O

UNIVERSIDAD DE SOTAVENTO, A.C.

ESTUDIOS INCORPORADOS A LA UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE INFORMÁTICA

"DESARROLLO DEL PLAN DE SEGURIDAD INFORMÁTICA PARA EL DEPARTAMENTO DE SISTEMAS DE LA EMPRESA EL HILO NEGRO S.A DE C.V"

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

MIGUEL ANGEL HERNÁNDEZ MARTÍNEZ

ASESOR DE TESIS

LIC. RAÚL OCAMPO COLÍN

COATZACOALCOS, VER. SEPTIEMBRE 2007

AGRADEZCO DE TODO CORAZÓN:

A DIOS POR QUE SE QUE NUNCA ME ABANDONA Y ME DIO FUERZAS PARA PODER CONSOLIDAR ESTE PROYECTO.

A MIS PADRES POR QUE HAN HECHO DE SU ESFUERZO TODA UNA REALIDAD

A MIS HERMANOS POR TODO EL APOYO MORAL QUE ME BRINDARON

A MI ESPOSA POR SU PACIENCIA Y APOYO.

GRACIAS!!!

PROBLEMÁTICA

En la época actual los puntos importantes en cuanto a la problemática siguen siendo similares: los mismos desafíos, mayores responsabilidades, pocos recursos, nivel de maduración, regulaciones.

El mercado aparentemente no reacciona ante los problemas de seguridad informática, vulnerabilidades básicas siguen apareciendo en los programas, los administradores todavía no realizan upgrades y no aplican patches a los sistemas y los usuarios siguen haciendo click sobre los archivos adjuntos enviados por correo electrónico.

Las empresas no pueden solucionar los problemas de seguridad porque si lo hacen, las aplicaciones críticas que están en producción entran en crisis y los proveedores siguen tratando de explicar que tener permisos habilitados para todo el mundo, utilizar usuarios genéricos y guardar passwords en plano, no es tan inseguro.

JUSTIFICACIÓN

El presente proyecto de investigación esta elaborado para cumplir dos objetivos específicos, el primero es obtener la acreditación de licenciado en el área de Informática Administrativa, ya que de esta manera se cumple al 100% con el propósito de la ética profesional.

El segundo objetivo es poder mostrar una vez más a través de este escrito la importancia de la seguridad informática en la actualidad, programas espías que roban información la cual envían a su creador (spam), virus que destruyen datos (troyanos), son solo alguno de los términos que son utilizados hoy en día no solo por los expertos en el área de la computación, si no en la vida cotidiana de cualquier ser Humano que en su trabajo diario dependa de una PC.

Día a día empresas importantes pierden millones de dólares solo por que un intruso (hacker) ya entró a su sistema y causa perdidas de datos muy valiosas para la entidad, pero no se necesita ser un hacker para poder penetrar y destruir sistemas, pueden ser empleados comunes que sin ningún conocimiento en el área de programación de virus, provoquen daños a la empresa, esto sin contar también con los fenómenos naturales, los cuales pueden causar desastres inesperados para las instituciones y de esta manera dejar en la ruina a mas de un inversionista.

Y por último no solo un problema lógico (virus) puede causar estragos, también uno físico (robo de hardware), es por esto que se definirá de una manera general los lineamientos para la establecimiento de políticas, análisis y estrategias de seguridad informática mas importantes para que se puedan aplicar en las instituciones y hacer de la seguridad un problema que pueda ser monitoreado y controlado, aunque la “seguridad real” no exista.

INDICE

PAG.

7.3.2 INGENIERÍA SOCIAL INVERSA
7.3.3 TRASHING (CARTONEO)
7.3.4 ATAQUES DE MONITORIZACIÓN
7.3.4.1 SHOULDER SURFING
7.3.4.2 DECOY (SEÑUELOS)
7.3.4.3 SCANNING (BÚSQUEDA)
7.3.4.3.1 TCP CONNECT SCANNING
7.3.4.3.2 TCP SYN SCANNING
7.3.4.3.3 TCP FIN SCANNIG – STEALTH PORT SCANNING
7.3.4.3.4 FRAGMENTATION SCANNING
7.3.4.3.5 EAVESDROPPING- PACKET SNIFFING
7.3.4.5 SNOOPING- DOWNLOADING
7.4.5 ATAQUES DE AUTENTIFICACIÓN
7.4.5.1 SPOOFING-LOOPING
7.4.5.2 SPOOFING
7.4.5.3 IP SPOOFING
7.4.5.3.1 DNS SPOOFING
7.4.5.4 WEB SPOOFING
7.4.5.5 IP SPLICING – HIJACKING
7.4.5.6 UTILIZACIÓN DE BACKDOORS
7.4.5.7 UTILIZACIÓN DE EXPLOITS
7.4.5.8 OBTENCIÓN DE PASSWORDS
7.4.5.8.1 USO DE DICCIONARIOS
7.4.6 DENIAL OF SERVICE (DOS)
7.4.6.1 JAMMING O FLOODING
7.4.6.2 SYN FLOOD
7.4.6.3 CONNECTION FLOOD
7.4.6.4 NET FLOOD
7.4.6.5 LAND ATTACK
7.4.6.6 SMURF O BROADCAST STORM
7.4.5.7 OBB, SUPERNUKE, O WINNUKE
7.4.6.8 TEARDROP I Y II – NEWTEAR – BONK – BOINK
7.4.6.9 MAIL BOMBING – SPAMMING
7.4.7 ATAQUES DE MODIFICACIÓN-DAÑO
7.4.7.1 TAMPERING O DATA DIDLING
7.4.7.2 BORRADO DE HUELLAS
7.4.7.3 ATAQUE MEDIANTE JAVA APPLETS
7.4.7.4 ATAQUES CON JAVASCRIP Y VBSCRIP
7.4.7.5 ATAQUES MEDIANTE ACTIVE X
7.4.7.6 VULNERABILIDADES DE LOS NAVEGADORES
7.4.8 ERRORES DE DISEÑO, IMPLEMENTACION Y OPERACIÓN
7.4.9 IMPLEMENTACIÓN DE ESTAS TECNICAS
7.4.10 ¿CÓMO DEFENDERSE DE ESTOS ATAQUES?
7.5 CREACIÓN Y DIFUSIÓN DE VIRUS
7.5.1 VIRUS INFORMÁTICOS VS VIRUS BIOLÓGICOS
7.5.2 ORIGEN
7.5.3 LOS NÚMEROS HABLAN
7.5.4 DECRIPCIÓN DE UN VIRUS
7.5.4.1 TÉCNICAS DE PROPAGACIÓN
7.5.4.2 TIPOS DE VIRUS

8.7 SISTEMAS ANTI – SNIFFERS
8.8 GESTION DE CLAVES “SEGURAS”
8.8.1 NORMAS DE ELECCIÓN DE CLAVES
8.8.2 NORMAS PARA PROTEGER UNA CLAVE
8.8.3 CONTRASEÑAS DE UN SOLO USO
8.9 SEGURIDAD EN PROTOCOLOS Y SERVICIOS
8.9.1 NETBIOS
8.9.2 ICMP
8.9.3 FINGER
8.9.4 POP
8.9.5 NNTP
8.9.6 NTP
8.9.7 TFTP
8.9.8 FTP
8.9.8.1 FTP ANÓNIMO
8.9.8.2 FTP INVITADO
8.9.9 TELNET
8.9.10 SMTP
8.9.11 SERVIDORES WWW.
8.10.1 CRIPTOLOGIA –HISTORIA
8.10.2 CRIPTOGRAFIA
8.10.3 CRIPTOANALISIS
8.10.4 CRIPTOSISTEMA
8.10.4.1 TRANSPOSICIÓN
8.10.4.2 CIFRADOS MONOALFABETICOS
8.10.4.2.1 ALGORITMO DE CESAR
8.10.4.2 SUSTITUCIÓN GENERAL
8.10.5 ALGORITMOS SIMETRICOS MODERNOS (LLAVE PRIVADA)
8.10.5.1 REDES DE FIESTEL
8.10.5.2 DES
8.10.5.2.1 DES MÚLTIPLE
8.10.5.3 IDEA
8.10.5.4 BLOWFISH
8.10.5.5 RC5
8.10.5.6 CAST
8.10.5.7 RIJNDAEL (EL NUEVO ESTANDAR AES)
8.10.5.8 CRIPTOANALISIS DE ALGORITMOS SIMETRICOS
8.10.6 ALGORITMOS ASIMETRICOS (LLAVE PRIVADA PUBLICA)
8.10.6.1 RSA
8.10.6.1.1 ATAQUES A RSA
8.10.6.2 CURVAS ELÍPTICAS (CEE)
8.10.7 AUTENTIFICACIÓN
8.10.7.1 FIRMA DIGITAL
8.10.7.1.1 MD5
8.10.7.1.2 SHA-1
8.10.8 PGP (PRETTY GOOD PRIVANCY)
8.10.8.1.1 ANILLOS DE CLAVES
8.10.8.1.2 CODIFICACION DE MENSAJES
8.10.8.1.3 DECODIFICACIÓN DE MENSAJES
8.10.8.1.4 COMPRESIÓN DE ARCHIVOS

CAPITULO I

INTRODUCCION

"Ser lo que soy, no es nada sin la seguridad". Sin duda W.Shakespeare (1564-1616) tenía un concepto mas evolucionado de la seguridad que sus contemporáneos del siglo XV y quizás también que algunos de los nuestros.

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

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

El motivo del presente, es desarrollar un estudio completo referente a seguridad informática, enfocado a la empresa El Hilo Negro SA de CV, con el cual se podrá tener la información necesaria para llevar a cabo la implementación de políticas estrictas en cuanto a la utilización de los equipos de cómputo, e incrementar la cultura informática en cuanto a seguridad de cada uno de los usuarios que desempeñan actividades diferentes dentro de la organización. Se expondrán metodologías y completos planes de estrategias que si bien no resolverán el problema de la seguridad al menos podrán tapar "el agujero" que conlleva al hablar de seguridad informática para las empresas y específicamente de la institución para la que se esta realizando este estudio.

La mayoría de las empresas que manejan en su organigrama un departamento de sistemas desconocen la magnitud del problema al que se enfrentan, y eso trae como consecuencia que no inviertan ni en capital humano y económico necesario para prevenir el daño y/o pérdida de su información que al final de cuentas es la razón de ser de la misma.

La empresa El Hilo Negro SA de CV demanda el uso de un sistema de seguridad informático que le brinde un campo de acción "limpio" en el que pueda desarrollar sus operaciones importantes, y la finalidad del estudio es proporciónale lo necesario para satisfacer esta petición.

ANTECEDENTES

La empresa El Hilo Negro, se estableció en junio de 1999, como la visión de dos jóvenes emprendedores, cuya finalidad era hacer mejoras en la distribución de la línea de ropa para su venta en las boutiques de la cadena restaurantera Anderson's una de las más importantes a nivel nacional e internacional.

La empresa comenzó a funcionar con un contrato con la empresa "Vaporeto S. A. de C. V." Esta firma tenía la exclusiva de ventas para estas boutiques de ropa y accesorios. Dicho contrato le permitió bordar y estampar prendas para su venta exclusivamente en las tiendas del caribe mexicano.

Surgió la oportunidad de adquirir un taller de serigrafía completamente montado, el cual fue adquirido y montado en la ciudad de Cancún, Quintana Roo, lo cual permitió la expansión de la empresa, y llegar a ser el principal distribuidor del grupo Anderson's.

CAPITULO 1

1.1 EVOLUCION DEL TÉRMINO SEGURIDAD

La "seguridad es una necesidad básica. Estando interesada en la prevención de la vida y las posesiones, es tan antigua como ella"[1].

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 a.c) o el Hammurabi (2000 a.c). También la

[1] Presentación del libro "Seguridad: una introdución" Dr MANUNTA, Giovanni. Consultor y Profesor de Seguridad de cranfield University. Revista Seguridad Corporativa. http://www.seguridadcorporativa.org.

Biblia, Homero, Cicerón, cesar han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

Los descubrimientos arqueológicos marcan, sin duda, las mas importantes pruebas de seguridad de los antiguos: las pirámides egipcias, el palacio de Sargon, el templo Karnak en el valle del Nilo; el dios anubis representado con una lleve en su mano.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo, para eliminar o evitar la causa. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar alarmar y reaccionar ya eran manejados por ellos.

Como todo concepto, la seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias, y esto se convirtió en un elemento limitante para huir. Se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las perdidas eran inaceptables contra las posibles ganancias.

El próximo paso de la seguridad fue la especialización. Así nace la Seguridad Externa (aquella que se preocupa por la amenaza de entes externos a la organización); y la Seguridad Interna (aquella preocupada por las amenazas de nuestra organización con la organización misma). De estas dos se pueden desprender la Seguridad Privada y Pública al aparecer el estado y depositar su confianza en unidades armadas.

Desde el siglo VXIII, los descubrimientos científicos y el conocimiento resultante de la imprenta han contribuido a la cultura de la seguridad. Los principios de probabilidad, predicción y reducción de fallos y pérdidas han traído una nueva luz a los sistemas de seguridad.

La seguridad moderna se originó con la Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero del Menagement, Henry Fayol en 1919 identifica la seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva.

Al definir el objetivo de la seguridad Fayol dice: "…salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Es, generalmente hablando, todas las medidas para conferir la requerida Paz y tranquilidad (peace of mind) al personal".

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los "cerebros electrónicos", esta mentalidad se mantuvo, porque ¿quién seria capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?..

Hoy la seguridad desde el punto de vista legislativo, esta en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera. Este proceso ha

logrado importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre Seguridad.

En cambio desde el punto de vista técnico, la seguridad está de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

Es en este proceso en donde se aprecia que no se ha añadido ningún nuevo elemento a los ya conocidos en la antigüedad; los actuales son innovaciones de aquellos: llaves, cerraduras, cajas fuertes, puertas blindadas, trampas, etc.

1.2 PUNTO DE PARTIDA

Conceptos como seguridad son "turbios" o su definición se maneja con cierto grado de incertidumbre teniendo diferente significado para distintas personas. Esto tiene la peligrosa consecuencia de que la función de seguridad puede ser frecuentemente catalogada como inadecuada o negligente, haciendo imposible a los responsables justificar sus técnicas ante reclamos basados en ambigüedades de conceptos y definiciones.

"la seguridad es hoy día una profesión compleja con funciones especializadas"[2].

Para dar una respuesta satisfactoria es necesario eliminar la incertidumbre y distinguir entre la seguridad filosófica y la operacional o práctica.

Como es de conocimiento de todos los problemas nunca se resuelve: la energía del problema no desaparece, sólo de transforma y la "solución" estará dada por su transformación en problemas diferentes, más pequeños y aceptables. Por ejemplo: la implementación de un sistema informático puede solucionar el problema de velocidad de procesamiento pero abrirá problemas como el de personal sobrante o reciclable. Estos a su vez, descontentos pueden generar un problema de seguridad interno.

Analicemos. En el problema planteado pueden apreciarse tres figuras[2]:

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

Luego, la Seguridad **se definirá como:**

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

Algunas aclaraciones:

1. **El protector no siempre es el poseedor de valor.**
2. **El agresor no siempre es el aspirante a poseedor.**
3. **Ambas figuras pueden ser delgadas a terceros por el cambio de otro valor, generalmente dinero.**
4. **El valor puede no ser algo concreto. Por ejemplo se podría querer cuidar el honor, la intimidad el conocimiento, etc.**

[2] Presentación del libro "Seguridad: una introdución" Dr MANUNTA, Giovanni. Consultor y Profesor de Seguridad de cranfield University. Revista Seguridad Corporativa. http://www.seguridadcorporativa.org.

5. **La situación global indica que no será lo mismo el robo de un comercio en Argentina que en Andorra en donde sus habitantes se ven obligados a robar para subsistir.**

Los competidores se pueden subdividir en:

- Competidor interno: **es aquel que piensa que el interés de la organización está por encima de sus intereses y, por lo tanto, actúa para sobreponer su interés personal, provocando daños a la organización.**
- Competidor externo: **es aquel que actúa para arrebatar al poseedor lo que para él significa un valor empresarial o personal (clientes, mercado, información, etc.).**

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

En el plano social, comercial e industrial hemos evolucionado técnica y científicamente desde una era primitiva agrícola a una era postmoderna tecnológica, pero utilizando los mismos principios (e inclusos inferiores) a la época de las cavernas en el ambiente virtual:

No es mi interés en el presente texto iniciar mis argumentaciones explicando la evolución y cambios que ha causado la última de las tres grandes revoluciones de la humanidad, la revolución de la era de la información, ("Tercera Ola"); que sigue a las anteriores revoluciones agrícola e industrial. Pero sí está en mi interés demostrar en que medida nos crea un nuevo problema, el de la Seguridad Informática. Y también es mi interés demostrar que ella, como tal, para las organizaciones y empresas, todavía no existe"[3].

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

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

Luego:

"el objetivo de la seguridad informática será mantener la integridad, disponibilidad, privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora."

[3] TOFFLER, Alvin. La Tercera Ola. Editorial Sudamericana. España. 1998.

Contrario a lo que se piensa, este concepto no es nuevo y nació con los grandes centros de cómputos. Con el pasar de los años, y como se sabe, las computadoras pasaron de ser grandes monstruos, que ocupaban salas enteras, a pequeños elementos de trabajo perfectamente ubicables sobre un escritorio de oficina. En este proceso de digitalización y miniaturización llamado "downsizing" la característica mas importante que se perdió fue la seguridad.

Los especialistas de Seguridad Informática de hoy se basan en principios de aquellos antiguos MainFrames (grandes computadoras).

1.2.1 ANÁLISIS DEL OBJETIVO DE SEGURIDAD INFORMÁTICA

Para comenzar el análisis de Seguridad Informática se deberá conocer las características de lo que se pretende proteger: la información.

De esta manera, definimos Dato **como "la unidad mínima con la que compone cierta información. Datum es una palabra latina, que significa "lo que se da".**

La Información. **"es una agregación de datos que tiene un significado específico más allá de cada uno de éstos"[4], y tendrá un sentido particular según como y quien lo procese.**

Ejemplo: 2, 4, 3 y 5 son datos; su agregación 2435 es información.

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

Existe información que debe o puede ser Pública: puede ser visualizada por cualquier persona (por ejemplo índice de asesinatos en un país), y aquella que debe de ser privada sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo archivos del departamento de Recurso de personal). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la información:

1. **Es crítica: es indispensable para garantizar la continuidad operativa**
2. **Es valiosa: es un activo con valor en si misma.**
3. **Es sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.**

[4] CALVO, Rafael Fernández. Glosario Básico Ingles-Español para usuarios de Internet. 1994-2005 http://www.ati.es/novatica/glointv2.html

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

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

La Privacidad **o** Confidencialidad **de la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).**

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 válida 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 relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- Protección a la Réplica**: por medio de la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que recibieron múltiples peticiones del mismo remitente original.**
- No Repudio**: mediante el cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o 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 qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuándo las realiza.**

Cabe definir 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 conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

1. La prevención (antes)**: mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.**
2. La detección (durante)**: mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoria.**
3. La recuperación (después)**: mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionando normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizas.**

Las preguntas que se hace un técnico en sistemas de información ante un problema de seguridad, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, sólo lo transforma o retrasa. La amenaza o riesgo sigue allí y las preguntas que este técnico debería hacerse son:

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

Para responderlas definiremos Riesgo **como "la proximidad o posibilidad de daño sobre un bien".**

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales cada riesgo debería ser atacado de las siguientes maneras:

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

Luego el Daño **es el resultado de la amenaza; aunque esto es sólo la mitad del axioma. El daño también es el resultado de la no-acción, o acción defectuosa, del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza pero también para la figura del protector.**

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

La seguridad indicará el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas imposible) en un 100% por lo que sólo se habla de Fiabilidad **y se la define como "la probabilidad de que un sistema se comporte tal y como se espera de él"[5], y se habla de Sistema Fiable en vez de sistema seguro.**

Luego para garantizar que un sistema sea fiable se deberá garantizar las características ya mencionadas de Integridad, Operatividad, Privacidad, Control y Autenticidad. Se deberá conocer "qué es lo que queremos proteger", "de quien lo queremos proteger", "cómo se puede lograr esto legislativa y técnicamente"; para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución (¿anulación?) de los riesgos.

Comprender y conocer de seguridad ayudará a llevar a cabo análisis sobre los riegos, las Vulnerabilidades, Amenazas y Contramedidas; evaluar la ventaja o desventaja de la situación; a decir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base a las necesidades de seguridad.

Es importante remarcar que cada una de estas técnicas parten de la premisa de que no existe la el 100% de seguridad esperado o deseable en estas circunstancias. (por ejemplo: al salir de viaje ¿estamos 100% seguros que nada nos pasara?.

1.2.2 SISTEMAS DE SEGURIDAD

En los siguientes capítulos se estudiarán las distintas funciones que se deben asegurar en un sistema informático.

1. Reconocimiento: **cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso se quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta quede registrada.**
2. Integridad**: un sistema integro es aquel en el que todas las partes que lo constituyen funcionan en forma correcta y en su totalidad.**
3. Aislamiento**: los datos utilizados por un usuario deben ser independientes de los de otro física y lógicamente (usando técnicas de ocultación y/o compartimiento). También se debe lograr independencia entre los datos accesibles y los considerados críticos.**
4. Auditabilidad**: procedimiento utilizado en la elaboración de exámenes demostraciones, verificaciones o comprobaciones del sistema. Estas comprobaciones deben ser periódicas y tales que brinden datos precisos y aporten confianza a la dirección. Deben apuntar a contestar preguntas como:**
    - **¿El uso del sistema es adecuado?**
    - **¿El sistema se ajusta a las normas internas y externas vigentes?**
    - **¿Los datos arrojados por el sistema se ajustan a las expectativas creadas?**

[5] HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital – www.kriptopolis.com

- **¿Todas las transacciones realizadas por el sistema pueden ser registradas adecuadamente?**
- **¿Contienen información referentes al entorno: tiempo, lugar, autoridad, recurso empleado, etc.?**

5. Controlabilidad**: todos los sistemas y subsistemas deben estar bajo control permanente.**
6. Recuperabilidad**: en caso de emergencia, debe existir la posibilidad de recuperar los recursos perdidos o dañados.**
7. Administración y Custodia**: la vigilancia nos permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una realimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.**

1.2.3 ¿DE QUIENES DEBEMOS PROTEGERNOS?

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

Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita[6] contesta lo siguiente:

"Los tipos de intrusos podríamos caracterizarlos desde el punto de vista del nivel de conocimiento, formando una pirámide.

1. Clase A: **el 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, están jugando (…) son pequeños grupitos que se juntan y dicen vamos a probar.**
2. Clase B: **es el 12% son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo está usando la victima, testean las vulnerabilidades del mismo e ingresan por ellas.**
3. Clase C: **es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.**
4. Clase D: **el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.**

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

1.2.4 ¿QUÉ DEBEMOS PROTEGER?

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

Por hardware **entendemos el conjunto de todo lo material del sistema informático: cpu, cableado, impresoras, CD-ROM, cintas, componentes de comunicación.**

[6] ARDITA, Julio Cesar. Director de Cybsec S.A Security System y ex-Hacker http://www.cybsec.com

El software **son todos los elementos lógicos que hacen que funcione el hardware: sistema operativo, aplicaciones, utilidades.**

Entendemos por datos **al conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos.**

Además, generalmente se habla de un cuarto elemento llamado fungible**; que es todo aquello que se gasta o desgasta con el uso continuo: papel, tóner, 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, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde 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 copias de seguridad, y aún así es difícil de devolver los datos a su forma anterior al daño.

Para cualquiera de los elementos descriptos existen multitud de amenazas y ataques que se los puede clasificar en:

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

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

    Es posible evitar el éxito, si bien no el ataque, mediante el cifrado de la información y otros mecanismos que se expondrán posteriormente.

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

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

Con demasiada frecuencia se cree que los piratas son los únicos que amenazan nuestro sistema, siendo pocos los administradores que consideran todos los demás riesgos analizados en el presente.

1.2.5 RELACIÓN OPERATIVIDAD - SEGURIDAD

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

Para ilustrar lo antes dicho imaginemos una computadora "extremadamente" segura:

- **Instalada a cierta distancia de profundidad de la tierra.**
- **Aislada de otras computadoras.**
- **Aislada eléctricamente y alimentada por un sistema autónomo de triple reemplazo.**

Ahora imaginemos la utilidad de está "súper Segura" computadora: tendiente a nula.

Con esto refleja que la seguridad y la utilidad de una computadora son inversamente proporcionales; es decir que incrementar la seguridad es un sistema informático, su operatividad desciende y viceversa.

$$\text{Operatividad} = \frac{1}{\text{Seguridad}}$$

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

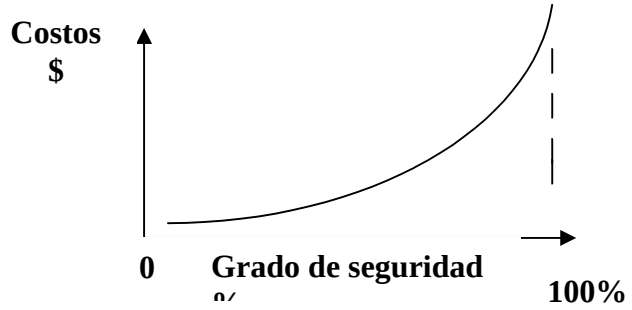


Gráfico 1.2 – Relación Operatividad – Seguridad. Fuente: ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1º Edición. Argentina. Página 26.

Más allá de ello, al tratarse de una ciencia social, no determinística, se mantendrá la incertidumbre propia del comportamiento humano, que puede permitir a un atacante violar el sistema, haciendo que los costos hayan sido, si bien no inútiles, excesivos.

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

Para ubicarnos en la vida real, veamos los datos obtenidos en mayo de 2001 por la consultora Ernst & Young [7] sobre 273empresas de distintos sectores de actividad y países.

- **El 75% de las empresas manifiestan tener planes de continuidad del negocio, pero sólo un tercio los ha puesto a prueba.**
- **Los miedos a la inseguridad continúan siendo el mayor inhibidor a la expansión del comercio electrónico.**
- **Sólo el 33% de los encuestados están muy seguros de que podrían detectar un ataque de hackers.**
- **Los sistemas críticos para el negocio continuarán fallando. Cerca del 75% de las empresas han experimentado fallos en los sistemas decisivos para el negocio en el último año.**
- **Más de la mitad de las compañías que participan en la encuesta admiten no disponer de una estrategia clara en comercio electrónico y no obstante acometen significativas actividades en e-business.**

[7] "Encuesta de Seguridad Informática 2001". Mayo 2001. http://www.hispasec.com/unaaldia/937

CAPITULO 2

SEGURIDAD FÍSICA

Es muy importante ser consciente que por mas que nuestra empresa sea la mas segura desde el punto de vista de ataques externos, Hackers, Virus etc. (conceptos luego tratados); la seguridad de la misma será nula si no de ha previsto como combatir un incendio.

La seguridad física es uno de los aspectos mas olvidados a al hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de operaciones de la misma, no.
Esto puede derivaran en que para un atacante será mas fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así **Seguridad Física** consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los dos recursos e información confidencial"[1]. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Computó así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

2.1 TIPOS DE DESASTRES

No será la primera vez que se mencione en este trabajo, que cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendaran pautas de aplicación general y no procedimientos específicos. Para ejemplificar todo esto: valdrá de poco tener en cuenta aquí, en Entre Ríos, técnicas de seguridad ante terremotos; pero si será de máxima utilidad en los Ángeles EE.UU.

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

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

[1] HUERTA Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 digital Open Publication Licence v. 10 o Later 10 de mayo de 2004. *http://www.kriptopolis.com*.

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

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

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

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

2.1.1 INCENDIOS

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

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

Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos.

Los diversos factores a contemplar para reducir los riesgos de incendios a los que se encuentra sometido un centro de cómputos son:

1. El área en la que se encuentran las computadoras debe de estar en un local que no se combustible e inflamable.

2. El local no debe situarse encima, debajo o adyacente a áreas Donde se procesen, fabriquen o almacenen materiales Inflamables, explosivos, gases tóxicos o sustancias Radioactivas.

3. Las paredes deben hacerse de materiales incombustibles y Extenderse desde el suelo al techo.

4. Debe construirse un “falso piso” instalado sobre el piso real Con materiales y combustibles y resistentes al fuego.

5. No debe estar permitido fumar en el área de proceso.

6.-Deben emplearse muebles incombustibles, y cestos Metálicos para papeles. Deben evitarse los materiales Plásticos e inflamables.
El piso y el techo en el recinto del centro de computo y de Almacenamiento de los medios magnéticos deben ser Impermeables.

2.1.1.1 SEGURIDAD DEL EQUIPAMIENTO

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

Para protegerlos se debe tener en cuenta que:

- La temperatura debe sobrepasar a los 18º C y el límite de humedad no debe superar el 65 % para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios de relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

2.1.1.2 RECOMENDACIONES

El personal designado para usar extinguidotes de fuego debe ser entrenado en su uso.

Si hay sistemas de detención de fuego que activan el sistema de extinción todo el personal de esa área debe estar entrenado para no interferir este proceso automático.

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

Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales

especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel.

Suministra información, del centro de cómputo, al departamento local de bomberos antes de que ellos sean llamados en una emergencia. Hacer que este departamento este consciente de las particularidades y vulnerabilidades del sistema, Además, ellos pueden ofrecer excelentes consejos como precauciones para prevenir incendios.

2.1.2 INUNDACIONES

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

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

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

2.1.3 CONDICIONES CLIMATOLÓGICAS

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

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

2.1.3.1 TERREMOTOS

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

2.1.4 SEÑALES DE RADAR

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

2.1.5 INSTALACIÓN ELÉCTRICA

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

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

2.1.5.1 PICOS Y RUIDOS ELECTROMAGNÉTICOS

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También esta el tema del ruido que interfiere en el funcionamiento de los componentes eléctricos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

2.1.5.2 CABLEADO

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

Los riesgos más comunes para el cableado son:

- 1.-Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de el) por acción de campos electrónicos, que si sufren los cambios metálicos.

- 2.-Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.

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

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

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

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

Luego, no hace falta penetrar en los cables físicamente para obtener los datos que trasportan.

2.1.5.2.1 Cableado de Alto Nivel de Seguridad

Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreos de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

2.1.5.2.2. Pisos de Placas Extraíbles

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

2.1.5.3 SISTEMA DE AIRE ACONDICIONADO

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

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

2.1.5.4 EMISIONES ELECTROMAGNÉTICAS

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

Según recomendaciones científicas estas emisiones podrán reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente seguras para las personas.

Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

2.1.6 ERGONOMETRÍA

"La **ergonomía** es una disciplina que se ocupa de estudiar la forma en que interactúa con el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible."[2]

El enfoque ergonómico plantea la adaptación de los métodos, los objetos, las maquinarias, herramientas he instrumentos o medios y las condiciones de trabajo a la anatomía, la fisiología y la psicología del operador. Entre los fines de su aplicación se encuentran, fundamentalmente, la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro.

2.1.6.1 TRASTORNOS ÓSEOS Y/O MUSCULARES

Una de las maneras de provocar una lesión ósea o muscular es obligar al cuerpo a ejecutar movimientos repetitivos y rutinarios, y esta posibilidad se agrava enormemente si dichos movimientos se realizan en una posición incorrecta o antinatural.

En el ambiente informático, la operación del teclado es un movimiento repetitivo y continuo, si a esto le sumamos el hecho de trabajar con una

[2] ADELGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 2ª Edición. Argentina. 2002. Página 30.

distribución ineficiente de las teclas, el diseño antinatural y la ausencia (ahora atenuada por el uso del Mouse) de movimientos alternativos al de teclado, tenemos un potencial riesgo de enfermedades o lesiones en los músculos, nervios y huesos de manos y brazos.

En resumen, el lugar de trabajo debe de estar diseñado de manera que permita que el usuario se coloque en la posición más natural posible. Como esta posición variara de acuerdo a los distintos usuarios, lo fundamental en todo esto es que el puesto de trabajo sea ajustable, para que pueda adaptarse a las medidas y posiciones naturales propias de cada operador.

2.1.6.2 TRASTORNOS VISUALES

Los ojos, sin duda, son las partes mas afectadas por el trabajo con computadoras.

La pantalla en una fuente de luz que incide directamente sobre el ojo del operador, provocando luego de exposiciones prolongadas el típico cansancio visual, irritación y lagrimeo, cefalea y visión borrosa.

Si a esto le sumamos un monitor cuya definición no sea la adecuada, se debe considerar la exigencia a la que se someterán los ojos del usuario al intentar descifrar el contenido de la pantalla. Además de la fatiga del resto del cuerpo al tener que cambiar la posición de la cabeza y el cuello para acercar los ojos a la misma.

Para prevenir los trastornos visuales en los operadores podemos tomar recaudos como:

- 1.-Tener especial cuidado a elegir los monitores y placas de video de las computadoras.
- 2.-Usar de pantallas antirreflejos o anteojos con protección para el monitor, es una medida preventiva importante y de relativo bajo costo, que puede solucionar varios de los problemas antes mencionados.

2.1.6.3 LA SALUD MENTAL

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

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

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

Los efectos del estrés pueden encausarse dentro de varias categorías:

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

2.1.6.4 AMBIENTE LUMINOSO

Se parte de la base que las oficinas mas iluminadas son la principal causa de la perdida de la productividad de las empresas y de un gasto energético excesivo. Una iluminación deficiente provoca dolores de cabeza y perjudica a los ojos.

2.1.6.5 AMBIENTE CLIMÁTICO

En cuanto al ambiente climático, la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe de estar comprendida entre el 45 % y el 65 %. En todos los lugares hay que contar con sistemas que remueven el aire periódicamente. No menos importante es el ambiente sonoro por lo que se recomienda no adquirir equipos que superen los 55 decibeles, sobre todo cuando trabajan muchas personas en un mismo espacio.

