no.

1.5.5 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 llamó previamente.

1.5.6 Sistemas Anti – sniffers: esta técnica consiste en detectar sniffers en el sistema. Generalmente estos programas se basan en verificar el estado de la placa de red y el tráfico de datos en ella.

1.6 VIRUS INFORMATICOS:

1.6.1 Creación y difusión de virus: Este es uno de los temas más conocidos y sobre más información se consigue en el ámbito informático, veamos, que son los virus informáticos y como se propagan, además cuales son los más populares y que hacer en caso de encontrarnos con uno en el equipo de cómputo.

Virus informático: pequeño programa, invisible para el usuario (no detectable para el sistema operativo) y de actuar especifico y subrepticio, cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador , pueden reproducirse formando replicas de si mismos (completas, en forma discreta, en un archivo, disco u computadora distinta a la que ocupa), susceptibles de mutar resultando de dicho proceso la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados (en forma lógica).

1.6.2 ¿Cómo actúa un Virus Informático? Un virus informático se asemeja a un virus biológico, el cual lleva su ciclo de propagación:

1. Infección: Al ejecutar un archivo infectado (el código del virus se ha implantado en el archivo anteriormente) comienza la fase de infección, duplicándose e implantándose en otros archivos ejecutables. Comienza la "invasión" del sistema informático. La víctima, aún no es consciente de la existencia del virus ya que este permanece oculto y sin causar daños apreciables.
2. Expansión: El virus pasará a otros ordenadores, a través de redes informáticas, disquetes, CD, discos duro, memorias flash y otro dispositivo que contengan archivos infectados, software en Internet, archivos adjuntos a mensaje electrónicos, etc.
3. Explosión: Si el virus no ha sido detectado y destruido por algún *programa antivirus*, en un momento determinado o bajo determinadas circunstancias, tomará el control del ordenador infectado, ejecutando la acción para la que fue programado. En este momento, debido a los trágicos efectos que pueden llegar a ocasionar, se hará evidente su existencia, acabando con información vital contenida en el sistema informático.

1.6.3 Síntomas apreciables antes de la Explosión del Virus: los síntomas más usuales son:

- Los programas tardan más tiempo en cargarse y se produce una disminución considerable y global de la velocidad de procesamiento del sistema.
- Reducción del espacio libre de memoria y aumento en el tamaño de los archivos ejecutables.
- Aparición de continuos e inusuales mensajes de error.
- Programas que misteriosamente dejan de funcionar.

- Caídas frecuentes del sistema.

El buen programador de virus intentará minimizar estos cinco "efectos colaterales", de manera que el virus, en la fase de Infección, consuma muy pocos recursos del sistema, interfiriendo muy poco y de forma mínima en su funcionamiento normal.

1.6.4 Formas de Infección: debemos que recordar que un virus no puede ejecutarse por si solo, necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse a un programa portador necesita modificar la estructura de este, para que durante su ejecución pueda realizar una llamada al código del virus.

Las partes del sistema más susceptibles de ser infectadas son el sector de arranque de los disquetes, la tabla de partición y el sector de arranque del disco duro, y los ficheros ejecutables (*.EXE y *.COM. Para cada una de estas partes tenemos un tipo de virus, aunque muchos son capaces de infectar por sí solos estos tres componentes del sistema.

En los disquetes, el sector de arranque es una zona situada al principio del disco, que contiene datos relativos a la estructura del mismo y un pequeño programa, que se ejecuta cada vez que arrancamos desde disquete.

En este caso, al arrancar con un disco contaminado, el virus se queda residente en memoria RAM, y a partir de ahí, infectará el sector de arranque de todos los disquetes a los que se accedan, ya sea al formatear o al hacer un DIR en el disco, dependiendo de cómo esté programado el virus.

El proceso de infección consiste en sustituir el código de arranque original del disco por una versión propia del virus, guardando el original en otra parte del disco; a menudo el virus marca los sectores donde guarda el *boot* original como en mal estado, protegiéndolos así de posibles accesos, esto suele hacerse por dos motivos: primero, muchos virus no crean una rutina propia de arranque, por lo que una vez residentes en memoria, efectúan una llamada al código de arranque original, para iniciar el sistema y así aparentar que se ha iniciado el sistema como siempre, con normalidad. Segundo, este procedimiento puede ser usado como técnica de ocultamiento.

Normalmente un virus completo no cabe en los 512 bytes que ocupa el sector de arranque, por lo que en éste suele copiar una pequeña parte de si mismo, y el resto lo guarda en otros sectores del disco, normalmente los últimos, marcándolos como defectuosos. Sin embargo, puede ocurrir que alguno de los virus no marquen estas zonas, por lo que al llenar el disco estos sectores pueden ser sobrescritos y así dejar de funcionar el virus.

La tabla de partición esta situada en el primer sector del disco duro, y contiene una serie de bytes de información de cómo se divide el disco y un pequeño programa de arranque del sistema. Al igual que ocurre con el boot de los disquetes, un virus de partición suplanta el código de arranque original por el suyo propio; así, al arrancar desde disco duro, el virus se instala en memoria para efectuar sus acciones. También en este caso el virus guarda la tabla de partición original en otra parte del disco, aunque algunos la marcan como defectuosa y otros no. Muchos virus guardan la tabla de partición y a ellos mismos en los últimos sectores de disco, y para proteger esta zona, modifican el contenido de la tabla para reducir el tamaño lógico del disco. De

esta forma el DOS no tiene acceso a estos datos, puesto que ni siquiera sabe que esta zona existe.

Casi todos los virus que afectan la partición también son capaces de hacerlo en el *boot* de los disquetes y en los ficheros ejecutables; un virus que actuara sobre particiones de disco duro tendría un campo de trabajo limitado, por lo que suelen combinar sus habilidades.

Con todo, el tipo de virus que más abunda es el de fichero; en este caso usan como vehículo de expansión los archivos de programa o ejecutables, sobre todo *.EXE* y *.COM*, aunque también a veces *.OVL*, *.BIN* y *.OVR*. AL ejecutarse un programa infectado, el virus se instala residente en memoria, y a partir de ahí permanece al acecho; al ejecutar otros programas, comprueba si ya se encuentran infectados. Si no es así, se adhiere al archivo ejecutable, añadiendo su código al principio y al final de éste, y modificando su estructura de forma que al ejecutarse dicho programa primero llame al código del virus devolviendo después el control al programa portador y permitiendo su ejecución normal.

Los efectos que causan los virus son variados; entre éstos se encuentran él formateo completo del disco duro, eliminación de la tabla de partición, eliminación de archivos, ralentización del sistema hasta limites exagerados, enlaces de archivos destruidos, archivos de datos y de programas corruptos, mensajes o efectos extraños en la pantalla, emisión de música o sonidos.

1.6.5 Prevención, Detección y Eliminación: una buena política de prevención y detección nos puede ahorrar sustos y desgracias. Las medidas de prevención pasan por el control, en todo momento, del software ya introducido o que se va a introducir en nuestro ordenador,

comprobando la fiabilidad de su fuente. Esto implica el escaneo, con un buen programa antivirus, de todo el software que nos llega, y ante la más mínima duda lo mejor es deshacerse inmediatamente de este.

Por supuesto, el sistema operativo, que a fin de cuentas es el elemento software más importante del ordenador, debe ser totalmente fiable; si éste se encuentra infectado, cualquier programa que ejecutemos resultara también contaminado. Por eso, es imprescindible contar con una copia en disquetes del sistema operativo, protegidos éstos contra escritura; esto último es muy importante, no solo con el sistema operativo sino con el resto de disquetes que poseamos. Es muy aconsejable mantenerlos siempre protegidos, ya que un virus no puede escribir en un disco protegido de esta forma. Por último es también imprescindible poseer un buen software antivirus, que detecte y elimine cualquier tipo de intrusión en el sistema.

1.6.6 Virus de Macros: Esta entre las novedades surgidas últimamente en el mundo de los virus, aunque no son totalmente nuevos, parece que han esperado hasta 1995 para convertirse en una peligrosa realidad. Por desgracia, ya existe un número importante de virus de este tipo catalogados, que han sido escritos en WordBasic, el potente lenguaje incluido en Microsoft Word.

Estos virus sólo afectan a los usuarios de Word para Windows y consisten en un conjunto de macros de este procesador de textos. Aunque el peligro del virus se restringe a los usuarios de Word, tiene una importante propagación ya que puede infectar cualquier texto, independientemente de la plataforma bajo la que éste se ejecute: Mac, WindowsXP, Windows NT y OS/2. Este es el motivo de su

peligrosidad, ya que el intercambio de documentos en disquete o por red es mucho más común que el de ejecutables.

El primer virus de este tipo que salió a la luz se llamaba «WordMacro/DMV» y era inofensivo, ya que sólo anunciaba su presencia y guardaba un informe de sus acciones. Escrito por Joel McNamara para el estudio de los virus de macros, fue desarrollado en 1994 pero su autor guardó el resultado hasta que observó la aparición del virus conocido por «WordMacro/Concept». Tras ello, McNamara decidió hacer público su desarrollo esperando que la experiencia adquirida sirviera de enseñanza para todos los usuarios. Y aunque probablemente tenga un efecto negativo, McNamara ha publicado también las pautas para crear virus que afecten a los ficheros de Excel.

«WinMacro/Concept», también conocido como «WW6Infector», «WBMV-Word Basic Macro Virus» o «WWW6 Macro», no es demasiado molesto, ya que al activarse infecta el fichero «normal.dot» y sólo muestra en pantalla un cuadro de diálogo con el texto «1». Microsoft tiene disponible un antivirus llamado «prank.exe» que distribuye gratuitamente entre sus usuarios registrados, pero que también puede encontrarse en numerosas BBS, Internet o Compuserve.

Sin embargo, la evolución de este tipo de virus siguió su camino y pronto se detectaron dos nuevas creaciones llamadas «WordMacro/Nuclear» y «WordMacro/Colors». El primero de ellos puede llegar a introducir un virus tradicional en el sistema o modificar la salida impresa o por fax en determinados momentos. El «WordMacro/Colors», también conocido por Rainbow o arco iris,

cambia (cada 300 ejecuciones de la macro) la configuración de colores de Windows.

De momento la macros conocidas para Word no son capaces de infectar las versiones nacionales del programa, los usuarios españoles pueden estar tranquilos ya que los comandos del lenguaje de macros han sido traducidos al castellano y las macros creadas con versiones en inglés no funcionan. No obstante, siempre es posible que alguien traduzca el virus o cree uno nuevo.

1.6.7 Virus en Internet: En ocasiones se propagan rumores que dan por cierto noticias de dudosa procedencia. Más o menos esto es lo que ha sucedido de un tiempo a esta parte con el virus por correo electrónico de Internet conocido por Good Times. Lógicamente las primeras noticias de esta maligna creación aparecieron en la «red de redes», en un mensaje alarmante que decía que si algún usuario recibía un mensaje con el tema «Good Times» no debía abrirlo o grabarlo si no quería perder todos los datos de su disco duro. Posteriormente el mensaje recomendaba que se informara a todo el mundo y se copiara el aviso en otros lugares. En esta ocasión el rumor es totalmente falso, aunque todavía sigue existiendo gente que se lo cree y no es raro encontrar en algún medio de comunicación electrónica nuevo reenvíos del mensaje original. De hecho, es totalmente inviable la posibilidad de una infección vía correo electrónico.

El riesgo de contraer un virus en la Internet es menor que de cualquier otra manera, tanto los mensajes de correo, como las página WEB transfieren datos. Sólo si te traes un software por la red o viene como archivo adjunto en un e-mail y lo instalas en tu ordenador puedes

contraer un virus. Mucho cuidado con los ficheros Word o Excel adjuntos a un e-mail, podrían contener virus de macro.

1.6.8 ¿Qué debemos buscar en un Antivirus? Por lo que de poco nos sirve un antivirus que detecte y elimine virus muy extendidos en América y que desconozca los más difundidos en España. Por tanto, estaremos mejor protegidos por un software que, de alguna forma, esté más "especializado" en virus que puedan detectarse en nuestro país. Por otro lado, hemos de buscar un software que se actualice el mayor número posible de veces al año; puesto que aparecen nuevos virus y mutaciones de otros ya conocidos con mucha frecuencia, el estar al día es absolutamente vital.

1.6.9 Variantes muy relacionadas con los Virus: En ocasiones de habla de estas variantes como si de virus se tratara, cuando en realidad son conceptualmente diferentes. Algunos antivirus pueden detectarlos.

- Troyanos: se introducen en el sistema bajo una apariencia diferente a la de su objetivo final. Por ejemplo Happy99.exe presenta una felicitación de año nuevo. Sin embargo su función es infectar archivos del correo electrónico del computador. Después de la infección, cada vez que se envían correos se transfiere el virus
- Bombas de tiempo: se ocultan en la memoria o en ciertas áreas de los discos. Luego en un día o una hora determinados, producen una serie de actividades que suelen ser dañinas para la computadora.
- Gusanos: programas que se reproducen asimismo y no requieren de un programa anfitrión ejecutable. Se arrastran literalmente por las áreas de la memoria de la computadora o a través de las redes. Borran los datos de las áreas de memoria que ocupan. Además

producen fallas y pérdida de datos en los programas que se están ejecutando.

- Mutantes: se ocultan y engañan a los antivirus. Cambian su código utilizando esquemas de encriptación o codificación.
- Worms: son programas que se reproducen transmitiéndose de un sistema a otro, copiándose a si mismos, y usando las redes informáticas para extenderse. Hoy en día con la difusión de Internet, el correo electrónico es su principal vía de transmisión. Generalmente no causan graves daños a los sistemas, pero pueden colapsar las redes.

Entre los virus mas conocidos del mundo se encuentran los siguientes:

AIRCOP, Jerusalén, Miguel Ángel, Paquistan, Stoned, Viena, Virus de la Galletita, Virus de Turín o de la pelotita, Bubbleboy, Fix2001.exe y Melissa.

2. SERVICIOS DE SEGURIDAD

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

- **Autentificación:** requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

- **Confidencialidad:** requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje, por ejemplo enviando los datos confidenciales a muchos destinos además

del verdadero, así como el volumen y el momento de tráfico intercambiado, por ejemplo produciendo una cantidad de tráfico constante al añadir tráfico espurio al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda.

- **Integridad:** requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, por ejemplo mediante un hash criptográfico con firma, mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas, por ejemplo mediante time-stamps.

- **No repudio:** requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, por ejemplo mediante un hash criptográfico con firma, mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas, por ejemplo mediante time-stamps.

- **Control de acceso:** requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones,

entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación.

- **Disponibilidad:** requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

2.1 MECANISMOS DE LA SEGURIDAD: no encontramos aun un mecanismo que provea todos los servicios de seguridad. Sin embargo la criptografía es un mecanismo usado en muchos de los servicios de seguridad. Miremos unos conceptos relacionados con ella.

- Criptografía: mecanismo de seguridad usado para la escritura secreta mediante la transformación del mensaje original a un código diferente llamado criptograma.

- Mensaje: Mensaje original que se quiere transformar en un código secreto o criptograma aplicando la técnica de criptografía.

- Criptograma: Código secreto obtenido a partir de un mensaje o texto claro y una clave.

- Clave: procedimiento o estructura usado en criptografía para convertir un mensaje en un criptograma y viceversa.
- Ciframiento o enciframiento: proceso en el cual se convierte un mensaje de texto claro en un texto cifrado o criptograma, es decir es la técnica de ocultar un mensaje.

- Desciframiento: proceso inverso, del anterior, es decir, se convierte el criptograma al mensaje que se desea leer.
- Cifrador: algoritmo que convierte un mensaje, en un criptograma.
- Descifrador: algoritmo que convierte un criptograma, en un mensaje.

Hay otros mecanismos de seguridad, basados en la criptografía. A continuación se mencionan algunos ejemplos más generales de mecanismos de seguridad:

- La configuración adecuada de los kits de seguridad de una plataforma específica.
- La implantación de una herramienta de seguridad en una red: (Firewall, scanner).
- La adopción e implantación de políticas de seguridad.
- El seguimiento a los registros de una red.
- Implementación de técnicas y procedimientos para mejorar la seguridad de un sitio.
- Implementación de protocolos de seguridad, para un propósito específico. Por ejemplo, un protocolo de envío de correo seguro.
- La educación de los usuarios acerca la seguridad de la red.
- La instalación de actualizaciones y correctivos a huecos de seguridad.

2.2 CRIPTOLOGÍA

2.2.1 Historia: se puede decir que la criptografía[6] es tan antigua como la civilización, cuestiones militares, religiosas o comerciales impulsaron desde tiempos remotos el uso de escrituras secretas; los antiguos egipcios usaron métodos criptográficos, mientras el pueblo utilizaba la lengua demótica los sacerdotes usaban la escritura hierática (jeroglífica) incomprensible para el resto.

Los antiguos babilónicos también utilizaron métodos criptográficos en su escritura cuneiforme. El primer caso claro de uso de métodos criptográficos se dio durante la guerra entre Atenas y Esparta, el cifrado se basaba en la alteración del mensaje original mediante la inclusión de símbolos innecesarios que desaparecían al enrollar la lista en un rodillo llamado escitala, el mensaje quedaba claro cuando se enrollaba la tira de papel alrededor de un rodillo (escitala) de longitud y grosor adecuados.

Carlomagno sustituía ya las letras por símbolos extraños. En la época de los romanos se utilizó el cifrado de César que consistía en cambiar cada letra por la ocupaba tres lugares más adelante en el abecedario.