2.2 ACCIONES HOSTILES

2.2.1 ROBO

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera,

robar tiempo de maquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, A los que dan menor protección que la que otorgan a una maquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraible y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

2.2.2 FRAUDE

Cada año millones de dólares son sustraídos de empresas y en muchas ocasiones las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, si no que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

2.2.3 SABOTAJE

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

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

2.3 CONTROL DE ACCESOS

El control de acceso no solo requiere la capacidad de identificación, si no también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

2.3.1 UTILIZACIÓN DE GUARDIAS

2.3.1.1 CONTROL DE PERSONAS

El Servicio de Vigilancia es el encargado de control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en

los lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

A cualquier personal ajeno a la planta se le solicitara completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de regreso etc.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal de distintos sectores de la empresa.

En este caso la persona se identifica **por algo que posee**, una tarjeta de identificación. Cada una de ellas tiene un PIN (Personal Identification Number) único, siendo este el que se almacena en una base de datos para su posterior seguimiento, si fuera necesario.

Su mayor desventaja es que estas tarjetas pueden ser copiadas, robadas, etc. permitiendo ingresar a cualquier persona que la posea.

Estas credenciales se pueden clasificar de la siguiente manera:

- Normal o Definitiva: para el personal permanente de planta.
- Temporaria: para el personal recién ingresado.
- Contratistas: personas ajenas a la empresa, que por razones de servicios deben ingresar a la misma.
- Visitas

Las personas también pueden acceder mediante **algo que saben** (por ejemplo un numero de identificación o una password) que se solicitara a su ingreso. Al igual que el caso de las tarjetas de identificación los datos ingresados se contrastaran contra una base donde se almacena los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se eligen identificaciones sencillas, bien se olvidan dichas identificaciones o incluso las bases de datos pueden verse alteradas o robadas por personas no autorizadas.

2.3.1.2 CONTROL DE VEHÍCULOS

Para controlar el ingreso y egreso de vehículos, el personal de vigilancia debe asentar en una planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la empresa.

2.3.2 DESVENTAJA DE UTILIZACIÓN DE GUARDIAS

La principal desventaja de la aplicación del personal de guardia es que este puede llegar hacer sobornado por un tercero para lograr el acceso a sectores donde no este habilitado, como así también para poder ingresar o egresar de la planta con materiales no autorizados. Esta situación de soborno es muy frecuente, por lo que es recomendable la utilización de sistemas biométricos para el control de los accesos.

2.3.3 UTILIZACIÓN DE DETECTORES DE METAL

El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual.

La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activara el alma.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuara como elemento disuasivo.

2.3.4 UTILIZACIÓN DE SISTEMAS BIOMÉTRICOS

Definimos la biometría como “la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos”.

La biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

2.3.4.1 LOS BENEFICIOS DE UNA TECNOLOGÍA BIOMÉTRICA

Puede eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años, el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración utilizando un dispositivo biométrico los costos de administración son mas pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizadas. Sumando a esto, las características biométricas de una persona son intransferibles a otra.

2.3.4.2 EMISIÓN DE CALOR

Se mide la emisión de calor del cuerpo (termograma) , realizando un mapa de valores sobre la forma de cada persona.

2.3.4.3 HUELLA DIGITAL

Basado en el principio de que no existen dos huellas dactilares, iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados.

Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos etc. (llamados minucias) características y la posesión relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen mas de ocho minucias iguales y cada una posee mas de 30, lo que hace al método sumamente confiable.

2.3.4.4 VERIFICACIÓN DE VOZ

La dicción de una (o más) frase es grabada y en el acceso se compra la vos (entonación, diptongos, agudeza etc.).

2.3.4.5 VERIFICACIÓN DE PATRONES OCULARES

Estos métodos pueden estar basados en los patrones de iris o de la retina y hasta el momento son los considerados mas efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

2.3.5 VERIFICACIÓN AUTOMÁTICA DE FIRMAS (VAF)

En este caso lo que se considera es **lo que el usuario es capaz de hacer,** aunque también podría encuadrarse dentro de las verificaciones biométricas.

Mientras es posible para un falsificador producir una buena copia visual o fascimil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud.

La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura se ejecuta.
El equipamiento de colección de firmas e inherentemente de bajo costo y robusto. Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

2.3.6 SEGURIDAD CON ANIMALES

Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente el costo de cuidado y mantenimiento se disminuye considerablemente utilizando este tipo de sistema. Así mismo, este sistema posee desventaja de que los animales pueden ser engañados para lograr el acceso deseado.

2.3.7 PROTECCIÓN ELECTRÓNICA

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

2.3.7.1 BARRERAS INFRARROJAS Y DE MICRO-ONDAS

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

Las invisibles barreras fotoeléctricas pueden llegar a cubrir áreas de hasta 150 metros de longitud (distancias exteriores). Pueden reflejar sus rayos por medio de espejos infrarrojos con el fin de cubrir con una misma barrera diferentes sectores.

Las micro-ondas son ondas de radio de frecuencias muy elevada. Esto permite que el sensor opere con señales de muy bajo nivel sin ser afectado por otras emisiones de radio, ya que están muy alejadas en frecuencia.

Debido a que estos detectores no utilizan aire como medio de propagación, poseen la ventaja de no ser afectados por turbulencias de aire o sonidos muy fuertes.

Otra ventaja importante es la capacidad de atravesar ciertos materiales como son el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

2.3.7.2 DETECTOR ULTRASÓNICO

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, genera una perturbación en dicho campo que accionara la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas. La cobertura de este sistema puede llegar a un máximo de 40 metros cuadrados.

2.3.7.3 DETECTORES PASIVOS SIN ALIMENTACIÓN

Estos elementos no requieren alimentación extra de ningún tipo, solo van conectados a la central de control de alarmas para mandar la información de control. Los siguientes están incluidos dentro de este tipo de detectores:

1.-Detector de aberturas: Contactos magnéticos externos o de embutir.
2.-Detector de roturas de vidrios: inmune a falsas alarmas provocadas por Sonidos de baja frecuencia; sensibilidad regulable.
3.-Detector de vibraciones: detecta golpe o manipulaciones extrañas sobre La superficie controlada.

2.3.7.3.1 SONORIZACIÓN Y DISPOSITIVOS LUMINOSOS

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

Se pueden usar transmisores de radio a corto enlace para las instalaciones de alarmas locales. Los sensores se conectan a un trasmisor que envía la señal de radio a un receptor conectado a la central de control de alarmas encargada de procesar la información recibida.

2.3.7.3.2 CIRCUITOS CERRADOS DE TELEVISIÓN

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben de estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizadas como medida disuasiva) u ocultas (para evitar que el intruso sepa que esta siendo captado por el personal de seguridad).

Todos los elementos anteriormente descriptos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviara una señal a la central de alarma para que este accione los elementos de señalización correspondientes.

2.3.7.3.3 EDIFICIOS INTELIGENTES

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

El edificio inteligente (surgido hace unos 10 años) se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación. Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadoras, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación, y aire acondicionado, etc.) y todas las formas de administración de energía.

Una característica común de los Edificios Integrales es la flexibilidad que deben tener para asumir modificaciones de manera conveniente y económica.

2.4 CONCLUSIONES

Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- trabajar mejor manteniendo la sensación de seguridad.
- descartar falsas hipótesis si se produjeran incidentes.
- Tener los medios para luchar contra accidentes.

Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos: y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de las áreas que recorren ciertas personas hasta el extremo de evacuar el edificio en caso de accidentes.

CAPITULO 3

SEGURIDAD LÓGICA

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

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

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

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

Los objetivos que se plantean son:

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

3.1 CONTROLES DE ACCESO

Estos controles pueden implementarse en el sistema operativo, sobre los sistemas de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Constituyen una importante ayuda para proteger al sistema de aplicación y demás de la utilización o modificaciones no autorizadas; para mantener la integridad de la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario)a un determinado recurso. Al respecto, el Nacional Instiutute for Standars and Tecnología (NIST)[1] ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

3.1.1 IDENTIFICACIÓN Y AUTENTIFICACIÓN

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

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

- Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- Algo que la persona **posee:** por ejemplo una tarjeta magnética.
- Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales a la voz.
- Algo que el individuo es capaz de **hacer** por ejemplo: los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado los controles de autenticación biométricos serian los mas apropiados y fáciles de administrar, resultando ser también, los mas costosos por lo dificultoso de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autentificados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto de denomina “single long-in” o sincronización de password.

[1] *http://www.nist.gov*

Una de las posibilidades técnicas para implementar esta única identificación de usuarios seria la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que este pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográficas como lógicamente, de acuerdo con los requerimientos de carga de áreas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso de los recursos informáticos, basados en la identificación, autenticación, y autorización de accesos. Esta administración abarca:

- **1.-**Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema optativo o en la aplicación según corresponda.
- **2.-**Además la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
- **3.-**Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoria o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.
- **4.-**Las revisiones deben orientarse a verificar la educación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de periodos de inactividad o cualquier otro aspecto anormal que permite una redefinición de la necesidad de acceso.
- **5.**-Detección de actividades no autorizadas. Además de autorizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de las actividades no autorizadas. Alguna de ellas se basan en evitarla dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuado rotaciones periódicas a las funciones asignadas a cada una.
- **6.-**Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
- **7.-**Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que

en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando “bombas lógicas” o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también pueden causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularan de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

3.1.2 ROLES

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serian los siguientes: programador, líder de proyecto, gerente de una área usuaria, administrador del sistemas, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

3.1.3 TRANSACCIONES

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

3.1.4 LIMITACIONES A LOS SERVICIOS

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

3.1.5 MODALIDAD DE ACCESO

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

- **Lectura:** el usuario puede únicamente leer o visualizar la información pero no puede alentarla. Debe considerarse que la información puede ser copiada o impresa.
- **Escritura:** este tipo de acceso permite agregar datos, modificar o borrar información.
- **Ejecución:** este acceso otorga al usuario el privilegio de el privilegio de ejecutar programas.
- **Borrado:** permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- Todas las anteriores.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- **Creación:** permite al usuario crear nuevos archivos, registros o campos.
- **Búsqueda:** permite listar los archivos de un directorio determinado.

3.1.5 UBICACIÓN Y HORARIO

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

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

3.1.6 CONTROL DE ACCESO INTERNO

3.1.6.1 PALABRAS CLAVES (PASSWORDS)

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de password débiles.

- **Sincronización de passwords:** consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un

usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan accesos, y que si se los fuerza a elegir diferentes password tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aun mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.

- **Caducidad y control:** este mecanismo controla cuando pueden y/o deben cambiar sus passwords los usuarios. Se define el periodo mínimo que debe pasar para que los usuarios puedan cambiar su passwords, y un periodo máximo que pueda transcurrir para que estas caduquen.

3.1.6.2 ENCRIPTACIÓN

La información encriptada solamente puede ser descriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso. Este tema será abordado con profundidad en el Capitulo sobre Protección del presente.

3.1.6.3 LISTAS DE CONTROL DE ACCESOS

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

3.1.6.4 LIMITES SOBRE INTERFASE DE USUARIO

Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre las base de datos limites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario solo puede ejecutar ciertas funciones presionando teclas especificas.

3.1.6.5 ETIQUETAS DE SEGURIDAD

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que puede utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables.

3.1.7 CONTROL DE ACCESO EXTERNO

3.1.7.1 DISPOSITIVOS DE CONTROL DE PUERTOS

Estos dispositivos autorizan el acceso a un puerto determinado y puede estar físicamente separado o incluido en otro dispositivo de comunicaciones, como por ejemplo un modem.

3.1.7.2 FIREWALLS O PUERTAS DE SEGURIDAD

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Este tema será abordado con posterioridad.

3.1.7.3 ACCESO DE PERSONAL CONTRATADO O CONSULTORES

Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

3.1.7.4 ACCESOS PÚBLICOS

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

Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.

3.1.8 ADMINISTRACIÓN

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

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

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible

clasificar la información, determinado el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

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

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

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

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

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

3.1.8.1 ADMINISTRACIÓN DEL PERSONAL Y USUARIOS

3.1.8.1.1 Organización del Personal

Este proceso lleva generalmente cuatro pasos:

- 1.-definición de puestos: debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
- 2.-Determinación de la sensibilidad del puesto: para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
- Elección de la persona para cada puesto: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales.
- El entrenamiento inicial y continuo del empleado: cuando la persona seleccionada ingresa y la organización, además de sus responsabilidades individuales para la ejecución de la tares que se asignen, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se opera de el.

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

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

3.2 NIVELES DE SEGURIDAD INFORMÁTICA

El estándar de niveles de seguridad mas utilizado internacionalmente es el TCSEC Orange Book[2] desarrollado en 1983 de acuerdo a las normas de seguridad de computadoras del Departamento de Defensa de los Estados Unidos.

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad máximo.

Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) luego internacionales (ISO/IEC).

Cabe aclarar que cada nivel requiere de todos los niveles definidos anteriormente: así el subnivel B2 abarca los subniveles B1, C2, C1, y el D.

3.2.1 NIVEL D

Este nivel contiene solo una división y esta reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad. Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS Y System 7.0 de Macintosh.

3.2.2 NIVEL C1 : PROTECCIÓN DISCRECIONAL

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas cotidianas de la administración del sistema solo pueden ser realizadas por este “súper usuario” quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que una organización encontremos

[2] ORANGE BOOK. Department of Defense. Library No S225, 771 EEUU. http://www.doe.gov

dos o tres personal cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumera los requerimientos mínimos que debe cumplir la clase C1:

- Acceso de control discrecional: distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios)y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
- Identificación y Autentificación: se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

3.2.3 NIVELC2 : PROTECCIÓN DE ACCESO CONTROLADO

Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de acceso e intentos fallidos de accesos a objetos. Tiene una capacidad de restringir aun mas el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no solo en los permisos, si no también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoria esta utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios. La auditoria requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores. Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

3.2.4 NIVEL B1: SEGURIDAD ETIQUETADA

Este subnivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y la ultrasecreta. Se establece que el dueño de archivo no puede modificar los permisos de un objeto que esta bajo el control de acceso obligatorio. A cada objeto del sistema (usuario, dato,

etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto, secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nominas, ventas,etc.)

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados. También se establecen controles para limitar para la propagación de derecho de accesos a los distintos objetos.

3.2.5 NIVEL B3: DOMINIOS DE SEGURIDAD

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad. Existe un monitor de referencia a que las peticiones de acceso de cada usuario y las permite o las desniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y testeos ante posibles violaciones. Este nivel requiere que la trámite del usuario se conecte al sistema por medio de una conexión segura.

Además cada usuario tiene asignado los lugares y objetos a los que puede acceder.

3.2.6 NIVEL A :PROTECCIÓN VERIFICADA

Es el nivel mas elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el Hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

CAPITULO 4

DELITOS INFORMÁTICOS

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

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades. La cuantía de los prejuicios así ocasionado es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o a castigarse.

Es propósito de los siguientes capítulos desertar sobre los riesgos “no naturales”, es decir, los que escuadran en el marco del delito. Para ello deberemos dejar en claro, nuevamente, algunos aspectos.

4.1 INFORMACIÓN Y DELITO

El delito informativo implica actividades criminales que los países han tratado de exponer en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

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

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin he luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wuzburgo (Alemania), adopto diversas recomendaciones respecto a los delitos informáticos, entre ellas que en la medida que el Derecho Penal no se suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas, como por ejemplo, el “principio de subsidiariedad”.

Se entiende delito como “acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquellas”.

Finalmente la OCDE publicó un delito sobre estudios informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define **Delito Informático** como “cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el proceso automático de datos y/o transmisiones de datos.

“Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del “injusto” la información en si mismo”[1]

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

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

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

En este punto debe hacerse notar lo siguiente:

- No es la computadora que atenta contra en hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.
- No es la computadora la que afecta nuestra vida privada, si no el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no esta frente al peligro de la informática si no frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.
- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.
- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

[1] CARRION, Hugo Daniel. Tesis “Presupuestos para la punibilidad del Hacking “. Julio 2004. *www.delitosinformaticos.com/tesis.htm*

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás sino todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

Julio Tellez Valdez clasifica los delitos informáticos en base a dos criterios:

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

Ejemplos:

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

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

Ejemplos:

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

Este mismo autor sostiene que las acciones delictivas informáticas presentan las siguientes características:

1.-Solo una determinada cantidad de personas (con conocimientos técnicos por encima de lo normal) puede llegar a cometerlos.
2.-Son conductas criminales del tipo “cuello blanco”: no de acuerdo al interés protegido (como en los motivos convencionales) si no de acuerdo al sujeto que los comete. Generalmente este sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
3.-Son acciones ocupacionales, ya que generalmente se realiza cuando el sujeto atado se encuentra trabajando.
4.-Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando.

5.-Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
6.-Ofrecen posibilidades de tiempo y espacio.
7.-Son muchos los casos y pocas las denuncias, y todo ellos por la falta de regulación y por miedo al desprestigio de la organización atacada.
8.-Presentan grandes dificultades para su comprobación, por su carácter técnico.
9.-Tienden a proliferar, por lo que se requiere su urgente regulación legal.

Maria Luz Lima, por su parte, presenta la siguiente clasificación de “delitos electrónicos”

1.-Como método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2.-Como Medio: conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
3.-Como: Fin: Conductas criminales dirigidas contra la entidad física del objeto o maquina electrónica o su material con objeto de dañarla.

4.2 TIPOS DE DELITOS INFORMÁTICOS

La organización de Naciones Unidas (ONU) reconoce los siguientes tipos de delitos informáticos:

1.-Fraudes cometidos mediante manipulación de computadoras

- Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático mas común ya que es fácil de cometer y difícil de descubrir.
- La manipulación de programas: consiste en modificar los programas existentes en el sistema o e insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación.
- Manipulación de los datos de salida: se efectúa fijando un objeto al funcionamiento del sistema informático: El ejemplo mas común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para computadora en la fase de adquisición de datos.
- Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina “técnicas de salchichón” en la que “rodajas muy finas” apenas perceptibles de transacción financiera, se van sacando repentinamente de una cuenta y se transfieren a otra. Se basa en el principio de que 10,66es igual a 10.65 pasando 0,01 centavos a la cuenta del ladrón n veces.

2. Manipulación de los datos de entrada.

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

3. Daños o modificaciones de programas o datos computarizados

- Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
- Acceso no autorizado a servicios y sistemas informáticos: estos accesos se pueden realizar por diversos motivos, desde la simple curiosidad hasta el sabotaje o espionaje informático.
- Reproducción no autorizada de programas informáticos de protección legal: esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y las han sometidos a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas, Al respecto, se considera, que la reproducción no autorizada de programas informáticos no un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

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

- Fraude en el campo de la informática.
- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Trafico de claves informáticas obtenidas por medio de ilícito.
- Distribución de virus o programas delictivos.[2]

4.3 DELINCUENTE Y VÍCTIMA

4.3.1 SUJETO ACTIVO

Se llama así a **las personas que cometen los delitos informáticos.** Son aquellas que poseen ciertas características que no presentan el denominador

[2] CARRION, Hugo Daniel. Tesis "Presupuestos para la punibilidad del Hacking ". Julio 2004. *www.delitosinformaticos.com/tesis.htm*

común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

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

El nivel típico de aptitudes del delincuente informático es el tema de controversia ya que para algunos el nivel de aptitudes no listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, estudiosos de la materia los han catalogado como “delitos de cuello blanco” término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

La “**cifra negra”** es muy alta: no es fácil descubrirlos ni sancionarlos, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños económicos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad.
A los sujetos que cometen este tipo de delitos no se consideran delincuentes; no se les segrega, ni se les desprecia, ni se les desvaloriza; por el contrario, es considerado y se considera a sí mismo “respetable”. Estos tipos de delitos, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad.

4.3.2 SUJETO PASIVO

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

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los delitos informáticos, ya que mediante el, podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos.

Es imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las victimas de estos delitos; la falta de preparación por falta de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado; el temor

por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes perdidas económicas, trae como consecuencia que las estadísticas de sobre este tipo de conductas se mantengan bajo la llamada “cifra negra”.

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

En el mismo sentido, podemos decir que con:

1. la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras.
2. alertas a las potenciales víctimas, para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática.
3. creación de una adecuada legislación que proteja los intereses de las víctimas;
4. una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas;

   Se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

   Además se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos, se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

LEGISLACIÓN NACIONAL

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

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

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

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

- Este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna, de julio 1971 para la Protección de Obras Literarias y Artísticas.
- Las complicaciones de datos posibles de ser legibles será protegidos como creaciones de carácter intelectual y que;
- Para los casos de falsificación dolorosa de marcas de fabrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que, "los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias".[3]

La Convención sobre la Propiedad Intelectual de Estocolmo (julio de 1967) y el Convenio de Berna (julio de 1971) fueron ratificados en nuestro país por la ley 22195 el 17 de marzo de 1980 y el 8 de julio de 1990 respectivamente.

La Convención para la Protección y Producción de Phonogramas de octubre de 1971, fue ratificada por la ley 19.963 el 23 de noviembre de 1972.

La Convención relativa la Distribución de Programas y Señales de abril de 1994, fue ratificada por la ley 24.425 el 23 de diciembre de 1994.

Hay otros Convenios no ratificados aun por nuestro país, realizados por la Organización Mundial de la Propiedad Intelectual (OMPI), de la que Argentina es parte integrante a partir del 8 de Octubre de1980.

Nuestra legislación regula Comercial y Permanente las consultas ilícitas relacionadas con la informática, pero que aún no contemplan en sí los delitos informáticos:

1. La ley 111 de Patentes de Invención regula la protección a la propiedad intelectual.
2. La ley penal 11.723 de "Propiedad Científica, Literaria y Artística ", modifica por el decreto165/94, han modificado los Artículos 71. 72, 72 bis, 73y 74 (ver anexo 1).

Por esta ley, en el país solo están protegidos los lenguajes de bases de datos, planillas de cálculo, el software y su documentación dentro del mismo.

Si bien, en el decreto de 1994, se realizó la modificación justamente para incluir esos items en el concepto de propiedad intelectual, no tiene en cuenta la posibilidad de plagio ya que no hay jurisprudencia que permita establecer que porcentaje de igualdad en la escritura de dos programas se considera plagio.

[3] Artículo 61, Convenio de Berna de 1971para la Protección de Obras Literarias y Artísticas.

Las copias ilegales de software también son penalizadas, pero por reglamentaciones comerciales.

A diferencia de otros países, en la Argentina la información no es un bien o propiedad, por lo tanto no es posible que sea robada, modificada o destruida.

De acuerdo con los Art. 1072 y 2311 del Código Civil y 183 del Código Penal se especifica que para que exista robo o hurto debe de afectarse una ”cosa” como algo que ocupa lugar en el espacio; los datos se sabe, son intangibles.

En resumen, si alguien destruye, mediante los métodos que sean, la información almacenada en una computadora, no cometió delito; pero si rompió el hardware o un diskette será penalizado: en ese caso, deberá hacerse cargo de los costos de cada elemento pero no de lo que contenía. También especifica (Art.1109) que el damnificado no podrá reclamar indemnización si hubiera existido negligencia de su parte.

Ahora cabe preguntarse ¿En Argentina, que amparo judicial se tiene ante hechos electrónicos ilícitos? La respuesta es el Código Penal Argentino (con 77 años de vida) no tiene reglas específicas sobre los delitos cometidos a través de computadoras. Esto es así porque cuando se sancionaban las leyes no existía la tecnología actual y por lo tanto no fueron previstos los ataques actuales.

Dentro del Código Penal se encuentran sanciones respecto de los delitos contra el honor (Art. 109 a 117); instigación al suicidio (Art. 83); hurto (Art. 162), estafas (Art., 172) además de los de defraudación, falsificación, tráfico de menores, narcotráfico, etc. Todas las conductas que puedan ser cometidas utilizando como medio la Tecnología Electrónica, pero nada referente a delitos cometidos sobre la información como bien.

El mayor inconveniente es que no hay forma de determinar fehacientemente cual era el estado anterior de los datos, puesto que la información en estado digital es fácilmente adulterable. Por otro lado, aunque fuera posible determinar el estado anterior, sería difícil determinar el valor que en dicha información tenía.

El problema surge en que los datos almacenados tiene el valor que el cliente o “dueño” de esos datos le asigna (y que razonablemente forma parte de su patrimonio). Esto desde el punto de vista legal es algo totalmente subjetivo. Son bienes intangibles, donde solo el cliente pueda valorar los “unos y ceros” almacenados.

Así, las acciones comunes de hurto, robo, daño, falsificación, etc. (art. 162 del Código Penal) que habla de un apoderamiento material NO pueden aplicarse a los datos almacenados por considerarlos intangibles.

Hablar de estafa (contemplada en el art.172 de código penal) no es aplicable a una maquina porque se la concibe como algo que no es susceptible de caer en error, todo lo contrario a la mente humana.

En función del Código Penal, se considera que entrar a un domicilio sin permiso o violar correspondencia constituyen delitos. (Art.153). Pero el acceso a una computadora, red de computadoras o medios de transmisión de la información (violando un cable coaxial por ejemplo) sin autorización, en forma directa o remota, no constituyen un acto penable por la justicia, aunque si el daño del mismo.

La mayor dificultad es cuantificar el delito informático. Estos pueden ser muy variados: reducir la capacidad informativa de un sistema como un virus o un caballo de Troya, saturar el correo electrónico de un proveedor con infinidad de mensajes, etc. Pero ¿Cuál de ellos es mas grave?

Si se considera el Internet, el problema se vuelve aún mas grave ya que se caracteriza por ser algo completamente descentralizado. Desde el punto de vista del usuario esto constituye un beneficio, puesto que no tiene ningún control ni necesita autorización para acceder a los datos. Sin embargo, constituyen un problema desde el punto de vista legal. Principalmente porque las leyes penales son aplicables territorialmente y no puede pasar la barrera de los países.

La facilidad de comunicación entre diversos países que brinda la telemática dificulta la sanción de leyes claras y eficaces para castigar las intrusiones computacionales.

Si ocurre un hecho delictivo por medio del ingreso a varias páginas de un sitio distribuidas por distintos países: ¿Qué juez será el competente en la causa? ¿Hasta que punto se pueden regular los delitos a través de Internet sabiendo que no se puede aplicar las leyes en forma extraterritorial?

Ver una pantalla con información, ¿es un robo? Ante esta pregunta Julio C. Ardita[4] responde (…), si, desde el punto de vista del propietario, si es información confidencial y/o personal es delito porque se violó su privacidad".

Si un intruso salta de un satélite canadiense a una computadora en Taiwán y de allí a otra alemana ¿con las leyes de que país se juzgara?

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

Por lo pronto en febrero de 1997 se sancionó la ley 24,766, (ver anexo 1) por la que se protege la información confidencial a través de acciones penales y

[4] ARDITA, Julio César. Director de Cybsec S.A. *http://www.cybsec.com*

civiles, considerando información confidencial aquella que cumple los siguientes puntos:

- Es secreta en el sentido que no sea generalmente conocida, ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información.
- Tenga valor comercial para ser secreta.
- Se hayan tomado medidas necesarias para mantenerla secreta, tomadas por la persona que legítimamente la controla.

Por medio de esta ley la sustracción de disquetes, acceso sin autorización a una red o computadora que contenga información confidencial será sancionado a través de la pena de violación de secretos.

En cuanto a la actividad típica de los hackers, las leyes castigan el hurto de energía eléctrica y de líneas telefónicas, aunque no es fácil de determinar la comisión del delito. La dificultad radica en establecer donde se cometió el delito y quien es el damnificado.

Los posibles hechos de hacking se encuentran en la categoría de delitos comunes como defraudaciones, estafas o abuso de confianza, y la existencia de una computadora no modifica el castigo impuesto por la ley.

La División Computacional de la Política Federal no realiza acciones o investigaciones preventivas (a modo de las organizaciones estadounidenses) actúa en un aspecto parcial cuando el operativo ya esta en marcha.

Este vació en la Legislación Argentina se agrava debido a que las empresas que sufren ataques no lo difunden por miedo a perder el prestigio y principalmente porque no existen conceptos claros para definir nuevas leyes jurídicas en función de los avances tecnológicos.

Estos problemas afectan mucho a la evolución del campo informático de la Argentina, generando malestar en empresas, usuarios finales y todas las personas que utilicen una computadora como medio para realizar o potenciar una tarea. Los mismos se sienten desprotegidos por la ley ante cualquier acto delictivo.

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

Desde la óptica legal y ante la inexistencia de normas que tipifiquen los delitos cometidos a través de la computadora que la ley contemple accesos ilegales a las redes como a sus medios de transmisión. Una futura reforma debería prohibir toda clase de acceso no autorizado a un sistema informático,

como lo hacen las leyes de Chile, Francia, Estados Unidos, Alemania, Austria, etc.

Lo “gracioso” es que no existe sanción legal para la persona que destruye información almacenada en un soporte, pero sí para la que destruye la misma información impresa sobre papel.

No obstante, existe en el Congreso Nacional diversos proyectos de ley que contempla esta temática (ver anexo 11).

LEGISLACIÓN INTERNACIONAL

ALEMANIA

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley la Criminalidad Económica. Esta ley reforma el Código Penal (Art. 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

- Espionaje de datos (202ª).
- Estafa informática (263ª).
- Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño entre el tráfico jurídico mediante la elaboración de datos, falsedad ideológico, uso de documentos falsos (270, 271, 273).
- Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
- Sabotaje Informático (303b).
- Destrucción de datos de especial significado por medio del deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b).
- Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los países escandinavos y en Austria.

4.5.2 AUSTRIA

Según la Ley de Reforma del Código Penal del 22 de diciembre de 1987, se contemplan los siguientes delitos:

- Destrucción de datos (Art.126) no solo datos personales si no también los no personales y los programas.
- Estafa informática (Art.148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos o por actuar sobre el procesamiento de

datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

4.5.3 CHILE

Chile fue el primer país latinoamericano es sancionar una Ley contra Delitos Informáticos. La ley 19223 pública en el Diario Oficial (equivalente del boletín oficial argentino) el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco.

Como no se estipula la condición de acceder a ese sistema, puede motivar a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.

El hacking, definido como el ingreso, es un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en este, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver con su contenido no constituye delito.

Dar a conocer la información almacenada a un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años.

Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

4.5.4 CHINA

El Tribunal Supremo Chino castigara con la pena de muerte el espionaje desde Internet, según se anunció el 23 de enero de 2001.

Todas las personas “implicadas en actividades de espionaje”, es decir que “roben, descubran, compren o divulguen secretos de Estado “desde la red podrán ser condenadas con penas que van de diez años de prisión hasta la muerte ¿castigo ejemplar?

La corte determina que hay tres tipos de actividades donde la vigilancia será externa: secretos de alta seguridad, los secretos estatales y aquella información que dañe seriamente la seguridad estatal y sus intereses. Se consideran actividades ilegales de infiltración de documentos relacionados con el Estado, la defensa, las tecnologías de punta, o la difusión de virus informático.

El tribunal a hecho especial énfasis al aparato del espionaje desde la red, a los llamados “criminales” además de tener asegurada una severa condena (la muerte), también se les puede ¡confiscar los bienes!

4.5.5 ESPAÑA:

Este país quizá sea el que mayor experiencia ha obtenido en caso de delitos informáticos, en Europa.

Su actual Ley Orgánica de Protección de Carácter Personal (LOPDCP) aprobada el 15 de de diciembre de 1999, la cual remplaza una veintena de leyes anteriores de la misma índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreaking, la introducción de virus, etc. Aplicando pena de prisión y multa, agravándola cuando existe una intención dolorosa o cuando el hecho es cometido por parte de funcionarios públicos.

Así mismo su nuevo Código Penal establece castigos de prisión y multas, “a quien por cualquier medio destruya, altere inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

4.5.6 ESTADOS UNIDOS DE AMÉRICA

El primer abuso de una computadora se registró en 1958 mientras que recién en 1966 se llevó adelante el primer proceso por la alteración de los datos de un barco de Miniápolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían, si el delito informático era el resultado de una nueva tecnología o un tema específico, los ataques computacionales se hicieron mas frecuentes. Para acelerar las comunicaciones, enlazar compañías, centros de investigación y transferir datos, las redes debían (y deben) ser accesibles, por eso el pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en el banco de los intrusos.

Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entretenimiento para sus agentes acerca de los delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985.

Esta ley fue la base para que Florida, Michigan, Colorado, Rodee Island y Arizona se constituyeran en los primeros estados de legislación especifica, anticipándose un año al dictado de la Computer Fraud Active 1986.

Este se refiere a su mayor parte, a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras e instituciones financieras o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal y el uso de passwords ajenas o propias en forma inadecuada. Pero solo es aplicable en caso de que se verifiquen daños cuyo valor supere el mínimo de mil dólares.

En 1994 se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986. Aquí se contempla la regulación de los virus (computer contaminat) conceptualizándolos a los que no los limita, a los comúnmente llamados virus o gusanos, si no que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos.

Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

El aumento de cantidad de casos hacking y la sensación de inseguridad permanente que generaron (fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas), cambiaron la percepción de las autoridades con respecto a los hackers y sus ataques. Los casos que demostraron ese cambio fueron los del “cóndor” Kevin Mitnicky y los de “ShadowHawk” Herbert Zinn hijo (ver anexo 11).

El FCIC (Federal Computers Investigation Comité), es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS) quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son “forenses de las computadoras” y trabajan, Además de los Estados Unidos, en Canadá, Taiwán e Irlanda.

4.5.7 FRANCIA

Aquí la ley 88/19 del 5 de Enero de 1988 sobre el fraude informático contempla:

- Acceso fraudulento a un sistema de elaboración de datos, Se sanciona tanto el acceso al sistema como al que se mantenga en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje Informático: Falsear el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos: Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión

- Falsificación de documentos. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar perjuicio a otro.

4.5.8 HOLANDA

Hasta el día 1 de Marzo de 1993, día en que entró en vigilancia la Ley de los Delitos Informáticos, Holanda era un paraíso para los hackers. Esta ley contempla artículos específicos sobre técnicas de hacking y Phreacking.

El mero hecho de entrar en una computadora en el cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si se usó ésta computadora Hackeada para acceder a otra, la pena sube a cuatro años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la maquina hackeada o procesar datos en ella también conlleva un castigo de cuatro años en la cárcel. Publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de intereses públicos es legal.

El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años de prisión pero, si se hizo vía remota aumenta a cuatro.

Los virus están considerados de manera especial en la ley. Si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel; si simplemente, se “escapo”, la pena no supera el mes.

El usar el servicio telefónico mediante un truco técnico (Prehacking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres años de prisión. La venta de elementos que permitan el prehacking se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres. La ingeniería social también es castigada con hasta tres años de cárcel.

Recibir datos del aire es legal (Transmisiones satelitales), siempre y cuando no haga falta un esfuerzo especial para conseguirlos: la declaración protege datos encriptados, como los de ciertos canales de televisión satelital. Falsificar tarjetas de crédito de banca electrónica y usarlas para obtener beneficios o como si fueran las originales esta penado con hasta seis años. Aunque…hacerlas y no usarlas parece ser legal.

4.5.9 INGLATERRA

Luego de varios casos de hacking surgieron nuevas leyes sobre delitos informáticos. En agosto de 1990 comenzó a regir la Computer Misusi Act. (Ley de Abusos Informáticos) por la cual cualquier intento exitoso o no de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin límite.

El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas.

El acta se puede considerar dividida en tres partes: hacker (ingresar sin permiso en una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada.

El último apartado se refiere tanto al hacking (por ejemplo, la modificación de un programa, para instalar el backdoor, la infección con virus o, lleno al extremo, a la destrucción de datos como la inhabilitación de funcionamiento de la computadora.

Bajo esta ley liberar un virus es delito y en enero de 1993 hubo un raid contra el grupo de creadores de virus. Se produjeron varios arrestos en la que fue considerada la primera prueba de la nueva ley en un entorno real.

4.6 CONCLUSIONES

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

De la criminología debemos señalar que en el anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados como un factor criminógeno que favorece la multiplicación de autores que utilicen los métodos electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley.

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

“Al final, la gente se dará cuenta de que no tiene ningún sentido escribir leyes específicas para la tecnología. El fraude es el fraude, se realice mediante el correo postal, el teléfono o Internet. Un delito no es más o menos delito si se utilizó criptografía (….). Y el chantaje no es mejor o peor si se utilizaron virus informáticos o fotos comprometedoras, a método antiguo. Las buenas leyes son escritas para ser independientes de la tecnología. En un mundo donde la tecnología avanza mucho más de prisa que las sesiones del congreso, eso es lo único que puede funcionar hoy en día. Mejores y mas rápidos mecanismos de legislación, juicios y sentencias… quizás algún día.”[5]

[5] SCHNEIER, Bruce. Secrets & Lies. Página 28-29.

CAPITULO 5

AMENAZAS HUMANAS

Este capítulo trata sobre cada uno de los personajes que pueden ser potenciales atacantes de nuestro sistema: el mundo under y el personal perteneciente a la organización.

Será difícil mantener una posición objetiva de la situación global en cuanto a los hackers y las fuerzas de seguridad, ya que siempre he visto marcado mi camino de conocimiento por la curiosidad: principal ingrediente (como veremos) del hacker. Así mismo, siempre me he mantenido en la raya de la legalidad y la ética, siendo prueba de esto el presente documento.

Desde los inicios del hacking siempre se ha mantenido una extraña relación entre estos particulares personajes, lo legal, lo ético y lo moral, siendo estas características lo que intentan resaltar para establecer la diferencia entre cada uno de los canales existentes en la red (como se llama comúnmente en jerga).

El presente tratara de exponer el perfil de la persona encargada de una de las principales, publicitariamente, si bien no la mayor amenaza que asecha nuestro sistema informático; para luego así entrar en las formas de ataques propiamente dichos.

5.1 PATAS DE PALO Y PARCHES

Se mueven en una delgada e indefinida barrera que separa lo legal de lo ilegal. Las instituciones y las multinacionales del software les temen, la policía los persigue y hay quien los busca para contratarlos. Se pasean libremente por las mayores computadoras y redes del mundo sin que ellas tengan secretos.

Como expresa Cybor , hay quienes los llaman piratas y delincuentes. Ellos reivindican su situación e intentan acalorar las diferencias entre los distintos clanes del Underground asegurado que sus acciones se rigen por un código ético.

Alguien aseguró que el que no usa su PC para escribir cartas, lleva un hacker dentro. Esta afirmación es una falacia si entendemos como hacker a un pirata informático, o quizás después de aclarar lo que significa este término, el resultado será que existan mayores cuestionamientos que respuestas pero, sin duda, estos serán de una índole radicalmente distinta a la planteada hasta ahora.

“La policía quiere creer que todos los hackers son ladrones. Es una tortuosa y casi insoportable por parte del sistema judicial, poner a la gente en la cárcel, simplemente porque quieren aprender cosas que les esta prohibido saber…

La familia es grande, y el término más conocido es hacker. Pero ¿Qué son? ¿Quiénes son? ¿Qué persiguen? ¿Existen? ¿Cuántos son? ¿Dónde están?...

Los años han hecho que esta palabra sea prácticamente intraducible, dando esto diversos resultados negativos y casi siempre acusadores sobre la persona que realiza hacking.

Actualmente el término acepta, según la "jergón" (jerga hacker) hasta siete definiciones y variados orígenes de la palabra. En el presente se maneja la etimología más ampliamente aceptada en el Underground digital.

La palabra inglesa **Hack** literalmente **significa** "golpear" o "hachear" y proviene de los tiempos en que los técnicos en telefonía "arreglaban" algunas máquinas con un golpe seco y certero: es decir, que éstos técnicos eran Hackers y se dedicaban a hachear máquinas.

Estos inocentes golpes no parecen tener nada en común con las fechorías que hoy se les atribuyen. Estos hackers tampoco parecen ser el estereotipo formado en la actualidad de ellos: un chico con gruesos lentes, con acne y ojeroso por estar todo el día delante de su computadora, vagando por Internet tratando de esconder su último golpe y gastando cifras astronómicas en cuentas de teléfono que pagará su vecino, alguien en otro continente o nadie.

Estudiemos historia y veamos los puntos en común que hacen que un técnico en telefonía sea igual que un chico curioso y hace que cada uno de nosotros sea pirata al fotocopiar un libro o copiar el último procesador de palabras del mercado.

En el MIT (Massachustts Institute on Technology) existen diferentes grupos con intereses especiales, fraternidades y similares que cada año intentan reclutar a los nuevos estudiantes para sus filas. En el otoño de 1958, durante su primera semana en el MIT, Peter Samson, que siempre había estado fascinado por los trenes y en especial por los metros, fue a ver la espectacular maqueta que el TMRC (Telch Model Railroad Club) tenía instalada en el Edificio 20 del Instituto.

En el TMRC existían dos fracciones claramente diferenciadas: aquellos que se encargaban de construir los modelos de los trenes, edificios y paisajes que formaban la parte visible de la instalación y; el Subcomité de Señales y Energía que tenía a su cargo el diseño, mantenimiento y mejora de el sistema todo aquello que quedaba bajo los tableros, hacia funcionar los trenes y que permitía controlarlos. El TMRC daba una llave de sus instalaciones a sus miembros cuando estos acumulaban 40 horas de trabajo y "Sansón" obtuvo la suya en un fin de semana.

Los miembros de subcomité de Señales y Energía no se limitaban a trabajar en las instalaciones del TMRC, si no que no era extraño encontrarlos a altas horas de la madrugada recorriendo edificios y túneles de servicio intentando averiguar como funcionaba el complejo sistema telefónico del MIT, sistema que llegaron a conocer mejor que quienes lo habían instalado.

En la primavera de 1959, se dictaba el primer curso de programación al que se podían apuntar alumnos en su primer año. Sansón y otros miembros del TMRC estaban en el (…).

Fue en aquel entonces, cuando un antiguo miembro del TMRC y entonces profesor del MIT hizo una visita al club y les pregunto a los miembros del Subcomité de Señales y Energía si les apetecería usar el TX-0. Este era una de las primeras computadoras que funcionaban con transistores en lugar de con lámparas de vació.

El TX-0 no usaba tarjetas si no que disponía de un teclado en el que el propio usuario tecleaba sus programas, que quedaban codificados en una cinta perforada que luego se introducía en el ordenador. El programa era entonces ejecutado y si algo iba mal el mismo usuario se podía entrar en la consola del TX-0 e intentar corregir el problema directamente usando una serie de interruptores y controles.

Dado que solo se disponía una equivalente a 9 KB de memoria, es fundamental optimizar al máximo los programas que se hacían, por lo que una de las obsesiones fundamentales de los que lo usaban y se consideran hábiles era hacer los programas tan pequeños como fuera posible, eliminando alguna instrucción aquí y allá o creando formas ingeniosas de hacer las cosas. A estos "apaños" ingeniosos se les llama "hacks" y de ahí es de donde viene el término "Hacker" denominación que uno reciba de sus compañeros (…)…

De esta historia podemos obtener el perfil principal:

- Un hacker es a todas luces, alguien con profundos conocimientos sobre la tecnología.
- Tienen ansias de saberlo todo, de obtener conocimiento.
- Le gusta (apasiona) la investigación.
- Disfruta del reto intelectual y de rodear las limitaciones en forma creativa.
- Busca la forma de comprender las características del sistema estudiando, aprovechar sus posibilidades y por último modificarlo y observar los resultados.
- Dicen NO a la sociedad de la información y SI a la sociedad informada.

Hoy los hackers se sienten maltratados por la opinión pública, incomprendidos por una sociedad que no es capaz de comprender su mundo y, paradójicamente, perseguidos por las fuerzas de orden y por multinacionales que desean contratarlos.

La policía compra su incursión en una computadora ajena con la de un ladrón en un domicilio privado; pero para ellos la definición valida es: "no rompemos la cerradura de la puerta ni les robamos nada de sus casas, nosotros buscamos puertas abiertas, entramos, miramos y salimos". Eso lo pintes como lo pintes, no puede ser un delito.

La opinión del abogado español, experto en delito informático, Carlos Sánchez Almeida parece coincidir con esta última posición, es decir, si un hacker entra en un sistema, sin romper puertas y sin modificar los contenidos no se puede penalizar su actuación y va mas allá al afirmar, que tampoco será delito, en cambio, el robo de bases de datos privadas con información confidencial y también es denunciable la “dejadez” que cometen algunas empresas que disponen de información y datos privados de usuarios y, sin embargo no tienen sus sistemas de seguridad suficientemente preparados para evitar el robo.

5.1.1 ACTITUD DEL HACKER

Como en las artes creativas, el modo mas efectivo de transformarse en un maestro es imitar la mentalidad de los maestros, no solo intelectualmente, si no además emocionalmente.

Se deberá aprender a puntuarse, principalmente, en función de que los otros hackers lo denominen así de manera consistente. Este echo esta empañado por la imagen del trabajo de hacker como trabajo solitario; también por un tabú cultural de los hackers (si bien en la actualidad es menor, aún es frente) que impide que se admita al ego o la validación externa como elementos involucrados en la propia motivación.

El estatus y reputación se gana no mediante la dominación de otras personas, no por ser hermoso/a, ni por tener cosas que las otras personas desean, si no por donar cosas: específicamente su tiempo, su creatividad y el resultado de sus habilidades.

Específicamente, el hackerismo es lo que los antropólogos denominan “cultura de la donación”. Existen básicamente cinco clases de cosas que un hacker puede hacer para obtener el respeto de otros hackers:

1.-Lo primero (el aspecto central y más tradicional es escribir programas que los otros hackers opinen son divertidos y/o útiles, y donar los fuentes del programa a la cultura hacker para que sean utilizados. Los más reverenciados semidioses del hackers son las personas que han escrito programas de gran magnitud, con grandes capacidades que satisfacen necesidades del largo alcance, y los donan, de tal manera que cualquiera puede utilizarlos (free).

2.-Ayudar a probar y depurar software libre. Son reconocidas aquellas personas que depuran los errores de software libre. Es considerado un buen Beta-Tester aquel que sabe como describir claramente los síntomas, que puede localizar correctamente los problemas, que tolera los errores en una entrega apurada, y que esta dispuesto a aplicar unas cuantas rutinas sencillas de diagnostico.

3.-Recolectar y filtrar información útil e interesante y construir paginas Web o documentos como FAQs y ponerlos a disposición de los demás.

4.-La cultura hacker funciona gracias al trabajo voluntario. Los administradores de listas de correo, moderados de foro de discusión y sitios donde se archivan grandes cantidades de software, desarrolladores de RFCs y otros estándares técnicos gozan de mucho respeto, porque se sabe que estos son trabajos consumidores de tiempo y no tan divertido. Llevar adelante este trabajo demuestra mucha dedicación.

5.-Hacer algo por la cultura hacker en sí misma. Esta cultura no tiene líderes exactamente pero tiene héroes culturales, historiadores triviales y voceros. La búsqueda visible de esta clase de fama es peligrosa, por lo que la molestia es siempre recomendada.

5.1.2 DEFINICIÓN DE HACKER

Un Hacker es una persona que esta siempre en una continua búsqueda de información (free, información), distribución de software sin costo y la globalización de la comunicación.

El concepto de hacker generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

- Un hacker es pirata. Esto no es así ya que los piratas comercian con la información que obtiene. Entre otras cosas y un verdadero hacker solo obtiene esa información para su uso personal.
- Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que el que destruye información y sistemas ajenos no es el hackers sino el Cracker.

Pero entonces veamos que si es un **hackers**

1.-Un hackers es pirata. Esto no es así ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero hackers solo obtiene esa información para su uso personal.

2.-Un verdadero hacker no se mete en el sistema para borrarlo todo, para vender lo que consiga. Quiere aprender y satisfacer su curiosidad. Esa es la única finalidad de introducirse en el sistema. Buscan dentro de un lugar en el que nunca han estado, exploran todos los pequeños rincones de un mundo diferente del que ya conocen y que les aburre ¿Por qué destruir algo y perderse el placer al decir a los demás que hemos estado en un lugar donde ellos no han estado?

3.-Un hacker es inconformista ¿Por qué pagar por una información que solo van a utilizar una vez?

4.-Un verdadero hacker no se mete en el sistema para borrarlo todo o para vender lo que consiga. Quiere aprender y satisfacer su curiosidad. Esa es la única finalidad de introducirse en el sistema. Buscan dentro de un lugar en el que nunca han estado, exploran todos los pequeños rincones de un mundo

diferente del que ya conocen y que les aburre ¿Por qué destruir algo y perderse el placer de decir a los demás que hemos estado en un lugar donde ellos no han estado?

5.-Un hacker disfruta con la exploración de los detalles de los sistemas programables y aprovecha sus posibilidades; al contrario de la mayoría de los usuarios, que prefieren aprender solo lo imprescindible.

6.-Un hacker programa de forma entusiasta (inclusive obsesiva), rápido y bien.

7.-Un hacker es experto en un programa en particular, o realiza trabajos frecuentemente usando ciertos programas. Por ejemplo “un hacer de Unix programador en C”.

8.-Los hackers suelen congregarse. Tiende a connotar participación como miembro en la comunidad global definida “como la Red”.

9.-Un hacker disfruta el reto intelectual de superar o de rodear las limitaciones de forma creativa.

10.- Antiguamente en esta lista se incluía: Persona maliciosa que intenta descubrir información sensible: contraseñas, acceso a redes, etc. Pero para este caso en particular los verdaderos hackers han optado por el termino Cracker y siempre se espera (quizás inútilmente) que se los diferencie.

Nótese que ninguna definición define al Hacker como un criminal. En el mejor de los casos, los Hackers cambian precisamente la fabricación de la información en la que se sustenta la sociedad y contribuyen al flujo de la tecnología. En el peor, los Hackers NO escriben dañinos virus de computadora. Quienes lo hacen son los programadores tristes, inseguros, y mediocres. Los virus dañinos están completamente en contra de la ética de los Hackers.

5.1.3 LA CONEXIÓN HACKER – NERD

Contrariamente al mito popular, no es necesario ser un nerd para ser un hacker. Ayuda, sin embargo, y muchos Hackers son nerds, Al ser un marginado social, el nerd puede mantenerse concentrado en las cosas realmente importantes, como pensar y Hachear.

Por esta razón, muchos Hackers han adoptado la etiqueta de “nerd” e incluso utilizan el termino **“Geek”** como insignia de orgullo: es una forma de declarar su propia independencia de las expectativas sociales normales.

5.1.4 CRACKERS

Los Crackers en realidad, son hackers cuyas intenciones van mas allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de manera equivocada o simplemente personas que hacen daño solo por diversión. Los Hackers opinan de ellos que son…hackers mediocres, no demasiados brillantes, que buscan violar (literalmente “break” un sistema.

5.1.5 PHREAKERS

Otro personaje en el Underground es el conocido como: **Phreaker.** El Phreaking, es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software, pueden engañar a las compañías telefónicas para que estas no cobren las llamadas que se hacen.

La realidad indica que los Phreackers son Cracker de las redes de comunicación. Personas con amplios conocimientos en telefonía. (a veces mayor que el de los mismos empleados de las compañías telefónicas).

Se dice que el Phreacking es el antecesor del Hachikg ya que es mucho más antiguo. Comenzó en los albores de la década de los ´60 cuando un tal Mark Bernay descubrió como aprovechar un error de seguridad de Bell basada en la utilización de los mecanismos para la realización de llamadas gratuitas. Lo que Bernal descubrió, fue que dentro de Bell existían unos números de prueba que servían para que los operarios comprobaran las conexiones.
Hasta aquí eran todos simples adolescentes que hacían llamadas gratuitas a sus padres en otro estado.

La situación cambio cuando se describió que Mama Bell (como suele llamarse a Bell) era un universo sin explorar y al que se le podría sacar más partido que el de unas simples llamadas. Se comenzaron a utilizar ciertos aparatos electrónicos, los cuales son conocidos como Boxers (cajas). La primera fue Blue Box que fue hallada en 1961 en el Washington State Collage, era un aparato con una carcasa metálica que estaba conectada al teléfono. Estas Boxes lo que hacían era usar el nuevo sistema de Bell (los tonos) para redirigir las llamadas. Cuando se marcaba un número, Bell lo identificaba como una combinación de notas musicales que eran creadas por seis tonos maestros, los cuales eran los que controlaban Bell y por lo tanto eran secretos (al menos eso pretendía y creían los directivos de Bell).

El como los Phreackers llegaron a enterarse del funcionamiento de estos tonos fue algo muy simple: Bell, orgullosa de su nuevo sistema, lo publico detalladamente en revistas que iban dirigidas única y exclusivamente a los operarios de la compañía telefónica.
Lo que sucedió es que no cayeron en la cuenta de que todo suscriptor de esa revista recibió también en su casa un ejemplar que narraba el funcionamiento del nuevo sistema.

Al poco tiempo hubo en la calle variaciones de la Blue Box inicial que fueron llamadas gratis desde teléfonos públicos.

Las Blue Boxees no solo servían para realizar llamadas gratuitas, si no que proporcionaban a sus usuarios los mismos privilegios que los operadoras de BEI.

Lo realmente curioso, y desastroso para Bell, seque algunas cosas eran capaces de silbar 2600 ciclos (lo cual significa que la línea esta preparada para recibir una llamada) de forma completamente natural.

El primer Phreaker que utilizo este método fue Joe Engressia, quien era ciego, a los 8 años, y por azar, silbo por el auricular de su teléfono cuando escuchaba un mensaje pregrabado y la llamada se corto. Realizo esto varias veces y en todas se les cortaba. La razón es un fenómeno llamado Talk-Offque consiste en que cuando alguien silba y alcanza casualmente a los 26000 Hz, la llamada se corta, como si fuera un Blue Box orgánica. Joe aprendió a como potenciar su habilidad para silbar los tonos del número con el que quería conectarse.

Otro Phreaker que utilizaba el método de Engressia, fue Jhon Draper, mas conocido como Capitán Crunch que creo un silbato que regalaban con la marca de cereales Capitán Crunch, el cual podría utilizarse como instrumento para hacer Phreaking. Draper hacia algo parecido a lo que hacia Joe Egressia: soplaba su silbato y la línea se queda libre.

Muchos Phreakers evolucionaron mas tarde al hacking, como es el caso del pionero Mark Bernay, que bajo el nick de The Midniht Skuller (el vigilante de medianoche) se rió de todos los fallos de seguridad de muchas empresas.

Hoy, el Hacking y el Phreacking viven en perfecta armonía y en pleno auge con las nuevas tecnologías existentes. Es difícil delimitar el terreno de cada uno, ya que un Hacker necesitara, tarde o temprano hacer Phreacking si desea utilizar la línea telefónica mucho tiempo en forma gratutita y; de la misma forma un Phreacker necesitara del hacking si desea conocer en profundidad cualquier sistema de comunicaciones.

5.1.6 CARDING - TRASHING

Entre las personas que dedicaban sus esfuerzos a romper la seguridad como reto intelectual hubo un grupo (con no tan buenas intenciones) que trabaja para conseguir una tarjeta de crédito ajena. Así nació:

1.-El **Carding**, es el uso (o generación) ilegitimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener los bienes realizando fraude con ellas. Se relaciona mucho con el Hacker y el Cracking, mediante los cuales se consiguen los números de las tarjetas.

2.-El **Trashing** que consiste en rastrear en las papeleras en busca de información contraseñas o directorios.

5.1.8 DESAFIOS DE UN HACKER

1. El mundo esta lleno de problemas fascinantes que esperan ser resueltos.
2. El esfuerzo requiere motivación. Los atletas exitosos obtienen su motivación a partir de una clase de placer físico que surge de trabajar su cuerpo, al forzarse a si mismos mas allá de sus propios limites físicos. De manera similar un Hacer siente un estremecimiento de tipo primitivo cuando resuelve un problema, agudiza sus habilidades, y ejercita su inteligencia.

3. Nadie debería tener que resolver un problema dos veces.
4. Los cerebros creativos son un recurso valioso y limitado. No debe desperdiciarse reinventando la rueda cuando hay tantos y tan fascinantes problemas nuevos esperando por allí.
5. Lo aburrido y lo rutinario es malo.
6. Los Hackers (y las personas creativas en general) no deberían ser sometidas a trabajos rutinarios porque cuando esto sucede significa que no están resolviendo nuevos problemas.
7. La libertad es buena.
8. Los Hackers son naturalmente anti-autoritaristas. Cualquiera que le pueda dar ordenes, puede hacer que deba dejar de resolver ese problema con el cual esta fascinado.
9. La actitud no es sustituto para la competencia.
10. Tener la actitud para hacer Hacker no alcanza para transformarse en un atleta campeón o en estrella del rock. Para transformarse en Hacker necesitará inteligencia, práctica, dedicación, y trabajo pesado. Por lo tanto, debe respetar la competencia en todas sus formas.

5.1.9 HABILIDADES BÁSICAS EN UN HACKER

El conjunto de habilidades cambia lentamente a lo largo del del tiempo a medida que la tecnología crea nuevas tecnologías y descarta otras por obsoletas. Por ejemplo hace tiempo, se incluía la programación en lenguaje de máquina y Asembler, y no se hablaba de HTML. Un buen Hacker incluye las siguientes reglas en su itinerario.

1.- Aprender a programar. Esta es, por supuesto, la habilidad fundamental de Hacker. Se deberá aprender como pensar en los problemas de programación de una manera general, independientemente de cualquier lenguaje. Se debe llegar al punto en el cual se pueda aprender un lenguaje nuevo en días, relacionado lo que esta en el manual con lo que ya sabe de antes. Se debe aprender varios lenguajes muy diferentes entre si. Es una habilidad compleja y la mayoría de los mejores hackers lo hacen de forma autodidacta.

2.- Aprender Unix. El paso mas importante es obtener un Unix libre instalarlo en una maquina personal y hacerlo funcionar. Si bien se puede aprender a usar Internet sin saber Unix, nunca se podrá hacer en Internet sin conocerlo. Por este motivo, la cultura Hacer actual esta centrada fuertemente en Unix.

5.1.10 ¿CÓMO LO HACEN?

Quizás esta sea la pregunta más escuchada cuando se habla de hackers y los ataques por ellos perpetrados.

Para contestarla debemos ser conscientes de cada una las características de los hackers entre las que se destacan la paciencia y la perseverancia ante el desafió planteado. Será común ver a algunos de ellos fisgonear durante meses a la victima luego recién intentar un ataque que además de efectivo debe ser invisible.

En capítulos posteriores se analizaran las técnicas (si bien no las herramientas específicas) por ellos utilizadas para perpetrar un ataque, así

como también las utilizadas por los expertos en seguridad a la hora de descubrir y tirar por tierra las ambiciones hackers.

5.1.11 ETIQUETA DEL HACKER

Desde el principio los hackers desarrollaron un código de ética o una serie de principios que eran tomados como un acuerdo implícito y no como algo escrito o fijo:

I. **El acceso a las computadoras debe ser ilimitado y total.**
II. **El acceso a la información debe ser libre y gratuito.**
III. **Desconfíen de la autoridad, promuevan la descentralización.**
IV. **Los hackers deben ser juzgados por su habilidad, no por criterios absurdos como títulos, edad, raza, o posición social.**
V. **Se puede crear arte y belleza en una computadora.**
VI. **Las computadoras pueden cambiar tu vida para mejor.**

Así también, se desarrollaron algunos “Mandamientos” en los cuales se basa un hacer a la hora de actuar sobre los sistemas que ataca.

I. Nunca destroces nada intencionalmente en la PC que estés hacheando.
II. Modifica solo los ficheros que hagan falta para evitar tu detección y asegurar tu acceso futuro al sistema.
III. Nunca dejes tus datos reales, tu nombre o tu teléfono en ningún sistema, por muy seguro que creas que es.
IV. Ten cuidado a quien le pasas información. De ser posible no le pases nada a nadie que no conozcas, su voz, número de teléfono y nombre real.
V. Nunca dejes tus datos personales en un BBS, si no conoces el SysOp, déjale un mensaje con la lista de gente que pueda responder por ti.
VI. Nunca hackees en computadoras de gobierno. El gobierno puede permitirse gastar fondos en buscarte, mientras que las universidades y las empresas particulares no.
VII. No uses Blue Box a menos que no tengas un Pad local o número gratuito al que conectarte, si se abusa de la Blue Box, puede ser cazado.
VIII. No dejes en mucha información del sistema que estas hacheando, di sencillamente “estoy trabajando en”. pero no digas a quien pertenece, ni el número del teléfono, dirección etc.
IX. No te preocupes en preguntar, nadie te contestara. Piensa que por responderte a una pregunta, pueden cazarte a ti, al que te contesta o a ambos.
X. Punto Final. Hasta que no estés realmente hackeado, no sabrás que es…

5.1.12 MANIFIESTO HACKER

En los principios, un grupo hackers llamado Legion of Doom, dirigido por, The Mentor, quería demostrar hasta donde era capaz de llegar. Para ello

modificaron la página principal del sitio Web de la NASA, durante media hora, con el siguiente “manifiesto”

Fermín (alias) es un estudiante universitario español, trabaja en una empresa de seguridad informática ganado un sueldo impactante. Este trabajo lo consiguió siendo hacker y según dice el por… nacer y ser curioso por hacer el hacking una forma de vida, un espíritu de superación y un reto de intelectual continuo (…) También declara que en la red hay gente con los mismos conocimientos que el que los utilizan para delinquir e incluso son buscados y pagados para ello, “… pero este no es un hacker”.

Un ejemplo de este es accionar puramente hacker lo demuestra al denunciar a un hospital sus fallos de seguridad (luego de haber penetrado el sistema) y recibiendo “como premio” una denuncia por intrusión ilegal. Acciones como estas son comunes en el mundo hacker pero “tapados” y generalmente distorsionados en contra de “estos personajes siniestros”.

5.1.13 OTROS HABITANTES DEL CIBERESPACIO

5.1.13.1 GURUS

Son considerados los maestros y los encargados de “formar” a los futuros hackers. Generalmente no están activos pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales solo enseñan las técnicas básicas.

5.1.13.2 LAMERS O SCRIPT – KIDDERS

Son aficionados jactosos. Prueban todos los programas (con el titulo “como ser un hacker en 21 días) que llegan a sus manos. Generalmente son los responsables de soltar virus y bombas lógicas en la red solo con el fin de molestar y que otros se enteren que usa tal o cual programa. Son aprendices que presumen de lo que no son aprovechados los conocimientos del hacker y lo ponen en práctica sin saber.

5.1.13.3 COPY HACKERS

Literalmente son falsificadores sin escrúpulos que comercializan todo lo copiado (robado).

5.1.13.4 BUCANEROS

Son comerciantes sucios que venden los productos crackeados por otros. Generalmente comercian con tarjetas de crédito y de acceso y compran a los copyhackers. Son personas sin ningún (o escaso) conocimiento de informática y electrónica.

5.1.13.5 NEWBIE

Son los novatos de hackers. Se introducen en sistemas de fácil acceso y fracasan en muchos intentos, solo con el objetivo de aprender las técnicas que puedan hacer de el, un hacker reconocido.

5.1.13.6 WANNABER

Es aquella persona que desea ser hacker pero estos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva fácilmente consiga avanzar en sus propósitos.

5.1.13.7 SAMURAI

Son lo más parecido a una amenaza pura. Sabe lo que busca, donde encontrarlo y como lograrlo. Hace su trabajo por encargo y a cambio de dinero. Estos personajes, a diferencia de los anteriores. No tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers. Se basa en el principio de que cualquiera puede ser atacado y saboteado. Solo basta que alguien lo desee y tenga el dinero para pagarlo.

5.1.13.8 PIRATAS INFORMÁTICOS

Este personaje (Generalmente confundido con el hacker) es el realmente peligroso desde el punto de vista del Copyright, ya que copia soportes audiovisuales (discos compactos, casettes, DVD, etc.) y los vende legalmente.

5.1.13.9 CREADORES DE VIRUS

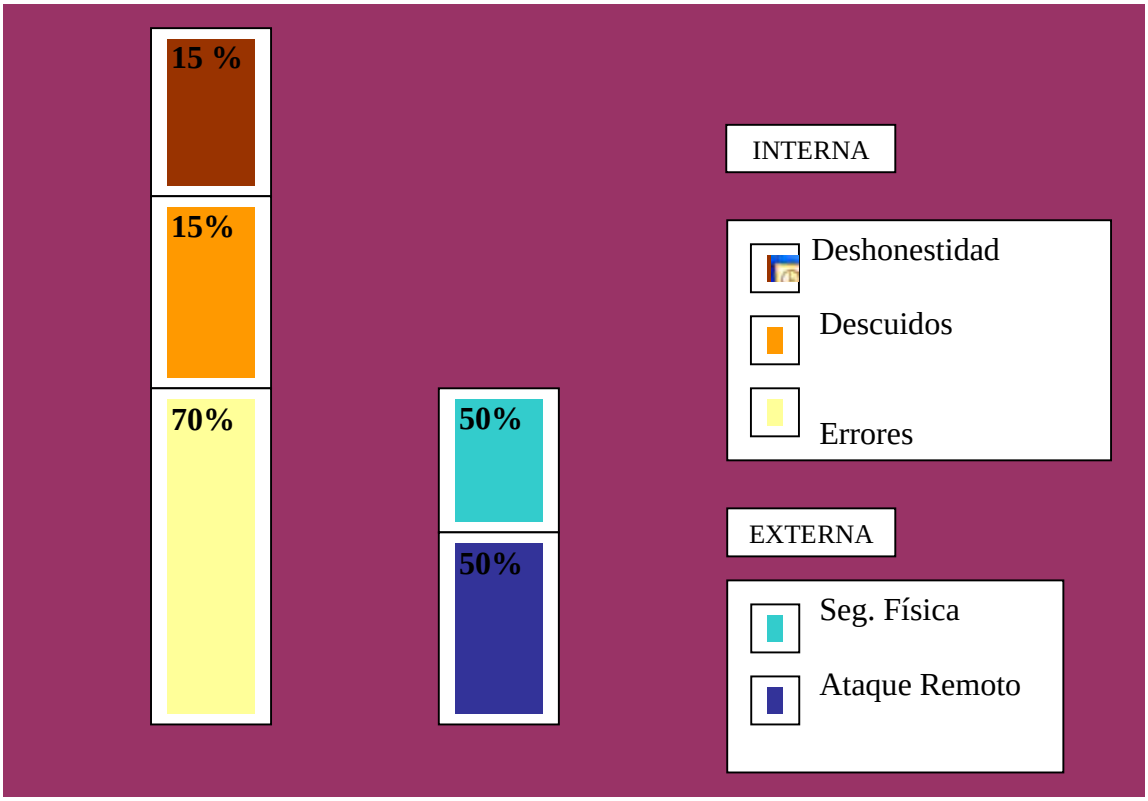
Si de daños y mala fama se trata estos personajes se llevan todos los premios. Aquí una vez más, se debe hacer la diferencia entre los creadores: que se consideran a si mismos desarrolladores del software; y los que infectan los sistemas con los virus creados. Sin embargo es difícil imaginar cualquier “desarrollador” no se vea complacido al ver que su “creación” ha sido “ampliamente” adquirida por el publico.

5.2 PERSONAL (INSIDERS)

Hasta aquí se ha presentado al personal como victima de atacantes externos; sin embargo, de los robos, sabotajes o accidentes relacionados con los sistemas informáticos, el 70% son causados por el propio personal de la organización propietaria de dichos sistemas.

Hablando de los insiders Julio C. Ardita. Explica que (…) desde mitad de 1996 hasta 1999la empresa tuvo dos casos de intrusiones pero en el 2000registramos siete, de las cuales 5 eran intrusos internos o ex – empleados (…).

El siguiente grafico detalla los porcentajes de intrusiones clasificado a los atacantes en internos y externos.