En la Edad Media San Bernardino evitaba la regularidad de los signos (con lo que el criptoanálisis por el método de las frecuencias no era efectivo) sustituyendo letras por varios signos distintos, así tenía un

[6] http://ieee.udistrital.edu.co/concurso/ciencia_tecnologia_info_3/introduccion.html

símbolo para cada consonante, usaba tres signos distintos para cada una de las vocales y utilizaba signos sin ningún valor.

El libro más antiguo del que se tiene constancia y que trata sobre criptografía es el *Liber Zifrorum* escrito por Cicco Simoneta en el siglo XIV. En el siglo XV destaca León Battista Alberti que es considerado por muchos el padre de la criptología; crea la primera máquina de criptografiar que consiste en dos discos concéntricos que giran independientes consiguiendo con cada giro un alfabeto de transposición.

En el siglo XVI, Girolamo Cardano utilizó el método de la tarjeta con agujeros perforados, que se debía colocar sobre un texto para poder leer el mensaje cifrado; en ese mismo siglo Felipe II utilizó una complicada clave que el francés Viete logró descifrar. En ese mismo siglo, Blaise de Vigenère publica *Traicté des Chiffres* donde recoge los distintos métodos utilizados en su época, el método Vigenère es un método clásico de cifrado por sustitución que utiliza una clave.

Carlos I de Inglaterra usó en el siglo XVII códigos de sustitución silábica. Napoleón, en sus campañas militares y en los escritos diplomáticos, usó los llamados métodos Richelieu y Rossignol y para evitar la regularidad de los símbolos asignaba números a grupos de una o más letras.

En el siglo XIX se utiliza ampliamente el método de transposición, consistente en la reordenación según distintos criterios de los símbolos del mensaje. Kerckhoffs escribe el libro *La Criptografía Militar*, en el que da las reglas que debe cumplir un buen sistema criptográfico.

En Primera Guerra Mundial los alemanes usaron el sistema denominado ADFGX en el que a cada combinación de dos letras del grupo ADFGX se le hace corresponder una letra del alfabeto y a la que posteriormente se le hacía una transposición en bloques de longitud 20.

El mayor desarrollo de la criptografía se dio en el periodo de entreguerras por la necesidad de establecer comunicaciones militares y diplomáticas seguras.

En 1940 se construyó la máquina Hagelin C-48 consistente en seis volantes unidos por el eje y con distinto número de dientes. En la Segunda Guerra Mundial se construyó por parte alemana la máquina Enigma, que se basaba en un perfeccionamiento del cilindro de Jefferson, pero la máquina británica Colossus consiguió descifrar los mensajes cifrados con Enigma. Los americanos construyeron la máquina Magic utilizada para descifrar el código púrpura japonés; los americanos a su vez usaron a los indios navajos con su difícil lenguaje para la transmisión de mensajes.

Con el desarrollo de la informática en la segunda mitad de este siglo y con el uso cada vez más extendido de las redes informáticas y del almacenamiento masivo de información se ha dado paso a un gran salto en el estudio de sistemas criptográficos.

En 1975 Diffie y Hellman establecieron las bases teóricas de los algoritmos de clave pública, hasta entonces no se concebía un sistema de cifrado que no fuese de clave secreta. En la actualidad se usan distintos métodos criptográficos, el DES (de clave secreta), método RSA, método de Merkle y Hellman, etc.

2.2.2 Técnicas criptográficas: aunque los criptosistemas se pueden clasificar por varias dimensiones, en este capitulo abordaremos solamente a dos según el número de claves que usan y según el tipo de operaciones que realizan.

2.2.2.1 Según el número de claves que usan:

- Criptografía simétrica: este tipo de criptografía se caracteriza por usar la misma clave para cifrar como para descifrar. Son llamados criptosistemas de clave secreta, tradicionales o convencionales.
- Criptografía Asimétrica: A diferencia del anterior, este utiliza dos claves diferentes, una para cifrar y otra para descifrar. Tiene la ventaja de separar los servicios de privacidad y autenticidad.

2.2.2.2 Según el tipo de operaciones que realizan:

- Cifradores de sustitución: este tipo de cifrador sustituye cada letra o grupo de letras por otra letra o grupo de letras para disfrazarlas. El cifrado más antiguo que se conoce es el cifrado de César, atribuido a Julio César.

Ejemplo:

1. Cifrador de Julio Cesar: este es el cifrador más sencillo de sustitución el cual fue inventado por Julio Cesar. Consiste en reemplazar cada letra del alfabeto por otra letra del alfabeto por otra letra que se mueve k lugares en el alfabeto, donde k es la clave.

Si las letras del alfabeto desde la A hasta la Z, se numeran de 0 a 26.

Letra	**a**	**b**	**c**	**d**	**E**	**f**	**G**	**H**	**i**	**J**	**k**	**l**	**m**	**N**	**ñ**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Numero	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tabla 1 Cifrador de Julio Cesar

Si k = 3, entonces

Mensaje: J U L I O C E S A R

Criptograma: M X Ñ L R F H V D U

Criptoanálisis: este cifrador no es resistente a un ataque de fuerza bruta, el cual es muy fácil de realizar con el menor esfuerzo computacional, puesto que solo hay 27 posibles claves (para el caso del alfabeto español)

1. Cifrador Monoalfabético: este cifrador utiliza una sustitución arbitraria o en otras palabras la clave de permutación de 27 caracteres alfabéticos.

Letra	**a**	**B**	**c**	**D**	**e**	**F**	**G**	**H**	**i**	**j**	**k**	**L**	**m**	**n**	**ñ**	**o**	**P**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Sustitución	g	P	h	A	r	Ñ	I	b	m	j	v	U	c	s	o	f	D	n	z	e	w	x	t	y	k	q	l

Tabla 2 Cifrador Monoalfabetico

Para cifrar:

Mensaje: A L F A B E T O

Criptograma: G U Ñ G P R W F

Para descifrar:

Criptograma:	E	R	I	X	Z	M	A	G	A
Mensaje:	S	E	G	U	R	I	D	A	D

Criptoanálisis: este cifrador es resistente a un ataque de fuerza bruta puesto que existen 27! posibles claves, aunque es fácil de romperlo haciendo un análisis estadístico del criptograma.

Si se conoce que el mensaje original esta en un idioma específico, español por ejemplo, y se compara la estadística de repetición de letras del criptograma con una frecuencia de repetición de las letras del alfabeto en el lenguaje español, que es conocida, es muy fácil romper el criptograma. Como se trata de un análisis estadístico, mientras mas grande sea el criptograma, mucho más fácil es romperlo.

Una de las técnicas usadas para contrarrestar este tipo de ataque es la de realizar una compresión del texto plano y después aplicarle este cifrador, ya que en este caso no se tiene información estadística del texto plano.

2. Cifrador de Vigenére : este cifrador de sustitución esta clasificado dentro de los polialfabéticos, debido a que un conjunto de reglas de sustitución monoalfabéticas son usadas y la clave es la que determina que reglas en particular se deben escoger para cada transformación.

   El cifrador Vigenère esta basado en la tabla que se muestra a continuación correspondiente al conjunto de sustituciones del cifrador de Julio Cesar. Básicamente se trata de una combinación entre los dos cifradores mencionados anteriormente.

Tabla de Vigenère

	A	**B**	**c**	**d**	**…**	**w**	**x**	**y**	**z**
A	A	B	C	D	…	W	X	Y	Z
B	B	C	D	E	…	X	Y	Z	A
C	C	D	E	F	…	Y	Z	A	B
D	D	E	F	G	…	Z	A	B	C
…	…	…	…	…	…	…	…	…	…
W	W	X	Y	Z	…	S	T	U	V
X	X	Y	Z	A	…	T	U	V	W
Y	Y	Z	A	B	…	U	V	W	X
Z	Z	A	B	C	…	V	W	X	Y

Tabla 3 Cifrador de Vigenere

Clave:	R	E	D	E	S				
Mensaje:	S	E	G	U	R	I	D	A	D
Clave:	R	E	D	E	S	R	E	D	E
Criptograma:	K	I	J	Y	K	Z	H	D	H

Criptoanálisis: este cifrador es un poco más resistente a un ataque estadístico. Cuando dos técnicas secuencias de letras del texto plano ocurren a una distancia que es un entero múltiplo de la longitud de la clave, se generan secuencias idénticas del criptograma.

3. Cifradores de transposición: reordenan las letras pero no las disfrazan; algunos de ellos aceptan un bloque de entrada de longitud fija, y producen un bloque de salida de longitud fija.

   Ejemplo: cifrador de carrilera, donde k = 3

   C T A

   R P O R F A

   I G I

Mensaje:	C	R	I	P	T	O	G	R	A	F	I	A
Criptograma:	**C**	**T**	**A**	**R**	**P**	**O**	**R**	**F**	**A**	**I**	**G**	**I**

   Ejemplo 2: otro algoritmo de transposición más común es el de tipo de columnas; la clave del cifrador debe ser una palabra que no tenga ninguna letra repetida, en el ejemplo que se presenta a continuación la clave COLUMNA. El propósito de la clave es el de numerar las diferentes columnas que se formaran, de forma que la columna 1 es aquella que queda bajo la letra de la clave más próxima al principio del alfabeto y así sucesivamente. El texto en claro se escribe debajo de la clave en renglones horizontales; el texto cifrado se lee por columnas, comenzando por la columna cuya letra clave tiene el menor valor.

Mensaje: lacriptografiaesunaciencia

Clave de cifrado: COLUMNA

C	O	L	U	M	N	A
2	6	3	7	4	5	1
l	**a**	**c**	**r**	**i**	**p**	**t**
o	**g**	**r**	**a**	**f**	**i**	**a**
e	**s**	**u**	**n**	**a**	**c**	**i**
e	**n**	**c**	**i**	**a**	**a**	**b**

Texto cifrado:

TAIB LOEE CRUC IFAA PICA AGSN RANI

Tabla 4 Cifrador de Transposición

Para desbaratar un cifrador de transposición, el criptoanalista debe estar primero enterado de que se trata efectivamente de un cifrador de transposición. Esto puede comprobarse de una forma relativamente sencilla, observando la frecuencia de las letras e, t, a, o, i, n, ya que en los cifradores de este tipo se cambia de lugar las letras, pero no se cambian las letras propiamente, por lo que si la frecuencia de aparición de las letras se corresponde con la observada para el lenguaje natural, es decir, la e es la que más aparece, entonces se podría afirmar con mucha seguridad que el cifrador es de transposición y no de sustitución.

El siguiente paso consistiría en determinar cuál es el número de columnas. En muchos casos una palabra o frase probable, puede llegar a adivinarse a partir del contexto del mensaje. Si el criptoanalista sabe, o supone que una determinada palabra o frase está contenida en el mensaje, entonces no le costará mucho esfuerzo determinar el número de columnas.

El último paso consistiría en ordenar las columnas.

4. Cifradores de producto: este tipo de cifradores es una mezcla de los dos anteriores, es decir, de los de sustitución y los de transposición.

   1. Ejemplo: DES: es un cifrador producto que combina las técnicas de sustitución y transposición, el cual es el más conocido esquema de encriptación hoy en día. DES esta basado en el “Data Encription Standard” adoptado en 1977 por National Bureau of Standards, ahora National Institute of Standards and Technology (NIST) como un estándar de procesamiento de información federal.

   Los datos en DES son cifrados en bloques de 64 bits usando una clave de 56 bits. El algoritmo transforma los 64 bits de entrada, realizando una serie de pasos hasta obtener 64 bits de salida. Los mismos pasos y con la misma clave son utilizados en sentido inverso para la desencripción.

   El algoritmo de encriptamiento se divide en tres fases:

      Fase 1: los 64 bits del texto plano pasan por una permutación inicial donde se reordenan los bits para producir una entrada permutada.

      Fase 2: consiste en 16 iteraciones de la misma función, la cual tiene funciones internas de permutaciones y sustituciones.

      Fase 3: recibe un bloque de 64 bits el cual es función del bloque inicial y de la clave. Este bloque es dividido en dos bloques de 32 bits, los cuales intercambiados para producir una pre-salida.

Finalmente la pre-salida es pasada por una permutación inicial, para producir un criptograma de 64 bits.

2. Ejemplo: IDEA: El algoritmo IDEA es bastante más joven que DES, pues data de 1992. Para muchos constituye el mejor y más seguro algoritmo simétrico disponible en la actualidad. Trabaja con bloques de 64 bits de longitud y emplea una clave de 128 bits. Como en el caso de DES, se usa el mismo algoritmo tanto para cifrar como para descifrar.

IDEA es un algoritmo bastante seguro, y hasta ahora se ha mostrado resistente a multitud de ataques, entre ellos el criptoanálisis diferencial. No presenta claves débiles y su longitud de clave hace imposible en la práctica un ataque por la fuerza bruta.

Como ocurre con todos los algoritmos simétricos de cifrado por bloques, IDEA se basa en los conceptos de sustitución y transposición, haciendo uso de las siguientes operaciones elementales (todas ellas fáciles de implementar):

1. XOR.
2. Suma módulo 2^{16}.
3. Producto módulo $2^{16} + 1$.

Funcionamiento: El algoritmo IDEA consta de ocho iteraciones. Dividiremos el bloque X a codificar, de 64 bits, en cuatro partes X_1, X_2, X_3 y X_4 de 16 bits. Denominaremos Z_i a cada una de las 52 subclaves de 16 bits que vamos a necesitar. Las operaciones que llevaremos a cabo en cada iteración son las siguientes:

1. Multiplicar X_1 por Z_1.
2. Sumar X_2 con Z_2.

3. Sumar X_3 con Z_3.
4. Multiplicar X_4 por Z_4.
5. Hacer un XOR entre los resultados del paso 1 y el paso 3
6. Hacer un XOR entre los resultados del paso 2 y el paso 4.
7. Multiplicar el resultado del paso 5 por Z_5.
8. Sumar los resultados de los pasos 6 y 7.
9. Multiplicar el resultado del paso 8 por Z_6.
10. Sumar los resultados de los pasos 7 y 9.
11. Hacer un XOR entre los resultados de los pasos 1 y 9.
12. Hacer un XOR entre los resultados de los pasos 3 y 9.
13. Hacer un XOR entre los resultados de los pasos 2 y 10.
14. Hacer un XOR entre los resultados de los pasos 4 y 10.

La salida de cada iteración serán los cuatro sub-bloques obtenidos en los pasos 11, 12, 13 y 14, que serán la entrada del siguiente ciclo, en el que emplearemos las siguientes seis subclaves, hasta un total de 48. Al final de todo intercambiaremos los dos bloques centrales (en realidad con eso deshacemos el intercambio que llevamos a cabo en los pasos 12 y 13).
Después de la octava iteración, se realiza la siguiente transformación:

1. Multiplicar X1 por Z_{49}.
2. Sumar X2 con Z_{50}.
3. Sumar X3 con Z_{51}.
4. Multiplicar X4 por Z_{52}.

Las primeras ocho subclaves se calculan dividiendo la clave de entrada en bloques de 16 bits. Las siguientes ocho se calculan rotando la clave de entrada 25 bits a la izquierda y volviendo a dividirla, y así sucesivamente.

Las subclaves necesarias para descifrar se obtienen cambiando de orden las Z_i y calculando sus inversas para la suma o la multiplicación. Puesto que $2_{16} + 1$ es un número primo, nunca podremos obtener cero como producto de dos números, por lo que no necesitamos representar dicho valor. Cuando estemos calculando productos, utilizaremos el cero para expresar el número 2_{16}. Esta representación es coherente puesto que los registros que se emplean internamente en el algoritmo poseen únicamente 16 bits.

2.3 ESTEGANOGRAFIA

Este es otro tipo de ocultamiento de mensajes, a diferencia de la criptografía esta no es una ciencia. La esteganografía consiste en ocultar en el interior de la información aparentemente inocua, otro tipo de información (cifrada o no). El texto se envía como texto plano, pero entre mezclado con mucha cantidad de basura que sirve de camuflaje al mensaje enviado. Los mensajes suelen ir ocultos entre archivos de sonidos o imágenes

Un ejemplo, muy claro podemos nombrar el siguiente: Tomando el jugo de un limón exprimido, una hoja de block y una vela. Este experimento consiste en escribir con el jugo de limón, y después de haber secado, se toma el papel y se le acerca a la vela encendida para poder ver el mensaje oculto, esta técnica era muy usada por nuestros antepasados para enviar los mensajes secretos.

2.4 APLICACIONES CRIPTOGRAFICAS

Entre las muchas aplicaciones de la criptografía, se encuentran la autenticación, la firma digital, la identificación de usuario, seguridad en redes y protocolos criptográficos, PGP, Kerberos, etc. En este capitulo nos enfatizaremos en dos los dos últimos.

2.4.1 PGP**:** el software, Pretty Good Privacy, (Privacidad Bastante Buena) creado por Phill Zimmermann, que es el estándar que mas se usa para la encriptación de correos electrónicos, discos duros, comunicaciones cifradas en Internet y muchas otras aplicaciones.

PGP Enterprise Security ofrece una infraestructura de cifrado y autentificación capaz de mantener la seguridad de los datos del correo electrónico, de los archivos, las carpetas y los volúmenes en el disco. Las aplicaciones "cliente" de PGP incluyen interfaz fáciles de utilizar para mantener la seguridad de los datos, mientras que las aplicaciones "servidor" PGP proporcionan la adaptabilidad necesaria para ampliaciones y el cumplimiento de las políticas de los sistemas.