Interna 70% Externa 30%

TIPO DE INFRUSION

Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de una maquina conoce perfectamente el sistema, sus puntos débiles y fuertes; de manera que un ataque realizado por esa persona podrá ser mas directo, difícil de detectar y mas efectivo que el que un ataque externo pueda realizar.

Existen diversos estudios que tratan sobre los motivos que llevan a una persona a cometer delitos informáticos contra su organización, pero sean cuales sean, estos motivos existen y deben prevenirse y evitarse. Suele decirse que todos tenemos un precio (dinero, chantaje, factores psicológicos, etc.) por lo que nos pueden arrastrar a robar y vender información o simplemente proporcionar acceso a terceros.

Como ya se ha mencionado los ataques pueden ser de tipo pasivo y activos, y el personal realiza ambos indistintamente dependiendo de la situación concreta. Dentro de este espectro podemos encontrar:

5.2.1 PERSONAL INTERNO

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad pero también pueden ser del tipo intencional.

Es de destacar que un simple electricista puede ser más dañino que el más peligroso de los piratas informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema.
Al evaluar la situación, se vera que aquí el daño no es intencionado por ello no esta en discusión, el daño existió y eso es lo que compete a la seguridad informática.

5.2.2 EX – EMPLEADO

Este grupo puede estar especialmente interesado en violar la seguridad de nuestra empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes o bien aquellos que han renunciado para pasar a trabajar en la competencia. Generalmente se trata de personas descontentas con la organización que conoce a la perfección la estructura del sistema y tienen los conocimientos necesarios como cardar cualquier tipo de daño. También han existido casos donde el desempleado deja Bombas Lógicas que exploran tipo después de marcharse.

5.2.3 CURIOSOS

Suelen ser los atacantes más habituales del sistema. Son personas que tienen un alto interés en las nuevas tecnologías, pero aun no tienen los conocimientos ni experiencia básica para considerarlos hackers o crackers (podrían ser nebíes. En la mayoría de los casos son estudiantes intentados penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para el vedada. Generalmente no se trata de ataques de daño pero afectan el entorno de fiabilidad con confiabilidad generado en un sistema.

5.2.4 TERRORISTAS

Bajo esta definición se engloba a cualquier persona que ataca el sistema para causar daño de cualquier índole en el; y no solo a la persona que coloca bombas o quema automóviles. Son ejemplos concretos de este tipo, ataque de modificación de los datos de clientes entre empresa competidora, o de servidores que albergan paginas, bases de datos entre partidos políticos contrarios, etc.

5.2.5 RECOMENDACIONES

Una norma básica, seria verificar cada aspirante a ser nuevo empleado; aunque tampoco debemos olvidar que el hecho de que alguien entre limpio a la organización no implica a que valla a seguir así durante el tiempo que trabaje en la misma, y mucho menos cuando abandone su trabajo.

Para minimizar el daño que un atacante interno puede causar se pueden seguir estos principios fundamentales:

- **Necesidad de conocimiento (Need to Know):** comúnmente llamado mínimo privilegio. Cada usuario debe tener el minimo privilegio que necesite para desempeñar correctamente su función es decir, que solo se le debe permitir que sepa lo necesario para realizar su trabajo.
- **Conocimiento parcial (dual control) :**Las actividades mas delicadas dentro de la organización deben ser realizadas por dos personas competentes, de forma que si uno comete un error en las políticas de seguridad el otro pueda subsanarlo. Esto también es apilable al caso de que si uno abandona la organización el otro pueda seguir operando el sistema mientras se realiza el reemplazo de la persona que se retiro.
- **Rotación de funciones:** La mayor amenaza del conocimiento parcial de tareas es la complicidad de dos responsables, de forma tal, que se pueda ocultar sendas violaciones a la seguridad. Para evitar el problema, una norma común es rotar (dentro de ciertos límites)a las personas a lo largo de diferentes responsabilidades, para establecer una vigilancia mutua.
- **Separación de funciones:** Es necesario que definan y separen correctamente las funciones de cada persona, de forma que alguien cuya tarea es velar por la seguridad del sistema no posea la capacidad para violarla sin que nadie se percate de ello.
- **Cancelación inmediata de cuenta:** cuando un empleado abandona la organización se debe cancelar inmediatamente el acceso a sus antiguos recursos y cambiar las claves que el usuario conocía. Quizás este ultimo punto sea el mas difícil de implementar debido a la gran cantidad de usuarios que se deben informar de los nuevos accesos y de la movilidad de algunos de ellos.

En estos puntos se encuentran las vulnerabilidades de un sistema ya que, por ejemplo suelen encontrarse cuentas de usuario que hace años que no se utilizan, y por ende tampoco se han cambiado sus passwords.

- Si bien estas normas pueden aplicarse a las organizaciones, no podrán hacerlo en instituciones como una universidad, donde la mayoría de los atacantes son alumnos y no podrán verificarse los antecedentes (tampoco ético prohibir su acceso por ser estos dudosos). De esta forma en las redes de investigación y desarrollo de acceso público debemos ceñirnos a otros mecanismos de control y casi siempre se opta por las sanciones a todos aquellos que utilicen el centro para cometer delitos informáticos.

CAPITULO 6

COMUNICACIONES

Durante el siglo XX la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención del radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de las computadoras, así como la puesta en orbita de los satélites de comunicación.

A medida que avanzábamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y además las diferencias entre la captura, transporte y almacenamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo un botón. Mientras crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de procesos mas sofisticados crece todavía con mayor rapidez.

La industria de informática ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener una sola computadora para satisfacer todas las necesidades de calculo de una organización se esta remplazando por otro que consideran un numero grande de computadoras separadas, pero interconectadas, que efectúan el mismo trabajo. Estos sistemas se conocen con el nombre de redes. Se dice que los sistemas están interconectados, si son capaces de intercambiar información. Esta conexión puede realizarse a través de un alambre de cobre, fibra óptica, láser, microondas o satélites de comunicaciones.

6.1 OBJETIVOS DE LAS REDES

Las redes en general, consisten en “compartir recursos” y uno de sus objetivos es el hacer que todos los programas, datos y equipos estén disponibles para cualquier usuario de la red que asi lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a miles de kilómetros de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta finalidad, al contar con fuentes alternativas de suministros. La presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque el rendimiento global sea menor.

Otro objetivo es el ahorro económico. Las computadoras pequeñas tienen una mejor relación costo/rendimiento, comparada con la ofrecida por las maquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido que los microprocesadores pero su costo es miles de veces

mayor. Este desequilibrio ha ocasionado que muchas diseñadoras construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario y con los datos guardados en una o mas maquinas que funcionan como servidor de archivo compartido.

Este concepto conduce al concepto de redes con varias computadoras en el mismo edificio. A este tipo de red se denomina LAN, en contraste con el extenso de una WAN.

Un punto muy relacionado es la capacidad para aumentar el rendimiento de sistema en forma gradual a medida que crece la carga, simplemente añadiendo más procesadores.

Otro objeto del establecimiento de una red, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre si.

Una forma que muestra el amplio potencial del uso de redes como medio de comunicación es el Internet y el uso del correo electrónico (e-mail), que se envié a una persona situada en cualquier parte del mundo que disfrute de este servicio.

6.1.1 ESTRUCTURAS

Definir el concepto de redes implica diferenciar entre el concepto de redes físicas y redes de comunicación.

Respecto a la estructura física, los modos de conexión y de los flujos de datos, etc.; una **Red** la constituyen dos o más computadoras que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento, etc.). O software (aplicaciones o archivos, datos, etc.).

Desde una perspectiva mas comunicativa y que expresa mejor lo que puede hacerse con las redes, podemos decir que existe una red cuando están involucrados un componente humano que comunica, un componente tecnológico (computadoras, telecomunicaciones) y un componente administrativo (institución que mantienen los servicios). Así, a una **red** más que varias computadoras conectadas, las constituyen personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.

Las redes deberían ser lo mas transparentes posibles, de tal forma que el usuario final no requiera tener conocimiento de la tecnología (equipos y programas) utilizada para la comunicación.

6.1.1.1 TECNOLOGÍAS DE TRANSMISIÓN

Al crear una red, se toman en cuenta dos factores principales: el medio físico de transmisión y las reglas que rige la transmisión de datos. El primer factor se llama nivel físico y el segundo protocolo.

Este nivel físico generalmente encontramos señales de voltaje que tienen un significado preconcebido. Estas señales se agrupan e interpretan para formar entidades llamadas paquetes de datos. La forma de acceder a estos paquetes la determina la tecnología de transmisión, aceptándose a dos tipos:

1. Las redes de tipo **Broadcast** se caracterizan porque todos los miembros (nodos) pueden acceder a todos los paquetes que circulan por el medio de transmisión.
2. Las redes **Point-To-Point** solo permite que un nodo se conecte a otro en un momento dado.

6.1.1.2 MODELO CLIENTE / SERVIDOR

En vez de construir sistemas informáticos como elementos monolíticos, existe el acuerdo general de construirlos como sistemas Cliente/Servidor. El cliente (un usuario de PC) solicita un servicio (por ejemplo imprimir) que un servidor (un procesador conectado a la LAN) le proporciona. Este enfoque común de la estructura de los sistemas informáticos se traduce en una separación de las funciones que anteriormente formaban un todo. Los detalles de la realización van desde los planteamientos sencillos hasta la posibilidad real de manejar todas las PC´s de modo uniforme.

6.1.1.3 TECNOLOGÍA DE OBJETOS

Otro de los enfoques para la construcción de los sistemas parte de la hipótesis de que deberían estar compuestos por elementos perfectamente definidos, objetos cerrados y materializados haciendo de ellos agentes independientes. La adopción de los objetos como medios para la construcción de sistemas informáticos ha colaborado a la posibilidad de intercambiar los diferentes elementos.

6.1.1.4 SISTEMAS ABIERTOS

Esta definición alude a sistemas informáticos cuya arquitectura permite una interconexión y una distribución fácil. En la práctica, el concepto del sistema abierto se traduce en desvincular todos los componentes de un sistema y utilizar estructuras análogas en todos los demás. Esto conlleva una mezcla de normas (que indican a los fabricantes lo que deberían hacer) y de asociaciones (grupo de entidades a fines que les ayuden a realizarlo). El efecto final es que sean capaces de “hablar” entre si.

El objetivo ultimo de todo el esfuerzo invertidos en los sistemas abiertos consiste en que cualquiera pueda adquirir computadoras de diferentes fabricantes, las coloque donde quiera, utilice conexiones de banda ancha para enlazarlas entre si y las haga funcionar como una maquina compuesta, capaz de sacar provecho de las conexiones de lata velocidad.

Parece lógico suponer que las computadoras podrán trabajar en un conjunto cuando dispongan de una conexión entre ellas. Pero ¿Cómo conseguir, sin

embargo, que computadoras de diferentes fabricasen distintos países funcionen en común a través de todo el mundo? Hasta hace poco, un equipo podía comunicarse con otro de su misma “familia”, pero tenía grandes dificultades para hacerlo con un “extraño”.

6.1.1.5 EL MODELO OSI

El modelo conceptual OSI (Open System Interconection) es utilizado, por prácticamente, la totalidad de las redes del mundo. Este modelo fue creado por el ISO (International Estándar Organization), y consiste en siete niveles o capas donde cada una de ellas define las funciones que debe proporcionar los protocolos con el propósito de intercambiar información entre varios sistemas.

Esta clasificación permite que cada protocolo fuera desarrollado con una finalidad determinada, lo cual simplifica el proceso de implementación. Cada nivel depende de los que están por debajo de el, y a su vez proporciona alguna funcionalidad a los niveles superiores.

Los siete niveles del modo OSI son los siguientes:

1. Capa Física: esta capa tiene que ver con el envió de bits en un medio físico de transmisión y asegura de que si un extremo del medio se envía un 1 (carga eléctrica) del otro lado se reciba ese 1. Brinda los medios eléctricos, mecánicos, de procedimiento y funcionales para activar y mantener el enlace físico entre los sistemas.

2. Capa de Enlace: en esta capa se toman los bits que entrega la Capa Física y se agrupan para formar macros de bits (frames). Se realiza un chequeo de errores sobre cada frame. Si un marco se pierde o se daña en el medio físico este capa se encarga de retransmitirlo, aunque en ocasiones dicha operación provoca que un mismo marco se duplique en el destino. Dado el caso es obligación detectar tal anomalía y corregirla. También en esta capa se decide como acceder al medio físico.

3. Capa de red: se encarga de controlar la operación de la subred (medios físicos y dispositivos de enrutado). Una tarea primordial es decidir como hacer que los paquetes lleguen a su destino desde su origen en el formato predefinido por un protocolo. Otra función importante en este nivel es la resolución de cuellos de botella. En estos casos se pueden tener varias rutas para dar salida a los paquetes y en base a algunos parámetros de eficiencia o disponibilidad se eligen rutas dinámicas de salida. A los efectos de la obtención de estadísticas, se rija el tipo y cantidad de paquetes que circulan.

4. **Capa de Transporte:** el objetivo de esta capa es el de tomar datos de la Capa de Sesión y asegurarse que dichos datos llegan a su destino. En ocasiones los datos que vienen de la Capa de Sesión exceden el tamaño máximo de transmisión (MTU) Maximum Trasmisión Unit) de la interfaz de red, por lo cual es necesario partición arlos y enviarlos en unidades

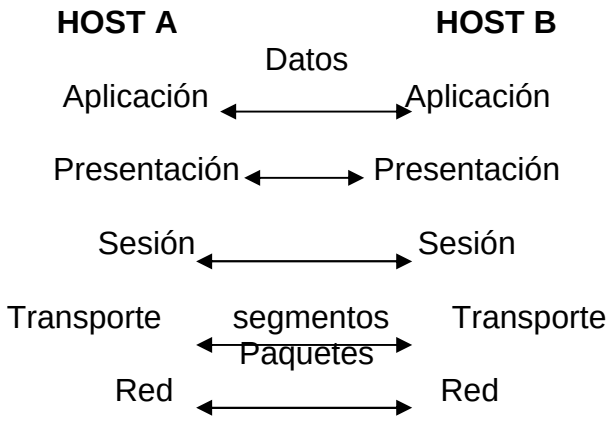
mas pequeñas, lo cual da origen a la fragmentación y ensamblado de paquetes cuyo control se realiza en esta capa.

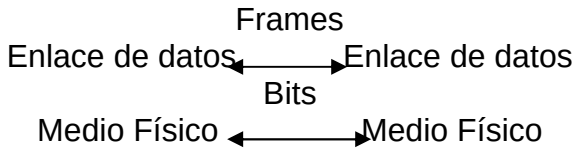
El último valor importante de la Capa de Transportes es ofrecer un mecanismo de nombrado que sirva para identificar y diferenciar las múltiples conexiones existentes, así como determinar en que momento se inician y se terminan las “conversaciones”, es decir, en esta capa hay un mecanismo de control de flujo. Por ejemplo, si el usuario “a” en el nodo (A) quiere iniciar una sesión de trabajo remoto en un nod (B) existirá una conexión que debe ser diferenciada de la conexión que el usuario “b” necesita para transferir un archivo del nodo (B) al nodo (A).

5. **Capa de Sesión:** esta capa ofrece el servicio de establecer sesiones de trabajo entre nodos diferentes de una red, sincroniza y establece puntos de chequeo. Por ejemplo, si se hace necesario trasferir un archivo muy grande entre dos nodos que tienen una alta probabilidad de sufrir una caída, es lógico pensar que una trasmisión ordinaria nunca terminaría porque algún interlocutor perderá la conexión. La solución esque se establezcan puntos de chequeo cada pocos minutos de manera que, si la conexión se rompe, mas tarde se puede reiniciar a partir del punto de chequeo, lo cual ahorra tiempo y permite la finalización de la transferencia.

6. **Capa de Presentación:** estas provee las facilidades para transmitir datos con la sintaxis propia de las aplicaciones o el nodo. En esta capa es posible convertir los datos a un formato independiente de los nodos que intervienen a la transmisión.
7. **Capa de Aplicación:** en esta capa se encuentran las aplicaciones de red que permiten explotar los recursos de otros nodos. Dicha explotación se hace, por ejemplo, a través de una emulación de una Terminal que trabaja en un nodo remoto, interpretando una gran variedad de secuencias de caracteres de control que permite desplegar en la Terminal local los resultados, aun cuando estos sean gráficos. Otra forma de explotación se da cuando se transmite desde una computadora origen que almacena sus archivos en un formato distinto al del destino. Es posible que el programa de transferencia realice las conversaciones necesarias de manera que el archivo puede usarse inmediatamente bajo alguna aplicación.

Gráficamente:





Esto se explica que HOST B (Capas del Host) entrega entre computadoras. Y capaz de medios (Entrega Física de mensajes).

6.1.1.5.1 TRANSMISIÓN DE DATOS

Un envió de datos típico bajo el modelo de referencia OSI comienza con una aplicación en un nodo cualquiera de la red. Esta aplicación genera los datos que quiere enviar a su contraparte en otro nodo.

- La Capa de Aplicación toma los datos y los encapsula añadiendo un encabezado que puede tener información de control o estar vació. Envía el paquete resultante a la Capa de Presentación.

- La capa de presentación recibe el paquete y no intenta decodificarlo o separar sus componentes, si no que lo toma como datos y le añade un encabezado con información de control de esta capa.

- Las Capas de Sesión y de Transporte reciben el paquete, que también son solo datos para ellas y le añaden un encabezado de control. El resultado es enviado a la capa inferior.

- La capa de red se encarga de enlutar el paquete a su destino.

- Las Capas de Red, Enlaces de datos y Física, toman, respectivamente, el paquete que les envía la capa superior y añade a este un encabezado definido por el protocolo que corresponde a cada capa y pasan el resultado a la capa inferior.

- La Capa Física, por ultimo traducirá el último paquete a las señales apropiadas para que viajen por el medio físico hasta el nodo destino.

- En el nodo destino comienza el camino inverso; es decir que cada capa quita su encabezado de control y envía el paquete a la capa superior hasta llegar a la de Aplicación en este nodo destino.

Como puede apreciarse, todas las capas, excepto la de Aplicación, Procesan los paquetes realizando operaciones que sirvan para verificar que el paquete de datos real esté integro, o para que este llegue a su destino sin que los datos sufran alguna alteración.

6.2 PROTOCOLOS DE RED

En las redes, las computadoras deben comunicarse entre si e intercambiar datos con sistemas operativos y hardware muy distintos.

El nivel físico, esto se realiza a través de placas de redes, y una conexión entre las mismas. Lógicamente se debe establecer una comunicación “del mismo lenguaje” entre distintos sistemas operativos y de placas. Este lenguaje es a lo que se le llama protocolo.

Algunos protocolos se encargan de transportar datos mientras que otros se encargan de la comunicación entre computadoras, y otros de convertir correctamente los datos. Así **Protocolo** es el conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

Actualmente existen protocolos para cualquier tipo de comunicación que nos imaginemos; muchos de ellos han caído en desuso y otros se encuentran en su plenitud de utilización. Esto es producto de una sociedad cada vez mas intercomunicada y relacionada, en donde lo importante es que la información llegue a su destino si, pero también lo es que llegue a las mismas condiciones en que ha sido enviada y en el tiempo previsto.

Algunos de los protocolos más conocidos y ampliamente difundidos son:

6.2.1 NETBIOS – NETBEUI-NWLINK-WINS

Network Basic Input Outuput System, es el protocolo más sencillo. Esta compuesto por menos de 20 comandos que se ocupan del intercambio de datos. Se ha perfeccionado y ampliado recibiendo el nuevo nombre NetBEUI (NetBIOS Extended User Interfase) pero continua utilizando el juego de comandos del NetBIOS y luego para hacerlo compatible con otros protocolos (como IPX-SPX) se amplio nuevamente recibiendo el nombre de NW Link (NetWare Link).

Net BIOS se toma el puerto 137-139 en computadoras que utilizan el sistema operativo Windows de la empresa Microsoft. Este considerado el protocolo más fácilmente vulnerable de los existentes, a punto tal que cualquiera especialista de seguridad recomienda no utilizarlo.

6.2.2 TCP/IP

En los años 80 una gran cantidad de instituciones estaban interesadas en conectarse a una gran red que se expandía por todo EE.UU. (ahora Internet). Para esto definieron un conjunto de reglas que establecen como conectar computadoras entre si para lograr el intercambio de información.

Actualmente TCP/IP se utilizan ampliamente en la versión 4 (IPv4) que no incluye la seguridad como parte de su construcción. Sin embargo se encuentra el desarrollo (Ipv4) que no incluye la seguridad como parte de su construcción.

Sin embargo se encuentra en desarrollo (Ipv6 o IPSec) que dentro de sus estándares soporta autenticación, integridad y confidencialidad a nivel de data gramas.

Basado en las capas de modelo OSI, se defendió un conjunto de protocolos de TCP/IP. Que consta de 4capas principales y que se han convertido en un estándar a nivel mundial.

6.2.2.1 LAS CAPAS DEL MODELO TCP/IP

El trasmisión Protocol/Internet Protocol es actualmente el protocolo mas ampliamente utilizado por su independencia del Sistema Operativo y hardware utilizando. Es un eficaz protocolo orientado por paquetes; es particularmente adecuado como plataforma para protocolos de los más distintos servicios y aplicaciones que se pueden conseguir a través de la red.

TCP/IP no es el único protocolo, sino que en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmisión Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. Se diferencian cuatro capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI como se muestra en el grafico 6.2.

Aplicación: Se corresponde con los niveles OSI de Aplicación, Presentación, y Sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de archivos (FTP), conexión remota (telnet) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).

Transporte: Coincide con el nivel de transporte del modelo OSI. Esta capa esta implantada por dos protocolos: El Transmission Control Protocol (TCP) y el User Datagram Protocolo (UDP). El primero es un protocolo confiable (reliable) y orientado a conexiones, lo cual significa que ofrece un medio libre de errores para enviar paquetes. El segundo es un protocolo no orientado a conexiones (connectionless) y no es confiable (unreliable). El TCP se prefiere para la transmisión de datos a nivel red de área amplia y el UPD para redes de área local

Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esa finalidad por los protocolos del nivel de transporte.

Interfaz de Red: correspondiente al nivel de Enlace y Físico de la pila OSI los protocolos que pertenecen a este nivel son los encargados de la

transmisión a través del medio físico al que se encuentra conectado cada hot, como se puede ser una línea punto a punto o una red Ethernet .

La capa inferior, que podemos nombrar como Física respecto al modelo OSI contiene varios estándares (conocidos con el nombre del IEEE 802.X) que establecen las reglas para evitar datos por cable coaxial delgado (10Base 2), cable coaxial grueso (10Base5), par trenzado (10-Base-T), fibra óptica (10-Base.f) y su propio método de acceso.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio; de forma que sea posible intercambiar información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, esta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren. En TCP/IP cada una de estas unidades de información recibe el nombre de “Data grama” (datagram), y son conjuntos de datos que se envían con los mensajes independientes.

6.2.2.2 FUNCIONAMIENTO

Las aplicaciones de la red presentan los datos a TCP. Este divide los datos en trozos (paquetes), y le otorga cada uno un número. El conjunto de paquetes ordenados puede presentar imágenes, documentos, videos, o cualquier otra información que el usuario desee enviar.

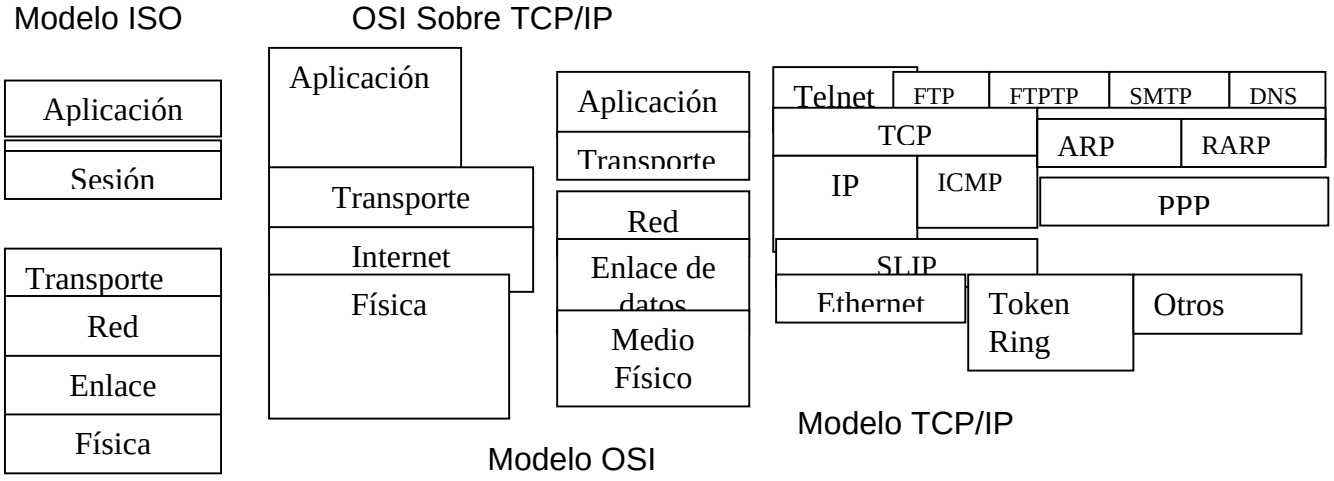
Luego el TCP presenta los datos a IP, quien agrega su información de control (como ser dirección de origen y destino). Si por algún motivo IP no puede entregar algún paquete, TCP pedirá el reenvió de los faltantes. Por ultimo TCP se encarga de re ensamblar los paquetes en el orden completo, basándose en los números asignados previamente.

6.2.2.3 COMPARACIÓN CON EL MODELO OSI

Si bien TCP/IP, este último no tuvo éxito debido a causas como el momento de su introducción, la tecnología existente en ese momento, malas implementaciones y políticas y parte de los investigadores. Sin embargo el OSI es un buen modelo y el TCP/IP es un buen conjunto de protocolos y la combinación de ambos es la que permite contar con las comunicaciones que se tiene hoy.

El modelo TCP /IP no tiene dividida las Capas de Enlace de Datos, Presentación y Sesión y la experiencia ha demostrado que en la mayoría de los casos son de poca utilidad.

Los estándares 802.X junto con el protocolo IP realizan todas las funciones propuestas en el modelo OSI hasta la Capa de Red. Los protocolos TCP y UDP cumplen con la Capa de Transportes. Finalmente, las aplicaciones ya mencionadas son ejemplos prácticos y reales de la funcionalidad de la Capa de Aplicación.
Gráficamente pueden apreciarse las siete capas del modelo y su relación directa en su implementación sobre el protocolo TCP/IP.



6.2.3 NIVEL FÍSICO DEL MODELO TCP/IP

6.2.3.1 ARP

El Address Resolución Protocol no se dedica al transporte de datos sino a convertir las direcciones IP en direcciones de la red física.

El protocolo consigue la dirección mediante la difusión de un paquete de petición ARP que contiene la dirección IP del sistema destinatario. Todos los ordenadores de la red detectan estas difusiones y aquel que contenga la dirección IP solicitada, la trasmitirá al sistema solicitante mediante una respuesta de paquete ARP. Luego el solicitante almacena estas direcciones en una tabla para su uso posterior; y esta tabla además servirá de referencia a otros equipos para evitar la búsqueda de las mismas direcciones.

6.2.3.2 RARP

El Reverse Address Resolución Protocol realiza el trabajo inverso de ARP. Es decir que obtiene la dirección IP a partir de una dirección física.

6.2.4 NIVEL DE DATOS DEL MODELO TCP/IP

6.2.4.1 SLIP

El serial Link Internet Protocol/Point to point protocol brinda una conexión de velocidad aceptable, con la posibilidad de admitir varias conexiones

simultaneas con un mismo modem. El mecanismo es sencillo: se llama al proveedor, quien oficia de puente entre su computadora y el resto de la red, y una vez establecida la comunicación se tiene acceso total a los servicios. Es un protocolo sencillo y pequeño, pensando en su fácil implementación; y en la baja velocidad de los enlaces telefónicos, por lo que ha caído en desuso.

Este protocolo apoya solamente IP, no provee detección de errores ni de autenticación y tienen la desventaja de que existen muchas implementaciones incompatibles entre ellas.

6.2.4.2 PPP

El Poínt To Point Protocolo fue desarrollo por el IETF (Internet Engineering Task Force) en 1993 para mejorar alguna deficiencia de SLIP, y crear un estándar internacional.

PPP es un protocolo mucho más amplio, más potente y adaptable. Proporciona un método de enlace bidireccional full dúplex para transportar data gramas multiprotocolo sobre enlaces simples (conexión directa) de un equipo a otro (punto a punto), en cualquier situación sin importar el tipo de conexión, el hardware y el sistema operativo.

Sus principales características son:

1. Es transparente a las capas superiores.
2. Transmite protocolos IP, IPX, Apple Tala, etc.
3. Es ampliable ya que no fue pensado para solucionar.

PPP esta dividido en dos subprotocolos:

1. **LCP (Link Control Protocola):** es el encargado de comenzar una conexión (fase abierta), definir como se producirá el intercambio de datos (tamaño de los paquetes, identificación, tiempos de espera, etc.) y de finalizar la conexión (enlace muerto).
2. **NCP (Network Control Protocola:** Se encarga de negociar y configurar las opciones de los diferentes protocolos de red, (IP/IPX, etc.) abriéndolos de a uno por vez. Una vez que un NCP ha alcanzado el estado abierto, PPP transportara los correspondientes paquetes. Cualquier paquete recibido mientras su NCP no este en el estado abierto es descartado.

6.2.5 NIVEL DE RED DEL MODELO TCP/IP

6.2.5.1 IPX-SPX

El Internetwok Packet Exchange – Sequenced PacketExchange es el protocolo de nivel de red propietario de NetWare (para su sistema operativo Novell) siendo utilizados en las redes tipo LAN.

6.2.5.2 IP

El Internet protocol define la base de todas las comunicaciones en Internet. Es utilizado por los protocolos del nivel de transporte (como TCP) para encaminar los datos hacia su destino. IP tiene únicamente la misión de encaminar el data grama, sin comprobar la integridad de la información que contiene. Para ello se utiliza una nueva cabecera que se antepone al datagrama que se esta tratando.

La cabecera IP tiene un tamaño de 160 bits y esta formada por varios campos del distinto significado entre los que se destaca el tipo de protocolo de transporte de datagrama, el numero de paquete (para su posterior ensamble), la dirección de origen y la de destino, etc.

Es de notar que este protocolo no garantiza la llegada de los paquetes a destino (conexión sin garantía) ni su orden; tan solo garantiza la integridad del encabezado IP. La fiabilidad de los datos deben garantizarla los niveles superiores. También se trata de una transmisión sin conexión porque cuando se envía el paquete, no se avisa al receptor para que este preparado (no existe una conexión directa emisor-receptor). De echo, muchas veces se mandan paquetes a un destino inasistente o que no se encuentra disponible.

El protocolo IP identifica a cada equipo que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bits que debe ser único para cada host y normalmente suele representarse como cuatro cifras de 8 bits separadas por puntos (por ejemplo: 205.025.076.233)

Este nivel IP se definen los siguientes aspectos de intercambio de información:

- Un mecanismo de direcciones que permite identificar de manera univoca al emisor y al receptor, sin considerar las ubicaciones ni las arquitecturas de las redes a las cuales pertenece cada uno. Este mecanismo permite la universidad de la red.
- Un concepto relativo de trasporte de los paquetes de datos, para que el mismo llegue al receptor a través de los nodos de las redes involucradas. Dentro de cada red tendrá que haber al menos un receptor (router) que esta conectado con otra computadora en otra red en el exterior. Los routers reconocen un paquete y comprueban que no sea para alguna maquina conectada a su red y entonces lo mandan a otra, mas cercana al destino. Esto se hace sucesivas veces hasta que el paquete llega al router de la red donde se encuentra la computadora destinataria del mensaje.
- Un formato para los paquetes (cabecera). Con esta, el Router podrá identificar al destinatario del mensaje, ya que como se explico, uno de los datos de la cabecera es el nombre de destino del mensaje.

La dirección IP se utiliza para identificar tanto a la computadora en concreto como a la red a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas

redes de tamaños muy diversos, se establecieron cuatro clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

1. **Clase A:** son los que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer bate para identificar la red , quedando los otros tres bates disponibles para cada una de las computadoras (hosts) que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de Hosts en cada una de las126 redes de esta clase. Este tipo de direcciones es usado por redes muy extensas.
2. **Clase B:** estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primero bytes de la dirección, debiendo ser un valor entre 128.001 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bates de la dirección constituyen el identificador de la computadora, permitiendo, por consiguiente, un numero máximo de 64.516ordenadores de la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes.
3. **Clase C:** en este caso el valor del primer byte tendrá que estar comprendido entre 129 y 233, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.001.001 hasta 223.254...254. De esta manera queda libre un byte para el hot, lo que permite que se conecten un máximo de 254 computadoras en cada red.
4. **Clase D:** esta clase se usa con fines de multidifusión a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.

Actualmente se planea la utilización de redes **Clase E** que comprenderían el rango desde 240.0.0.0 hasta 247.255.255.255.

6.2.5.2.1 DNS - NOMBRES DE DOMINIO

Ya que para el ser humano se hace difícil recordar direcciones IP como 209.89.67.156se creo lo que dio en llamar DNS (Domain Name Server), el cual es el encargado de convertir la dirección IP en un nombre de dominio generalmente fácil de recordar y viceversa. Así www.clarin.com será entendida, merced al servicio de DNS como 110.56.12.106 o // Carlos se convertirá en 10.0.0.33

6.2.5.2.2 PUERTOS

Para acceder desde el nivel de red a nivel de aplicaciones no sirve simplemente indicar la dirección IP; se necesitara mas especificaciones para que el Hot de destino pueda escoger la aplicación correa. Estas

especificaciones harán necesario la definición de **Puerto.** Un puerto se representa por un valor de 16 bits y hace la diferencia entre los posibles receptores de un mensaje.

La combinación Dirección IP +Puerto identifican una región de memoria única denominada **Socket**. Al indicar este Stocket, se puede trasladar el paquete a la aplicación correcta (FTP, telnet, WWW, etc.) y, si además recibe el puerto desde donde fue enviado el mensaje, se podrá suministrar una respuesta.

Actualmente existen miles de puertos ocupados a los 216=65535 posibles, de los cuales apenas unos cuantos son los más utilizados y se encuentran divididos entre tres ángulos:

- Desde el puerto 0 hasta el 1023: son los puertos conocidos y usados por aplicaciones de servidor.
- Desde el 1024 hasta el 49151: son los registrados y asignados dinámicamente.
- Desde el 49152 hasta 65535: son los puertos privados.

Puerto	**Aplicación**	**Protocolo**	**Descripción**
20 21 23	FTP-Data FTP TELNET	TCP/UDP TCP TCP/UDP	Transferencia archivos Control Transferencia Archivos Servicios remotos
25 43 53	SMTP Whois DNS	TCP/UDP TCP/UDP TCP/UDP	Envió de mails Servicio de nombre dominios
70 79 80	Ghoper Finger WWW-HTTP	TCP/UDP TCP/UDP TCP/UDP	 Word Wide Web
110	POP3(PostOffice)	TCP/UDP	Recepción de mail
119	UseNet	TCP	Newsgroup de usuarios
137	NetBIOS	UDP	
194	IRC (Internet Relay Chast	TCP/UDP	Chat
443	Kerberos IRC(Intenet Relay Chat)	TCP	http Seguro vía SSL

750 6667	Kerberos IRC (Internet relaychat)	TCP/UDP TCP	Chat

6.2.5.3 APPLE TALK

El protocolo de Control de Transmisión (TCP) nació principalmente por la necesidad de una “comunicación” segura entre el emisor y el destinatario del mensaje. Así, las aplicaciones pueden encargarse de su tarea sin preocuparse de la seguridad en la comunicación.

6.2.6 NIVEL DE TRASNPORTE DEL MODELO TCP/IP

6.2.6.1 TCP

El protocolo de Control de Transmisión (TCP) nació principalmente por la necesidad de una comunicación “segura” entre el emisor y el destinatario del mensaje. Axial, las aplicaciones pueden encargarse de su tarea sin preocuparse de la seguridad en la comunicación.

TCP divide el mensaje original en datagramas en menor tamaño (múltiplo de 32 bits), y por lo tanto, mucho mas manejables. Los data gramas serán divididos a través del protocolo IP de forma individual. El protocolo TCP se encarga, además de añadir cierta información necesaria al inicio de cada uno de los data gramas (cabecera). Luego, se ocupa de que los datos sean entregados y que los paquetes sean reemblansados correctamente asegurando así que lo se recibe sea efectivamente lo enviado.

Si ocurriera algún error en la transmisión, TCP se encargara de reenviar los paquetes. TCP sabrá que hubo errores o que el paquete fue entregado correctamente gracias a un paquete de respuesta (acuse de recibo) que envía el destinatario al emisor (para que vuelva a realizar el envió) en donde indica si faltan paquetes, tamaños o datos erróneos, etc.

Las principales características de este producto son:

- 1.-**Servicio orientado a conexión:** el destino recibe exactamente la misma secuencia de bytes que envía el origen.
- 2.-**Conexión de circuito virtual:** durante la transferencia, el protocolo en las dos maquinas continua comunicándose para verificar que los datos se reciban correctamente.
- 3.-**Transferencia con memoria intermedia:** la aplicación utiliza paquetes del tamaño que crea adecuado, pero el software de protocolo puede dividir el flujo en subpaquetes o armar uno con un grupo de ellos, independientemente de la aplicación. Esto se realiza para hacer eficiente el tráfico en la red. Así, si la aplicación genera piezas de un byte, el protocolo puede armar datagramas razonablemente más largos antes de hacer el envió, o bien, forzar la transferencia dividiendo el paquete de la aplicación en datagramas mas pequeños.
- 4.-**Flujo no estructurado:** se refiere a la posibilidad de envió de información de control del estado junto a los datos propiamente dichos.
- 5.-**Conexión FullDuplex:** permite la transferencia concurrente en ambas direcciones, sin ninguna interacción. La ventaja es evidente: el

protocolo puede evitar datagramas desde el origen al receptor e información de control en sentido opuesto, reduciendo el tráfico en la red.

El Grafico detalla la constitución de cada data grama del protocolo TCP (160-192 bits =20-24 bates). Comprender este diagrama es de especial interés para cualquiera que desee manipular datos en una comunicación actual.

Puerto Origen	**Puesto Destino**
Numero de secuencia	
Numero de reconocimiento	
Log Header Reserved (urg,ack,psh,rst,ryn,fin) Window	
Check Sum	**Urgent Pointer**
Datos	

Los puertos proporcionan una manera de distinguir entre las distintas transferencias, ya que un mismo sistema puede estar utilizando varios servicios o transferencias simultáneamente, e incluso puede que por medio de usuarios distintos.

El **Puerto de Origen** (16 bits) contendrá un número cualquiera que sirva para realizar cualquier distinción. Además el programa cliente que realiza la petición también debe conocer el numero del puerto en el que se encuentra el servidor adecuado. Mientras el programa del usuario utiliza números prácticamente aleatorios, el servidor debe tener asignado un numero estándar para que pueda ser utilizado por el cliente (ver tabla), Cuando es el servidor el que envía los datos, los números de puertos de origen y destino se intercambian.

El campo **Tamaño de la cabecera** (4bits) contiene la longitud total de la cabecera TCP expresada en el numero de palabras de 32 bits que ocupa (el tamaño real divido en 4). Esto permite determinar el lugar donde comienza los **Datos.**

En la trasmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y perdida de información en los data gramas, es necesario que el cliente envié de nuevo al servidor unas **Señales de Confirmación** (32 bates) una vez que se ha recibido y comprobado la información satisfactoriamente. Si el servidor no obtiene señal de confirmación adecuada transcurrido un periodo de tiempo razonable, el data grama completo se volverá a enviar.

Por razones de eficiencia los datagramas se envían continuamente sin respirar la confirmación, haciendo necesaria la numeración, mediante los **Números de Secuencia** (32 bits) de los mismos para que puedan ser ensamblados en el orden correcto.

También puede ocurrir que la información del data grama llegue con errores a su destino. Para poder detectarlos, cuando sucede eso, se incluye un Check

zum (16 bits), el cual contiene un valor calculado a partir de la información del data grama completo. En el otro extremo el receptor vuelve a calcular este valor; comprobando que el mismo que el suministrado en la cabecera. Si el valor es distinto se significara que el data grama es incorrecto.

La forma en que TCP numera los data gramas es contado los bates de datos que contiene cada una de ellas y añadiendo esta información al campo correspondiente de la cabecera del datagrama siguiente.

De esta manera el primero empezara en cero; el segundo contendrá el tamaño de la parte de datos; el tercero contendrá la suma de ese numero mas el tamaño de los datos del segundo datagrama; y axial sucesivamente. Por ejemplo, para un tamaño fijo de 500 bates de datasen cada data grama, la numeración seria la siguiente: 0 para el primero, 500 para el segundo, 1000 para el tercero, etc.

Existe otro factor mas a tener en cuenta durante la transmisión de información, y es la potencia y velocidad con que cada computadora puede procesarlos datos que le son enviados. Si esto no se tuviera en cuenta, el equipo de mayor potencia podría enviar la información demasiado rápido al receptor, de manera que este no pueda procesarla. Este inconveniente se soluciona mediante un campo **Windows** (16 bits) en el cual se introduce un valor indicadora cantidad de información que el receptor esta preparado para procesar en un momento dado.

El campo **Opciones** (32 bits) permite que una aplicación negocie durante la configuración de la conexión, las características como el tamaño máximo del segmento TCP. Si este campo tiene el primero octeto tiene el primero octeto a cero, indica que no hay opciones, quedando una data grama de 160 bits.

Por ultimo cada datagrama tendrá un **Estado** que le indicara al servidor el contenido, motivo y la forma en que deberá ser atendido ese paquete. Este campo puede contiene los siguientes estados (Estado =1-Verdadero):

- Bit 4 (Urgen): Identifica datos urgentes.
- BIT 5 (ACKnowledge): Indica que el campo de confirmación es valido.
- Bit 3 (PuSH): Aunque el buffer de datos no este lleno, se fuerza el envio .
- Bit 2 (ReSet): Abortar la conexión. Todos los buffers asociados se vacían.
- BIT 1 (Sincronice séquense Number): Sincronizar los números de secuencia.
- BIT 0 (Finís): Se solicita el cerrado de la conexión.

Todas estas características se traducen en un “protocolo pesado” por el envió de señales de confirmación y la velocidad se ve sacrificada en pos de la fiabilidad de los datos.

6.2.6.2 UDP

El usar Datagram Protocol puede ser la alternativa al TCP en algunos casos en los que no sea necesario el gran nivel de complejidad proporcionando por el TCP. Puesto que UDP no admite numeración de los datagramas, este protocolo se utiliza principalmente cuando el orden en que se recibe los mismos no es un factor fundamental, cuando se quiere enviar información de poco tamaño que cabe en una única data grama o si la fiabilidad de los datos no es un factor de relieve.

Cuando se utiliza UDP la garantía de un paquete llegue a su destino es mucho menor que con TCP debido a que no se utilizan las señales de confirmación. Por todas estas características a la cabecera de UDP es bastante menor en tamaño que la de TCP. Esta simplificación resulta en una mayor eficiencia en determinadas ocasiones. Es utilizado en redes con muy buen cableado.

6.2.7 NIVEL DE APLICACIÓN DEL MODELO TCP/IP

6.2.7.1 ICMP

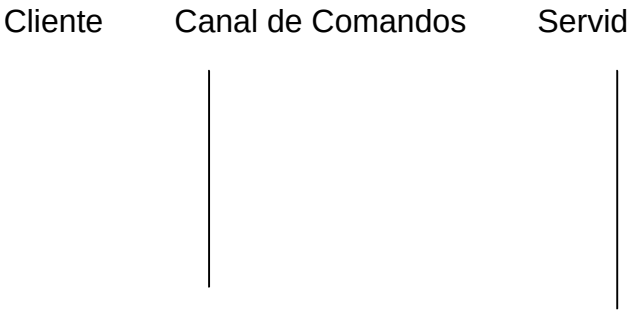
El Internet Control Mézale Protocola es de características similares al UDP, pero con un formato aun mas simple. Su utilidad no esta en el transporte de datos “de usuario”, si no en los mensajes de error y de control necesarios para los sistemas de la red.

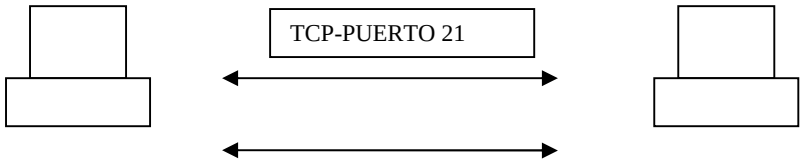
6.2.7.2 FTP

El file Transferí Protocol se incluye como parte del TCP/IP, estando destinando proporcionar el servicio de transferencia de archivos. El FTP depende del protocolo TCP para las funciones de transporte, y guarda alguna relación con telnet (protocol para la conexión remota).

FTP utiliza dos cables de conexión separados: uno es el canal de comandos que permanece abierto durante toda la sesión y el otro es el canal de transmisión de archivos.

Gráficamente:





Canal de datos
TCP-Puerto 20
Conexión FTP.

El FTP permite acceder acceder a algún servidor que disponga de este servicio y realizar tareas tales como moverse a través de su estructura de directorios, ver y descargar archivos al ordenador local, enviar y copiar archivos directamente de un servidor a otro de la red. Lógicamente y por motivos de seguridad se hace necesario contar con el permiso previo para poder realizar todas las operaciones. El servidor FTP pedirá el nombre de usuario y clave de acceso al iniciar la sesión (login). Este debe ser suministrado correctamente para poder utilizar el servicio.

La manera de utilizar FTP es por medio de una serie de comandos, los cuales suelen variar dependiendo del sistema en que se esta ejecutando el programa, pero básicamente con la misma funcionalidad. Existen aplicaciones de FTP para prácticamente todos los sistemas operativos.

Existe una forma muy utilizada para acceder a fuentes de archivos de carácter público por medio de FTP y es el acceso FTP anónimo, mediante el cual se pueden copiar archivos de uso público. Generalmente el acceso anónimo tendrá algunas limitaciones a otros permisos, siendo normal en estos casos que no se permite realizar acciones tales como añadir archivos o modificar existentes.

El FTP proporciona dos modos de transferencia de archivos. ASCII se utiliza cuando se quiere transmitir archivos de texto puro. El binario se debe utilizar en cualquier otro caso (datos que no son texto plano).

6.2.7.3 HTTP

Este Hipertexto Transferí Protocolo es la base de toda comunicación desarrollada en la web. Utilizando desde principios de los 90 es un protocolo ASCII que se ocupa de establecer una comunicación TCP segura entre el cliente y el servidor a través del puerto 80.

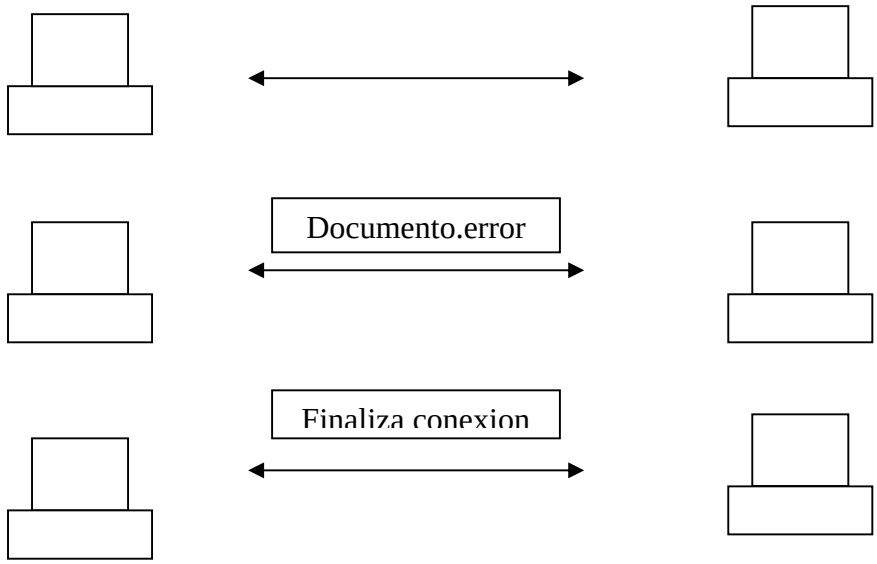
HTTP es un protocolo de aplicación para sistemas de información distribuidos, e hipermedíatico. Es un protocolo genérico, sin estado, orientado a objetos, que se pueden utilizar para muchas tareas, como servidores de nombres y sistemas de gestión de objetos distribuidos, por medio de la ampliación de sus métodos de petición o comandos.

Sus principales características son:

- Protocolo de aplicación: aunque generalmente se implementa sobre el TCP/IP, también es capaz de hacerlo sobre otros protocolos de capas mas bajas. HTTP presupone únicamente un transporte fiable, así que puede utilizar cualquier protocolo que garantice ese requisito mínimo.
- Sistemas de información distribuidos colaboradores, de hipermedios: HTTP soporta sistemas de información distribuidos es decir, sistemas esparcidos por múltiples servidores.
- Genérico: HTTP no dicta el contenido de los datos que transfiere; simplemente actúa como un conducto para mover datos de aplicación, por lo que se puede transferir cualquier tipo de información por medio de HTTP.
- Sin Estado: HTTP no mantiene un estado. Cuando se solicita una transferencia y se termina la conexión. Esta es una de las debilidades de HTTP, sin información de estado, cada pagina Web esta sola. Por ejemplo, es difícil desarrollar una aplicación basada en la Web esta sola. Por ejemplo es difícil desarrollar una aplicación que permita que un usuario se conecte en una página y que mantenga esta información de conexión durante todo el tiempo que el usuario este accediendo activamente al destino. Cualquier documento transferido a través de HTTP no tiene ningún contexto y es completamente independiente de todos los documentos transferidos antes de el.
- Orientando a objetos y escritura y negociación de la representación de los datos: HTTP no esta orientado a objetos en el mismo sentido que en un lenguaje de programación. Esta descripción significa simplemente HTTP tiene etiquetas que indican el tipo de datos que se van a transferir por medio de la red, así como métodos que son comandos que indica que debe transferirse.
- Sistema creado independientemente de los datos que se transfieren: debido a que HTTP solo mueve datos no necesita tener información sobre cada uno de los dos tipos a transferir. Por ejemplo, un servidor, Web no necesita un conocimiento específico sobre el funcionamiento interno del formato de un archivo de video para hacer el envió.

La comunicación que se establece en una conexión HTTP es de muy corta duración. El cliente establece la conexión con el servidor HTTP y le solicita un documento determinado. El servidor recibe la consulta, la evalúa y envía el documento solicitado (si existe) o un mensaje de error en caso contrario. Luego el servidor finaliza la conexión sin que existan otros estados intermedios.

Cliente Conexión Servidor
Solicitud de documentos



El protocolo HTTP en su estructura, divide el mensaje en encabezado (hender) y en cuerpo (Enity), separados entre si por una línea en blanco.

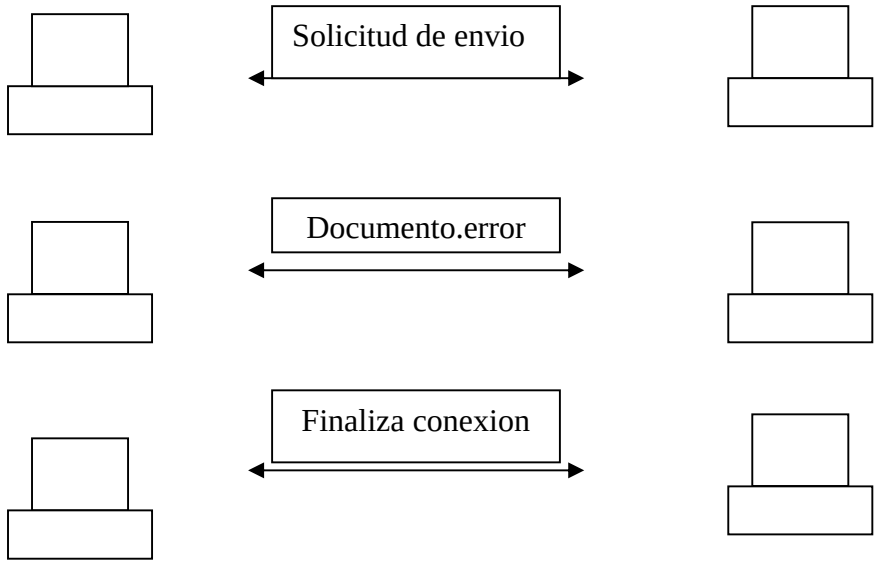
6.2.7.4 SMTP

El servidor de correo electrónico se proporciona a través del protocolo Simple Mail Transfer Protocol (empleado redes TCP/IP) y permite enviar mensajes a otros usuarios de la red. A través de estos mensajes no solo se puede intercambiar texto, si no también archivos binarios de cualquier tipo.

Generalmente los mensajes de correo electrónico no se envían directamente a las computadoras personales de cada usuario, si no a un servidor de correo que actúa como almacén de los mensajes recibidos. Los mensajes permanecerán en este sistema hasta que el usuario los transfiera a su propio equipo para leerlos de forma local (vía POP).

El cliente de correo envía una solicitud a su mail Server (al puerto 25) para enviar un mensaje (y almacenarlo en dicho servidor). El Server establece una conexión SMTP donde emisor y receptor intercambian mensajes de identificación, errores y el cuerpo del mail. Luego de esto el emisor envía los comandos necesarios para la liberación de la conexión.

Emisor Servidor



Conexión SMTP

6.2.7.5 POP

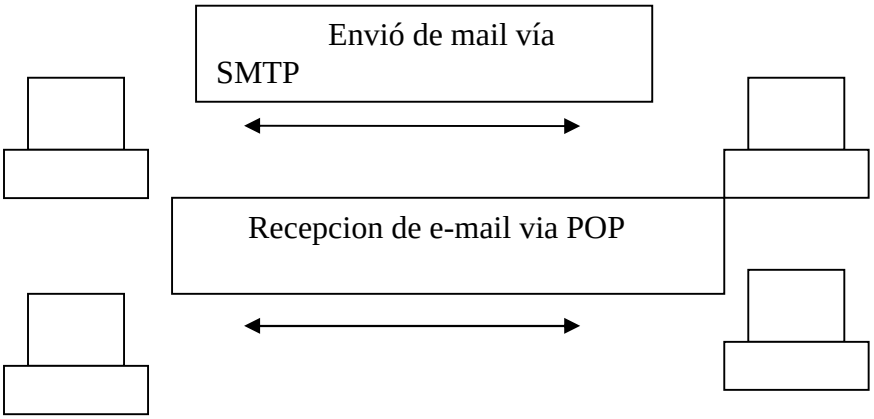
El servidor POP (Post Office Protocol) fue diseñado para la recuperacion de correo desde el e-mail Server hacia la computadora destinataria del mensaje.

Al igual que sucede con SMTP, inicialmente el proceso escucha el puerto del protocolo POP (el 110) y cuando el emisor solicita el mensaje se establece una conexión full duplex donde se intercambian los mensajes. Emisor-Server para luego finalizar la conexión cuando haya enviado cada uno de los mails que se almacena en el servidor.

Actualmente el protocolo POP se encuentra en su primera implementacion por lo que generalmente se escuchara sobre POP3.

Gráficamente la relacion entre el protocolo SMTP y el POP3 es la siguiente:

Cliente **Servidor**



Relación SMTP –POP

6.2.7.6 MIME

Multipurpose Internet Mail Extensions es una extensión de protocolo SMTP y se creo con el fin de soportar algunos juegos de caracteres extendidos (no US-ASCII) no soportados por este ultimo (parcialmente en francés y el alemán).

MIME especifica tres campos que se incluyen en la cabecera del mensaje, para hacer la conversación adecuada al sistema no US-ASCII utilizado.

- MIME-Versión: especifica la versión de MIME utilizando para codificar el mensaje.
- Content-Type: especifica el tipo y subtipo de los datos no ASCII.
- Contenet –Transfer-Encoding –especifica el tipo de codificación usado para traducir los datos en ASCII.

6.2.7.7 NNTP

El Network News Transfer Protocol fue diseñado para permitir la distribución, solicitud, recuperación y envió de noticias (News). NNTP esta basado en las especificaciones de UseNet (tratando también en este capitulo) pero con algunas modificaciones en su estructura que le permite ser adaptables a otros grupos de noticias no UseNet.

6.2.7.8 SNMP

El Simple Network Managment Protocol se utiliza para monitorizar, controlar y administrar múltiples redes físicas de diferentes fabricantes, donde no existe un protocolo común en la capa de enlace. La estructura de este protocolo se basa

en utilizar la capa de aplicación para evitar el contacto con la capa de enlace y aunque es parte de la familia TCP/IP no depende del IP ya que fue diseñado para ser independiente y puede correr igual de fácil sobre, por ejemplo, IPX de Novell.

6.3 ESTRUCTURA BÁSICA DE LA WEB

La estructura básica de la Word Wide Web (WWW) consiste en que el protocolo HTTP actúa como un transporte genérico que lleva varios tipos de información del servidor al cliente. Hoy en día las conexiones a servidores web son las mas extendidas entre usuarios de Internet, hasta el punto tal de que muchas personas piensan de que este servicio es el único existente, junto a IRC. Inicialmente se ideo para que unos cuantos físicos intercambiaran información entre universidades, hoy es uno de los pilares fundamentales de muchas empresas.

Cada entidad servidor se identifica de forma única con un Localizador de Recursos Universal (URI), que a su vez esta relacionado unívocamente con la dirección IP.

El tipo mas común de los datos transformados a través de HTTP es HTML (Hiper Text Markup Language) Además de incluir directrices para la "compresión" de textos, también tiene directrices que proporcionan capacidades como las de enlaces de hipertexto y la carga de imágenes en la línea. Los recursos hiperenlazados y los archivos de imágenes en línea están identificados con los URL intercalados dentro del documento HTML.

A pesar de algunos servidores Web personales de gama baja solo pueden enviar páginas estáticas, la mayoría de los servidores http admiten la CGI (Common Gateway Interface. Con GCI se pueden escribir programas que se integran en la Web y que realizan tareas tales como el proceso de formularios y la búsqueda en la base de datos0020las cuales, HTML np puede ejecutar.

La principal limitación de GCI es que esta restringida a programas en el lado del servidor. Por ejemplo, utilizando GCI la única forma en la que se puede interactuar con los usuarios es suministrándoles formularios a completar. Las tecnologías orientadas a objetos como Java afrontan esta limitación, permitiendo al servidor que envié al cliente pequeños programas para ejecutarlos locamente.

6.3.1 SERVICIOS DE INTERNET

Como sabemos, Internet es en la actualidad, la red de computadoras mas grande del mundo, Sin embargo la importancia de Internet no reside solamente en el numero de maquinas interconectadas sino en los servidores que brinda.

Los servicios y recursos de Internet (Gopher, News, Archie, WWW, etc.) son accesibles de diversas formas, principalmente tres: Telnet, por e-mail y por un programa cliente.

A través del Telnet o e-mail, el servicio presenta una interface ANSI (sin gráficos), solo con caracteres alfanuméricos. Con un programa cliente, la gestios es mas sencilla, visual, y agradable, como WWW donde se presenta cada una de las paginas en formato grafico.

6.3.1.1 TELNET

Este producto fue diseñado para proporcionar el servicio de conexión remota (remote login). Forma parte del conjunto de protocolos TCP/IP y depende del protocolo TCP para el nivel de transporte.

El protocolo Telnet es un emulador de Terminal que permite acceder a los recursos y ejecutar los programas de un equipo remoto en la red, de la misma forma que si se tratara de una Terminal real directamente conectado al mismo remoto. Una vez establecida la conexión el usuario podrá iniciar la sesión con su clave de acceso. De la misma manera que ocurre con el protocolo FTP, existen servidores que permiten un acceso libre cuando se especifica.”anonymous” como nombre del usuario.

El sistema local que utiliza el usuario se convierte en una Terminal no “inteligente” de todos los caracteres pulsados y las acciones que se realicen se envían a Hots remoto el cual devuelve el resultado de su trabajo. Para facilitar un poco la tarea a los usuarios, en algunos casos se encuentran desarrollados menús con las distintas opciones que se ofrecen.

Para utilizar Telnet se ejecuta un programa especial, llamado Telnet en el cliente. Este programa utiliza TCP para conectarse a un sistema especifico (su servidor) en el puerto 23 (por defecto). Una vez que se establece la conexión, telnet actúa como un intermediario entre el cliente y el servidor.

La mayoría de las computadoras que permiten este tipo de acceso cuentan con los programas necesarios diversos servicios de Internet, como Ghoper, Wais, FTP o cualquier otro programa-clientedisponoble en Server. Estas conexiones suelen ser mas economicas (pero mas lentas) y están restringidas a los servicios que brindan el servidor.

6.3.1.2 IRC

El Internet Realy Chat es un sistema de coloquio en tiempo real entre personas localizadas en distintos puntos de la red. Es un servicio basado exclusivamente en texto por teclado. Fue desarrollado en 1988 en Finlandia y es sin duda, hoy, uno de los servicios más populares de Internet.

Su gran atractivo es que permite las conversaciones en vivo de múltiples usuarios la mayor parte desconocidos entre si. El manejo del sistema es muy simple. El Incesta organizado por redes, cada una de los cuales esta formada por servidores que se encargan, entre otras cosas, de ofrecer canales de conversación (existiendo miles de ellos) y transmitir los mensajes entre usuarios.

Para acceder a un servidor de este tipo es necesario disponer de un gran programa cliente, siendo los cuatro mas populares el mIRC, Pirch, Ichat y Microsoft Chat.

Cada servidor IRC esta conectado a los servidores más cercanos. De esta manera, todos los servidores Incestan conectados (al menos indirectamente) unos con otros. El IRC mantiene un número de diferentes “Canales” teniendo que elegir al ingresar el canal de interés y pudiendo entrar y salir de los canales cuantas veces se desee y en cuantos canales se desee.

La mayoría de los nombres de canales empiezan con “numero”. Algunos canales son para discutir de temas específicos y otros surgen en el momento. Hay canales públicos, privados, secretos e individuales.

Se pueden crear canales (obteniendo la condición de operador) si el que desea no existe y esperar que otras personas ingresen en el. Se suele entrar en las charlas con apodos (nick), sin dar el nombre real, de manera que los usuarios conserven el anonimato. Cuando la ultima persona abandona un canal, IRC lo elimina.

6.3.1.3 USENET

Una de las areas mas populares de Internet son los grupos de discusión o NewGroups. El terminoUseNet surge de USEr NETwork (red de usuarios) y se refiere al mecanismo que soportan los grupos de discusión.

Los grupos se forman mediante la publicación de mensajes enviados (“posteados”) a un grupo en particular (generalmente de un tema específico). El software original de News fue desarrollado para los sistemas Unix en 1979 por los estudiantes graduados en la Universidad de Duke, como un mecanismo para la discusión técnica y conferencias.

Es una red que no se centra en un único servidor que distribuye los mensajes, si no en una cadena de servidores que se “pasan” los mensajes de los grupos que soporta ya que, normalmente, los servidores mantienen un grupo limitado de News.

Una vez creado un grupo, se puede evitar cualquier mensaje al mismo y cualquiera dentro del Internet podrá leerlo, a menos que sea un grupo “moderado” con lo cual nuestros mensajes pasan por la “censura” de un moderador.

Para hacer manejable toda la información que circula, se utiliza un sistema en el que los grupos de discusión se agrupan en categorías denominadas Jerarquías. Cada jerarquía tiene un nombre propio y se dedica a un área de interés particular.

Algunas de las jerarquías más relativas son:

Tema	Descripción
Alt (alternativa)	Diferentes Temas
Bionet	Biología
Biz (bussines)	Negocios
Comp (computer)	Computadoras e informática
Ddn	Red de Datos de Departamento de defensa
News	Grupo sobre UseNet
Rec (recreative)	Ocio
Sci (science)	Ciencias
Soc	Ciencias Sociales
Talk	Debates

La filosofía de la UseNet es la siguiente. Al dejar un mensaje, no solo se queda en el grupo en cuestión, si no que también les llega a todos los usuarios suscritos al mismo, vía e-mail.

Tiene una gran utilidad practica, ya que si un usuario determinado tiene algún comentario o duda acerca de un tema, puede acudir a un grupo temático indicado, dejar mensaje para pedir ayuda, y con seguridad recibirá la opinión de numerosas personas.

6.3.1.4 FINGER

La mayoría de las computadoras de Internet tiene una utilidad que permite buscar información sobre un usuario particular. Este servicio es conocido como Fingen (dedo).

En el Internet los usuarios se conocen como identificadores. Finger se puede utilizar para encontrar el nombre de un usuario si se conoce su identificador, ya que el objetivo de este servicio es obtener información sobre una persona en particular.

El servicio Finger es un Sistema cliente / servidor que proporciona tres tipos principales de información:

- Información publica sobre cualquier usuario.
- Comprobación de si un usuario esta utilizando actualmente un Host determinado en Internet, pudiendo ver un resumen de información para cada usuario que esta conectado.

- Conectar con determinado Host que se han configurado para ofrecer tipos de información.

6.3.1.5 WHOIS

¿Quién es? Es un servidor de directorio de páginas blancas que permite consultar una base de datos de nombres y direcciones de correo electrónico de un usuario (normalmente empresa).

El servicio Whols contacta a un servidor que tiene información básica sobre las redes que comprenden Internet y los nombres de las personas que dan mantenimiento. Por ejemplo la solicitud whoisHarvard produce una lista de todas las redes de la Universidad de Harvard y las compañías que tienen Harvard como parte de su nombre.

Originalmente la información sobre los usuarios de Internet se almacenaba en una base de datos central. Hoy en DIA muchas organizaciones corre este servicio que proporciona información sobre los usuarios de una organización. Uno de los servidores Wolf más conocido es whols.internic.net que contiene nombres y direcciones de Internet.

Es de remarcar que servicios como TelNet, Finger, Archie, Ghoper, Whols y Ping estan callendo en desusoa favor de las cada vez mas perfeccionadas herramientas basadas en World Wide Web. De todas maneras (como se vera en capitulos posteriores) siguen brindando gran utilidad a administradores de sistemas y usuarios avanzados, sobre todo en temas de seguridad.

CAPITULO 7

AMENAZAS LÓGICAS

La entropía es una magnitud termodinámica que cuantifica el grado de desorden de un sistema; y según las leyes físicas todo sistema tiende a su máxima entropía. Si extrapolamos este concepto a la seguridad resultaría que todo sistema tiende a su máxima inseguridad. Este principio supone decir:

- Los protocolos de comunicación utilizados carecen, en su mayoría, de seguridad o esta ha sido implementada, tiempo después de su creación, en forma de "parche".
- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.
- Todo sistema es inseguro.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

7.1 ACCESO – USO – AUTORIZACIÓN

La identificación de estas palabras es muy importante ya que el uso de algunas implica un uso desapropiado de las otras.

Específicamente "Acceso" y "Hacer Uso" no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso. Por ejemplo:

- Cuando un **usuario** tiene **acceso autorizado,** implica que tiene autorizado la utilización de un recurso.
- Cuando un **atacante** tiene acceso desautorizado esta haciendo uso desautorizado del sistema.
- Pero, cuando un atacante hace uso desautorizado de un sistema, esto implica que el acceso fue autorizado (simulación de usuario).