Cuando se implementa en entornos empresariales, PGP Enterprise Security se convierte en una infraestructura completa de cifrado y autentificación, adaptable a las ampliaciones y con facilidad de administrar.

PGP Enterprise Security es una solución adaptable y compatible entre plataformas, que permite a los usuarios proteger la correspondencia electrónica, las transacciones en línea y los archivos de datos mediante su cifrado de forma que únicamente los destinatarios previstos puedan descifrar su contenido. Debido a que los productos PGP, trabajan sobre complejos algoritmos criptográficos y longitudes de clave específicas, se asegura una

protección definitiva de los datos almacenados en las computadoras y que se transmiten por intranets e Internet. Para una mayor seguridad, PGP incorpora además, un sistema de firma digital que verifica la propiedad e integridad de los documentos.

PGP se conoce internacionalmente como el sistema estándar para mantener la seguridad del correo electrónico y de los archivos. PGP no sólo se adapta a un nivel superior para los entornos empresariales, sino que también se adapta a un nivel inferior para los individuos. Este hecho es cada vez más importante, porque las compañías intercambian sus datos críticos no sólo internamente, sino también con consultores o socios en el exterior.

Su funcionamiento es muy sencillo, cada usuario tiene dos llaves: una pública y otra privada. La pública es la que distribuye a los demás y sirve para que ellos puedan enviarle un mensaje codificado que solo él mediante su llave privada podrá descifrar. También ofrece la posibilidad de firmar un mensaje al colocar una parte de su llave privada (como su nombre lo indica es secreta) en una firma, que actúa como un certificado de autenticidad. Cuando el destinatario recibe el mensaje, el PGP comprueba la firma y texto y lo compara con la llave pública que tiene del remitente, y si algo en el texto o la firma ha cambiado envía un mensaje de error donde informa que el mensaje no corresponde a la persona que dice que nos envía el mensaje.

Sirve también para enviar ficheros codificados en formato ASCII por correo electrónico.

PGP puede descargarse gratuitamente en http://www.pgpi.com en donde encontramos la ultima versión que es compatible para Windows XP y otras versiones mas antiguas. También existen versiones de PGP para Macintosh, Unix, Linux y para casi cualquier sistema operativo actual que se haya comercializado.

Desde el punto de vista del usuario, el PGP es muy cómodo para gestionar las claves (que es precisamente lo más difícil en los sistemas de clave pública). Las claves se almacenan en dos archivos: secring.skr (que guarda las claves privadas) y pubring.pkr (que registra las claves públicas). Estos archivos son una especie de "llaveros", donde se colocan nuestras llaves privadas, públicas y las llaves públicas de los demás. Obviamente, si se pierde algunos de ellos, no se podrá desencriptar ni encriptar ningún mensaje, por lo que es buena idea guardar una copia en un lugar seguro.

También PGP guarda la "semilla" para generar nuestras claves aleatorias en el archivo randseed.bin, el cual es otro archivo importante que no puede quedar expuesto a terceras personas. Si randseed.bin se borra, PGP creará otro automáticamente a partir del reloj interno de la computadora, e igualmente es recomendable guardar una copia suya en algún lugar seguro.

PGP tiene además, una función muy útil llamada "armadura ASCII" que permite convertir los archivos encriptados de cualquier tipo en ficheros de texto ASCII. Así, por ejemplo, un archivo binario, como sucede con un programa, puede encriptarse, convertirse en texto ASCII y enviarse como texto simple por correo.

Las rutinas clave de PGP en peligro incluyen:

- Rutinas para generación de números aleatorios modificadas para arrojar resultados predecibles.
- Rutinas de clave de sesión modificadas para que se use siempre la misma clave.
- Rutinas IDEA, RSA o MD5 debilitadas.
- Mensajes cifrados siempre con una clave adicional encubierta.

La versión debilitada puede introducirse en el ordenador objetivo por medio de:

- Una aplicación de caballo de Troya que encubiertamente parchea el programa binario.
- Reemplazar físicamente la copia legítima con una copia debilitada cuando el usuario no se encuentra presente.
- Hacer pasar la copia debilitada como legitima y distribuirla por Internet.

2.4.1.1 Funcionamiento del PGP:

- Anillos de Claves: un anillo es una colección de claves almacenadas en un archivo. Cada usuario tiene dos anillos, uno para claves publicas y otro para claves privadas. Cada una de las claves, además, posee un identificador de usuario, fecha de expiración, versión de PGP y una huella digital única hexadecimal suficientemente corta que permita verificar la autenticidad de la clave.
- Codificación de las claves: como ya se conoce, los algoritmos simétricos de cifrado son mas rápidos que los asimétricos. Por esta razón PGP cifra primero el mensaje empleando un algoritmo simétrico con una clave generada aleatoriamente (clave de sesión) y posteriormente codifica la clave haciendo uso de la llave publica del destinario. Dicha clave es extraída convenientemente del anillo de claves publicas a partir del identificador suministrado por el usuario.
- Descodificación de mensajes: cuando se trata de decodificar el mensaje, PGP simplemente busca la cabecera las claves publicas con las que esta codificado, pide una contraseña para abrir el anillo de claves privadas y comprueba si se tiene una clave que permite decodificar el mensaje.

- Compresión de archivos: PGP generalmente comprime el texto plano antes de encriptar el mensaje (y lo descomprime después de desencriptarlo) para disminuir el tiempo de cifrado, de transmisión y de alguna manera fortalecer la seguridad del cifrado ante el criptoanálisis que explotan las redundancias del texto plano.
- Algoritmos utilizados por PGP: las diferentes versiones han ido adoptando diferentes combinación de algoritmos de signatura y cifrado. Las signaturas se realizan mediante MD5, SHA-1, y/o RIPE-MD6. Los algoritmos simétricos utilizados pueden ser IDEA, CAST y TDES y los asimétricos RSA y el Gamal.

2.4.2 Kerberos: en 1993 el MIT crea el proyecto Athena, y basándose en la mitología griega, nace kerberos.

Kerberos es un sistema de seguridad que provee autentificación a través de redes inseguras. Su objetivo es restringir los accesos solo a usuarios autorizados y poder autentificar los requerimientos a servicios, asumiendo un entorno distribuido abierto, en el cual los usuarios en las estaciones de trabajo acceden a estos servicios a través de una red.

Los modelos de autentificación hasta ahora vistos son principalmente, de dos tipos:

- Recursos
- Usuario
- Autentificación Service (AS)
- Tickets Grating Service (TGS)
- Autentificador

- La clave secreta del usuario

2.4.2.1 Ventajas: La mayoría de las redes usan esquemas de autenticación basados en contraseñas. Tales esquemas requieren que cuando un usuario necesita una autenticación en un servidor de red, debe proporcionar un nombre de usuario y una contraseña. Lamentablemente, la información de autenticación para muchos servicios se transmite sin estar encriptada. Para que un esquema de este tipo sea seguro, la red tiene que estar inasequible a usuarios externos, y todos los usuarios de la red deben ser de confianza.

Aún en este caso, una vez que la red se conecte a la Internet, ya no puede asumir que la red es segura. Cualquier intruso del sistema con acceso a la red y un analizador de paquetes pueden interceptar cualquier contraseña enviada de este modo, comprometiendo las cuentas de usuarios y la integridad de toda la infraestructura de seguridad.

El primer objetivo de Kerberos es el de eliminar la transmisión a través de la red de información de autenticación. Un uso correcto de Kerberos erradica la amenaza de analizadores de paquetes que intercepten contraseñas en su red.

2.4.2.2 Desventajas: A pesar de que Kerberos elimina una amenaza de seguridad común, puede ser difícil de implementar por una variedad de razones:

- La migración de contraseñas de usuarios desde una base de datos de claves estándar UNIX, tal como */etc/passwd o /etc/shadow*, a una base de datos de contraseña Kerberos puede ser tediosa y no hay un mecanismo rápido para realizar esta tarea.

- Kerberos es sólo parcialmente compatible con los Pluggable Authentication Modules (PAM) usados por la mayoría de los servidores en Red Hat Linux.
- Para que una aplicación use Kerberos, el código debe ser modificado para hacer las llamadas apropiadas a las librerías de Kerberos. Para algunas aplicaciones, esto puede suponer un esfuerzo excesivo de programación. Para otras aplicaciones incompatibles, los cambios se deben realizar en el protocolo usado entre el servidor de red y sus clientes; de nuevo, esto puede suponer una programación. Por defecto, las aplicaciones de código cerrado que no tienen soporte de Kerberos son usualmente las más problemáticas.

2.4.2.3 Problemas de Kerberos: la filosofía de kerberos esta basado en una fuerte centralización del sistema, ya que para su correcto funcionamiento se debe disponer de forma permanente del servidor, de forma que si esta falla toda la red se vuelve inutilizable por no disponer de forma para desencriptar los mensajes que circulan por ella. Este concepto es una contradicción a la teoría de sistemas distribuidos, sobre el que se basa el modelo que rige cualquier red (si una maquina falla el resto puede seguir su funcionamiento, sino a pleno, al menos correctamente).

Otra falencia es que casi toda la seguridad reside en el servidor que mantiene la base de datos de claves, por lo que si este se ve comprometido, toda la red estará amenazada.

Por ultimo, la implementación de kerberos actualmente, acarrea algunos inconvenientes ya que se debe realizar un proceso de keberizacion sobre cada programa que se desee utilizar, suponiendo esto un

conocimiento y tiempo considerable no siempre disponible. Si bien este inconveniente esta siendo subsanado en diversas versiones aun no se cuenta con la estandarización suficiente para su extensión masiva.

3. FIREWALLS

Un firewalls es un sistema ubicado entre dos redes y que ejerce una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es. (Por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo él trafico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
2. Solo el tráfico autorizado, definido por la política local de seguridad, es permitido.

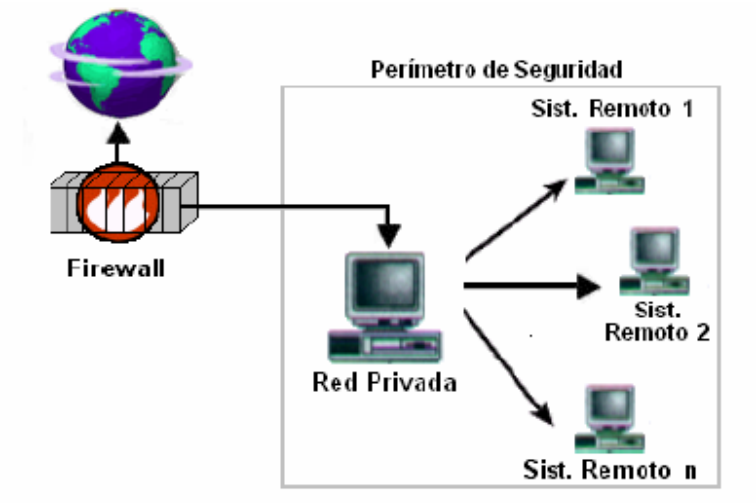

Figura 1 Firewalls

Como puede observarse un firewall solo sirve de defensa de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos firewalls están conectados, ambos deben hablar el mismo método de encriptación-desencriptacion para entablar la comunicación.

3.1 TIPOS DE FIREWALL

3.1.1 Filtrado de paquetes: Se usan routers con filtros y reglas basadas en políticas de control de acceso. El router es el encargado de filtrar los paquetes (un Choke) basados en cualquiera de los siguientes criterios:

1. protocolos utilizados
2. dirección IP de origen y de destino
3. puerto TCP-UDP de origen y de destino

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales maquinas la comunicación esta permitida.

Este tipo de firewalls permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la trasferencia de archivos vía FTP (puerto 21 cerrado)

3.1.2 Proxy – Gateways de aplicaciones: Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones.

Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host. El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes. Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.

Gráficamente:

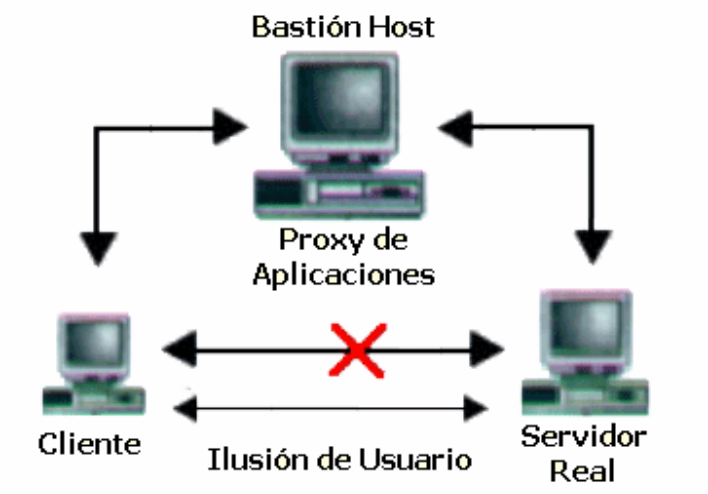

Figura 2 Tipos de Firewalls

3.1.3 Dual Homed – Host: está formado por simples máquinas Unix equipadas con dos o más tarjetas de red y denominadas anfitriones de dos bases (dual-homed hosts) o multibase (multi-

homed hosts), y en las que una de las tarjetas se suele conectar a la red interna a proteger y la otra a la red externa a la organización.

El sistema ha de ejecutar al menos un servidor proxy para cada uno de los servicios que deseemos pasar a través del cortafuegos, y también es necesario que el IP Forwarding esté deshabilitado en el equipo: aunque una máquina con dos tarjetas puede actuar como un router, para aislar el tráfico entre la red interna y la externa es necesario que el choke no enrute paquetes entre ellas. Así, los sistemas externos `verán' al host a través de una de las tarjetas y los internos a través de la otra, pero entre las dos partes no puede existir ningún tipo de tráfico que no pase por el cortafuegos: todo el intercambio de datos entre las redes se ha de realizar bien a través de servidores proxy situados en el host bastión o bien permitiendo a los usuarios conectar directamente al mismo. La segunda de estas aproximaciones es sin duda poco recomendable, ya que un usuario que consiga aumentar su nivel de privilegios en el sistema puede romper toda la protección del cortafuegos, por ejemplo reactivando el IP Forwarding); además - esto ya no relativo a la seguridad sino a la funcionalidad del sistema - suele ser incómodo para los usuarios tener que acceder a una máquina que haga de puente entre ellos e Internet. De esta forma, la ubicación de proxy es lo más recomendable, pero puede ser problemático el configurar cierto tipo de servicios o protocolos que no se diseñaron teniendo en cuenta la existencia de un proxy entre los dos extremos de una conexión.

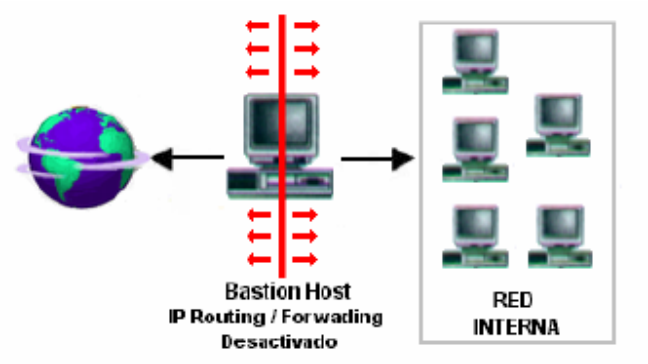

Figura 3

3.1.4 Screened Host: combina un router con un host bastión, y donde el principal nivel de seguridad proviene del filtrado de paquetes (es decir, el router es la primera y más importante línea de defensa). En la máquina bastión, único sistema accesible desde el exterior, se ejecutan los proxy de las aplicaciones, mientras que el choke se encarga de filtrar los paquetes que se puedan considerar peligrosos para la seguridad de la red interna, permitiendo únicamente la comunicación con un reducido número de servicios.

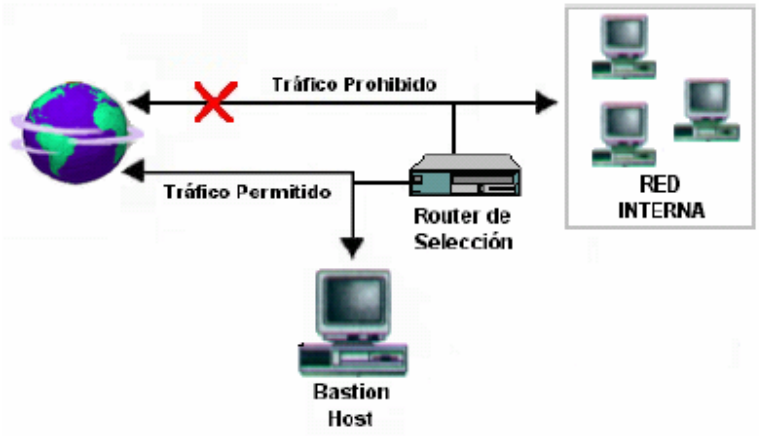

Figura 4

3.1.5 Screened Subset: La arquitectura Screened Subnet, también conocida como red perimétrica o De-Militarized Zone (DMZ) es con diferencia la más utilizada e implantada hoy en día, ya que añade un nivel de seguridad en las arquitecturas de cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al host bastión: como hemos venido comentando, en los modelos anteriores toda la seguridad se centraba en el bastión, de forma que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red. Como la máquina bastión es un objetivo interesante para muchos piratas, la arquitectura DMZ intenta aislarla en una red perimétrica de forma que un intruso que accede a esta máquina no consiga un acceso total a la subred protegida.

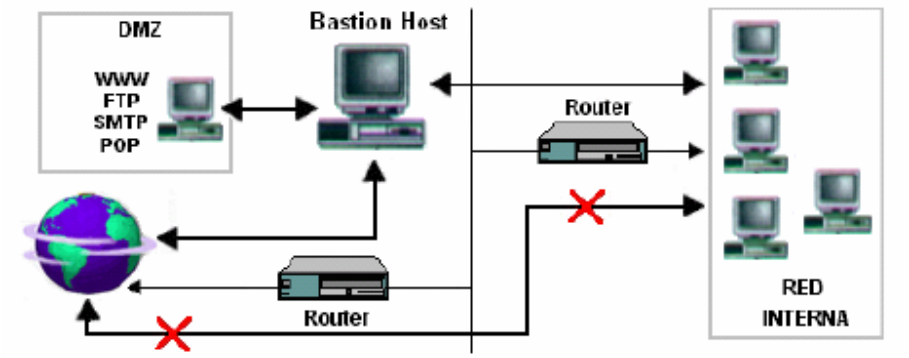

Figura 5

3.1.6 Inspección de paquetes: este tipo de firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también la procedencia y destino. Se

aplican desde la capa de red hasta la de aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

3.1.7 Firewalls personales: estos firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde una simple infección de virus hasta la pérdida de toda su información.

3.2 POLÍTICAS DE DISEÑO DE FIREWALLS

Las políticas de accesos en un Firewalls se deben diseñar poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura.

Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios.

Generalmente se plantean algunas preguntas fundamentales que debe responder cualquier política de seguridad:

- ¿Qué se debe proteger? Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).

- ¿De quién protegerse? De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir.

Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.

- ¿Cómo protegerse? Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:
    a. Paradigmas de seguridad
        - Se permite cualquier servicio excepto aquellos expresamente prohibidos.
        - Se prohíbe cualquier servicio excepto aquellos expresamente permitidos. La más recomendada y utilizada aunque algunas veces suele acarrear problemas por usuarios descontentos que no pueden acceder a tal cual servicio.
    b. Estrategias de seguridad
        - Paranoica: se controla todo, no se permite nada.
        - Prudente: se controla y se conoce todo lo que sucede.
        - Permisiva: se controla pero se permite demasiado.
        - Promiscua: no se controla (o se hace poco) y se permite todo.
- ¿Cuánto costará? Estimando en función de lo que se desea proteger se debe decidir cuanto es conveniente invertir.

3.3 RESTRICCIÓN EN EL FIREWALLS

La parte más importante de las tareas que realizan los Firewalls, la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

1. Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina **Trusted (validados).** Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.
2. Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interior de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.

3.4 BENEFICIOS DE UN FIREWALL:

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada maquina interna.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de Firewalls se halla convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

3.5 LIMITACIONES DE UN FIREWALL

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "NO es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Finalmente, un Firewall es vulnerable, él NO protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna.

4. HERRAMIENTAS DE SEGURIDAD INFORMATICA

En la actualidad existen en el mundo informático herramientas de seguridad que nos ayudan a fortalecer nuestros equipos informáticos contra las amenazas que atropellan nuestro sistema. Es así como encontramos en el mercado gran cantidad de antivirus y cortafuegos, pero como la tecnología avanza tenemos que estar a la vanguardia y no dejarnos sin la actualización de estos.
Acá vemos una lista de los más conocidos:

- **Nessus:** Es la herramienta de evaluación de seguridad "Open Source".
  Nessus, es un escáner de seguridad remoto para Linux, BSD, Solaris y Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad.

- **Ethereal:** Ethereal es un analizador de protocolos de red para Unix y Windows. Nos permite examinar datos de una red viva o de un archivo de captura en algún disco. Se puede examinar interactivamente la información capturada, viendo información de detalles y sumarios por cada paquete. Ethereal tiene varias características poderosas, incluyendo un completo lenguaje para filtrar lo que queramos ver y la

habilidad de mostrar el flujo reconstruido de una sesión de TCP. Incluye una versión basada en texto llamada tethereal.

- **Snort:** es una sistema de detección de intrusiones de red de poco peso (para el sistema), capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda/identificación de contenido y puede ser utilizado para detectar una gran variedad de ataques y pruebas, como por ejemplo: buffer overflows, escaneos indetectables de puertos, ataques a CGI, pruebas de SMB, intentos de reconocimientos de sistema operativos, etc. Snort utiliza un lenguaje flexible basado en reglas para describir el tráfico que debería recolectar o dejar pasar, y un motor de detección modular.

- **Netcat:** Una utilidad simple para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP. Está diseñada para ser una utilidad del tipo "back-end" confiable que pueda ser usada directamente o fácilmente manejada por otros programas y scripts. Al mismo tiempo, es una herramienta rica en características, útil para depurar y explorar, ya que puede crear casi cualquier tipo de conexión que podamos necesitar y tiene muchas habilidades incluídas.

- **TCPDump / WinDump:** El sniffer clásico para monitoreo de redes y adquisición de información y Puede ser utilizado para mostrar los encabezados de los paquetes en una interfaz de red, que concuerden con cierta expresión de búsqueda. Podemos utilizar esta herramienta para rastrear problemas en la red o para monitorear actividades de la misma. Hay una versión para Windows llamada WinDump. TCPDump es también la fuente de las bibliotecas de captura de paquetes

Libpcap y WinPcap que son utilizadas por Nmap y muchas otras utilidades. Hay que tener en cuenta que muchos usuarios prefieren el sniffer más nuevo Ethereal.

- **Hping2:** esta herramienta ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra las respuestas. Esta herramienta es particularmente útil al tratar de utilizar funciones como las de traceroute/ping o analizar de otra manera, hosts detrás de un firewall que bloquea los intentos que utilizan las herramientas estándar.

- **DSniff:** este diseño incluye varias herramientas: dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, y webspy las cuales monitorean pasivamente una red en busca de información valiosa (passwords, e-mail, archivos, etc.). arpspoof, dnsspoof, y macof facilitan la intercepción de tráfico en la red normalmente no disponible para un atacante.

- **GFI LANguard:** LANguard escanea redes y reporta información como el nivel de "service pack" de cada máquina, faltas de parches de seguridad, recursos compartidos, puertos abiertos, servicios/aplicaciones activas en la computadora, datos del registro, passwords débiles, usuarios y grupos, etc.

- **Ettercap:** Ettercap es un interceptor/sniffer/registrador para LANs con ethernet basado en terminales {terminal-based}. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También es posible la inyección de datos en una conexión establecida y filtrado al vuelo y aun manteniendo la conexión sincronizada. Muchos modos de sniffing fueron implementados para darnos un set poderoso y completo de sniffing. También soporta

plugins. Tiene la habilidad para comprobar si estamos en una LAN con switches o no, y de identificar huellas de sistemas operativos para dejarnos conocer la geometría de la LAN.

- **Whisker/Libwhisker**: Whisker es un escáner que nos permite poner a prueba servidores de HTTP con respecto a varias agujeros de seguridad conocidos, particularmente, la presencia de peligrosos scripts/programas que utilicen CGI. Libwhisker es una biblioteca para perl (utilizada por Whisker) que nos permite crear escáneres de HTTP a medida.

- **John the Ripper:** es un cracker de passwords rápido, actualmente disponible para Unix, DOS, Win32, BeOs, y OpenVMS. Su propósito principal es detectar passwords de Unix débiles. Soporta varios tipos de hashes de password, que son comúnmente encontrados en Unix, así como también AFS de Kerberos y las "LM hashes" de Windows NT/2000/XP. Otros varios tipos de hashes se pueden agregar con algunos parches que contribuyen algunos desarrolladores.

- **OpenSSH / SSH:** es un programa para loggearse en una máquina remota y para ejecutar comandos en una máquina remota. Provee de comunicaciones cifradas y seguras entre dos hosts no confiables sobre una red insegura. También se pueden redirigir conexiones de X11 y puertos arbitrarios de TCP/IP sobre este canal seguro. La intención de esta herramienta es la de reemplazar a **rlogin, rsh y rcp**, y puede ser usada para proveer de **rdist**, y **rsync** sobre una canal de comunicación seguro.

- **SamSpade:** SamSpade posee una interfaz de usuario gráfica (GUI) consistente y de una implementación de varias tareas de investigación

de red útiles. Fue diseñada con la idea de rastrear spammers en mente, pero puede ser útil para muchas otras tareas de exploración, administración y seguridad. Incluye herramientas como ping, nslookup, whois, dig, traceroute, finger, explorador de web crudo, transferencia de zona de DNS {"DNS zone transer"}, comprobación de "relay" de SMTP, búsqueda en sitios web, etc.

- **ISS Internet Scanner:** Internet Scanner comenzó en el año de 1992 como un pequeño escáner "Open Source" escrito por Christopher Klaus. ISS creció hasta ser una enorme empresa con una amplia gama de productos de seguridad.

- **Tripwire:** Tripwire es una herramienta que ayuda a administradores y usuarios de sistemas monitoreando alguna posible modificación en algún set de archivos. Si se usa regularmente en los archivos de sistema, Tripwire, puede notificar a los administradores del sistema, si algún archivo fue modificado o reemplazado, para que se puedan tomar medidas de control de daños a tiempo.

- **Nikto:** Un escáner de web de mayor amplitud. Nikto es un escáner de servidores de web que busca más de 2000 archivos/CGIs potencialmente peligrosos y problemas en más de 200 servidores. Utiliza la biblioteca LibWhisker pero generalmente es actualizado más frecuentemente que el propio Whisker.

- **Kismet:** es capaz de "sniffear" utilizando la mayoría de las placas inalámbricas; de detectar bloques de IP automáticamente por medio de paquetes de UDP, ARP, y DHCP; listar equipos de Cisco por medio del "Cisco Discovery Protocol"; registrar paquetes criptográficamente débiles y de generar archivos de registro compatibles con los de

ethereal y tcpdump. También incluye la habilidad de graficar redes detectadas y rangos de red estimados sobre mapas o imágenes.

- **SuperScan:** puede manejar escaneos por ping y escaneo de puertos utilizando rangos de IP especificados. También puede conectarse a cualquier puerto abierto descubierto utilizando aplicaciones "ayudantes" especificadas por el usuario (ejemplo: Telnet, Explorador de Web, FTP).

- **L0phtCrack 4:** intenta crakear los passwords de Windows a partir de las hashes que puede obtener (por medio de acceso apropiado) de máquinas con Windows NT/2000 independientes, servidores en red, controladores primarios de red {"primary domain controllers"}, o Active Directory. En algunos casos, puede sniffear las hashes directamente desde el cable. También tiene numerosos métodos de generar suposiciones de passwords (diccionario, fuerza bruta, etc.). L0phtCrack cuesta actualmente U$S 350 por máquina y no incluye el código fuente.

- **Retina:** Escáner para la evaluación de vulnerabilidades no-libre hecho por eEye. Al igual que Nessus y ISS Internet Scanner, la función de Retina es escanear todos los hosts en una red y reportar cualquier vulnerabilidad encontrada.

- **Netfilter:** es un poderoso filtro de paquetes el cual es implementado en el kernel Linux estándar. La herramienta iptables es utilizada para la configuración. Actualmente soporta filtrado de paquetes stateless o statefull, y todos los diferentes tipos de NAT (Network Address Translation) y modificación de paquetes.

- **SAINT:** Saint es otra herramienta no-libre de evaluación de seguridad (al igual que ISS Internet Scanner o Retina de eEye). A diferencia de esas herramientas basadas exclusivamente en Windows, SAINT corre exclusivamente sobre UNIX. Saint solía ser gratuito y "open source" pero ahora es un producto no-libre.

- **Network Stumbler:** Sniffer gratuito de 802.11 para Windows. Netstumbler es la más conocida herramienta para Windows utilizada para encontrar "access points" inalámbricos abiertos ("wardriving"). También distribuyen una versión para WinCE para PDAs y similares llamada Ministumbler. Esta herramienta es actualmente gratis pero sólo para Windows y no incluye el código fuente. Se hace notar que "El autor se reserva el derecho de cambiar este acuerdo de licencia a gusto, sin previo aviso." Los usuarios de UNIX (y usuarios de Windows avanzados) quizás quieran darle una mirada a Kismet.

- **SARA:** SARA es una herramienta de evaluación de vulnerabilidades derivada del infame escáner SATAN. Tratan de publicar actualizaciones dos veces al mes y de fomentar cualquier otro software creado por la comunidad de código abierto (como Nmap y Samba).

- **AirSnort:** Herramienta de crackeo del cifrado WEP de 802.11. AirSnort es una herramienta para LANs inalámbricas (WLAN) que recupera las llaves de cifrado. Fue desarrollada por el Shmoo Group y opera monitoreando pasivamente las transmisiones, computando la llave de cifrado cuando suficientes paquetes han sido recolectados. La versión para Windows es todavía demasiado preliminar.

- **NBTScan:** Recolecta información de NetBIOS de redes de Windows. NBTscan es un programa que escanea redes IP en busca de información de nombres de NetBIOS. Envía pedidos de "status" de NetBIOS a cada dirección en un rango provisto por el usuario y lista la información recibida de manera humanamente legible. Por cada host que responde, se lista su dirección, nombre de NetBIOS, nombre de usuario con sesión iniciada en la máquina {"logged in"} , y dirección de MAC.

- **GnuPG / PGP:** PGP es el famoso programa de encripción diseñado por Phil Zimmerman que ayuda a proteger nuestra información de curiosos y otros riesgos. GnuPG es una muy respetada implementación del estándar PGP (el nombre del ejecutable es, en realidad, gpg). Mientras GnuPG es software libre, PGP puede costar algo de dinero para algunas aplicaciones. En el capitulo anterior se profundizo sobre el.

- **Firewalk:** Firewalk emplea técnicas similares a las de traceroute para analizar las respuestas a paquetes de IP para determinar mapas de redes y filtros de listas de control de acceso (ACL) empleadas por gateways. Esta herramienta clásica fue reescrita desde cero en octubre del 2002.

- **Cain & Abel:** es una herramienta de recuperación de passwords gratuita para los sistemas operativos de Microsoft. Permite una fácil recuperación de varias clases de password, escuchando la red, crackeando los passwords cifrados utilizando ataques por diccionario y Fuerza Bruta, decodificando passwords codificados, revelando cuadros de diálogo del tipo password, develando passwords en

cachés y analizando protocolos de enrutamiento. El código fuente no viene incluído.

- **XProbe2:** herramienta de identificación de sistemas operativos activa. XProbe es una herramienta que sirve para determinar el sistema operativo de un host remoto. Logran esto utilizando algunas de las mismas técnicas que Nmap al igual que muchas ideas diferentes. Xprobe siempre ha enfatizado el protocolo ICMP en su enfoque de identificación.

- **NGrep:** Actualmente reconoce TCP, UDP, e ICMP sobre Ethernet, PPP, SLIP e interfaces nulas {"null interfaces"}, y comprende la lógica de un filtro "bpf" de la misma manera que herramientas más comunes de sniffing como tcpdump y snoop.

- **Perl / Python:** Lenguajes de scripting de propósito general para múltiples plataformas. Perl y Python hacen que sea muy fácil escribir scripts rápidos y portables para comprobar, abusar o incluso arreglar sistemas. Archivos como CPAN están llenos de módulos tales como NetRawIP e implementaciones de protocolos para facilitar nuestras tareas.

- **THC-Amap:** es un escáner nuevo pero poderoso que prueba cada puerto buscando identificar aplicaciones y servicios en lugar de confiar en un mapeo de puertos estático.

- **OpenSSL:** La más célebre biblioteca de cifrado para SSL/TLS. El proyecto OpenSSL es un esfuerzo de cooperación para desarrollar un set de herramientas robusto, de nivel comercial, completo en

características, y "Open Source" implementando los protocolos "Capa de sockets seguros" {"Secure Sockets Layer"} (SSL v2/v3) y "Seguridad en la Capa de Transporte" {"Transport Layer Security"} (TLS v1) así como también una biblioteca de cifrado de propósito general potente. El proyecto es administrado por una comunidad de voluntarios a lo ancho del mundo que utilizan Internet para comunicarse, planear, y desarrollar el set de herramientas OpenSSL y su documentación relacionada.

- **NTop:** es un monitor de uso de tráfico de red. Ntop muestra el uso de la red en una manera similar a lo que hace NTop por los procesos. En modo interactivo, muestra el estado de la red en una terminal de usuario. En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en NTop, y RRD para almacenar persistentemente estadísticas de tráfico.

- **Nemesis:** está diseñado para ser una pila de IP humana, portable y basada en línea de comandos para UNIX/LINUX. El set está separado por protocolos, y debería permitir crear scripts útiles de flujos de paquetes inyectados desde simples scripts de shell.

- **LSOF:** Esta herramienta forense y de diagnóstico específica de Unix lista información acerca de cualquiera archivo abierto por procesos que estén actualmente ejecutándose en el sistema. También puede listar sockets de comunicaciones abiertos por cada proceso.

- **Hunt:** fue hecho para ser usado sobre ethernet, y tiene mecanismos activos para olfatear conexiones en redes con switches. Las características avanzadas incluyen "ARP relaying" selectivo y sincronización de conexión luego de ataques. Si Hunt es de nuestro agrado, también podemos darle una mirada a Ettercap y a Dsniff.