Luego un ataque será un intento de acceso, o uso desautorizado de un recurso, sea satisfactorio o no. Un incidente envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos, etc.).

John D. Howard[1] en su tesis estudia la cantidad de ataques que puede tener un incidente. Al concluir dicho estudio y basado en su experiencia en los

[1] *HOWARD, John D. http://www.cert.org*

laboratorios del CERT[2] afirma que esta cantidad varía entre 10 y 1000 y estima que un número razonable para estudios es de 100 ataques por incidentes.

7.2 IDENTIFICACIÓN DE LAS AMENAZAS

La identificación de las amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podría clasificar en:

- **Data corruption:** la información que no contenía defectos pasa a tenerlos.
- **Denial of Service (Dos):** servicios que deberían estar disponibles no lo están.
- **Leakage:** los datos llegan a destinos a los que no deberían llegar.

Desde 1990 hasta nuestros días, el CERT viene desarrollando una serie de estadísticas que demuestran que cada día se registran más ataques informáticos, y estos son cada vez más sofisticados, automáticos y difíciles de rastrear.

Cualquier adolescente de 15 años (Script Kiddies), sin tener grandes conocimientos, pero con una potente y estable herramienta de ataque desarrollada por los Gurús, es capaz de dejar fuera de servicio de información de cualquier organismo en Internet, simplemente siguiendo las instrucciones que acompañan la herramienta.

7.3 TIPOS DE ATAQUE

A continuación se expondrán diferentes tipos de ataques perpetrados, principalmente, por Hackers. Estos ataques pueden ser realizados sobre cualquier tipo de red, sistema operativo, usando diferentes protocolos, etc.

En los primeros tiempos, los ataques involucraban poca sofisticación técnica. Los Insiders (operadores, programadores, data entrys) utilizaban sus permisos para alterar archivos o registros. Los Outsiders ingresaban a la red simplemente averiguando una password válida. A través de los años, se han desarrollado formas cada vez más sofisticadas de ataque para explotar “agujeros” en el diseño, configuración y operación de los sistemas.

Son muchos los autores que describen con detalle las técnicas y las clasifican de acuerdo a diferentes características de las mismas.

7.3.1 INGENIERÍA SOCIAL

[2] CERT: Computer Emergency Response Team. Grupo de Seguridad Internacional especializado en dar respuestas a las empresas y organizaciones que denuncian ataques informáticos a sus sistemas de información. *http:www.cert.org*

Es la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan para que revele todo lo necesario para superar las barreras de seguridad. Si el atacante tiene la experiencia suficiente, puede engañar fácilmente a un usuario (que desconoce las mínimas medidas de seguridad) en beneficio propio. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords.

Por ejemplo, suele llamarse a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa conveniente. O bien, podría enviarse a un mail (falsificando la dirección origen a nombre del administrador) pidiendo al usuario que modifique su password a una palabra que el atacante suministra.

Para evitar situaciones de IS es conveniente tener en cuenta estas recomendaciones:

- Tener servicio propio o de confianza.
- Instruir a los usuarios para que no respondan ninguna pregunta sobre cualquier característica del sistema y deriven la inquietud a los responsables que tenga competencia para dar esa información.
- Asegurarse que las personas que llaman por teléfono son quien dicen ser. Por ejemplo si la persona que llama se identifica como proveedor del Internet lo mejor es cortar y devolver la llamada a la forma de confirmación.

7.3.2 INGENIERÍA SOCIAL INVERSA (ISI)

Consiste en la generación, por parte de los intrusos, de una situación inversa a la originada en Ingeniería social.

En este caso el intruso publicita de alguna manera que es capaz de brindar ayuda a los usuarios, y estos lo llaman ante algún imprevisto. El intruso aprovechara esta oportunidad para pedir información necesaria para solucionar el problema del usuario y el suyo propio (la forma de acceso al sistema).

La ISI es más difícil de llevar a cabo y por lo general se aplica cuando los usuarios están alertados de acerca de las técnicas de IS. Puede usarse en algunas situaciones específicas y después de mucha preparación e investigación por parte del intruso:

1. Generación de una falla en el funcionamiento normal del sistema. Generalmente esta falla es fácil de solucionar pero puede ser difícil de encontrar por los usuarios inexpertos (sabotaje). Requiere que el intruso tenga un mínimo contacto con el sistema.
2. Comunicación a los usuarios de que la solución es brindada por el intruso (publicidad).
3. Provisión de ayuda por parte del intruso encubierto como servicio técnico.

7.3.3 TRASHING (CARTONEO)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando recuerda, lo arroja a la basura. Este procedimiento por más inocente que parezca es el que puede aprovechar un atacante para hacerse de una llave para entrar el sistema…….” Nada se destruye, todo se transforma”.

El trashing puede ser físico (caso anterior) o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.

El trashing físico suele ser común en organizaciones que no disponen de alta confidencialidad, como colegios y universidades.

7.3.4 ATAQUES DE MONITORIZACIÓN

Este tipo de ataque se realiza para observar a la victima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

7.3.4.1 SHOULDER SURFING

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (normalmente en post-it adheridos al monitor o teclado). Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso. Otra técnica relacionada al surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password.

7.3.4.2 DECOY (SEÑUELOS)

Los Decoy son programas diseñados con la misma interface que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras “visitas”.

Una técnica semejante es aquella que, mediante un programa se guardan todas las teclas presionadas durante una sesión. Luego solo hará falta estudiar el archivo generado para conocer nombres de usuarios y claves.

7.3.4.3 SCANNING (BÚSQUEDA).

El Scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma.

El scaneo de puertos pertenece a la Seguridad Informática desde que era utilizado en los sistemas de telefonía. Dado que actualmente existen millones de número s de teléfonos a los que se pueden acceder con una simple llamada, la solución lógica (para encontrar números que puedan interesar) es intentar conectarlos a todos.

La idea básica es simple: llamar a un número y si el modem devuelve un mensaje de conectado, grabar el número. En otro caso, la computadora cuelga el teléfono y llama al siguiente número.

Scanear puertos implica las mismas técnicas de fuerza bruta. Se envía una serie de paquetes para varios protocolos y se deduce que servicios están “escuchando” por las respuestas recibidas o no recibidas.

Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

7.3.4.3.1 TCP CONNECT SCANNING

Esta es la forma básica del scaneo de puertos TCP. Si el puerto está escuchando devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con él.

Las ventajas que caracterizan esta técnica es que no necesita de privilegios especiales y su gran velocidad.

Su principal desventaja es que este método es fácilmente detectable por el administrador del sistema. Se verá un gran número de conexiones y mensajes de error para los servicios en los que se ha conseguido conectar la maquina, que lanza el scanner, y también se verá su inmediata desconexión.

7.3.4.3.2 TCP SYN SCANNING

Cuando dos procesos establecen una comunicación usan el modelo Cliente/Servidor para establecerla. La aplicación del Servidor “escucha” todo lo que ingresa por los puertos.

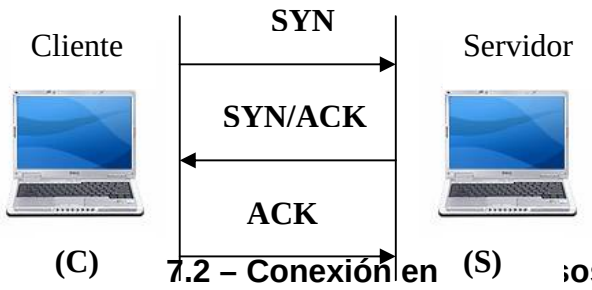
La identificación del Servidor se efectúa a través de la dirección IP del sistema en el que se ejecuta y del número de puerto del que depende para la conexión. El Cliente establece la conexión con el Servidor a través del puerto disponible para luego intercambiar datos.

La información de control de llamada HandShake (saludo) se intercambia entre el Cliente y el Servidor para establecer un dialogo antes de transmitir datos. Los “paquetes” o segmentos TCP tienen banderas que indican el estado mismo.

El protocolo TCP de Internet, sobre el que se basa la mayoría de los servicios (incluyendo el correo electrónico, el web y el IRC) implica esta conexión entre dos maquinas.

El establecimiento de dicha conexión se realiza mediante lo que se llama Three-Way Handshake (“conexión en tres pasos”) ya que intercambian tres segmentos

En forma esquemática se tiene:



7.2 – Conexión en ;os

1. El programa Cliente (C) pide conexión al Servidor (S) enviándole un segmento SYN. Este segmento le dice a S que C desea establecer una conexión.
2. S (si esta abierto y escuchando) al recibir este segmento SYN (activa el indicador) y envía una autentificación ACK de manera de acuse de recibo a C. Si S está cerrado envía un indicador RST.
3. C entonces ACK (autentifica) a S. Ahora ya puede tener lugar la transferencia de datos.

Cuando las aplicaciones conectadas terminan la transferencia realizaran otra negociación a tres bandas con segmentos FIN en vez SYN.

La técnica TCP SYN Scanning, implementa un scaneo de “media-apertura”, dado que nunca se abre una sesión TCP completa.

Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.

La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos. La desventaja es que en algunos sistemas Unix, se necesitan privilegios de administrador para construir estos paquetes SYN.

7.3.4.3.3 TCP FIN SCANNING- STEALTH PORT SCANNING

Hay veces en que inclusive el scaneo SYN no es lo suficientemente “clandestino” o limpio. Algunos sistemas (Firewalls y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos.

Para subsanar este inconveniente los paquetes FIN, en cambio, podrían ser capaces de pasar sin ser advertidos. Este tipo de scaneo está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente. Los puertos abiertos, en cambio, suelen ignorar el paquete en cuestión.

Este es un comportamiento correcto del protocolo TCP, aunque algunos sistemas, entre los que se hallan los de Microsoft ®, no cumplen con este requerimiento, enviando paquetes RST siempre, independientemente de si el puerto está abierto o cerrado. Como resultado, no son vulnerables a este tipo de scaneo. Sin embargo, es posible realizarlo en otros sistemas UNIX.

Este último es un ejemplo en el que se puede apreciar que algunas vulnerabilidades se presentan en las aplicaciones de tecnologías (en este caso el protocolo TCP que surgió en los años 70) y no sobre sus implementaciones. Es más, se observa que una implementación incorrecta (la de Microsoft) soluciona el problema.

"Muchos de los problemas globales de vulnerabilidades son inherentes al diseño original de algunos protocolos"[3]

7.3.4.3.4 FRAGMENTATION SCANNING

Esta no es una nueva técnica de scaneo como tal, sino una modificación de las anteriores. En lugar de enviar paquetes completos de sondeo, los mismos se particionan en una par de pequeños fragmentos IP. Así, se logra partir una cabecera IP en distintos paquetes para hacerlo más difícil de monitorizar por los filtros que pudieran estar ejecutándose en la máquina objetivo.

Sin embargo, algunas implementaciones de estas técnicas tienen problemas con la gestión de este tipo de paquetes tan pequeños, causando una caída de rendimiento en el sistema del intruso o en el de la víctima. Problemas de esta índole convierte en detectables a este tipo de ataque.

7.3.4.3.5 EAVESDROPPING – PACKET SNIFFING

Muchas redes son vulnerables al Eavesdropping, o a la pasiva intercepción (sin modificación) del tráfico de red.

Esto se realiza con Packet Sniffers, los cuales son programas que monitorean los paquetes que circulan por la red. Los Sniffeers pueden ser colocados tanto en una estación de trabajo conectada a la red, como a un equipo Router o a un Gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que han ingresado por otras vías.

[3] GONCALVES, Marcus. Firewalls Complete. Beta Book. McGraw Hill.2002. EE.UU. Página 30

Cada máquina conectada a la red (mediante una placa con una dirección única) verifica la dirección destino de los paquetes TCP. Si estas direcciones son iguales asume que el paquete enviado es para ella, caso contrario libera el paquete para que otras placas lo analicen.

Un Sniffer consiste en colocar a la placa de red en un modo llamado promiscuo, el cual desactiva el filtro de verificación de direcciones y por lo tanto todos los paquetes enviados a la red llegan a esta placa (computadora donde está instalado el Sniffer).

Inicialmente este tipo de software, era únicamente utilizado por los administradores de redes locales, aunque con el tiempo llegó a convertirse en una herramienta muy usada por los intrusos.

Actualmente existen Sniffers para capturar cualquier tipo de información específica. Por ejemplo passwords de un recuso compartido o de acceso a una cuenta, que generalmente viajan sin encriptar al ingresar a sistemas de acceso remoto. También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mails entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

Para realizar estas funciones se analizan las tramas de un segmento de red, y presentan al usuario sólo las que interesan.

Normalmente, los buenos sniffers, no se pueden detectar, aunque la inmensa mayoría y debido a que están demasiado relacionados con el protocolo TCP/IP, si puedan ser detectados con algunos trucos.

7.3.4.5 SNOOPING-DOWNLOADING.

Los ataques de esta categoría tienen el mismo objetivo que el Sniffing: obtener la información sin modificarla.

Sin embargo los métodos son diferentes. Aquí además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas resonantes de este tipo de ataques fueron: el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

7.4.5 **ATAQUES DE AUTENTIFICACIÓN**

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

7.4.5.1 SPOOFING-LOOPING

Spoofing puede traducirse como “hacerse pasar por otro” y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering (ver Ataques de Modificación y Daño).

Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, tiene la finalidad de “evaporar” la identificación y la ubicación del atacante.

El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del Looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor a una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un Insider, o por un estudiante a miles de Kilómetros de distancia, pero que ha tomado la identidad de otros.

La investigación de procedencia de un Looping es casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta.

El envío de falsos e-mails es otra forma de Spoofing que las redes permiten. Aquí el atacante envía e-mails a nombre de otra persona con cualquier motivo y objetivo. Tal fue el caso de una universidad en EE.UU. que en 1998, que debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina de estudiantes.

7.4.5.2 SPOOFING

Este tipo de ataques (sobre protocolos) suele implicar un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques tipo

Spoofing bastante conocidos son el IP Spoofing, el DNS Spoofing y el Web Spoofing.

7.4.5.3 IP SPOOFING

Con el IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete. Su utilización más común es enviar los paquetes con la dirección de un tercero, de forma que la víctima "ve" un ataque proveniente de esa tercera red, y no la dirección real del intruso.

El esquema con dos puentes es el siguiente:

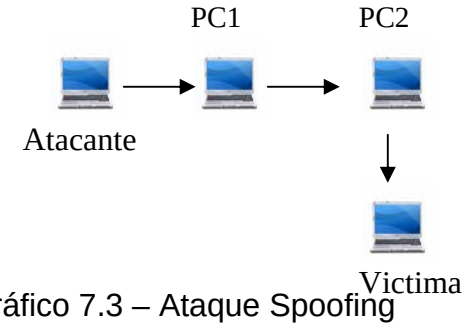


Gráfico 7.3 – Ataque Spoofing

Nótese que si la víctima descubre el ataque verá a la PC_2 como su atacante y no el verdadero origen.

Este ataque se hizo famoso al usarlo Kevin Mitnick.

7.4.5.3.1 DNS SPOOFING

Este ataque se consigue mediante la manipulación de paquetes UDP pudiéndose comprometer el servidor de nombres de dominios (Domain Name Server- DNS) de Windows NT ©. Si se permite el método de recursión en la resolución de "Nombre↔Dirección IP" en el DNS, es posible controlar algunos aspectos del DNS remoto. La recursión consiste en la capacidad de un servidor de nombres para resolver una petición de dirección IP a partir de un nombre que no figura en su base de datos. Este es el método de funcionamiento por defecto.

7.4.5.4 WEB SPOOFING

En el caso Web Spoofing el atacante crea un sitio Web completo (falso) similar al que la víctima desea entrar. Los accesos a este sitio están dirigidos por el atacante, permitiéndole monitorear todas las acciones de la víctima, desde sus datos hasta las passwords, números de tarjeta de créditos, etc.

El atacante también es libre de modificar cualquier dato que se esté transmitiendo entre el servidor original y la víctima o viceversa.

7.4.5.5 IP SPLICING-HIJACKING

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la victima se identifique ante el sistema y tras ello le suplanta como usuario autorizado.

Para entender el procedimiento supongamos la siguiente situación:

IP Cliente: IP 195.1.1.1
IP Servidor: IP 195.1.1.2
IP Atacante: IP 195.1.1.3

1. El cliente establece una conexión con su servidor enviando un paquete que contendrá la dirección origen, destino, número de secuencia (para luego armar el paquete) y un número de autentificación utilizado por el servidor para “reconocer” el paquete siguiente en la secuencia. Supongamos que este paquete contiene:
   IP Origen: 195.1.1.1 Puerto 1025
   IP Destino: 195.1.1.2 Puerto 23
   SEQ = 3DF45ADA (el primero es al azar)
   ACK = F454FDFS
   Datos: Solicitud
2. El servidor, luego de recibir el primer paquete contesta al cliente con paquete Echo (recibido).
   IP Origen: 195.1.1.2 Puerto 1025
   IP Destino: 195.1.1.1 Puerto 23
   SEQ = F454FDFS (ACK enviado por el cliente)
   ACK = 3DF454E4
   Datos: Recepción OK (Echo)
3. El cliente envía un paquete ACK al servidor, sin datos, en donde le comunica lo “perfecto” de la comunicación.
   IP Origen: 195.1.1.2 Puerto 1025
   IP Destino: 195.1.1.1 Puerto 23
   SEQ = 3DF454E4 (ACK enviado por el servidor)
   ACK = F454FDFF
   Datos: Confirmación de Recepción OK (Echo)

4.- El atacante que ha visto, mediante un Sniffer, los paquete que circularon por la red calcula el número de secuencia siguiente: el

actual + tamaño del campo de datos. Para calcular el tamaño de este campo:
1º paquete ACK Cliente = F454FDF5
2º Paquete ACK Cliente = F454FDFF
Tamaño del campo datos = F454FDFF – F454FDF5 = 0A

5. Hecho esto el atacante envía un paquete con el siguiente aspecto:
IP Origen: IP 195.1.1.1 (IP del Cliente por el atacante)
IP Destino: IP 195.1.1.2 (IP del Servidor)
SEQ= 3DF454E4 (ultimo ACK enviado por el cliente)
ACK = F454FE09 (F454FDFF + OA)

El servidor al recibir estos datos no detectará el cambio de origen ya que los campos que ha recibido como secuencia y ACK son lo que esperaba recibir. El cliente, a su vez, quedará esperando datos como si su conexión estuviera colgada y el atacante podrá seguir enviando datos mediante el procedimiento descripto.

7.4.5.6 UTILIZACIÓN DE BACKDOORS

"Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo"[4].

Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de controles normales.

7.4.5.7 UTILIZACIÓN DE EXPLOITS

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte de la empresa, o simplemente encontrando un error en los programas utilizados.

Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error encontrado en el sistema (hardware o software) para ingresar al mismo.

Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

[4] HUERTA, Antonio Villalón. "Seguridad en Unix y redes". Versión 1.2 Digital – Open Publication License v.10 o Later. 2 de octubre de 2004. 5- página 81 *http://www.kriptopolis.com*

7.4.5.8 OBTENCIÓN DE PASSWORDS

Este método comprende la obtención por “Fuerza Bruta” de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc, atacados.

Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además esta nunca (o rara vez) se cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y “diccionarios” que prueban millones de posibles claves hasta encontrar la password correcta.

La política de administración de password será discutida en capitulos posteriores.

7.4.5.8.1 USO DE DICCIONARIOS

Los diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha password en pruebas de fuerza bruta.

El programa encargado de probar cada una de las palabras encripta cada una de ellas, mediante el algoritmo utilizado por el sistema atacado, y compara la palabra encriptada contra el archivo de passwords del sistema atacado (previamente obtenido). Si coinciden se ha encontrado la clave de acceso al sistema, mediante el usuario correspondiente a la clave encontrada.

Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área especifica de acuerdo al tipo de organización que se este atacando.

7.4.6 DENIAL OF SERVICE (DOS)

Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma.

Más allá del simple hecho de bloquear los servicios del cliente, existente algunas razones importantes por las cuales este tipo de ataques pueden ser útiles a un atacante:

1. Se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto.

2. Se necesita cubrir inmediatamente sus acciones a un uso abusivo de CPU. Para ello provoca un “crash” del sistema, generando así la sensación de que ha sido algo pasajero y raro.
3. El intruso cree que actúa bien al dejar fuera de servicio algún sitio web que le disgusta. Este accionar es común en sitios pornográficos, religiosos o de abuso de menores.
4. El administrador del sistema quiere comprobar que sus instalaciones no son vulnerables a este tipo de ataques.
5. El administrador del sistema tiene un proceso que no puede “matar” en su servidor y, debido a este, no puede acceder al sistema. Para ello, lanza contra sí mismo un ataque DOS deteniendo los servicios.

7.4.6.1 JAMMING O FLOODING

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie mas pueda utilizarla.

Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando Spoofing y Looping. El sistema responde al mensaje, pero como no recibe respuesta, acumulan buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Muchos Hosts de Internet han sido dados de baja por el “ping de la muerte” (una versión – trampa del comando ping).

Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el bloqueo instantáneo del equipo. Esta vulnerabilidad ha sido ampliamente utilizada en el pasado pero, aún hoy pueden encontrarse sistemas vulnerables.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los sistemas destinos.

7.4.6.2 SYN FLOOD

Como ya se explicó en el TCP SYN Scanning el protocolo TCP se basa en una conexión en tres pasos. Pero, si el paso final no llega a establecerse, la conexión permanece en estado denominado “semiabierto”.

El SYN Flood es el más famoso de los ataques del tipo Denial of Service, publicado por primera vez en la revista under Phrack; y se basa en un “saludo” incompleto entre los dos hosts.

El cliente envía un paquete SYN pero no responde al paquete ACK ocasionando que la pila TCP/IP espere cierta cantidad de tiempo a que el Host

hostil responda antes de cerrar la conexión. Si se crean muchas peticiones incompletas de conexión (no se responde a ninguna) el Servidor estará inactivo mucho tiempo esperando respuesta. Esto ocasiona la lentitud en los demás servicios.

SYN Flood aprovecha la mala implementación del protocolo TCP, funcionando de la siguiente manera:

Se envía al destino, una serie de paquetes TCP con el bit SYN activado, (petición de conexión) desde una dirección IP spoofeada. Esta última debe de ser inexistente para que el destino no pueda completar el saludo con el cliente.

Aquí radica el fallo de TCP: ICMP reporta que el cliente es inexistente, pero TCP ignora el mensaje y sigue intentando terminar el saludo con el cliente de forma continua.

Cuando se realiza un Ping a una maquina, esta tiene que procesarlo. Y aunque se trate de un proceso sencillo, (no es más que ver la dirección de origen y enviarle un paquete Reply), siempre consume recursos del sistema. Si no es un ping, sino que son varios a la vez, la máquina se vuelve más lenta… si lo que se recibe son miles de solicitudes, puede que el equipo deje de responder (Flood).

Es obligatorio que la IP origen sea inexistente, ya que si no el objetivo, logrará responderle al cliente con un SYN/ACK, y como esa IP no pidió ninguna conexión, le va a responder al objetivo con un RST, y el ataque no tendrá efecto.

El problema es que muchos sistemas operativos tienen un límite muy bajo, en el número de conexiones “semiabiertas” que pueden manejar en un momento determinado (5 a 30). Si se supera ese límite, el servidor sencillamente dejará de responder a las nuevas peticiones de conexión que le vayan llegando. Las conexiones “semiabiertas” van caducando tras un tiempo, liberando “huecos” para nuevas conexiones, pero mientras el atacante mantenga el SYN Flood, la probabilidad de que una conexión recién liberada sea capturada por un nuevo SYN malicioso es muy alta.

7.4.6.3 CONNECTION FLOOD

La mayoría de las empresas que brindan servicios de Internet (ISP) tienen un límite máximo en el número de conexiones simultáneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, (como ocurre en el caso del SYN Flood) para mantener fuera de servicio el servidor.

7.4.6.4 NET FLOOD

En estos casos, la red víctima no puede hacer nada. Aunque filtre el tráfico en sus sistemas, sus líneas estarán saturadas con tráfico malicioso, incapacitándolas para cursar tráfico útil.

Un ejemplo habitual es el de un teléfono: si alguien quiere molestar, sólo tiene que llamar, de forma continua. Si se descuelga el teléfono (para que deje de molestar), tampoco se puede recibir llamadas de otras personas. Este problema es habitual, por ejemplo, cuando alguien intenta mandar un fax empleando el número de voz: el fax insiste durante horas, sin que el usuario llamado pueda hacer nada al respecto.

En el caso de Net Flooding ocurre algo similar. El atacante envía tantos paquetes de solicitud de conexión que las conexiones auténticas simplemente no pueden competir.

En casos así el primer paso a realizar es el ponerse en contacto con el proveedor del servicio para que intente determinar la fuente del ataque y, como medida provisional, filtre el ataque en su extremo de la línea.

El siguiente paso consiste en localizar las fuentes del ataque e informar a sus administradores, ya que seguramente se estarán usando sus recursos sin su conocimiento y consentimiento. Si el atacante emplea IP Spoofing, el rastreo puede ser casi imposible, ya que en muchos casos la fuente del ataque es, a su vez, víctima y el origen último puede ser prácticamente imposible de determinar (looping).

7.4.6.5 **LAND ATTACK**

Este ataque consiste en un Bug (error) en la implementación de la pila TCP/IP de las plataformas Windows.

El ataque consiste en mandar a algún puerto abierto de un servidor (generalmente al NetBIOS 113 o 139) un paquete, maliciosamente construido, con la dirección y puerto origen igual que la dirección y puerto destino.

Por ejemplo se envían un mensaje desde la dirección 10.0.0.1: 139 hacia ella misma. El resultado obtenido es que luego de cierta cantidad de mensajes enviados-recibidos la maquina termina colgándose.

Existen ciertas variantes a este método consistente, por ejemplo, en enviar el mensaje a una dirección específica sin especificar el puerto.

7.4.6.6 SMURF O BROADCAST STORM

Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones BroadCast para, a continuación, mandar una petición ICMP (simulando un ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen (máquina Víctima).

Este paquete maliciosamente manipulado, será repetido en difusión (Broadcast), y cientos ó miles de host mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.

Suponiendo que se considere una red de tipo C la dirección de BroadCast sería .255; por lo que el simple envío de un paquete se convierte en un efecto multiplicador devastador.

Desgraciadamente la víctima no puede hacer nada para evitarlo. La solución esta en manos de los administradores de red, los cuales deben configurar adecuadamente sus Routers para filtrar los paquetes ICMP de petición indeseados (broadcast); o bien configurar sus máquinas para que no respondan a dichos paquetes. Es decir, que lo que se parchea sonlas máquinas/redes que puedan actuar de intermediarias (inocentes) en el ataque y no a la máquina víctima.

También se podría evitar el ataque si el Router/Firewall de salida del atacante estuviera convenientemente configurado para evitar Spoofing. Esto se haría filtrando todos los paquetes de salida que tuvieran una dirección de origen que no perteneciera a la red interna.

7.4.6.7 OBB, SUPERNUKE O WINNUKE

Un ataque característico, y quizás el más común, de los equipos de Windows es el Nuke, que hace que los equipos que escuchan por el puerto NetBios sobre TCP/UDP 137 a 139, queden fuera de servicio, o disminuyan su rendimiento al enviarle paquetes UDP manipulados.

Generalmente se envían fragmentos de paquetes Out Of Band, que la máquina Víctima detecta como inválidos pasando aun estado inestable. OOB es el término normal, pero realmente consiste en configurar el bit Urgente (URG) en los indicadores del encabezamiento TCP, lo que significa que este bit es válido.

Este ataque puede prevenirse instalando los parches adecuados suministrados por el fabricante del sistema operativo afectado. Un filtro efectivo debería garantizar la detección de una inundación de bits Urgentes.

7.4.6.8 TEARDROP I Y II – NEWTEAR- BONK- BOINK

Al igual que el Supernuke, los ataques Teardrop I y Teardrop II afectan a fragmentos de paquetes. Algunas implementaciones de colas IP no vuelven a armar correctamente los fragmentos que se suponen, haciendo que el sistema

cuelgue. Windows NT 4.0 de Microsoft es especialmente vulnerable a este ataque. Aunque existen Patchs (parches) que pueden aplicarse para solucionar el problema. Muchas organizaciones no lo hacen, y las consecuencias pueden ser devastadoras.

Los ataques tipo Teardrop son especialmente peligrosos ya que existen multitud de implementaciones (algunas de ellas forman paquetes), que explotan esta debilidad. Las más conocidas son aquellas con el nombre Newtear, Bonk y Boink.

7.4.6.9 E- MAIL BOMBING – SPAMMING

El E-Mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así el mailbox del destinatario.

El Spamming, en cambio se refiere a enviar un e-mail a miles de usuarios, hayan estos solicitado el mensaje o no. Es muy utilizado por las empresas para publicar sus productos.

El Spamming esta siendo actualmente tratado por las leyes europeas (principalmente España) como una violación de los derechos de privacidad del usuario.

7.4.7 ATAQUES DE MODIFICACIÓN – DAÑO

7.4.7.1 TAMPERING O DATA DIDLING

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima, incluyendo borrado de archivos. Son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema.

Aún así, si no hubo intenciones de “bajar” el sistema por parte del atacante; el administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por Insiders u Outsiders, generalmente con el propósito de fraude o de dejar fuera de servicio a un competidor.

Son innumerables los casos de este tipo: empleados bancarios (o externos) que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule una deuda impositiva.

Múltiples Web Sites han sido víctimas del cambio en sus páginas por imágenes (o manifiesto) terroristas o humorísticos, como el ataque de The Motor, ya visto, a la NASA.

Otras veces se reemplazan versiones de software por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos, etc.). La utilización de programas troyanos y difusión de virus esta dentro de esta categoría, y se profundizará sobre el tema en otra sección el presente capítulo.

7.4.7.2 BORRADO DE HUELLAS

Es una de las tareas mas importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará como conseguir “tapar el hueco” de seguridad, evitar ataques futuros e incluso rastrear al atacante.

Las huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo.

Los archivos Logs son una de las principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos.

7.4.7.3 ATAQUES MEDIANTE JAVA APPLETS

Java es un lenguaje de programación interpretado, desarrollado inicialmente por la empresa SUN. Su mayor popularidad la merece por su alto grado de seguridad. Los más usados navegadores actuales, implementan máquinas virtuales Java (MVJ) para ser capaces de ejecutar programas (Applets) de java.

Estos Applets, al fin y al cabo, no son más que código ejecutable y como tal, susceptible de ser manipulado por intrusos. Sin embargo, partiendo del diseño, Java siempre ha pensado en la seguridad del sistema. Las restricciones a las que somete a los applets son de tal envergadura (imposibilidad de trabajar con archivos a no ser por el usuario especifique lo contrario, imposibilidad de acceso a zonas de memoria y disco directamente, firma digital, etc). Que es muy difícil lanzar ataques. Sin embargo, existe un grupo de expertos especializados en descubrir fallas de seguridad en las implementaciones de las MVJ.

7.4.7.4 ATAQUES CON JAVASCRIPT Y VBSCRIPT

JavaScript (de la empresa Netscape) y VBScript de (Microsoft) son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de java. Los programas realizados son interpretados por el navegador.

Aunque los fallos son muchos más numerosos en versiones antiguas de JavaScript, actualmente se utilizan para explotar vulnerabilidades específicas de navegadores y servidores de correo ya que no se realiza ninguna evaluación sobre si el código.

7.4.7.5 ATAQUES MEDIANTE ACTIVE X

Es una de las tecnologías más potentes que ha desarrollado Microsoft. Mediante active X es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft a Java.

Active X soluciona los problemas de seguridad mediante certificados y firmas digitales. Una autoridad certificadora (AC) expende un certificado que acompaña a los controles activos y ana firma digital del programador.

Cuando un usuario descarga una página con un control, se le preguntará si confía en la AC que expendio el certificado y/o en el control active x. si el usuario acepta el control, éste puede pasar a ejecutarse sin ningún tipo de restricciones (sólo las propias que tenga el usuario en el sistema operativo). Es decir, la responsabilidad de la seguridad del sistema se deja en manos del usuario, ya sea este un experto cibernauta consciente de los riesgos que puede traer la acción o un perfecto novato en la materia.

Esta última característica es el mayor punto débil de los controles Active X ya que la mayoría de los usuarios aceptan el certificado sin siquiera leerlo, pudiendo ser esta la fuente de un ataque con un control dañino.

La filosofía Active X es que las autoridades de Certificación se fían de la palabra del programador del control. Es decir, el programador se compromete a firmar un documento que asegura que el control no es nocivo. Evidentemente siempre hay programadores con pocos escrúpulos o con ganas de experimentar.

Así, un conocido grupo de hackers alemanes, desarrollo un control Active X maligno que modificaba el programa de Gestión Bancaria Personal Quicken95 de tal manera que si un usuario aceptaba el control, éste realizaba la tarea que supuestamente tenía que hacer y además modificaba el quicken, para que la próxima vez que la victima se conectara a su banco, se iniciara automáticamente una transferencia a una cuenta del grupo Alemán.

Otro control Active X muy especialmente “malévolo” es aquel que manipule el código de ciertos exploradores, para que éste no solicite confirmación al usuario a la hora de descargar otro control activo de la Web. Es decir, deja totalmente descubierto, el sistema de la víctima, a ataques con tecnología ActiveX.

La autentificación de usuarios mediante certificados y las autoridades certificadoras será abordada con profundidad en capitulo posteriores.

7.4.7.6 VULNERABILIDADES EN LOS NAVEGADORES

Generalmente los navegadores no fallan por fallos intrínsecos, si no que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los “Buffer Overflow”

Los “Buffer Overflows” consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Pro ejemplo, cuando el usuario escribe una dirección en formato URL ésta se guarda en un Buffer para luego procesarla. Si no se realizan las oportunas operaciones de comprobación, un usuario podría manipular estas direcciones.