- **Honeyd:** es un pequeño daemon que crea hosts virtuales en una red. Los hosts pueden ser configurados para ejecutar servicios arbitrarios, y su personalidad de TCP puede ser adaptada para que parezcan estar ejecutando ciertas versiones de sistemas operativos. Honeyd permite que un host alegue tener múltiples direcciones en una LAN para simulación de red. Es posible hacer ping o traceroute a las máquinas virtuales. Cualquier tipo de servicio en la máquina virtual puede ser simulado de acuerdo a un archivo de configuración simple. También es posible ser proxy de servicios para otras máquinas en lugar de simularlos.

- **Achilles (sitio no oficial):** Achilles intercepta los datos en una sesión de HTTP en cualquier dirección y le da al usuario la habilidad de alterar los datos antes de ser transmitidos. Por ejemplo, durante una conexión de HTTP SSL normal, un proxy típico pasa la sesión entre el servidor y el cliente y permite a ambos nodos negociar SSL. En contraste, cuando Achilles está en modo de intercepción, Achilles simula ser el servidor y negocia dos sesiones de SSL, una con el explorador de web cliente y otra con el servidor de web. Mientras la información se transmite entre ambos nodos, Achilles descifra los datos y le da al usuario la habilidad de alterar y/o registrar los datos en texto claro antes de su transmisión.

- **Brutus:** Un cracker de autenticación de fuerza bruta para redes. Este cracker sólo para Windows se lanza sobre servicios de red de sistemas remotos tratando de averiguar passwords utilizando un diccionario y permutaciones de éste. Soporta HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP, y más. El código fuente no está disponible. Los usuarios de UNIX deberían darle una mirada a THC-Hydra.

- **Stunnel:** Una envoltura criptográfica SSL de propósito general. stunnel está diseñado para trabajar como una envoltura de cifrado SSL entre un cliente remoto y un servidor local o remoto. Puede ser utilizado para agregarle funcionalidad SSL a daemons utilizados comúnmente como POP2, POP3, y servidores de IMAP sin cambios en el código del programa. Negocia una conexión SSL utilizando la biblioteca de OpenSSL o la SSLeay.

- **PakettoKeiretsu TCP/IP estreno:** es una colección de herramientas que utilizan nuevas e inusuales estrategias para manipular redes con **TCP/IP:** Modifican la funcionalidad dentro de una infraestructura existente y expanden los protocolos más de lo esperado por su diseño. Incluye Scanran, un sistema de descubrimiento de servicios de red y topología inusualmente rápido, Minewt, un router NAT/MAT para espacio de usuario, linkcat, que presenta un enlace Ethernet a la entrada/salida estándar. Paratrace, que rastrea los caminos de red sin realizar nuevas conexiones, y Phentropy, que utiliza OpenQVIS para graficar cantidades arbitrarias de entropía de fuentes de datos en un espacio de tres dimensiones.

- **Fragroute:** Entre sus características, se encuentra un lenguaje de reglas simple para retrasar, duplicar, descartar, fragmentar,

superponer, imprimir, reordenar, segmentar, especificar source-routing y otras operaciones más en todos los paquetes salientes destinados a un host en particular, con un mínimo soporte de comportamiento aleatorio o probabilístico. Esta herramienta fue escrita de buena fe para ayudar en el ensayo de sistemas de detección de intrusión, firewalls, y comportamiento básico de implementaciones de TCP/IP. Al igual que Dsniff y Libdnet, esta excelente herramienta fue escrita por Dug Song.

- **SPIKE PROXY:** es un proxy de HTTP que sirve para encontrar fallas de seguridad en sitios web. Es parte del Spike Application Testing Suite y soporta detección de inyección de SQL automatizada.

- **THC-Hydra:** Esta herramienta permite realizar ataques por diccionario rápidos a sistemas de entrada {login} por red, incluyendo FTP, POP3, IMAP, Netbios, Telnet, HTTP Auth, LDAP, NNTP, VNC, ICQ, Socks5, PCNFS, y más. Incluye soporte para SSL y aparentemente es ahora parte de Nessus. Al igual que Amap, esta versión es de la gente de THC.

- **hfnetchk:** Herramienta de Microsoft para evaluar el estado de los parches de todas las máquinas con Windows en una red desde una ubicación central.

- **cheops / cheops-ng:** Nos provee de una interfaz simple a muchas utilidades de red, mapea redes locales o remotas e identifica los sistemas operativos de las máquinas.

- **Zone Alarm:** El firewall personal para Windows. Tiene su versión gratuita. Las ventajas principales de Zone Alarm son la protección con servidor de seguridad, un servidor de seguridad fácil de usar que bloquea a los piratas informáticos y otras amenazas desconocidas.

  El bloque de intrusiones, identifica sistemáticamente a los piratas informáticos y bloquea los intentos de acceso.

  El modo silencioso hace a su computador invisible para cualquier usuario de Internet.

  Los requisitos del sistema son: Windows 98SE/ME/2000 Pro/XP. Pentium II o superior. 50 MB de espacio libre en el disco duro. Acceso a Internet. RAM mínima del sistema: 48 MB (98SE/ME), 64 MB (2000 Pro), 128 MB (XP). Protocolos admitidos para el análisis del correo electrónico: POP3 e IMAP4 para el correo recibido; SMTP para el correo saliente.

5. IMPORTANCIA DE LA SEGURIDAD EN NUESTRA SOCIEDAD

Hablar de seguridad informática en el momento actual no parece que suponga un alarde de modernidad y novedad. Con el desarrollo de los computadores, la vertiginosa evolución de Internet, la implantación del comercio electrónico, todo el mundo, sabe y se preocupa de la seguridad en estos ámbitos. De una estructura informática basada en sistemas propietarios y grandes servidores manejada por personal técnico, con una formación muy específica y alejada del conocimiento del común de los mortales, se ha evolucionado a otra más amigable y cercana al usuario final. Ello ha supuesto que los niveles iniciales de conocimiento sean rápidamente adquiridos por cualquier persona interesada, sin especiales conocimientos técnicos en la materia. La globalización en el conocimiento ha supuesto una quiebra de la seguridad de tiempos pasados amparada, en gran medida, en un cierto ocultismo. Se dice que los sistemas anteriores no eran más seguros que los actuales, tan sólo eran mucho más desconocidos, ya que el internet ha logrado que estos sistemas se pierdan el anonimato.

Existe una cierta tendencia a minimizar el ámbito de actuación del aspecto de la seguridad en el mundo de la Informática. Se cae, habitualmente, en abordar la implantación de la seguridad como respuesta a un problema o situación específica, sin estudiar todos los elementos que puedan estar relacionados. Si hablamos de una plataforma Web abierta a Internet, la seguridad no es responder si instalamos tal o cual cortafuegos, es bastante

más que eso: sistemas de alimentación interrumpida para máquinas críticas, duplicidad de almacenamiento, control físico, auditoría de conexiones internas y externas, blindaje de ficheros de sistema, control de modificación de ficheros, monitorización de tráfico de red, política de salvaguardas y muchas más.

Un concepto global de seguridad informática sería aquel definido como el conjunto de procedimientos y actuaciones encaminados a conseguir la garantía de funcionamiento del sistema de información, obteniendo eficacia, entendida como el cumplimiento de la finalidad para el que estaba establecido, manteniendo la integridad, entendida como la inalterabilidad del sistema por agente externo al mismo, y alertando la detección de actividad ajena, entendida como el control de la interacción de elementos externos al propio sistema. Si conseguimos todo esto, podremos decir que disponemos de un sistema seguro.

Ya hemos comentado el concepto pero sobre qué lo aplicamos, qué es lo que hay que proteger.

En el mundo de la Informática se utiliza habitualmente una división en dos grandes áreas que denominamos Hardware y Software. Si bien se puede tachar de algo simple vamos a emplearla para agrupar los objetivos de la seguridad, amparándonos en su universalidad.

Dentro del área del Hardware los objetos de nuestra atención son fundamentalmente tres: servidores, clientes y líneas de comunicaciones.

Los servidores, especialmente en instalaciones intermedias y grandes, suelen estar situados agrupados y en dependencias específicas como centros de procesos de datos. El acceso a dichas instalaciones debe estar controlado y auditado con reflejo del personal y material que entra y sale del mismo. La alimentación eléctrica debe garantizarse con sistemas

ininterrumpidos para responder a pequeños cortes de corriente y con medios alternativos ante grandes cortes. Los medios de almacenamiento deben duplicarse o cuando menos garantizar la recuperación de la información ante problemas de discos, además de garantizar la duplicidad de accesos caso de baterías de discos o cintas externas. Para grandes servidores hay que habilitar desde duplicidad de accesos a placas de sistema hasta soluciones de alta disponibilidad entre dominios o máquinas. Se deben disponer de elementos de salvaguarda alternativos para cubrir posibles averías. El control de la consola principal del sistema y su conectividad a la máquina que nos permita acceder al sistema, caso de pérdida de acceso remoto a la misma, es otro de los aspectos a los que prestar atención.

Las líneas de comunicaciones, de las que todo el mundo se preocupa de incrementar pero muy poco de controlar su actividad y uso. Una adecuada segmentación de la red además de mejorar su funcionamiento ayudará enormemente a su seguridad. La eliminación de los cuellos de botella y el estudio de las razones de que ocurra permitirá eliminar posibles quiebras de seguridad del sistema. La cifra de canales y la información que circula a través de ellos permitirán garantizar la confidencialidad, la integridad y el no repudio de la misma. A este respecto hay que hacer mención al avance que ha supuesto el empleo de las certificaciones digitales y el establecimiento de los procesos de firma digital, impulsados directamente por el comercio electrónico y el desarrollo de la denominada sociedad de la información.

Todo lo reflejado hasta el momento, además de otras consideraciones como mentalización, conocimiento y planificación, tiene un condicionante fundamental y se llama dinero. En la medida en la que queramos un sistema más seguro tendremos que contemplar una inversión económica mayor. El cliente tendrá que decidir, ponga en la balanza dinero y nivel de seguridad a alcanzar y encontrará el equilibrio.

Dentro del área de Software los objetos de nuestra atención son también tres: sistema operativo, bases de datos y aplicaciones.

Los sistemas operativos de nuestro sistema de información son la base del funcionamiento lógico del mismo, todo lo que esté alojado en el mismo estará íntimamente condicionado a la elección del sistema operativo y a su configuración personalizada. Un aspecto a vigilar desde el punto de vista de la seguridad es la elección de una versión y configuración estable, no hay que caer en la tentación de estar siempre a la última porque muchas veces lo único que conseguimos es hacer de conejillos de indias. Naturalmente antes de eso hay que elegir qué sistema instalar, casi todos son más o menos multipropósito pero cada uno está programado pensando en criterios diferentes en algo. Otro punto a tener en cuenta es el establecimiento de elementos alternativos de arranque que nos permitan hacer frente a incidencias que ocurren en el día a día, un sistema que permite arranque desde cinta es un auténtico seguro de vida. Hay que acordarse de activar las auditorías propias del sistema que nos va a dar información básica de actividad de aspectos críticos, caso de no disponer de herramientas propias, lo que es difícil que se dé, hay que invertir inexcusablemente en un desarrollo específico. Se debe establecer una política de salvaguardas que permita, ante cualquier fallo crítico, restablecer una situación estable lo más próxima al momento anterior en que surgió la incidencia. Hay que evitar en lo posible las instalaciones tipo por las facilidades que presenta de conocimiento del sistema ante un eventual agresor. La política de usuarios plasmada en una adecuada parcelación de niveles de acceso y en una estricta disciplina de palabras de paso, todos conocemos la teoría y ninguno la aplicamos. Hay que contemplar el control de ficheros en su propiedad y niveles de ejecución para detectar alteraciones en los mismos. La alteración en tamaño y fecha de ficheros básicos de configuración y actividad de sistema son indicios más que racionales de que puede existir una quiebra de la seguridad.

Por lo que respecta a bases de datos tendríamos que repetir mucho de lo expuesto con anterioridad para los sistemas operativos. Mencionaremos que aquí tendremos usuarios distintos lo que nos permitirá blindar aún más la seguridad con otra política de usuarios complementaria de la anterior. En el caso de las bases de datos es importante, además de contar con salvaguardas recientes, el contar con réplicas de la misma a tiempo real lo que permite minimizar el impacto de una quiebra de la integridad en la base explotada.

Cuando hablamos de aplicaciones hacemos referencia a aquellos programas que de una u otra manera nos permiten explotar las funcionalidades de nuestro sistema de información. Una vez en explotación es fundamental el control de la actividad de los usuarios para conocer en todo momento quién y qué está haciendo. Este aspecto se lo plantea todo el mundo pero algo que suele caer en el olvido es la fase de desarrollo de la aplicación. En el proceso de generación del programa se debe controlar todo el proyecto, las validaciones que se realicen y quedarse en poder del código fuente y posteriores modificaciones, con el objeto de poder filtrar aquel código erróneo o malicioso que pueda incorporar la aplicación.

Estamos hablando mucho de seguridad pero por qué, cuál es la razón de tanta preocupación.

El porqué de la seguridad viene derivado de tres aspectos fundamentales.

En primer lugar y directamente derivado del concepto que dábamos al inicio de este capitulo, para garantizar el correcto funcionamiento del sistema de información. Toda la inversión que se haga de nada servirá si no conseguimos alcanzar la funcionalidad para la que se creó el sistema.

En segundo lugar, por prestigio y futuro del sistema y, por extensión, de la empresa o Institución. Ello no quiere decir que caigamos en evitar todas

aquellas funcionalidades que puedan suponer una quiebra en la seguridad, lo que hay que plantearse es más funcionalidad con más seguridad y no sería malo recordar lo que se mencionaba anteriormente, más seguridad casi siempre es sinónimo de más inversión económica en la misma.

Hasta el momento hemos definido globalmente la seguridad informática, hemos hecho un muestreo de qué proteger y hemos valorado el porqué, pero de qué tenemos que proteger a nuestro sistema.

La potencial agresión sobre el sistema puede venir derivada de intervenciones de dos tipos.

Las intervenciones no maliciosas, ya sean por manipulaciones humanas o no, son imprevisibles y de resultado incierto. Las más habituales se refieren a cortes de corriente o alteraciones importantes en los niveles de tensión en la alimentación eléctrica que pueden provocar hasta daños irrecuperables en determinado hardware. Los fallos hardware están a la orden del día y no es extraña la inutilización de discos duros con la posibilidad de la consiguiente pérdida de información o el fallo de placas de sistema.

Las intervenciones maliciosas van ligadas a la manipulación humana. Las más peligrosas potencialmente, por el alcance del daño que se puede provocar y por la mayor dificultad en su detección, son las internas al propio sistema de información. El agresor lo enmarcaríamos dentro de los administradores del sistema, programadores o usuarios privilegiados, también incluiríamos a aquel que no teniendo acceso lógico al sistema sí lo tuviese físico a elementos críticos del mismo. Las grandes quiebras de seguridad han provenido siempre del interior de las estructuras atacadas y la mayor parte de las veces se han silenciado en un primer momento para no provocar reacciones incontroladas.

La mayor peligrosidad de este tipo de actuaciones viene derivada del mayor conocimiento que el agresor dispone del medio sobre el que actúa. El otro tipo de intervención maliciosa es la de origen externo y que se produce casi siempre a través de línea de comunicaciones, como ejemplo más claro y actual podemos contemplar las intrusiones a través de Internet.

5.1 LA RESPOSABILIDAD PROFESIONAL Y LA SEGURIDAD INFORMATICA

Las personas con formación profesional deben estar conscientes que, gracias a su preparación pueden ocupar cargos que imponen responsabilidades especiales. Por ejemplo: los médicos y los abogados tienen responsabilidades especiales como mantener la confidencialidad de sus pacientes o clientes que no tendrían sino estuviesen ejerciendo su labor de profesionales. Además el aumento de la importancia de tecnologías como los computadores y las redes en la sociedad actual obliga a los profesionales a meditar sobre ¿cuáles deben ser los lineamientos éticos que deben seguir para su uso?

5.1.1 LOS PROFESIONALES Y SU RESPOSABILIDAD AL USAR COMPUTADORES, REDES, SERVICIOS Y APLICACIONES:

Los computadores y las redes representan una de las innovaciones tecnológicas mas importantes del siglo pasado. Como ha sucedido con la mayoría de las innovaciones tecnológicas, permiten emerger nuevos problemas morales, ya que crean nuevas posibilidades que puedan beneficiar o dañar a otros. Algunos de estos nuevos aspectos son sugeridos

en el código de ética y conducta profesional de la ACM (Association for Computer Machinery) y que podemos asimilar a un código de ética profesional para usar tecnología de procesamiento de información.

Los miembros de la ACM deben tener las siguientes condiciones:

1. contribuir al bienestar de la humanidad.
2. evitar hacer daño a otros.
3. ser honesto
4. ser justo y adelantar acciones para no discriminar.
5. respetar los derechos del autor.
6. dar el crédito adecuado a la propiedad intelectual.
7. respetar la privacidad de otros.
8. respetar la confidencialidad.

Los puntos 1,2,3,4 y 8 generan obligaciones profesionales que son similares a los impuestos en código de ética profesional.
En los otros puntos aparecen 2 temas importantes: el licenciamiento de software (5) y la propiedad intelectual (6).
El uso inadecuado de los sistemas (7) que son parte de los objetivos de la seguridad informática.

CONCLUSIONES

Con este trabajo he llegado a la deducir que la seguridad computacional es muy importante y que a veces llegamos a desconocer cierta parte de la seguridad. No solamente debemos protegernos de los hackers, crackers, o llamados en otros términos “Piratas Informáticos”, sino también proteger la información de accidentes ocasionados como incendios, humedad, etc.

Debemos de tener una política de seguridad en nuestra empresa, por muy pequeña que sea, siempre se necesita hacer un plan de contingencia.

Sin importar que un profesional tenga o no información en el campo de la informática, tiene una responsabilidad directa, como profesional con la seguridad informática.

RECOMENDACIONES

Esta guía de seguridad computacional nos muestra de manera superficial, pero concisa algunos temas de seguridad computacional. Si queremos profundizar sobre estos temas con mayor grado de conocimiento podemos encontrar fuentes bibliograficas que nos hablan con mas detalle.

Cabe resaltar que cada día aparecen nuevos virus, y debemos estar a la vanguardia, por eso es bueno que nos mantengamos actualizados.

Si deseas profundizar sobre los algoritmos criptográficos puedes consultar libros de criptografía avanzada.

BIBLIOGRAFIA

ARCILA, Iriarte Jaime Msc. MANUAL DE CRIPTOGRAFIA. 7ª Edición. 2001. Profesor de la Universidad Tecnológica de Bolívar.

Dr. COLE, Eric; Dr KRUTS, Ronald y CONLEY, James W. NETWORK SECURITY BIBLE. Wiley Publishing inc.

http://www.seguridadcorporativa.org

http://www.delitosinformaticos.com/especial/seguridad/pgp.shtml

http://www.acis.org.co/fileadmin/inseg-inf.pdf

www.unal.edu.co/seguridad/documents/guia_para_elaborar_politicas_v1_0.pdf

http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=9&pagina=0

http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=14&pagina=0

ANEXOS

SEGURIDAD INFORMÁTICA

INTRODUCCION

La creciente globalización de la economía en el mundo ha incrementado la necesidad en las organizaciones ha abrir sus puertas a el entorno que las rodea y disponer de información íntegra y confiable en el momento adecuado. Debido al incremento en la complejidad de las operaciones de las organizaciones y a la disminución en los tiempos de respuesta requeridos, la única forma de disponer del recurso de la información es teniendo sistemas de información confiables que permitan a la Organización estar en la vanguardia tecnológica y responder oportunamente a las exigencias de un mercado cada vez más competitivo.

La integridad, confidencialidad, confiabilidad y disponibilidad de la información solo puede ser garantizada adoptando los mecanismos adecuados de seguridad en la organización. El aumento de la competencia incrementa la necesidad de establecer políticas y procedimientos de seguridad efectivas que disminuyan los riesgos de que se produzca un escape, alteración o destrucción de datos que sean de vital importancia para la organización.

Un sistema de información dentro de una organización juega el papel análogo al del sistema nervioso de un animal. Incluido en el sistema están los componentes que ejecutan funciones tales como la percepción, clasificación, transmisión, almacenamiento, recuperación, transformación. Su propósito

primordial es proporcionar información (en el momento en que se le solicite) para la toma de decisiones y la coordinación. En el sentido más amplio el sistema de información incluye todos los componentes envueltos en la toma de decisiones, coordinación y advertencia tanto humanos como automáticos. Es así como dada la importancia que tiene este hoy en día para la continuidad del negocio de la organización, que se debe enfrentar el tema de la seguridad de la información como un tema en el que esta en juego todos los componentes de la organización.

El objetivo principal de la Seguridad Informática es proteger los recursos informáticos del daño, la alteración, el robo y la pérdida. Incluyendo en esto los equipos, medios de almacenamiento, software, listados de impresora y los datos. Todo esto enmarcado en un metaobjetivo que es el de mantener la **continuidad de los procesos** organizacionales que soportan los sistemas de información.

La Seguridad es un elemento importante de cualquier Servicio y Sistema Informático, aunque a menudo esta es postergada, basta tan sólo una brecha en la seguridad para crear graves daños. Por esto, el papel de la Seguridad Informática es cada vez más importante y no podrá ser ignorado, especialmente por el aumento de la exposición al riesgo que implica la cada vez mayor integración y globalización de los Sistemas Informáticos.

Una Primera Aproximación

El tema de seguridad es complejo. Y hay varias razones para ello: la gran cantidad de información que manejan las empresas, la conectividad entre sistemas y equipos, pero por sobre todo, la falta de políticas globales al interior de la empresa para enfrentarlo en forma clara y con las herramientas apropiadas.

A continuación se presenta los resultados de encuestas hechas por la Sentry Market Research a 945 directivos de empresa con un nivel tecnológico medio-alto, el 80% está planeando implementar mayores medidas de seguridad en los próximos dos años, y el 29% ya implementó sistemas y software de seguridad.

Un estudio realizado por Intrusion Detection Inc a 32.250 usuarios de medianas y grandes empresas, extraía las siguientes conclusiones en cuanto a los principales problemas relacionados con la seguridad detectados en la empresa:

- Los usuarios no cambian los passwords con suficiente frecuencia
- El acceso a los archivos es demasiado libre
- La aplicación de normas de seguridad para nuevos usuarios es inconsistente
- Los passwords son fácilmente identificables
- Los identificadores de usuarios están inactivados

Una encuesta de Ernst&Young para Information Week, realizada en 1995 y 1996, trasladaba la siguiente pregunta a 1.320 directivos y profesionales de las telecomunicaciones: ¿Cuánta importancia concede el máximo responsable de su empresa a la información relacionada con Seguridad?. Los resultados desprenden un creciente interés por la Seguridad dentro de la empresa:

Grado de importancia que su empresa concede a la Seguridad	**Porcentaje de respuestas**
Ninguna importancia	5%

Alguna importancia	32%
Importancia	39%
La máxima importancia	24%

Fuente: Ernst&Young para Information Week

Otras interesantes conclusiones del estudio de Ernst&Young/Information Week son las siguientes:

Aumenta el número de organizaciones que experimentan problemas de seguridad, pero que no pueden contratar a más personas y adquirir los equipos y tecnologías necesarios para evitarlos por problemas de presupuesto. En general, muchas compañías no pueden o no quieren invertir en una estrategia de seguridad adecuada.

Obstáculos para incorporar estrategia de Seguridad en la empresa.

- Falta de utensilios y soluciones de seguridad
- Falta de administración
- Falta de presupuesto
- Falta de recursos humanos

Muchas organizaciones sufren pérdidas financieras apreciables por asuntos relacionados con la seguridad de la información. Así, el 54 % de los encuestados para la realización de este estudio afirmó que sus compañías habían sufrido pérdidas durante los dos años anteriores debido a la seguridad de la información y a la recuperación tras el desastre. Si además se incluyen las pérdidas causadas por los virus informáticos, este porcentaje aumenta hasta alcanzar un 78 %.

Problemas de seguridad que han supuesto pérdidas Financieras

- Virus

- Errores accidentales
- Tiempo de inactividad que no ha causado desastres
- Daños intencionados llevados a cabo por los empleados
- Desastres naturales
- Daños provocados desde el exterior
- Espionaje industrial

Las pérdidas de capital sufridas por las empresas consultadas fueron substanciales, aunque no cuantificables en algunos casos: cerca del 70 % de los encuestados no pudo calcular cuánto había perdido su empresa. Entre aquellas que sí conocían el alcance de las pérdidas, más del 25% las situaba hasta 250.000 dólares, y algunas incluso en más de un millón de dólares.

Definir los limites de seguridad en las empresas es casi imposible porque involucra a **toda la organización**. No solo se trata de protegerla del ambiente externo, si no que también del mal manejo que se puede producir en su interior . Y cada día se esta haciendo más común escuchar de firewalls, autentificación de usuarios, control de acceso, firmas digitales, etc. A nivel nacional estamos en una primera etapa, donde las grandes empresas han sido muy sensibles al tema (firewalls) lo que se debe en gran medida, a los temores que existen sobre la inseguridad de la internet tradicional, pero en el resto de las áreas se ha hecho muy poco. Es así como además el desarrollo de la seguridad de los SI/TI en las empresas esta en directa relación con la evolución de estas en ellas mismas, las pequeñas y medianas empresas (Pymes), en donde los SI/TI tienen poco tiempo de vida, son las que se encuentran más vulnerables.

SEGURIDAD DE SI/TI

¿ Qué es la seguridad informática ?

En realidad es un concepto cuya definición exacta es difícil de proporcionar, debido a la gran cantidad de factores que intervienen en ella y su corta vida aun. Sin embargo es posible enunciar que Seguridad es el conjunto de recursos (metodologías, planes, políticas documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

Existe una medida cualitativa para la Seguridad que dice "Un sistema es seguro si se comporta como los usuarios esperan que lo haga" (Dr. Eugene Spafford).

Objetivos que persigue

Como ya se mencionaba en la introducción los objetivos que persigue la seguridad de los SI/TI es proteger los recursos informáticos del daño, la alteración, el robo y la pérdida. Incluyendo en esto los equipos, medios de almacenamiento, software, listados de impresora y los datos. Todo esto enmarcado en un metaobjetivo que es el de mantener la **continuidad de los procesos** organizacionales que soportan los sistemas de información.

Como es sabido en todas las empresas existen **procesos críticos** que constituyen la medula espinal para que funcione el negocio y muchos de estos procesos críticos son apoyados por los sistemas de información, es por esto que la seguridad de estos resulta de vital importancia para que la empresa pueda mantenerse y continuar en su negocio.

La seguridad como problema cultural

Una de las paradojas es que ha pesar de que cada vez se destinan mayores recursos para el área informática y que esta se ha vuelto esencial para la gestión de negocios de las empresas, el presupuesto asignado específicamente al tema de seguridad, no ha crecido en la misma proporción. Por esto es fundamental crea **conciencia** al interior de las organizaciones para que puedan dimensionar en su justa medida la relevancia del problema, porque si se miran los presupuestos de informática dentro de las empresas,

vemos que han crecido notablemente, pero no ha ocurrido lo mismo con los presupuestos asignados a las áreas de seguridad (recordar los cuadros de las encuestas al principio). Mientras más tecnología se incorpora, mas se agranda la brecha en lo que son debilidades de seguridad. Actualmente hay empresas que basan sus procesos en de negocios en TI y eso provoca que la empresa este **dependiendo** cada vez mas de estas herramientas tecnológicas y paralelamente van creciendo los temas relacionados con la seguridad. Por esto es fundamental la creación de conciencia en las empresas.

Una de las razones por las cuales no ha despegado fuertemente el comercio electrónico en el país es que ante la decisión de las empresas de abrirse a este tema, que va a requerir el desarrollo de mecanismo de seguridad, prefieren postergarla y si ha este le sumamos la precaria condición de la legislación chilena con respecto al tema la opción queda desechada. La tecnología disponible hoy en día hace posible una transferencia electrónica en forma segura, el problema es que la que la gente no sabe como hacerlo y tiene como consecuencia que Chile se esta quedando atrás no por un problema tecnológico, si no por un problema de **mentalidad.** Sin duda como vemos la seguridad es fundamental no solo para evitar desastres o perdidas irrecuperables que afecten el funcionamiento de las organizaciones, sino que también para potenciar nuevas áreas de negocios que permitan el crecimiento de los diferentes actores del mercado.

La seguridad como proceso

Uno de los puntos de consenso en el tema es que la seguridad es un proceso y no actividad particular que desarrolla la empresa, un proceso que barre todas las unidades funcionales de esta. Al hablar de seguridad hay que involucrar muchos aspectos que no solo están relacionados con herramientas tecnológicas. Abordar el tema de seguridad no solo implica una solución de hardware y software, también involucra un conocimiento sobre el riesgo que significa no dar **confiabilidad** a la información, lo que en

ocasiones tiene que ver con un desconocimiento de parte de los administradores de sistemas sobre el tema.

El problema hay que enfrentarlo con tecnología, pero también debe involucrar a los tomadores de decisiones, que son finalmente quienes deciden las inversiones, ellos deben comprender claramente la problemática para destinar los recursos necesarios para garantizar la confiabilidad, disponibilidad e integridad de los datos.

Propiedades de la Información que protege la Seguridad Informática

La Seguridad Informática debe vigilar principalmente por las siguientes propiedades:

Confidencialidad: Se define como la "condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados". La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. A menudo se la relaciona con la Intimidad o Privacidad, cuando esa Información se refiere a personas físicas.

Integridad: Se define como la "condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado". La integridad está vinculada a la **fiabilidad funcional** del sistema de información (o sea su eficacia para cumplir las funciones del sistema de organización soportado por aquél). La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la Integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.

Disponibilidad: Se define como el "grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un Sistema de Información en un periodo de tiempo considerado aceptable". Se asocia a menudo a la **fiabilidad técnica** (tasa de fallos) de los componentes del sistema de información. La información debe estar en el momento que el usuario

requiera de ella. Un ataque a la disponibilidad es la negación de servicio (En Inglés Denial of Service o DoS) o "tirar" el servidor .

Autentificación o no repudio: Se define como "el mecanismo que permite conocer si la persona que esta accediendo a un sistema, es realmente quien debe acceder y no un extraño". El no repudio se refiere a los que se hacen sobre en temas de correo electrónico para garantizar la autenticidad del remitente (un mecanismo son las firmas digitales).

Factores que afectan a los sistemas de Información

Los principales factores que se ciernen sobre los sistemas Informáticos tienen orígenes diversos. Así, si consideramos las amenazas externas, el hardware puede ser físicamente dañado por agua, fuego, terremotos, sabotajes,... Las mismas causas pueden dañar los medios magnéticos de almacenamiento externo. La información contenida en éstos, también puede verse afectada por campos magnéticos intensos y frecuentemente, por errores de operación. Las líneas de comunicación pueden ser interferidas, etc.

Otros tipos de amenazas provienen de usuarios o empleados infieles. Así, los primeros pueden usurpar la personalidad de usuarios autorizados y acceder indebidamente a datos para su consulta o borrado, o aunque algo más complicado, modificar en su provecho programas de aplicación.

Otras amenazas más sutiles provienen de inadecuados controles de programación. Así, el problema de residuos, es decir, de la permanencia de información en memoria principal cuando ésta es liberada por un usuario o, en el caso de dispositivos externos cuando ésta es incorrectamente borrada.

Una técnica fraudulenta muy usada consiste en transferir información de un programa a otro mediante canales ilícitos y no convencionales (canales ocultos).

Factores que afecta la integridad de los datos

- **Desastres naturales:** Inundaciones, incendios, tormentas, terremotos etc.
- **Fallas de Hadware:** Discos, controladores, energía, memoria, dispositivos etc.
- **Fallas Humanas:** Accidentes, inexperiencias, estrés, problemas de comunicación, venganza, interés personal.
- **Fallas en la red:** Controladores, tarjetas, componentes, radiación
- .**Problemas de SW o lógicos:** Requerimientos mal definidos, corrupción de archivos, errores de programas o aplicaciones, problemas de almacenamiento, errores de SO.

Factores que afectan a la seguridad de los datos

- **Autentificación :** La forma en que se hace el proceso de acceso a los sistemas, passwords, perfiles de usuario.
- **Basados en cables:** Todos los cables son "pinchables" es decir se acceder fácilmente a los datos que circulan de un nodo a otro en una red , para esto se utilizan las técnicas de encriptación.
- **Físicas:** averías en los componentes físicos, robo, espionaje industrial etc.

- **Programación:** Aplicaciones mal construidas, los bugs en el software de la industria que necesita de parches para reducir el riesgo de perder los datos

- **Puertas Falsas:** En la mayoría de los software existen puertas falsas que permiten alterar o manipular los datos con los cuales estos trabajan (ej.: manipulación de tablas en las base de datos).

En Resumen

La información y los sistemas que la soportan constituyen recursos valiosos e importantes para la Organización. Su seguridad suele ser imprescindible para mantener valores esenciales, sean propios del sector público (servicio, seguridad procedimental, imagen), propios del sector privado (competitividad, rentabilidad) o comunes a ambos (permanencia del funcionamiento, cumplimiento de la legalidad). Dicha seguridad consiste al final en un depósito de confianza suficiente en la capacidad de dicha información y sistemas para sostener el funcionamiento adecuado de las funciones y los valores de la Organización.

Cualquier amenaza que se materialice contra el flujo normal de la información en una Organización, pone de relieve la dependencia y la vulnerabilidad de toda la Organización (en un grado que es consecuente con la gravedad de la amenaza, como es lógico).

El crecimiento de las redes y la consecuente conectividad entre sistemas representa nuevas oportunidades, no sólo positivas, sino también negativas al facilitar por ejemplo los accesos no autorizados y al reducir las facilidades de control centralizado y especializado de los sistemas de información.

Los sistemas de información de cualquier Organización están sometidos a *amenazas* más o menos destructivas (como ampliamente difunden los medios de comunicación incluso los no especializados). Amenazas que van desde fallos técnicos y accidentes no intencionados (pero no menos peligrosos), hasta acciones intencionadas, más o menos lucrativas, de curiosidad, espionaje, sabotaje, vandalismo, chantaje o fraude. Todas las opiniones aseguran que las amenazas a la seguridad de los sistemas de

información y a la información misma serán cada vez más ambiciosas y sofisticadas.

El objeto o propósito de la seguridad de los sistemas de información consiste sobre todo en mantener la *continuidad de los procesos* organizacionales que soportan dichos sistemas. Asimismo intentar minimizar tanto el *costo global* de la ejecución de dichos procesos como las *pérdidas* de los recursos asignados a su funcionamiento.

El sujeto global de la seguridad se determina como un Dominio del conjunto de la Organización, que suele considerarse compuesto por Activos (como sujetos elementales de la seguridad), estructurados metódicamente de forma jerarquizada.