Los protocolos usados pueden ser http, pero también otros menos conocidos, internos de cada explorador, como el “res:” o el “mk:” Precisamente existen fallos de seguridad del tipo “Buffer Overflow” en la implementación de estos dos protocolos.

7.4.8 ERRORES DE DISEÑO, IMPLEMENTACIÓN Y OPERACIÓN.

Muchos sistemas están expuestos a “agujeros” de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por varias razones, y miles de “puertas invisibles” son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y todas clases de servicios informáticos disponibles.

Los sistemas operativos abiertos (como UNIX y LINUX) tienen agujeros más conocidos y controlados que aquellos que existen en sistemas operativos cerrados (Windows). La importancia y ventaja del código abierto radica en miles de usuarios analizan dicho código en busca de posibles bugs y ayudan a obtener soluciones en forma inmediata.

Constantemente se encuentran en Internet avisos de nuevos descubrimientos de problemas de seguridad, herramientas de Hacking y Exploits que los explotan, por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades, puedan diagnosticarlas y actualizar el programa afectado con el parche adecuado.

7.4.9 IMPLEMETACIÓN DE ESTAS TÉCNICAS

Cada una de las técnicas explicadas puede ser utilizada por un intruso en un ataque. A continuación se intentarán establecer el orden de utilización de las mismas, pero siempre remarcando que un ataque insume mucha paciencia, imaginación acumulación de conocimientos y experiencia dada, en la mayoría de los casos por prueba y error.

1.- Identificación del problema (víctima): en esta etapa se recopila toda la información posible de la víctima. Cuanta más información se acumule, más

exacto y preciso será el ataque, más fácil será eliminar las evidencias y más difícil será su rastreo.

2.- Exploración del sistema víctima elegido: en esta etapa se recopila información sobre los sistemas activos de la víctima, cuales son los más vulnerables y cuales se encuentran disponibles. Es importante remarcar que si la víctima parece apropiada en la etapa de Identificación, no significa que esto resulte así en esta segunda etapa.

3.- Enumeración: en esta etapa se identificaran las cuentas activas y los recursos compartidos mal protegidos. La diferencia con las etapas anteriores es que aquí se establece una conexión activa a los sistemas y la realización de consultas dirigidas. Estas intrusiones pueden (y deberían) ser registradas, por el administrador del sistema, o al menos detectadas para luego ser bloqueadas.

4.- Intrusión. En esta etapa el intruso conoce perfectamente el sistema y sus debilidades y comienza a realizar las tareas que lo llevaron a trabajar, en muchas ocasiones, durante meses.

Contrariamente a lo que se piensa, los sistemas son difíciles de penetrar si están bien administradores y configurados. Ocasionalmente los defectos propios de la arquitectura de los sistemas proporciona un fácil acceso, pero esto puede ser, en la mayoría de los casos, subsanado aplicando las soluciones halladas.

7.4.10 ¿CÓMO DEFENDERSE DE ESTOS ATAQUES?

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son “solucionables” en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todo los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes son medidas preventivas. Medida que toda red y administrador deben conocer y desplegar cuanto antes:

1. Mantener las máquinas actualizadas y seguras Físicamente.
2. Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).
3. Aunque una máquina no contenga información valiosa. Hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DOS coordinado o para ocultar su verdadera dirección.
4. No permitir el tráfico “broadcast” desde fuera de nuestra red. De esta forma evitamos ser empleados como “multiplicadores” durante un ataque smurf.
5. Filtrar el tráfico IP Spoof.
6. Auditorias de Seguridad y sistemas de detección.
7. Mantenerse informado constantemente sobre cada una de las vulnerabilidades encontradas y parches lanzados.

8. Por último, pero quizás lo más importante, **la capacitación continúa del usuario.**

7.5 CREACIÓN Y DIFUSIÓN DE VIRUS

Quizás uno de los temas más famosos y sobre los que más mitos e historias fantásticas se corren en el ámbito informático sean los virus (del Latín Veneno) y que son realmente estos “parásitos”.

7.5.1 VIRUS INFORMÁTICOS VS VIRUS BIOLÓGICOS

Un análisis comparativo de analogías y diferencias entre las dos “especies”, muestra que las similitudes entre ambos son poco menos que asombrosas. Para notarlas ante todo debemos saber que es un virus Informático y que es un Virus Biológico.

Virus Informático (VI): Pequeño programa, invisible para el usuario (no detectable por el sistema operativo) y de actuar específico 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, puedan reproducirse formando réplicas de sí 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).

“Un virus responde al modelo DAS: Dañino, Autorreplicante y subrepticio.”

Virus Biológico (VB): Fragmentos de ADN o ARN cubiertos de una capa proteica. Se reproducen solo en el interior de las células vivas, para lo cual toman, el control de sus enzimas y metabolismo. Sin esto son tan inertes como cualquier otra macromolécula.

Algunas analogías entre ambos son:

1.- Los VB están compuestos por ácidos nucleicos que contienen información (programa dañino o VI) suficiente y necesaria para que utilizando los ácidos de la célula huésped (programa infectado por los VI) puedan reproducirse a si mismos.

2.- Los VB no poseen metabolismo propio, por lo tanto no manifiestan actividad fuera del huésped. Esto también sucede en los VI, por ejemplo, si se apaga la máquina o si el virus se encuentra en un disquete.

3.- El tamaño de un VB es relativamente pequeño en comparación con las células que infectan. Con los VI sucede lo mismo. Tanto los VB como los VI causan un daño sobre el huésped.

4.- Ambos virus inician su actividad en forma oculta y sin conocimiento de su huésped, y suelen hacerse evidentes luego de que el daño ya es demasiado alto como para corregirse.

5.- La finalidad de un VB (según la ciencia) es la reproducción y eventual destrucción del huésped como consecuencia. La de los VI pueden ser muchos los motivos de su creación (por parte de su autor), pero también terminan destruyendo o modificando de alguna manera a su huésped.

6.- Ambos virus contienen la información necesaria para su aplicación y eventual destrucción. La diferencia radica en la forma de contener esta información: en los VB es un código genético y en los VI es código binario.

7.- El soporte de la información también es compartida por ambos "organismos". En los VB el soporte lo brinda el ADN o ARN (soporte orgánico). En los VI el soporte es un medio magnético (inorgánico).

8.- Ambos tipos de virus son propagados de diversas formas (y raramente en todas ellas). En el caso de los VB su medio de propagación es el aire, agua, contacto directo, etc. Los VI pueden propagarse introduciendo un disquete infectado en una computadora sana (y ejecutando la zona infectada, ¡claro esta!); o viceversa: de RAM infectada a un disquete sano; o directamente aprovechando el flujote electrones: MODEM, red, etc.

9.- En ambos casos sucede que la reproducción es de tipo replicativo del original y cuya exactitud dependerá de la existencia de mutaciones o no.

10.- Ambas entidades cumplen con el patrón de epidemiología médica.

11.- El origen de una entidad generalmente es desconocido, pero lo que se sabe con exactitud, es que los VI son producidos por seres humanos y que los VB son entidades de origen biológico y últimamente de origen humano (armas biológicas).

Son, sin dudas, muchas las analogías que pueden encontrarse haciendo un análisis más exhaustivo de ambas entidades, pero que transcenderían notablemente los límites de este informe. La idea es solamente dejar bien en claro que no existe ningún extraño oscuro o sobrenatural motivo que dé explicación a un VI. Simplemente es un programa más, que cualquiera de nosotros sería capaz de concebir…..con las herramientas apropiadas del caso.

7.5.2 ORIGEN

Los orígenes de los VI se pueden establecer al observar investigaciones sobre Inteligencia y Vida Artificial. Estos conceptos fueron desarrollados por John Von Neuman hacia 1950 estableciendo por primera vez la idea de programas autorreplicables.

Luego, en 1960 en los laboratorios de Bell se desarrollaron juegos (programas) que "luchaban" entre sí con el objetivo de lograr el mayor espacio de memoria posible. Estos programas llamados Core Wars hacían uso de técnicas de ataque, defensa, ocultamiento y reproducción que luego adoptaron los VI.

En 1970, John Shoch y Jon Up elaboraron, en el Palo Alto Research Center (PARC) de Xerox, programas autorreplicables que servían para controlar la salud de las redes informáticas. Días después de su lanzamiento el programa se propago en todas las máquinas y sus múltiples (miles) copias de sí mismo colapsaron la red. Cabe aclarar que el fin de estos programas era, en un principio, solo experimental y sin fines maléficos.

En los años 80 nacen los primeros VI propiamente dichos y en 1983 se establece una definición para los mismos. En 1985 infectaban el MS-DOS y en 1986 ya eran destructivos (Brain, Vienna, Viernes13, etc. Estos utilizaban disquetes para su propagación y dependían totalmente de la ignorancia del público que hacía copias indiscriminadas de los mismos.

En palabras del Dr Fred Cohen:

“El 3 de noviembre de 1983, el primer virus fue concebido como un experimento para ser presentado en un seminario semanal de Seguridad Informática. El concepto fue introducido por el autor y el nombre “virus” fue dado por Len Adleman. Después de 8 horas de trabajo sobre un VAX 11/1750 ejecutando UNIX, el primer Virus estuvo listo para la demostración. En esa semana fueron obtenidos los premios y cinco experimentos fueron realizados. El 10 de noviembre el virus fue mostrado. La infección inicial fue realizada en “vd” (un prgrama que mostraba la estructura de UNIX gráficamente) e introducido a los usuarios vía un BBS (…)”.

De aquí quizás provenga la ¿leyenda? En donde se sugiere que los VI surgieron como una medida de seguridad de compañías de desarrollo de software para disuadir a los usuarios de la adquisición de software ilegal. Esta versión no ha sido demostrada ni desmentida, pero el tiempo ha demostrado que los verdaderos perjudicados son las mismas compañías acusadas en su momento.

El 2 de noviembre de 1988 se produce el primer ataque masivo a una red (ARPAnet, precursora de Internet). El método utilizado para su autorreplicación era el correo electrónico y en tres horas el gusano se hizo conocer en todo EE.UU. La erradicación de este gusano costó un millón de dólares y demostró que podía ser un programa autorreplicable fuera de control.

El autor, Robert Morris (hijo de uno de los programadores de Core Wars), graduado de Harvard de 23 años reconoció su error y lo calificó de “fallo catastrófico”, ya que su idea no era hacer que los ordenadores se relentizaran.

En este mismo año, como consecuencia de lo acontecido y de la concientización, por parte de la industria informática, de la necesidad de defender los sistemas Informáticos, aparecen los primeros programas antivirus.

En 1991 aparecen los primeros Kits para la construcción de virus, lo que facilitó su creación e hizo aumentar su número a mayor velocidad. El primero fuel VCL (Virus Creation Laboratory), creado por Nowhere Man.

En 1992 nace el virus Michelangelo (basado en el Stoned), y aunque es un virus no especialmente destructivo, la prensa lo "vendió" como una grave amenaza mundial. Algunos fabricantes de antivirus, aseguraron que cinco millones de computadoras se verían afectadas por el virus. El número no pasó de cinco mil. Pese a ello, la noticia provocó una alarma injustificada entre los usuario de ordenadores personales, aunque en cierto modo también sirvió para concienciar a estos mismos usuarios de la necesidad de estar alerta frente a los virus, que ya habían dejado definitivamente de ser una curiosidad científica para pasar a convertirse en una plaga peligrosa.

A partir de aquí, los virus alcanzaron notoriedad y son perfeccionados día a día mediante técnicas de programación poco comunes. Su proliferación se debió, principalmente, al crecimiento de las redes y a los medios para compartir información.

7.5.3 LOS NÚMEROS HABLAN

A mediados de los noventa se produjeron enormes cambios en el mundo de la informática personal que llegan hasta nuestros días y que dispararon el número de virus, según la International Computer Security Association (ICSA), oscilaba en los 4000, en los siguientes cinco años esa cifra se multiplicó por diez, y promete seguir aumentando.

Cientos de virus son descubiertos mes a mes (de 6 a 20 por día), y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada.

La NCSA es el principal organismo dedicado al seguimiento del fenómeno de lo virus en todo el mundo. Según sus informes, en Estados Unidos más del 99% de las grandes y medianas empresas han sufrido la infección por virus en alguna de sus computadoras. Sólo un 0.67% asegura no haberse encontrado nunca con un virus.

Se calcula que, en término medio, se infectan 40.6 % computadoras al año. La proporción de infecciones anuales ha crecido ampliamente, ya que en 1996 este índice era sólo del 12%.

7.5.4 DESCRIPCIÓN DE UN VIRUS

Si bien un VI es un ataque de tipo Tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (diskettes) o a través de la red (e-mails u otros protocolos) sin intervención directa del atacante.

Dado que el virus tiene como característica propia su autoreproducción, no necesita de mucha ayuda para propagarse rápidamente.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.EXE, .COM, .DLL, etc), los sectores de Boot y la tabla de partición de los discos. Actualmente los que causan mayores problemas son los macro-virus y script-virus, que están ocultos en simples documentos, planillas de cálculo, correo electrónico y aplicaciones que utiliza cualquier usuario de PC. La difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además son multiplataforma, es decir, no depende de un sistema operativo en particular, ya que un documento puede ser procesado tanto en Windows 95/98/NT/2000/XP, como en Macintosh u otras.

7.5.4.1 TÉCNICAS DE PROPAGACIÓN

Actualmente las técnicas utilizadas por los virus para lograr su propagación y subsistencia son muy variadas y existen aquellos que utilizan varias de ellas para lograrlo.

1. **Disquetes y otros medios removibles.** A la posibilidad de que un disquete contenga un archivo infectado se une el peligro de que integre un virus de sector de arranque (boot). En este segundo caso, y si el usuario lo deja en la disquetera, infectará el ordenador cuando lo encienda, ya que el sistema intentará arrancar desde el disquete.
2. **correo electrónico:** El usuario no necesita hacer nada para recibir mensajes que, en muchos casos ni siquiera ha solicitado y que pueden llegar de cualquier lugar del mundo. Los mensajes de correo electrónico pueden incluir archivos, documentos o cualquier objeto ActiveX-Java infectado que, al ejecutarse contagian a la computadora del usuario. En las ultimas generaciones de virus se envían e-mails sin mensajes pero con archivos adjuntos (virus) que al abrirlos proceden a su ejecución y posterior infección del sistema atacado. Estos virus poseen una gran velocidad de propagación ya que se envían automáticamente a los contactos de la libreta de direcciones del sistema infectado.
3. **IRC o CHAT.** Las aplicaciones de mensajería instantánea (ICQ, AOL, Instant Messenger, etc.) o Internet Relay Chat (IRC), proporcionan un medio de comunicación anónimo, rápido, eficiente, cómodo y barato. Sin embargo, también son peligrosas, ya que los entornos de Chat ofrecen, por regla general, facilidades para la transmisión de archivos, que conllevan un gran riesgo en un entorno de red.
4. **Paginas web y transferencias de archivos vía FTP:** los archivos que se descargan de Internet pueden estar infectados, y pueden provocar acciones dañinas en el sistema en el que se ejecutan.
5. **Grupos de Noticias.** Sus mensajes e información (archivos) pueden estar infectados y, por tanto, contagiar al equipo del usuario que participe en ellos.

7.5.4.2 TIPOS DE VIRUS

Un virus puede causar daño lógico (generalmente) o físico (bajo ciertas circunstancias y por repetición) de la computadora infectada y nadie en su sano juicio deseará ejecutarlo. Para evitar la intervención del usuario los creadores de virus debieron inventar técnicas de las cuales valerse para su “programa” pudiera ejecutarse. Estas son diversas y algunas de lo más ingeniosas:

7.5.4.2.1 ARCHIVOS EJECUTABLES (VIRUS EXEVIR).

El virus se adosa a un archivo ejecutable y desvía el flujo de ejecución a su código, para luego retornar al huésped y ejecutar las acciones esperadas por el usuario. Al realizarse esta acción el usuario no se percata de lo sucedido. Una vez que el virus es ejecutado se aloja en memoria y puede infectar otros archivos ejecutables que sean abiertos en esa máquina.

En este momento su dispersión se realiza en sistema de 16 bits (DOS) y de 32 bits (Windows) indistintamente, atacando programas .COM, .EXE, .DLL, .SYS, .PIF, etc, según el sistema infectado.

7.5.4.2.2 VIRUS EN EL SECTOR DE ARRANQUE (VIRUS CASO ANTERIOR A LA CARGA DEL SO)

En los primeros 512 bytes de un disquete formateado se encuentran las rutinas necesarias para la carga y reconocimiento de dicho disquete. Entre ellas se encuentra la función invocada si no se encuentra el Sistema Operativo. Es decir que estos 512 bytes se ejecutan cada vez que se intenta arrancar (bootear) desde un disquete (o si se dejó olvidado uno en la unidad y el orden de booteo de la PC es A: y luego C:). Luego, esta área es el objetivo de un virus de booteo.

Se guarda la zona de booteo original en otro sector del disco (generalmente uno muy cercano a lo más altos). Luego el virus carga la antigua zona de booteo. Al arrancar el disquete se ejecuta el virus (que obligatoriamente debe tener 512 bytes o menos) quedando residente en memoria; luego ejecuta la zona de booteo original, salvada anteriormente. Una vez más el usuario no se percata de lo sucedido ya que la zona de booteo se ejecuta iniciando el sistema operativo (si existiera) o informando la falta del mismo. Ejemplo: 512, Stoned, Michelangelo, Diablo.

7.5.4.2.3 VIRUS RESIDENTE

Como ya se mencionó, un virus puede residir en memoria. El objetivo de esta acción es controlar los accesos a disco realizados por el usuario y el sistema Operativo. Cada vez que se produce un acceso, el virus verifica si el disco o archivo objetivo al que se accede, está infectado y si no lo esta procede a almacenar su propio código en el mismo. Este código se almacenará en un archivo, tabla de partición, o en el sector de booteo, dependiendo del tipo de virus que se trate.

7.5.4.2.4 MACROVIRUS

Estos virus afectan archivos de información generados por aplicaciones de oficina que cuentan con lenguajes de programación de macros. Son no de los más expandidos, ya que todos los usuarios necesitan hacer intercambio de documentos para realizar su trabajo. Los primeros antecedentes de ellos fueron con las macros de Lotus 123 que ya eran lo suficientemente poderosas como permitir este tipo de implementación. Pero los primeros de difusión masiva fueron desarrollados a principios de los 90`s para el microprocesador de texto Microsoft Word, ya que este cuenta con el lenguaje de programación Word Basic.

Su principal punto fuerte fue que terminaron con un paradigma de la seguridad informática: “los únicos archivos que pueden infectarse son los ejecutables” y todas las tecnologías antivirus sucumbieron ante este nuevo ataque.

Su funcionamiento consiste en que si una aplicación abre un archivo infectado, la aplicación (o parte de ella) se infecta y cada vez que se genera un nuevo archivo o se modifique uno existente contendrá el macrovirus.

Ejemplos:
De Microsoft Word: CAP I, CAP II, CONCEPT, WAZZU.
De Microsoft Excel: Laroux.
De lotus Amipro: GreenStripe.

7.5.4.2.5 VIRUS DE MAIL

El “último grito de la tecnología” en cuestión de virus. Su modo de actuar, al igual que los anteriores, se basa en la confianza excesiva por parte del usuario: a este le llega vía mail un mensaje con un archivo comprimido (.ZIP por ejemplo), el usuario lo descomprime y al terminar esta acción, el contenido (virus ejecutable) del archivo se ejecuta y comienza el daño.

Este tipo de virus tomó relevancia estos últimos años con la explosión masiva de Internet y últimamente con el virus Melissa, I Love You y Kamasutra. Generalmente estos virus se auto envían a algunas de las direcciones de la libreta. Cada vez que uno de estos usuarios recibe el supuesto mensaje no sospecha y lo abre, ocurriendo el mismo reenvío y la posterior saturación de los servidores al existir millones de mensajes enviados.

7.5.4.2.6 VIRUS DE SABOTAJE

Son virus construidos para dañar un sistema o entorno especifico. Requieren de conocimientos de programación pero también una acción de inteligencia que provea información sobre el objetivo y sus sistemas.

7.5.4.2.7 HOAX, LOS VIRUS FANTASMAS

El auge del correo electrónico generó la posibilidad de transmitir mensajes de alerta de seguridad. Así comenzaron a circular mensajes de distinta índole (virus, cadenas solitarias, beneficios, catástrofes, etc.) de casos inexistentes. Los objetivos de estas alertas pueden causar alarma, la pérdida de tiempo, el robo de direcciones de correo y la saturación de los servidores con las consecuencias pérdidas de dinero que esto ocasiona.

7.5.4.2.8 VIRUS DE APPLETS JAVA Y CONTROLES ACTIVEX

Si bien, como ya se comentó, estas dos tecnologías han sido desarrolladas teniendo como meta principal la seguridad, la práctica demuestra que es posible programar virus sobre ellas. Este tipo de virus se copian y se ejecutan a si mismos mientras el usuario mantiene una conexión a Internet.

7.5.4.2.9 REPRODUCTORES- GUSANOS

Son programas que se reproducen constantemente hasta agotar totalmente los recursos del sistema huésped y/o recopilar información relevante para enviarla a un equipo al cual su creador tiene acceso.

7.5.4.2.10 CABALLOS DE TROYA

De la misma forma que el antiguo caballo de Troya de la mitología griega escondía en su interior algo que los troyanos desconocían, y que tenía una función muy diferente a la que ellos podían imaginar; Un caballo de Troya es un programa que aparentemente realiza una función útil pero además realiza una operación que el usuario desconoce y que generalmente beneficia al autor del troyano o daña el sistema huésped.

Si bien este tipo de programas NO cumplen con la condición de auto-reproducción de los virus, encuadran perfectamente en la característica de programa dañino.

Consisten en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

Los ejemplos más conocidos de troyanos son el Back Oriffice y el Net Bus que, si bien no fueron desarrollados con ese fin, son una poderosa arma para tomar el control de la computadora infectada. Estos programas pueden ser utilizados para la administración total del sistema atacado por parte de un tercero, con los mismos permisos y restricciones que el usuario de la misma.

7.5.4.2.11 BOMBAS LÓGICAS

Este suele ser el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que

en una fecha determinada o dado algún evento particular en el sistema, bien destruye y modifica o provoca la baja en el sistema.

7.5.4.3 MODELO DE VIRUS INFORMÁTICO

Un virus está compuesto por su propio entorno, dentro del cual pueden distinguirse tres módulos principales:

1. **Modulo de Reproducción:** es el encargado de manejar las rutinas de parasitación de entidades ejecutables con el fin de que el virus pueda ejecutarse subrepticiamente, permitiendo su transferencia a otras computadoras.
2. **Módulo de Ataque:** Es el que maneja las rutinas de daño adicional al virus. Esta rutina puede existir o no y generalmente se activa cuando el sistema cumple alguna condición. Por ejemplo el virus Chernovil se activa cada vez que el reloj del sistema alcanza el 26 de cada mes.
3. **Modulo de Defensa:** Este módulo, también optativo, tiene la misión de proteger al virus. Sus rutinas tienden a evitar acciones que faciliten o provoquen la detección o remoción del virus.

7.5.5 TIPOS DE DAÑOS OCASIONADOS POR LOS VIRUS

Los virus informáticos no afectan (en su gran mayoría) directamente el hardware sino a través de los programas que lo controlan; en ocasiones no contienen código nocivo, o bien, únicamente causan daño al reproducirse y utilizar recursos escasos como el espacio en el disco rígido, tiempo de procesamiento, memoria, etc. En general los daños que pueden causar los virus se refieren a hacer que el sistema se detenga, borrado de archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desorden en los datos del disco, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.

Para realizar la siguiente clasificación se ha tenido en cuenta que el daño es una acción de la computadora, no deseada por el usuario:

a. **Daño Implícito: es** el conjunto de todas las acciones dañinas para el sistema que el virus realiza para asegurar su accionar y propagación. Aquí se debe considerar el entorno en el que se desenvuelven el virus ya que el consumo de ciclos de reloj en un medio delicado (como un aparto biomédico) puede causar un gran daño.
b. **Daño Explicito.** Es el que produce la rutina de daño del virus. Con respecto al modo y cantidad de daño, encontramos:
    a. **Daños Triviales:** daños que no ocasionan ninguna pérdida grave de funcionalidad del sistema y que originan una pequeña molestia al usuario. Desha0cerse del virus implica, generalmente, muy poco tiempo.
    b. **Daños Menores:** daños que ocasionan una pérdida de la funcionalidad de las aplicaciones que poseemos. En el peor de los casos se tendrá que reinstalar las aplicaciones afectadas.

c. **Daños Moderados:** los daños que el virus provoca son formatear el disco rígido o sobrescribir parte del mismo. Para solucionar esto se deberá utilizarla última copia de seguridad que se ha hecho y reinstalar el sistema operativo.
d. **Daños Mayores:** algunos virus pueden, dada su alta velocidad de infección y su alta capacidad de pasar desapercibidos, lograr que el día que se detecta su presencia tener las copias de seguridad no infectada, pero será tan antigua que se haya perdido una gran cantidad de archivos que fueron creados con posterioridad.
e. **Daños Severos:** son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No se sabe cuando los datos son correctos o han cambiado, pues no unos indicios claros de cuando se ha infectado el sistema.
f. **Daños Ilimitados:** el virus "abre puertas" del sistema a personas no autorizadas. El daño no lo ocasiona el virus, sino esa tercera persona que, gracias a él, puede entrar en el sistema.

7.5.6 LOS AUTORES

Tras su alias (nic), los creadores de virus sostienen que persiguen un fin educacional para ilustrar las flaquezas de los sistemas a los que atacan. Pero…. ¿es necesario crear un problema para mostrar otro?

La creación de virus no es ilegal, y probablemente no debería serlo: cualquiera es dueño de crear un virus siempre y cuando lo guarde para sí. Infectar a otras computadoras sin el consentimiento de sus usuarios es inaceptable, esto sí es un delito y debería ser penado, como ya lo es en algunos países.

Inglaterra pudo condenar a ¡18meses! de prisión al autor de SMEG. Sin embargo, el autor del virus Loverletter no fue sentenciado por que la legislación vigente en Filipinas (su país de origen) no era adecuada en el momento del arresto.

Existen otros casos en que el creador es recompensado con una oferta de trabajo millonaria por parte de multinacionales. Este, y no las condenas, es el mensaje que reciben miles de jóvenes para empezar o continuar desarrollando virus y esto se transforma en una "actividad de moda", lejos de la información ética sobre la cual deberían ser educados.

7.5.7 PROGRAMA ANTIVIRUS

Un antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus. Esto sirve para combatirlos, aunque no para prevenir la creación e infección de otros nuevos.

Actualmente existen técnicas, conocidas como heurísticas, que brindan una forma de “adelantarse” a los nuevos virus. Con esta técnica el antivirus es capaz de analizar archivos y documentos y detectar actividades sospechosas. Esta posibilidad puede ser explotada gracias a que de los 6- 20 nuevos virus diarios, solo aparecen unos cinco totalmente novedosos al año.

Debe tenerse en cuenta que:

a. un programa antivirus forma parte del sistema y por lo tanto funcionará correctamente si es adecuado y está bien configurado.
b. No será eficaz el 100% de los casos, no existe la protección total y definitiva.

Las funciones presentes en un antivirus son:

1. **Detección:** se debe poder afirmar la presencia y/o accionar de un VI en una computadora. Adicionalmente puede brindar módulos de identificación, erradicación del virus o eliminación de la entidad infectada.
2. **Identificación de un Virus:** existen diversas técnicas para realizar estación:

a. **Scanning:** técnica que consiste en revisar el código de los archivos (fundamentalmente archivos ejecutables y de documentos) en busca de pequeñas porciones de código que puedan pertenecer a un virus (sus huellas digitales). Estas porciones están almacenadas en una base de datos del antivirus. Su principal ventaja reside en la rápida y exacta que resulta la identificación del virus. En los primeros tiempos (cuando los virus no eran tantos ni su dispersión era tan rápida), esta técnica fue eficaz, luego se comenzaron a notar sus deficiencias. El primer punto desfavorable es que brinda una solución a posteriori y es necesario que el virus alcance un grado de dispersión considerable para que llegue a mano de los investigadores y estos lo incorporen a su base de datos (este proceso puede demorar desde uno a tres meses). Este modelo reactivo jamás constituirá una solución definitiva.

b. **Heurística:** búsqueda de acciones potencialmente dañinas perteneciente a un virus informático. Esta técnica no identifica de manera certera el virus, sino que rastrea rutinas de alteración de información y zonas generalmente no controladas por el usuario (MBR, Boot Sector, FAT, etc). Su principal ventaja reside en que es capaz de detectar virus que no han sido agregados a la base de datos de los antivirus (técnica preactiva). Su desventaja radica en que puede “sospechar” de demasiadas cosas y el usuario debe ser medianamente capaz de identificar falsas alarmas.

c. **Chequeadores de Integridad:** consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar sectores críticos de la misma. Su ventaja reside en la prevención aunque muchas veces pueden ser vulnerados por los virus y ser desactivados por ellos, haciendo que el usuario se crea protegido, no siendo así.

Es importante diferenciar los términos **detectar**: determinación de la presencia de un virus e **identificar**: determinación de qué virus fue el detectado. Lo importante es la detección del virus y luego, si es posible, su identificación y erradicación.

7.5.7.1 MODELO DE UN ANTIVIRUS

Un antivirus puede estar constituido por dos módulos principales y cada uno de ellos contener otros módulos.

1. **Módulo de Control:** Posee la técnica de Verificación de Integridad que posibilita el registro de posibles cambios en las zonas y archivos considerados de riesgo.
2. **Módulo de respuesta:** La función de “alarma” se encuentra en todos los antivirus y consiste en detener la ejecución de todos los programas e informar al usuario de la posible existencia de un virus. La mayoría ofrecen la posibilidad de su erradicación si la identificación ha sido positiva.

7.5.7.2 UTILIZACIÓN DE LOS ANTIVIRUS

Como ya se ha descrito un VI es un programa y, como tal se ejecuta, ocupa un espacio en memoria y realiza las tareas para las que ha sido programado. En el caso de instalarse un antivirus en una computadora infectada, es probable que este también se a infectado y su funcionamiento deje de ser confiable. Por lo tanto si se sospecha de la infección de una computadora, nunca deben realizarse operaciones de instalación o desinfección desde el sistema. El procedimiento adecuado sería reiniciar el sistema y proceder a la limpieza desde un sistema limpio y seguro.

La mayoría de los antivirus ofrecen la opción de reparación de los archivos dañados. Puede considerarse este procedimiento o la de recuperar el/los archivos perdidos desde una copia de seguridad segura.

7.5.8 ASPECTOS JURÍDICOS SOBRE VIRUS INFORMÁTICOS

El análisis de la responsabilidad derivada de la difusión de un virus merece especial atención en estos momentos en que el uso de las redes telemáticas permite un mayor alcance de sus efectos. Prueba de ello tenemos en la reciente difusión por correo electrónico del antes mencionado virus “I Love You” o “Kamasutra”.

Para analizar los diferentes supuestos que generan responsabilidad, debemos tener en cuenta los canales de difusión que contribuyen a potenciar el efecto pirámide en el que los virus basan su efectividad. En todos ellos es aplicable el régimen de la responsabilidad extracontractual establecida en el Código civil (ver anexo leyes) que obliga a reparar los daños a quien, por acción u omisión, causa un perjuicio a otro, interviniendo la culpa o negligencia.

La mera creación de un virus puede obedecer a una intención distinta a la puesta en circulación. Cabe recordar aquí la diferencia que hacen los Hackers entre el creador de un virus y el diseminador del mismo.

En cuanto a la puesta en circulación es difícil obtener una identificación plena del responsable de la misma. Aunque en el caso de redes telemáticas es posible encontrar rastros de la primera aparición del virus, es posible alterar esa información. En cualquier caso, la responsabilidad de la persona que inicia la cadena de efectos nocivos de un virus, planificando la difusión intencionada del mismo a través de un medio está clara, pues el daño es perfectamente previsible (aunque no su magnitud) y seguro.

En cuanto a la introducción intencionada en un sistema específico, por su tipificación como delito de daños, los actos de sabotaje informático pueden generar responsabilidad civil y penal. Pueden tener su origen en personas del interior de la empresa que por un motivo como, por ejemplo, la ruptura de la relación laboral, deciden cuasar un daño, o en personas del exterior de la empresa, que acceden al sistema informático por medios telemáticos, por ejemplo. En ambos casos se cumplen los requisitos para reclamar una indemnización.

Como ya se ha mencionado, en argentina, la Información no es considerada un bien o propiedad. Según el Art. 183 del Código Penal "..se castiga al que dañe una cosa, inmueble o animal". Hasta el momento de la realización del presente este castigo sólo es teórico, ya que en la práctica no existen casos en donde se haya podido probar la culpa de un creador o deseminador de virus dañando una "cosa, inmueble o animal".

La difusión de un virus entre usuarios de sistemas informáticos puede ser debida a una conducta negligente o la difusión de virus no catalogados. La diligencia debida en el tratamiento de la información obliga a realizar copias de seguridad y a instalar sistemas de detección de virus. En el caso de archivos que se envían a otros usuarios, la ausencia de control previsto puede ser calificada como negligente, puesto que el riesgo de destrucción de datos se está traspasando a terceros y ello podía haberse evitado de una manera sencilla y económica. Pero también puede alegarse que el usuario receptor del archivo afectado podría haber evitado el daño pasando el correspondiente antivirus, a lo que cabe replicar que este trámite se obvió por tratarse de un remitente que ofrecía confianza.

Por último, en algunos países en donde se han tratado Leyes de Propiedad Intelectual, se establece la exclusión de los VI de las creaciones protegidas por el derecho de autor. El objetivo de este precepto es facilitar las actividades de análisis necesarias para la creación de un antivirus, aunque esto resulta innecesario por la sencilla razón de que el creador de un virus no acostumbra a reclamar la titularidad del mismo de forma pública.