La seguridad siempre es barata a largo plazo (y lo es también cada vez más a corto plazo). El ahorro y la eficacia que proporciona son relativos, pues dependen de su costo propio y su implantación inteligente; pero siempre son muy superiores si los requerimientos y especificaciones de seguridad se incorporan en el propio desarrollo de los sistemas y los servicios de información. *Cuanto más temprano se actúe para dar seguridad a los sistemas de información, más sencilla y económica resultará ésta a la Organización.*

GESTION DE RIESGOS EN LOS SI

La gestión de riesgos de los sistema de información constituye la principal forma de hacer frente al problema de la seguridad de la información en las organizaciones, esta pasa ha ser una labor de vital importancia ya no a nivel funcional si no ha nivel corporativo. De ella se desprende la planificación de la seguridad de los SI, y por ende las políticas y medidas de seguridad ha implantar como también los objetivos, estrategias, y organización de la seguridad. La gestión de riesgos en los SI es una acción permanente cíclica

y recurrente, es decir, se ha de realizar continuamente debido a los cambios del sistema y de su entorno.

Objetivos

Sus objetivos son **identificar, analizar, y eliminar o controlar** las fuentes de riesgos antes de que empiecen ha amenazar el funcionamiento continuo y confiable de los sistemas de información.

Definición de algunos términos

Activos

Los *Activos: "recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección"* se pueden así estructurar en 5 categorías:

- El *entorno* del Sistema de Información necesario para su funcionamiento: instalación física, infraestructura de comunicaciones y otras, suministros, personal operacional o desarrollador de aplicaciones.
- El S*istema de Información* (hardware, redes propias, software básico, aplicaciones).
- La propia *Información*.
- Las *Funcionalidades de la Organización* que justifican y dan finalidad a la existencia de los Sistemas de Información, incluido el personal usuario o los objetivos propuestos por la dirección.
- *Otros Activos* (por ejemplo la credibilidad de una persona jurídica o física, su intimidad, la imagen ...).

El fallo de un Activo de una categoría o nivel pueden generar cadenas de fallos en otros niveles. Así, fallos en Activos del *Entorno* (1) provocarían otros

fallos en el *Sistema de Información* (2); éstos inciden en fallos de la *Información* (3), que soporta las *Funcionalidades de la Organización* (4) y ésas condicionan los *otros Activos* (5).

Una frase común a la cual se suele recurrir es que *"Una cadena se rompe por el eslabón más débil"* lo mismo ocurre en materia de seguridad no importa que la seguridad para un activo sea alta si para otro esta es débil.

Amenazas:

Se definen como *"los Eventos que pueden desencadenar un Incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus Activos".* Las Amenazas se pueden materializar y transformarse en agresiones. El modelo debe ver las Amenazas bajo un enfoque dinámico, o sea como *acciones* capaces de modificar el Estado de seguridad del Activo amenazable; acciones de tipo evento, pues hay otras de tipo decisión humana.

Vulnerabilidad:

Definida como *la "ocurrencia real de materialización de una Amenaza sobre un Activo"*, la Vulnerabilidad es una propiedad de la relación entre un Activo y una Amenaza. Ejerce entre ambos una función de mediación en el cambio del Estado de Seguridad del Activo; siendo también el mecanismo de paso desde la Amenaza a la Agresión materializada. La Vulnerabilidad tiene así dos aspectos: el estático, ligado a la función (forma parte del Estado de Seguridad del Activo); y el dinámico, ligado al mecanismo (convierte la Amenaza en agresión). El término Vulnerabilidad cubre dos acepciones distintas: Vulnerabilidad intrínseca del Activo respecto al tipo de Amenaza y Vulnerabilidad efectiva, que tiene también en cuenta las Salvaguardas aplicadas en cada momento. La intrínseca puede descomponerse en la posibilidad de ocurrencia de la Amenaza independiente del Activo amenazado (por ejemplo la probabilidad de desbordamiento de un río

determinado) y la Accesibilidad de la Amenaza al Dominio, sea física (por ejemplo la su proximidad a ese río) o bien lógica.

Impacto:

Se define como "daño producido a la organización por un posible incidente" y es el resultado de la Agresión sobre el Activo, o visto de manera más dinámica, "la diferencia en las estimaciones de los estados (de seguridad) obtenidas antes y después del evento". Podemos clasificar los Impactos sobre los Activos a partir de sus consecuencias: o Pérdidas bien Cualitativas; por reducción de subestados de seguridad. El Impacto puede ser cuantitativo(si representa Pérdidas cuantitativas monetarizables directas o indirectas); cualitativo con pérdidas orgánicas (por ejemplo, de fondo de comercio, daño de personas); y cualitativo con pérdidas funcionales (o de los subestados de seguridad).

Riesgo

Se ha definido como la "Posibilidad de que se produzca un impacto dado en la organización". Su importancia como resultado de todo el Análisis organizado sobre los elementos anteriores (activos, amenazas, vulnerabilidades e impactos) queda velada por su apariencia como Indicador resultante de la combinación de la Vulnerabilidad y el Impacto que procede de la Amenaza actuante sobre el Activo.

Este *riesgo calculado* permite tomar decisiones racionales para cumplir el objetivo de seguridad de la organización. Para dar soporte a dichas decisiones, el riesgo calculado se compara con el *umbral de riesgo,* un nivel determinado con ayuda de la política de seguridad de la Organización. Un riesgo calculado superior al umbral implica una decisión de reducción de riesgo. Un riesgo calculado inferior al umbral queda como un *riesgo residual* que se considera asumible.

Criticidad

Nivel de impacto que tendría en los procesos vitales de una empresa la paralización total o parcial de uno de sus proceso de producción. El impacto no solo podría entenderse en términos económicos local/regional, sino también en el ámbito nacional/internacional de sus negociaciones.

Un ejemplo Trivial

La comprensión de los mecanismos de seguridad de los SI puede aclararse con un ejemplo trivial como es la seguridad de otro sistema bien conocido: nuestro cuerpo y su salud. En este caso el cuerpo es el *dominio* compuesto por distintos activos (los órganos atacables) y las **amenazas** son los distintos agentes infecciosos de carácter bacteriano o bien vírico que pulupan en el entorno.

Un individuo concreto adopta habitualmente **medidas de seguridad** (MS) elementales que pueden llamarse organizativas (por ejemplo abrigarse si baja la temperatura, lavarse las manos antes de comer instalarse de forma que se evite corrientes de aire). Pero ante riesgos mayores necesita realizar un **análisis de riesgos** mas profundo, aunque parezca evidente por lo habitual. El análisis de riesgos indica que la **vulnerabilidad** al avanzar la epidemia gripal de todos los otoños y que el **impacto** previsible será una cadena de degradaciones que van desde simples molestias ha posibles secuelas importantes de su salud; y desde la perdida de algún día laborable a graves dificultades para mantener el proyecto que tiene entre manos. Los dos factores que, Vulnerabilidad e Impacto permiten evaluar el **riesgo** de coger la gripe y sus secuelas. Según la importancia que se de al riesgo valorado, la persona preparara una batería consecuente de MS para 'gestionar' ese riesgo (no para anularlo, pues es infalible, sino imposible erradicar la gripe del ambiente o no ir a trabajar varios meses para evitar contagios).

Por lo tanto para reducir la vulnerabilidad (la probabilidad de coger la gripe) y como no puede evitar drásticamente los ambientes contagiosos (como el transporte publico o el lugar de trabajo), la persona decide vacunarse como

MS preventiva. Así ha disminuido el riesgo, pero no lo ha eliminado: la amenaza suele materializase como **agresión** del agente virico en forma de afección gripal.

Etapas de la Gestión de Riesgos

A continuación se presenta una figura que describe todos los alcances de la gestión de riesgos.

Identificación de Riesgos

Es la primera etapa a emprender, para abordarla, hay que listar los recursos con los que cuente la organización. Es posible que se requiera conocer más detalladamente los procedimientos, leyes, políticas de la organización, recursos disponibles e inclusive si se cuenta con seguro sobre los bienes inmuebles. Existen recursos tangibles (monitores, computadoras, impresoras, etc.), e intangibles (privacidad de los usuarios, contraseñas de los usuarios, imagen pública, etc.) A la vez identificación de las amenazas que constituyen riesgos para la organización. Se debe hacer por lo tanto una lista de amenazas que afecten los recursos, dichas amenazas pueden ser ambientales como: incendios y terremotos, amenazas extrañas como: fallas estructurales del edificio, relámpagos, epidemias, inundaciones, pérdida del servicio telefónico, etc., amenazas de introducción de virus informáticos y "bugs" en el software. Después de determinar las amenazas es necesario estimar qué tan factible es que suceda cada una de ellas, esta es una tarea difícil por la cantidad de información a recabar, por ejemplo: informes estadísticos de salud, seguros, daños, etc.

Análisis de Riesgos

Un análisis del riesgo puede ser efectuado en cualquier momento y tiene como objetivo principal cuantificar las exposiciones existentes a fin de que se establezca una base para una selección posterior de las medidas de control con un costo apropiado.

Los objetivos específicos del análisis de riesgo son:

Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas.

Determinar cuales son los activos existentes.

Efectuar un minucioso análisis de los peligros identificando exposiciones, debilidades y amenazas potenciales.

Identificar, definir y revisar todos los controles de seguridad ya existentes.

Determinar si es necesario incrementar las medidas de seguridad, los costos del riesgo y los beneficios esperados.

Reducir la probabilidad de que ocurra un evento.

Proporcionar los elementos de seguridad y protección adecuada para que en el caso de que acontezca un desastre, los costos en que se incurran no sean tan altos.

En el análisis de riesgos se debe determinar la **probabilidad de ocurrencia** del riesgo y evaluar el **impacto** que tendría en el negocio en el caso de pasar a un siniestro. Este no es trabajo fácil dado que la cantidad de información a recopilar es bastante y los criterios a adoptar para evalurla deben estar acorde a la realidad de la empresa .Muchas veces, determinar la probabilidad de que ocurra un desastre es altamente complicado. Tal determinación depende del conocimiento que se tenga del fenómeno en particular. Todas las circunstancias desconocidas involucran necesariamente un elemento aleatorio. Cuando se da el caso de que los acontecimientos se presentan frecuentemente, el elemento azar puede ser modelado hasta cierto punto.

Entonces, bajo un criterio frecuentista se puede calcular la probabilidad de que ocurra el evento en un momento dado. Sin embargo, la mayoría de los desastres naturales no ocurren con altas frecuencias.

Cuando no se cuenta con información suficiente sobre algún fenómeno, lo que se hace es buscar la opinión de los expertos. Existe el método DELPHI, que consiste en reunir un grupo de expertos en cierto tema y hacerles preguntas sobre el mismo, hasta llegar un consenso.

Por lo general, los eventos con menor probabilidad de ocurrencia son los que pueden llegar a producir mayores daños. Sin embargo, no se deben menospreciar los pequeños eventos ocurridos a diario, ya que muchas veces el costo acumulado de enfrentarlos sobrepasa el costo producido por un desastre de mayor magnitud, y la ocurrencia de dos eventos simultáneamente pude superar con creces el impacto producido por cada uno en forma separada (sinergia).

Es así como a partir de la probabilidad de ocurrencia del riesgo y el impacto que este podría producir se obtiene la exposición al riesgo.

Priorizacion de Riesgos

Esta etapa se lleva a cabo una vez concluida la de análisis de riesgos y tiene como objetivo determinar donde se **centrara el esfuerzo** en nuestro plan de gestión, en función de nuestros recursos y los objetivos de nuestro negocio. Es aquí donde que áreas atacar con mayor fuerza y cuales no tanto , que procesos son críticos para la empresa y cuales no tanto. Esto permitirá establecer que hacer frente al riesgo .

Resolución del Riesgo

Aquí se decide que hacer frente al riesgo, se debe adoptar un camino, con la evaluación del costo que puede tener para seguirlo. Entre las resoluciones que se puede esta:

Evitar que el riesgo exista

- Trasladar el Riesgo (por ej.: pasarlo de un proceso critico a uno que no lo sea)

- Asumir el riesgo (Aquí se establecen planes de contingencia)
- Comunicar el Riesgo
- Recordar el Riesgo
- Eliminar el Riesgo
- Otros

Planificación del Control de Riesgos

El objetivo de la planificación es obtener una serie de medidas (ya sean políticas, planes de contingencia, reglas etc) para limitar los riesgos que atentan contra los SI (disminuir su probabilidad de ocurrencia).

A continuación se enumeran una serie de actividades y tareas para llevar a cabo en esta etapa

Actividad 1: Identificación de mecanismos de seguridad

Tarea 1.1: Identificar mecanismos posibles

Tarea 1.2: Estudiar mecanismos implantados

Tarea 1.3: Incorporar restricciones

Actividad 2: Selección de mecanismos de salvaguarda

Tarea 2.1: Identificar mecanismos a implantar

Tarea 2.2: Evaluar el riesgo (mecanismos elegidos)

Tarea 2.3: Seleccionar mecanismos a implantar

Actividad 3: Especificación de los mecanismos a implantar

Tarea 3.1 (única): Especificar los mecanismos a implantar

Actividad 4: Planificación de la implantación

Tarea 4.1 Priorizar mecanismos

Tarea 4.2: Evaluar los recursos necesarios

Tarea 4.3: Elaborar cronogramas tentativos

Actividad 5: Integración de resultados

Tarea 5.1 (única): Integrar los resultados

Monitoreo de Riesgos

Esta etapa debe estar en continua ejecución y servirá como medio para evaluar los efectos de los mecanismos de seguridad implantados, permitirá ir mejorando el plan de control de riesgos como también permitirá que se reevalúen las probabilidades de ocurrencia de ciertos riesgos, existiendo la posibilidad que algunos desaparezcan o también que surjan nuevos riesgos que obligaran a la empresa a modificar su plan para hacerles frentes.

Plan de Contingencia o Plan Contra emergencias

El objetivo del proceso de generar un Plan de Contingencia es producir un documento denominado *Plan de Contingencia o Gestión*. El cual proporciona la cohesión que permite al grupo de personas encargadas de la recuperación, actuar como un equipo al adjudicar a cada miembro una lista concreta de responsabilidades y procedimientos a seguir ante el surgimiento del problema. Este es uno de los principales elementos que tiene la enfrentar los riesgos que lleguen a ser siniestros.

Disponibilidad de Datos.

Un Plan de Contingencia no incluye, necesariamente, operaciones de copia de seguridad como parte de su contenido, sin embargo, la realización de estas debe ser un requisito previo al Plan de Contingencia. De no ser así, tan sólo se perderá tiempo pensando que es posible recuperar algo. Luego si se quiere pensar en la construcción de un plan se debe considerar alguno de estos puntos con anterioridad:

- Realizar copias de seguridad todos los días y verificar su finalización; la verificación debe efectuarse puesto que existen demasiadas cosas que pueden salir mal en la realización de dichas copias de seguridad. Obviamente, estas copias factibles de recuperar se encontrarán en cintas o discos extraibles.

- Almacenar y renovar regularmente las cintas de seguridad en una ubicación externa para asegurar la recuperación en el caso de un desastre en la instalación principal.
- Familiarizarse con la recuperación de datos a través del sistema de copias de seguridad; las actividades de recuperación pueden acarrear desagradables sorpresas. Luego, se debe conocer de antemano las limitaciones del sistema de copias de seguridad, para no encontrárselas cuando ya sea demasiado tarde.

Metodología para el Plan de Contingencia.

Teniendo en claro el punto anterior, respecto a las copias de seguridad y almacenamiento de datos, tan sólo ahora se puede reflexionar sobre lo que se necesitará en caso de ocurrir un desastre. A continuación se presenta una metodología que puede emplearse para formalizar el proceso dentro de la organización. Los conceptos básicos son los siguientes:

- Análisis de riesgos.
- Valoración de riesgos.
- Asignación de prioridades a las aplicaciones.
- Establecimientos de requerimientos de recuperación.
- Elaboración de la documentación.
- Verificación e implementación del plan.
- Distribución y mantenimiento del plan.

Análisis de Riesgos.

Esta etapa la preocupación esta relacionada con tres simples preguntas:

¿Qué está bajo riesgo?.

¿Cómo se puede producir?.

¿Cuál es la probabilidad de que suceda?.

¿Qué está bajo riesgo?.

Está pregunta necesita incorporar todos los componentes del sistema susceptibles a ser dañados, dando lugar a la pérdida de conexiones, computadores o datos. Un diagrama de la arquitectura de todos los componentes del sistema facilitará la realización de un inventario de los elementos que pueden necesitar ser restituidos después de un desastre. Esto resuelve el problema de todos los dispositivos físicos, sin embargo, no hay que olvidar que el software y la información relevante también deben ser identificados.

Un inventario debiera de ser completo y mostrar en forma clara la complejidad del sistema, hay que tener siempre presente que una omisión en el inventario fácilmente puede dar lugar a una recuperación fallida tras un desastre.

¿Cómo se puede producir?.

La respuesta a esta pregunta varía desde lo evidente hasta lo casi increíble. Las clases más obvias de desastres son los desastres naturales que conllevan tormentas de todo tipo, maremotos, terremotos, etc..

Los propios incendios constituyen uno de los peores y más comunes desastres posibles, el fuego, calor, humo y agua que involucra un desastre de este tipo son tremendamente perjudiciales para los sistemas informáticos.

Los dispositivos de almacenamiento se deterioran fácilmente debido a las altas temperaturas y el humo. La eliminación de los residuos tóxicos tras el incendio de una oficina pueden llevar meses o incluso años. Esto implica que puede no ser posible disponer de los sistemas y datos hasta bastante tiempo después de ocurridos los sucesos.

Deben considerarse mecanismos alternativos de acceso a la red en el caso de que, por alguna razón, sea imposible acceder al edificio, incluso aunque el edificio este de pie y operacional.

Por otro lado, los errores humanos son una de las causas más probables de la pérdida o deterioro de los datos. Si un error de este tipo provoca la pérdida

de un sistema en la red, tiene el mismo efecto que cualquier otro tipo de desastre, y como tal debe ser tratado.

¿Cuál es la probabilidad de que suceda?.

Si fuera posible protegerse contra todas las calamidades, esta pregunta carecería de interés. Sin embargo, no se dispone de recursos infinitos, de hecho, generalmente los recursos son bastante escasos. Por lo tanto se deben seleccionar los tipos de desastres contra los que se intentará proteger al sistema. Obviamente, estos serán los que tengan la mayor probabilidad de afectar a la organización.

Valoración de Riesgos.

Es el proceso de determinar el costo para la organización de experimentar un desastre que afecte a la actividad empresarial.

Los costos de un desastre pueden clasificarse en las siguientes categorías:

- Costos reales de reemplazar el equipo informático; este costo es fácil de calcular y dependerá de si se dispone de un buen inventario de todos los componentes necesarios en la red.
- Costos de producción; pueden determinarse midiendo la producción asociada a la red, la empresa tiene una correcta valoración de la cantidad de trabajo realizado diariamente y su valor relativo, luego, la pérdida de producción debido a la interrupción de la red, puede ser calculada utilizando esta información.
- Costos por negocio perdido; son los ingresos perdidos por las organizaciones de ventas y marketing cuando la red no esta disponible.
- Costos de reputación; son más difíciles .de evaluar, pero, sin embargo, es deseable incluirlos en la valoración. Estos costos se producen cuando los clientes pierden la confianza en la empresa y

crecen cuando los retardos en el servicio son más prolongados y frecuentes.

Asignación de Prioridades a las Aplicaciones.

Después de que un desastre acontece y se inicia la recuperación de los sistemas, debe conocerse que aplicaciones recuperar en primer lugar, no se debe perder el tiempo restaurando los datos y sistemas equivocados cuando la actividad primordial que se desarrolla necesita de otras aplicaciones esenciales.

Esto implica la necesidad de determinar por anticipado cuales son las aplicaciones fundamentales de la organización. Para la determinación de las aplicaciones preponderantes sobre las demás, el plan debe estar asesorado y respaldado por la Dirección, para minimizar las desavenencias entre los distintos departamentos. Este plan debe incluir una lista de los sistemas, aplicaciones y prioridades.

Una vez determinado lo que se va a restaurar, se debe disponer de todo lo necesario para la disponibilidad de tales aplicaciones. Teniendo siempre presente que lo importante es hacerlas funcionar, para lo cual no es, generalmente, necesario que estas estén a un cien por ciento. Es mucho mejor intentar lograr que un sistema pequeño funcione, de esta manera se ahorra gran cantidad de tiempo en el proceso.

Establecimientos de Requerimientos de Recuperación.

La clave de esta fase del proceso del plan de contingencia es definir un periodo de tiempo aceptable y viable para lograr que el sistema esté nuevamente activo. Tal y como se ha planteado en la sección anterior, la preocupación básica debería ser disponer de las aplicaciones más importantes en primer lugar. el personal directivo de la organización deseará

saber cuándo estarán sus aplicaciones funcionando para planificar las actividades de la compañía.

Es muy importante conceder una cantidad de tiempo adecuada y no realizar estimaciones poco realistas sobre las pocas posibilidades. no es el deseo de nadie tener a un montón de gente alrededor esperando la finalización de las operaciones de recuperación; una distracción de este tipo probablemente perturbe las labores. El término para este tiempo es *tiempo de recuperación objetivo* (TRO). El TRO definido debe ser verificado para comprobar que es realista y factible, no sólo por uno mismo, sino por el resto de la organización, que puede ser requerido para realizar el trabajo.

La dirección de la organización debe colaborar íntimamente con el personal de administración del sistema para determinar el TRO de las aplicaciones. Aplicaciones diferentes tendrán TRO diferentes.

Elaboración de la Documentación.

Crear un documento que mucha gente pueda tener como referencia es la clave del plan de plan de contingencia. Esto puede implicar un esfuerzo significativo para algunas personas, pero ayudará a comprender otros aspectos del sistema y puede ser primordial para la empresa en caso de ocurrir un desastre.

El Compromiso de la Dirección

Los recursos necesarios para escribir y mantener un plan de contingencia, necesariamente demandan mucho tiempo. La dirección de la organización debe apoyar la iniciativa para que ésta sea exitosa. Uno de los problemas del plan de contingencia en un entorno computacional es que la tecnología de sistemas cambia tan rápidamente que resulta difícil permanecer al día. Esto incluye nuevos dispositivos, así como nuevos sistemas de aplicación que introducen su propio nivel de complejidad en este campo.

Dado que la tecnología informática evoluciona tan rápidamente, debe planificarse la actualización del plan de contingencia periódicamente; por

ejemplo, una vez al año. aunque la redacción del plan inicial supondrá una gran cantidad de trabajo, una vez que se dispone del plan, las actualizaciones son relativamente fáciles.

Contenidos del Plan de Contingencia

El plan de contingencia de un sistema informático debe intentar definir las siguientes cinco áreas:

- Listas de notificación, números de teléfono, mapas y direcciones; hay que cerciorarse de que se sabe a quién notificar en primer lugar cuando ocurre un desastre, mapas mostrando las ubicaciones del centro de instalaciones temporal y las instalaciones externas.
- Prioridades, responsabilidades, relaciones y procedimientos; al responder a un desastre en primer lugar hay que centrarse en las prioridades establecidas, el trabajo debe empezar por recuperar inmediatamente las aplicaciones de mayor prioridad, las personas deben disponer de instrucciones y responsabilidades precisas, además la relación entre tareas debe hallarse documentada de manera que pueda identificarse cualquier contratiempo que pudiera surgir, finalmente deben incluirse, detalladamente, los procedimientos que muestren las labores de instalación y recuperación necesarias, debiendo ser fáciles de leer y seguir.
- Información sobre adquisiciones y compras; debe saberse cómo expedir una solicitud de compra y obtener los equipos para el centro de operaciones temporal, esto significa proporcionar a los vendedores la dirección y cualquier instrucción necesaria para el transporte.
- Diagramas de red; estos simplifican en gran medida la labor de construir una red, un diagrama detallado de la red facilita y agiliza la reanudación de las actividades.
- Sistemas, configuraciones y copias de seguridad en cintas; es posible ahorrar mucho tiempo en el proceso de recuperación si existe la posibilidad de almacenar algunos sistemas de repuesto para

diferentes tareas, si se desconocen los productos que los usuarios tienen en sus computadores, un inventario de red puede ayudar en la recopilación de esta información, después que la red alternativa se encuentre funcionando será posible restaurar los computadores con sus configuraciones anteriores utilizando la información de configuración extraída de los informes de inventario, además hay que asegurarse la disponibilidad de un sistema de copias de seguridad de cinta en funcionamiento, en este caso estos sistemas deben mantenerse constantemente actualizados.

Verificación e Implementación del Plan.

Una vez redactado el plan, hay que probarlo. Se debe estar seguro de que el plan va a funcionar. Para ello, se debe ser escéptico y situarse de manera imparcial ante la fiabilidad del plan de tal forma de realizar las pruebas que permitan encontrar problemas para así perfeccionar el plan de contingencia.

Comprobación del Plan por Partes

Para ello no es necesario desconectar el sistema algún día para ver si el plan de contingencia es capaz de recuperarlo. existen muchas y mejores formas e verificarlo sin causar mayores interrupciones en el trabajo de la organización. Por ejemplo, se puede ahorrar mucho tiempo posteriormente con tan solo llamar a los números telefónicos incluidos en las listas del plan para confirmar si están vigentes, entre estos números tenemos a los vendedores a los cuales se le puede comprobar si disponen de los productos que se pueden llegar a requerir para nuestro sistema, puesto que los inventarios de estas empresas proveedoras pueden ir variando.

Por supuesto, también es necesario verificar los procedimientos que se emplearán para verificar los datos. Comprobándose el SW para la realización de las copias de seguridad, para confirmar si pueden recuperarse las

aplicaciones de mayor prioridad de la manera esperada. Esto debería hacerse en una red aislada para evitar problemas con el servidor.

Una vez recuperada la información, verifíquese si el usuario puede acceder a ella. Esto requiere de algunas estaciones de trabajo conectadas a la red para simular auténticos usuarios finales con cuentas en los servidores originales. En este punto, puede ser necesario actualizar el plan para incluir información sobre el establecimiento de cuentas de usuario.

Como habíamos dicho anteriormente debe realizarse un chequeo sobre las operaciones de copias de seguridad verificando la finalización correcta de las mismas. Además, supervisar esto asegurándose de que las personas de la organización saben realizar las copias de seguridad adecuadamente y comprobar su finalización. Recordar que esta es la base para el desarrollo del plan de contingencia, puesto que sin la realización de esta no habría una información real que recuperar.

Distribución y Mantenimiento del Plan.

Por último, cuando se disponga del plan definitivo ya verificado, es necesario distribuirlo a las personas encargadas de llevarlo a cargo. Tratando siempre de controlar que todas ellas posean la última versión del plan que les concierne, de manera que no exista confusión producto de otras versiones. Así mismo, es necesario asegurar la disponibilidad de copias extras del plan para su depósito en alguna instalación exterior o en cualquier otro lugar además del lugar de trabajo.

Habrá que tener una lista de todas las personas que interactuarán en el plan de gestión junto con los teléfonos y lugares donde se encontrarán con mayor probabilidad en las distintas horas del día. cuando se utilice el plan, deberán restituirse todas las copias y recoger las versiones antiguas.

El mantenimiento del plan es un proceso sencillo. se comienza con una revisión del plan existente y se examina en su totalidad realizando los

cambios a cualquier información que pueda haber variado en al sistema y agregando los cambios que fuesen hechos. Se vuelve a evaluar los sistemas de aplicación y determinar cuales son los más importantes de la organización. Las modificaciones en esta parte del plan causarán modificaciones consecutivas a los procedimientos de recuperación.

Este proceso llevará tiempo, pero posee algunos valiosos beneficios que se percibirán aunque nunca tengan que utilizarse. Más gente conocerá el sistema lo cual proporcionará a la organización una base técnica más amplia para mantenerlo correctamente.

Utilización de los Recursos Existentes

Se debe tener presente que pueden existir recursos disponibles no conocidos que ayuden a realizar el plan de contingencia. En ocasiones, las grandes compañías cuentan con empleados con responsabilidades como "Planificador de contingencias" o " Planificador para la continuidad de la actividad" asignados a la tarea de estudiar y planificar la reanudación de las actividades de la compañía tras una catástrofe. Sus trabajos no están enfocados directamente a recuperar sistemas informáticos, pero ellos, ciertamente, deben saber bastante sobre cómo definir los planes de los recursos y servicios. si se dispone de este tipo de recurso dentro de la organización, se puede ahorrar gran cantidad de tiempo utilizando su preparación y conocimiento.

Cabe destacar que como todas las cosas que necesitan disciplina y práctica, restablecer un sistema de comunicaciones después de un desastre requiere de práctica y análisis para tener aptitudes y poder realizarlo con un alto nivel de experiencia. Probablemente, llevó años construir y diseñar la actual red; de repente, será necesario reconstruir la red en unos días. Esto requerirá toda la pericia disponible para que sea un éxito.

CONCLUSIONES

Los Mecanismos de Seguridad de la Información buscan proteger a la información de las diversas amenazas a las que se ve enfrentada. De acuerdo con las tendencias actuales la información se ve amenazada cada día por una cantidad mayor de factores que definitivamente pueden producir una situación catastrófica dentro de la CPD, y esto indudablemente afectaría a la Organización.

Es responsabilidad del Administrador de la Información definir, comunicar y controlar los riesgos que existen para así asignarle una mayor confiabilidad a las personas de la empresa que trabajan con los datos. Además, debe luchar contra un conjunto de factores de diversa naturaleza que pueden impedir que la información sea protegida, entre ellos podemos mencionar:

- La Organización no le da realmente a la Seguridad de la Información la importancia que merece
- No existe una conciencia de parte tanto de los Administradores, como de los Usuarios que ayuden a cumplir con los objetivos de las políticas
- Existe incompetencia o desconocimiento por parte de los Administradores

Las amenazas a la información pueden ser de origen diverso, ya que –como se mencionó anteriormente- con los tiempos se van generando nuevas formas de daño a ella. Hay amenazas de origen natural (terremotos, tormentas, etc.), origen humano (deseos de venganza, problemas psicológicos, entre otros) y origen técnico (fallas de SW, alta tensión,…). Esto lleva a que la función de definir los planes a seguir en cuestión de seguridad debe ser una tarea realmente completa.

Concluyendo, la puesta en marcha de los planes a seguir es responsabilidad del encargado de la seguridad, pero también debe existir un compromiso de parte de los usuarios de sistema de información, ejecutivos y todas las personas que de alguna u otra forma ayudan a que este sistema satisfaga a los requerimientos que se ve enfrentado, manteniendo sobretodo la integridad y confidencialidad (si es necesario) de la información.

ANEXO

CONSEJO DE PROTECCION GENERAL

El Centro de Alerta Temprana Antivirus, órgano de prevención y fomento de la seguridad en internet, propone una serie de reglas para proteger los nuevos equipos y conexiones. Con ello se pretende que desde el primer día de uso, los nuevos internautas puedan navegar seguros y establecer sus comunicaciones de correo electrónico sin temor a ver infectados sus computadores de forma sorpresiva.

1. **Instale un cortafuegos:** un cortafuegos o 'firewall' es un software destinado a garantizar la seguridad en sus comunicaciones vía Internet. El cortafuegos bloquea las entradas sin autorización a su ordenador y restringe la salida de información. Instale un software de este tipo antes de conectar su equipo a Internet o a otras redes.
2. **Use el Antivirus:** antes de conectar su ordenador a Internet, compruebe que cuenta con un antivirus instalado. Este antivirus puede estar incluido en las aplicaciones propias de su PC, o ser un servicio más de su proveedor de Internet.
3. **Haga copias de seguridad.** Es la medida más sensata para asegurarse que no pierde información que pueda verse afectada por algún virus.
4. **Actualice su sistema operativo y el software:** compruebe que el sistema operativo que instale en su ordenador es la última versión del mismo, de tal forma que incluya todas las aplicaciones de seguridad previstas. Puede actualizar su sistema operativo en la página web del CATA (alerta-antivirus.red.es). Actualice también el software: todas las

compañías del sector publican actualizaciones de sus productos de forma regular; además, la web del CATA ofrece acceso a las últimas versiones.

5. **Tenga cuidado con los mensajes que le soliciten contraseñas y nombres de usuario.** El 2004 ha registrado un importante incremento de los casos de 'phising' (envíos en forma de correo electrónico que le piden sus claves o contraseñas para acceder de forma fraudulenta a su cuenta bancaria). Hay que tener en cuenta que ninguna entidad bancaria emplea ese método.
6. **Utilice software legal:** es seguro, en tanto que las copias piratas tienen grandes riesgos ante problemas de seguridad.
7. **Vigile su correo electrónico:** desconfíe de aquellos correos que le lleguen en otros idiomas. Desconfíe de los correos de procedencia desconocida, o que ofrecen productos mágicos, vacaciones gratuitas, o fotos que no debe dejar de ver. Verifique el origen de los correos electrónicos: es habitual en los virus actuales 'robar' la libreta de correo de algún amigo suyo. Si recibe un mensaje de un conocido con un 'Asunto' poco habitual en él, compruebe su procedencia real antes de abrirlo.
8. **Desconfíe de los mensajes repetidos:** si recibe dos o más correos con remites diferentes y un mismo asunto, puede tratarse de un virus que disimula su origen. Compruebe en la web del CATA si se trata de mensajes ya detectados como virus.
9. **Evite las ventanas indeseadas:** si no desea ver las ventanas publicitarias emergentes que en ocasiones se disparan al navegar por Internet, no olvide instalar las aplicaciones que lo evitan, disponibles también en la web del CATA.
10. **Compras a través del comercio electrónico:** Lo más recomendable a la hora de utilizar el comercio electrónico es que la web donde se realicen las compras online esté dotada de medidas de seguridad

certificadas y reconocidas. El Centro de Alerta sugiere utilizar una única tarjeta para comprar en Internet y mantenerla con el saldo mínimo necesario. Es importante informarse periódicamente de los movimientos bancarios registrados en las cuentas.

11. **Para los usuarios más jóvenes que estrenan al ordenador o que utilizan Internet por primera vez:** Los jóvenes que estrenen ordenador o se conecten por primera vez a Internet debe estar acompañados por sus progenitores. Padres e hijos comprobarán juntos que el PC está correctamente protegido. Si el menor de edad accede a Internet por primera vez, Red.es pone a su disposición el portal www.chaval.es para iniciarle de forma segura y pedagógica.
12. **Para mayor seguridad de los padres** existen herramientas que permiten a los progenitores limitar la visualización de determinados contenidos. Los documentos adjuntos en el correo electrónico, las redes de intercambio P2P, los chats y los sitios web de juegos online pueden traer consigo software espía, programas nocivos y enlaces a contenidos maliciosos.
13. **Manténgase informado:** la información es la mejor vacuna. Esté atento a los medios de comunicación y visite las páginas del Centro de Alerta Antivirus de forma habitual.