7.5.9 CONSEJOS

Aunque existe una relativa concientización, generalmente no se toman todas las precauciones necesarias para anular el peligro. No bastaron tener un antivirus, si no que éste hay que actualizarlo periódicamente para contemplar los nuevos virus que van apareciendo.

Además de poseer la cualidad de chequeo manual, detección y eliminación, debe ser sobre todo capaz de actuar como vacuna o filtro, impidiendo la entrada de los nuevos virus que aparecen cada día. De esta forma, aunque al usuario se le olvide pasar el antivirus, sabe que al menos existe una protección automática. La mayoría de los antivirus que se comercializan poseen estas características.

Algunos consejos para mantener nuestro sistema protegido de virus[5] se enlistan a continuación:

1. No abra jamás ningún archivo adjunto que usted no solicitó, sea cuál sea su remitente.
2. No abra ningún mensaje ni archivo recibido a través del correo electrónico de fuentes desconocidas o muy poco conocidas. En el caso de personas conocidas, se deben igualmente tomar las precauciones correspondientes respecto a los adjuntos. Asegúrese con esa persona del envío (la mayoría de los gusanos actuales pueden ser enviados por conocidos que ignoran estar mandando el virus en sus mensajes).
3. Aún siguiendo los pasos anteriores, nunca ejecute directamente (doble clic) archivos adjuntos, guárdelos primero en una carpeta temporal (o en el escritorio, con un simple clic con el botón derecho, seleccionando "Guardar como...") y revise luego esa carpeta con al menos dos o tres antivirus actualizados, antes de tomar la opción de ejecutarlos (.EXE) o abrirlos (.DOC, .RTF, etc.). Ante cualquier duda, simplemente borre el mensaje (y los archivos adjuntos). Como se dice vulgarmente, "la confianza mata al hombre", en este caso a la PC.
4. Los archivos ejecutables o que puedan causar una modificación con solo abrirlos (Ej.: EXE, COM, BAT, REG, DLL, VBS, SCR, LNK, etc.) o que contengan macros (DOC, RTF, XLS, etc.), no deberían ser aceptados vía e-mail. Los archivos RTF (Rich Text Format), por naturaleza, no pueden contener macros, sin embargo, si se renombra un .DOC como .RTF, Word lo abrirá sin quejarse, dando lugar a la ejecución de los posibles macros. Téngalo también en cuenta.
5. Use regularmente un programa anti-virus. Nosotros siempre recomendamos no confiar en uno solo, pero usar más de uno no significa que debamos tenerlos a todos instalados (jamás tenga más de un antivirus monitoreando). Simplemente ejecutamos esos antivirus en su opción de escaneo bajo demanda, sobre la carpeta que contenga los archivos a revisar.

   Y por supuesto, de nada vale usar algún antivirus si no lo mantenemos actualizado con los upgrades, updates o add-ons correspondientes. Actualmente, las actualizaciones son diarias (KAV -AVP-, Panda y otros). No deje pasar más de 24 horas entre actualizaciones, y en el peor de los casos, jamás espere más de una semana para hacerlo.

[5] http://www.vsantivirus.com/guia-de-supervivencia.htm

No existen los "virus demasiados nuevos y sin antídotos", la reacción de las casas de antivirus es inmediata en todos los casos. Pero mejor pregúntese, si la suya también lo es a la hora de actualizarse.

En nuestro sitio podrá encontrar enlaces a las actualizaciones de muchos de esos antivirus, para que usted no tenga que buscarlas por toda la Web.

Además de todo ello, realice al menos una vez al mes, un escaneo total de todos los archivos de su computadora.

6. Considere la instalación de un software "cortafuego", que disminuye el riesgo de troyanos, virus y otros códigos maliciosos, que intenten conectarse desde y hacia su computadora, sin su consentimiento.

   El Zone Alarm, gratuito para uso personal, es una excelente opción. Además, lo protege de muchos de los códigos malignos que se propagan por correo electrónico, cambiando las extensiones de los archivos potencialmente peligrosos, antes que lleguen a la base de datos de los mensajes. En nuestro sitio se explica como instalarlo y configurarlo:

   VSantivirus No. 117 - 2/nov/00
   Zone Alarm - El botón rojo que desconecta su PC de la red
   http://www.vsantivirus.com/za.htm
7. Acostúmbrese a no enviar sus mensajes con formato. Prefiera mandar su correo en modo solo texto, dentro de lo posible. Ocultar un virus en un archivo HTML es muy fácil, incluso se puede llegar a ejecutar sin necesidad del "doble clic". Pídale a quien le envía mensajes con formato, que no lo siga haciendo. Es un riesgo demasiado alto, por algo que suele ser innecesario.
8. Deshabilite el panel de vista previa en el Outlook. Ello evita la visualización de un mensaje hasta que hacemos doble clic sobre él. Sin embargo, debe tener en cuenta que no por sacar esta opción, un código malicioso dejará de ejecutarse cuando se abra el mensaje (no estamos hablando de un adjunto, sino la simple visualización del texto del mensaje). Para quitar el Panel de vista previa, diríjase al menú del Outlook, seleccione la opción "Ver" y luego "Diseño". Desmarque la casilla "Mostrar panel de vista previa".
9. Jamás envíe archivos adjuntos de cualquier tipo, a una persona que no se lo pidió. Y en caso de que se lo haya pedido, asegúrese de revisar su sistema antes de hacerlo. O si ello fuera posible, prefiera enviarle la dirección del sitio desde donde podrá bajar el archivo solicitado, y no el propio archivo. Además, disminuirá así sus propios gastos telefónicos.
10. Recuerde que existe el riesgo de la "doble extensión". Windows por defecto, oculta las extensiones de los archivos más usados. Es así que un archivo NOMBRE.TXT, puede ser en realidad un archivo NOMBRE.TXT.EXE o .VBS, etc. Esta es la forma preferida por muchos virus, sobre todo del tipo gusanos. Los .VBS son ejecutables escritos en Visual Basic Script. Al ser su extensión .TXT.VBS por ejemplo, la

extensión .VBS quedará oculta, y por lo tanto aparentará ser un archivo de texto: .TXT, haciéndole pensar en su inocencia. Para que ello no ocurra, DESMARQUE dicha opción, a los efectos de poder ver siempre la verdadera extensión de un archivo.

Para poder ver las extensiones verdaderas de los archivos y además visualizar aquellos con atributos de "Oculto", proceda así:

- En Windows 95, vaya a Mi PC, Menú Ver, Opciones.
- En Windows 98, vaya a Mi PC, Menú Ver, Opciones de carpetas.
- En Windows Me, vaya a Mi PC, Menú Herramientas, Opciones de carpetas.

Luego, en la lengüeta "Ver" de esa opción, DESMARQUE la opción "Ocultar extensiones para los tipos de archivos conocidos" o similar. También MARQUE la opción "Mostrar todos los archivos y carpetas ocultos" o similar.

11. Si corresponde, ponga al día su Windows e Internet Explorer, desde la actualización de productos de Microsoft, conectándose a su sitio:

    http://windowsupdate.microsoft.com/

    Seleccione "Actualización de productos", y luego lo que corresponda a su equipo entre las "Actualizaciones críticas" que sean detectadas, para asegurarse de que el equipo funciona sin problemas y para protegerlo ante posibles fallas de seguridad. Un "Paquete de actualizaciones críticas" aparece siempre que estas sean necesarias para su equipo. Descargue las que corresponda, o todo el paquete para actualizar todo su sistema en un solo paso.
12. Deshabilite el Windows Scripting Host (WSH). Esta característica puede ayudar a automatizar varias tareas dentro de Windows, pero también puede ser explotado por numerosos virus, los que no podrán ejecutarse sin el WSH.

    Para desactivarlo, vaya al Panel de Control (Mi PC, Panel de Control), Agregar o quitar programas, Instalación de Windows, Accesorios, pinche en Detalles, y desmarque "Windows Scripting Host". Reinicie su PC. Si usa Windows Me, utilice otras opciones, como el NOSCRIPT.EXE de Symantec. Más información sobre esto, la encontrará en nuestra página:

    VSantivirus No. 231 - 24/feb/01
    Algunas recomendaciones sobre los virus escritos en VBS
    http://www.vsantivirus.com/faq-vbs.htm
13. Aumente la seguridad en el Outlook. Vaya a Herramientas, Opciones. Seleccione la lengüeta "Seguridad". Pinche en "Zonas de seguridad", y luego pinche en "Zonas de sitios restringidos (más segura)". Pinche en ACEPTAR y confirme los cambios. Esto lo protegerá de ciertos códigos maliciosos. Más información en:

    VSantivirus No. 366 - 9/jul/01

Consejos: Outlook y Outlook Express más seguros
http://www.vsantivirus.com/consejos-outlook.htm

14. Si recibe un mensaje con una advertencia de virus, donde se le pida "reenviarlo a todos sus conocidos", jamás lo haga. Este tipo de virus o alarmas, SON TOTALMENTE FALSOS. Pero lo que es peor, estas advertencias activan un tipo de "contaminación" muy diferente, propagar cientos y hasta miles de mensajes de advertencia sobre los mismos (se les llama HOAXES, por lo de broma o engaño).

    Si alguien de buena fe le envía una de estas alarmas, avísele de páginas como la nuestra, donde se listan los hoaxes más comunes, para que salga de su engaño y obtenga más detalles. Una lista de los HOAXES más comunes, la tendrá siempre en nuestro sitio:

    http://www.vsantivirus.com/hoaxes.htm

    Allí también encontrará información de porqué es peligroso hacerle caso a trucos donde se nos promete una seguridad que no es tal (como el agregar un !0000 a la libreta de direcciones), o peor aún, borrar archivos solo porque alguien nos dice que es un virus... ¡sin siquiera haberlo escaneado con algún antivirus! (que es el caso del SULFNBK, por ejemplo).
15. No baje nada de sitios Web de los que no tenga referencias de seriedad, o que no sean medianamente conocidos. Y si baja archivos, proceda como con los archivos adjuntos. Cópielos a una carpeta y revíselos con dos o tres antivirus actualizados antes de optar por ejecutarlos o abrirlos.
16. Configure el BIOS de su computadora para que se inicie primero desde la unidad de disco duro, y no desde un disquete. Esto evitará la posible infección del sector de booteo, al arrancar inadvertidamente de un disquete infectado. Simplemente reinicie su computadora, pulse la tecla apropiada (DEL o SUPR, F1, etc.) y en las opciones de Setup del BIOS, busque y habilite, la opción "Boot Sequence" o similar como "C, A, ..." etc. o "C: -> A:", o "1st Boot Device" como "IDE-0", "2nd Boot Device" como "Floppy", o la que corresponda en su caso.
17. Tenga siempre a mano un disquete de inicio, debidamente protegido, para poder reiniciar su PC ante una infección. Imprima y tenga a mano las instrucciones para ejecutar el antivirus F-PROT desde un par de disquetes, tal como se explica en nuestro sitio:

    VSantivirus No. 158 - 13/dic/2000
    Cómo ejecutar F-PROT en un disquete (actualizado)
    http://www.vsantivirus.com/fprot-disq.htm

    F-PROT es un antivirus gratuito para uso personal. También es conveniente tener un respaldo actualizado de sus archivos más importantes.
18. Use contraseñas robustas. Una buena contraseña es difícil de adivinar, y si el sistema lo permite, típicamente incluye letras mayúsculas y minúsculas combinadas, y algunos números. También intente utilizar una contraseña diferente para cada cuenta que usted utilice. Si no lo

hace, una vez que alguien descubra una de sus contraseñas, las tendrá a todas.

19. Haga respaldos regulares de sus datos críticos. Planee un backup incremental cada día (solo lo que se ha actualizado), con un respaldo total por lo menos una vez a la semana. Y no olvide verificar estos respaldos una vez al mes. Además, asegúrese de tener a mano el software necesario para restaurar el respaldo cuando lo necesite. Y, para realmente proteger sus datos críticos, considere guardar alguno de sus backups lo más lejos posible de su lugar de trabajo, por ejemplo, en una caja de seguridad en el banco, en su casa, etc.
20. No deje sus computadoras "en-línea" cuando no las use. Desconecte físicamente el cable de su computadora con Internet mientras no esté usando esa conexión, aún si utiliza un enlace dedicado las 24 horas.
21. Manténgase informado de cómo operan los virus, y de las novedades sobre estos, alertas y anuncios críticos, en sitios como el nuestro.

CAPITULO 8

PROTECCIÓN

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

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

El presente capitulo, después del expuesto y vistas, la gran cantidad de herramientas con las que cuenta el intruso, es el turno de estudiar implementaciones en la búsqueda de mantener el sistema seguro.

Siendo reiterativo, ninguna de las técnicas expuestas a continuación representaran el 100 % de la seguridad deseado, aunque muchas parezcan la panacea, será de algunas de ellas las que convertirán un sistema interconectado en confiable.

8.1 VULNERAR PARA PROTEGER

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. El trabajo de los Administradores Y Testers no difiere mucho de eso. En lo que si se diferencia, y por completo; es en los objetivos; mientras que un intruso penetra en las redes para distintos fines (investigación, daño, robo etc.) un administrador lo hace para poder mejorar los sistemas de seguridad.

En palabras de Julio C. Ardita. (…) los intrusos cuentan con grandes herramientas como los Scanners, los Cracking de passwords, software de análisis de vulnerabilidades y los exploits (…) un administrador cuenta con todas ellas empleadas para bien, los Logs, los sistemas de detección de intrusos de rastreo de intrusiones.

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como Penetración Testing, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez mas eficaces.

Un test esta totalmente relacionado con el tipo de información que se maneja en cada organización. Por consiguiente, según la información que deba ser

protegida, se determina la estructura y las herramientas de seguridad; no a la inversa.

El Software y Hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina "políticas de seguridad interna" que cada organización (y usuario) debe generar e implementar.

8.1.1 ADMINISTRACIÓN DE LA SEGURIDAD

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

- **Autenticación:** se refiere a establecer las entidades que pueden tener acceso al universo de recursos de cómputo que cierto medio ambiente puede ofrecer.
- **Autorización:** es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.
- **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 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 esta suceda (proactividad). A continuación se citan algunos de los métodos de protección mas comúnmente empleados.

1. **Sistemas de detección de intruso:** son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.
2. **Sistemas orientados a conexión de red:** monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los contrafuegos (Firewalls) y los Wrappers.
3. **Sistemas de análisis de vulnerabilidades:** analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "desventaja" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso autorizado al sistema.
4. **Sistemas de protección a la integridad de información:** sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest (MD5) o Secure Hash Algorithm

(SHA), o bien sistemas que utilizan varios de ellos PGP, Tripwire y DozeCrypt.

5. **Sistemas de protección a la privacidad de la información:** Herramientas que utilizan criptografía para asegurar que la información solo sea visible para quien tiene autorización. Sui aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de ese tipo de herramientas se puede citar a Pretty Good Privacy (PGP), Secure Sockets Layer (SSL) y los Certificados Digitales.

Resumiendo, un modelo de seguridad debe estar formado por múltiples componentes o capaz 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 de Router-Firewall.
4) Ssietmas de detección de intrusos.
5) Plan de respuesta a incidentes.
6) Penetration Test

8.1.2 PENETRATION TEST, ETHICAL HACKING O PRUEBA DE VULNERABILIDAD

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

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

El Penetración Test se compone de dos grandes frases de testeo:

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

- Pruebas de usuario y la “fuerza” de su password.
- Captura de tráfico.
- Detección de conexiones externas y sus rangos de direcciones.
- Detección de protocolos utilizados.
- Scanning de puertos TCP, UDP, e ICMP.

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

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

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

8.1.3 HONEY POTS-HONEY NETS

Estas “trampas de red” son sistemas que se activan con la finalidad especifica de que los expertos en seguridad puedan observar en secreto la actividad de los Hackers / Crackers en su hábitat natural.

Actualmente un equipo de Honeynet Project, trabaja en el desarrollo de un documento sobre la investigación y resultados de su trampa, la cual fue penetrada a la semana de ser activada (sin publicidad).

Consiste en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos. Los Honeynetsdan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos (…)
Ellos juegan con los archivos y conversan animadamente entre ellos sobre todo los fascinantes programas que encuentran mientras el personal de seguridad observa con deleite cada movimiento que hacen dijo Dam Adams, francamente

siento una combinación de sentimientos con respecto a espiar a la gente, aunque no sean buenas personas.

Esta ultima frase se esta presentando a menudo en el tema de la investigación (y vigilancia) electrónica. Este es el caso del exdirector del proyecto Honeynet J.D Glaser, quien renuncio a su puesto después de aclarar que esta convencido que la vigilancia electrónica no es correcta, aunque se utilize en aras de la investigación. (…) Ampliar un Honeynet es parecido a estrampar los derechos de otros, aunque sean, los derechos de un delincuente.

8.2 FIRE WALLS

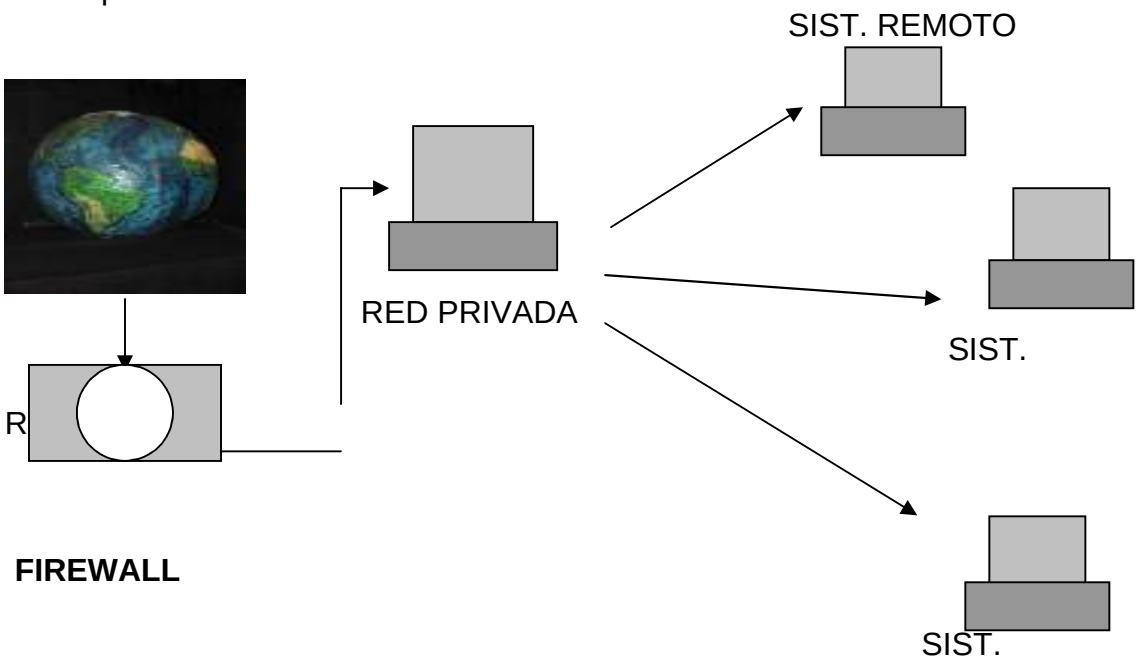
Quizás uno de los elementos mas publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe presentar atención, distan mucho de ser la solución final a los problemas de seguridad.

De hecho, los Firewalls no tienen nada que hacer contra técnicas como Ingeniería Social y el ataque de Insideres.

Un **Firewalls** es un sistema (o conjunto de ellos) 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 el Internet).

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

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



FIREWALL

REMOTO n

Como puede observarse, el Muro Contrafuegos, solo sirven de defensa perimetral 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.

8.2.1 ROUTERS Y BRIDGES

Cuando los paquetes de información viajan entre su destino y origen, vía TCP/IP estos pasan por diferentes Rotures (enrutadores a nivel de Red).

Los Rotures son dispositivos electrónicos encargados de establecer comunicaciones extensas 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.

La evolución tecnológica les ha permitido transformarse en computadoras muy especializadas capaz de determinar, si el paquete tiene un destino externo y el camino mas corto y mas descongestionado hacia el Router de la red destino. En caso de que el paquete provenga de afuera, determina el destino en la red interna y lo deriva a la maquina correspondiente o devuelve el paquete a su origen en caso de que el no sea el destinatario del mismo.

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.

8.2.2 TIPOS DE FIREWALL

8.2.2.1 FILTRADO DE PAQUETES

Se utilizan 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.

El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado)

Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de firewalls trabajan a los Niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

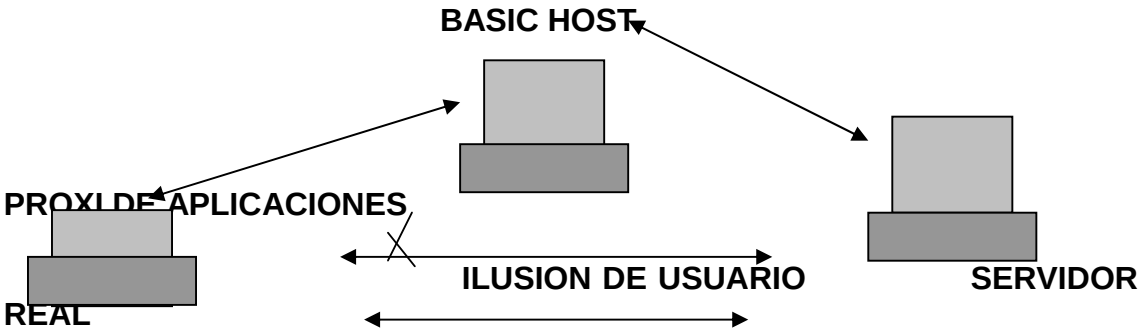
1. No protege las capas superiores a nivel OSI.
2. Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
3. No son capaces de esconder la topología de redes privadas, porlo que exponen la red al mundo exterior.
4. Sus capacidades de auditoria suelen ser limitadas, al igual que su capacidad de registro de actividades.
5. No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

8.2.2.2 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 maquina donde se ejecutan recibe el nombre de Gateway de Aplicación o Bastión Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de aplicación, siendo transparente a ambas partes.

Cuando un usuario desea un servicio, lo hace a travez del Proxy. Este realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue analizar el tráfico de red en busca de contenido que viole la seguridad de la misma. Gráficamente:

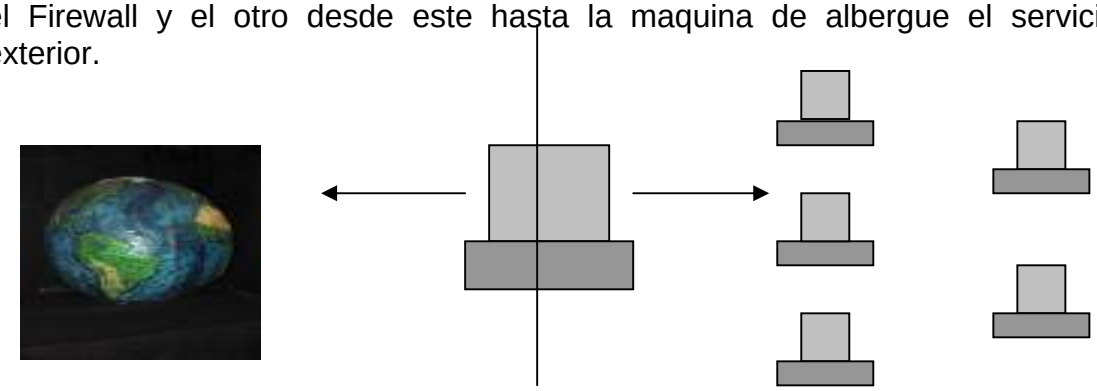


8.2.2.3 DUAL-HOMED HOST

Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del filtrado de paquetes), por lo que se dice que actúan con el IP-Forwarding desactivo.

Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función como su configuración impuesta en dicho Fireweall, se conectara al servicio exterior solicitado y hará de puente entre este y el usuario interior.

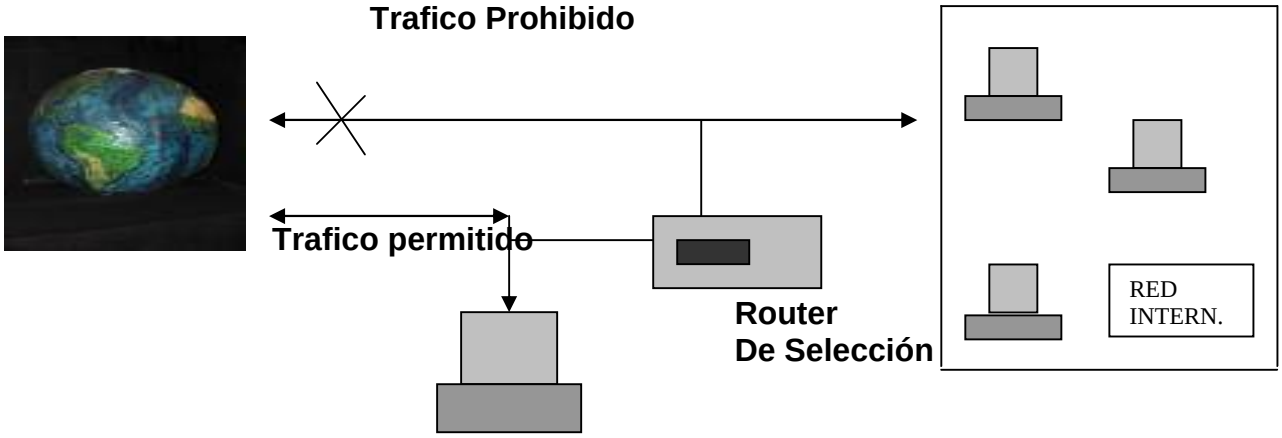
Es decir que se utilizan dos conexiones. Uno desde la maquina interior hasta el Firewall y el otro desde este hasta la maquina de albergue el servicio exterior.



Bastion Host
Ip Routing / Forwading Desactivado
RED INTERNA

8.2.2.4 SCREENED HOST

En este caso se combina un Router con un host bastion y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y solo se permiten un numero reducido de servicios.



8.2.2.5 SCREENED SUBNET

En este diseño se intenta aislar la maquina mas atacada y vulnerable de Firewall, el Nodon Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que si un intruso accede a esta maquina no consigue el acceso total a la subred protegida.

En este esquema se utilizan dos Routers: uno exterior y otro interior. El router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y la DMZ (zona entre el Router externo y el interno).

Es posible definir varios niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplifican a uno solo.

Como puede apreciarse la Zona Desmilitarizada aisla físicamente los servicios internos, separándolos de los servicios públicos. Además existe una conexión directa entre red interna y externa.

Los sistemas Dual-Homed Host y Screnned pueden ser complicados de configurar y comprobar, lo que puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien configurados y administrados pueden brindar un alto de protección y ciertas ventajas:

1. Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitado o sospechosa.
2. Registro de actividades y autenticación robusta: El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
3. Reglas de filtrado menos complejas: Las reglas de filtrado de los paquetes por parte del Router serán menos compleja dado a que el solo debe atender las solicitudes de Gateway.

Así mismo tiene la desventaja de ser intrusitos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr la comunicación. Se suma a esto lo que generalmente son más lentos porque deben revisar todo el tráfico de la red

8.2.2.6 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 su procedencia y destino. Se aplican desde la capa de Red hasta la de aplicaciones. Generalmente son instalados cuando re requiere seguridad sensible al contexto y en aplicaciones muy complejas.

8.2.2.7 FIREWALLS PERSONALES

Estos firewalls son aplicaciones disponibles para usuarios finales que desean conectarse desde un simple "cuelgue" o infección de virus hasta la perdida de toda su información almacenada.

8.2.3 POLÍTICAS DE DISEÑO DE FIREWALLS

Las políticas de accesos en un Firewalls se debe diseñar poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes de 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 quien protegerse? De cualquier intenso 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 o determinados servicios o denegado cualquier tipo de acceso a otros.

- ¿Cómo protegerse? Esta es la pregunta más difícil y esta orientada a establecer el nivel de motorización, 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- Estrategia 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 costara? Estimado en función de lo que se desea para proteger se debe decidir cuanto es conveniente invertir.

8.2.4 RESTRICCIONES EN EL FIREWALL

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**:

Sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red.

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

8.2.5 BENEFICIOS DE UN FIREWALL

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestos a ataques desde el exterior. Esto significa que la seguridad de toda la red estaría dependiendo de que tan fácil fura 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 internos de ataque, el administrador será responsable de la revisión de estos monitoreos.

Otra causa que ha hecho el uso de Firewalls se halla convertido en uso casi imperativo es el echo que en los últimos años en Internet han entrado en crisis el numero disponible de direcciones IP esto ha hecho que las intranet 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 “consumado” por el trafico de la red, y que procesos han influido mas en ese trafico, de esta manera el administrador de la red puede restringir el uso de estos procesos 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.

8.2.6 LÍMITACIONES DE UN FIREWALL

La limitación mas 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 aun 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 password o los huecos del Firewall y difunde esta información, el Firewallno se dará cuenta.

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

Finalmente un Firewall es vulnerable, el NO protege de la gente que esta dentro de la red interna. El firewall trabaja mejor si se complementa con una defensa interna: Como moraleja “cuanto mayor sea el trafico de entrada y salida permitiendo por el Firewall, menor será la resistencia contra paquetes externos, El único Firewall seguro (100%) es aquel que se mantiene apagado.

8.3 ACCES CONTROL LISTS (ACL)

Las listas de control de Acceso proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

8.4 WRAPPERS

Un Wrapper es un programa que controla el acceso a un segundo programa, obteniendo con esto un más alto nivel de seguridad. Los Wrappers son usados dentro de la seguridad en sistemas UNIXs . Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los Wrappers son ampliamente utilizados, y han llegado a formar parte de herramientas de seguridad por las siguientes razones:

- Debido a que la seguridad lógica esta conectada en un solo programa, los Wrappers son fáciles y simples de validar.
- Debido al que el programa protegido se mantiene como una entidad separada, este puede ser actualizado sin necesidad de cambiar el Wappers.
- Debido a que los Wrappers llaman al programa protegido mediante llamadas estándar al sistema, se puede usar un solo Wrappers 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.

El paquete Wrapper mas ampliamente utilizado es el TCP-Wrappers, el cual es un conjunto de utilidades de distribución libre, escrito por wietse Venema (co-autor de SATAN, con Dan Farmer, y considerado el padre de los sistemas Firewalls) en 1990.

Consiste en un programa que es ejecutado cuando llega una petición a un puerto específico. Este, una vez comprobada la dirección de origen de la petición, la verifica contra las reglas almacenadas, y es función de ellas, decide o no dar paso al servicio.
Adicionalmente, registra estas actividades del sistema, su petición y su resolución.

Algunas configuraciones avanzadas de este paquete, permite también ejecutar comandos en el propio sistema operativo, en función de la resolución de la petición. Por ejemplo es posible que interese detectar una posible maquina atacante, en el caso de un intento de conexión para tener mas datos a la hora de una posible investigación. Este tipo de comportamiento raya en la estrategia paranoica, ya vista cuando se definió la política de seguridad del Firewall.

Con lo mencionado hasta aquí, puede penarse que los Wrappers son Firewall ya que muchos de los servicios brindados son los mismos o causan los mismos efectos: usando Wrappers, se puede controlar el acceso a cada maquina y los servicios accedidos, así estos controles son el complemento perfecto de un Firewall y la instalación de uno no esta supeditada a la del otro.

8.5 DETECCIÓN DE INTRUSOS EN TIEMPO REAL

La seguridad se tiene que tratar en conjunto. Este viejo criterio es el que recuerda que los sistemas de protección hasta aquí abordado, si bien son eficaces, distan mucho de ser la protección ideal.

Así, debe de estar fuera de toda discusión la convivencia de añadir elementos que controlen lo que ocurre dentro de la red (detrás de los firewalls).

Como se ha visto, la integridad de un sistema se puede corromper de varias formas y la forma de evitar esto es con la instalación de sistemas de Detección de Intrusos en Tiempo Real, quienes:

- Inspeccionan el tráfico de la red buscando posibles ataques.
- Controlan el registro de los servidores para detectar acciones sospechas (tanto de intrusos como de usuarios autorizados.)
- Mantienen una base de datos con el estado exacto de cada uno de los archivos (Integrity Check) del sistema para detectar la modificación de los mismos.
- Controlan el ingreso de cada nuevo archivo al sistema para detectar Caballos de Troya o semejantes.

- Controlan el núcleo del Sistema Operativo para detectar posibles infiltraciones en el, con el fin de controlar los recursos y acciones del mismo.
- Avisan al administrador de cualquiera de las acciones mencionadas.

Cada una de estas herramientas permiten mantener alejados la gran mayoría de los intrusos normales, Algunos pocos, con suficientes conocimientos, experiencia y paciencia serán capaces de utilizar métodos sofisticados (u originales) como para voltear el perímetro de seguridad (interna + externa) y serán estos los casos que deban estudiarse para integrar a la política de seguridad existente mayor conocimiento y con el mayor seguridad.

8.5.1 INTRUSION DETECTIONS SYSTEMS (IDS)

Un sistema de detección de intrusos es un componente más dentro del modelo de seguridad de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómalas desde el exterior – interior de un sistema informático. Los sistemas de detección de intruso puede clasificarse, según su función y comportamiento en:

- **Host-Based IDS:** operar en un Host para detectar actividad maliciosa en el mismo.
- **Network-Based IDS:** operan sobre los flujos de información intercambiados en una red.
- **Knowledge-Based IDS:** sistemas basados en Conocimiento.
- **Behavior-Based IDS:** sistemas basados en Comportamiento. Se asume que una intrusión puede ser detectada observando una desviación respecto del comportamiento normal o esperando de un usuario en el sistema.

La idea central de este tipo de detección es el hecho de que la actividad intrusiva es un conjunto de actividades anómalas. Si alguien consigue entrar de forma ilegal al sistema, no actuara como un usuario comprometido se alejara del de un usuario normal.

Sin embargo en la mayoría de las ocasiones una actividad intrusiva resulta del agregado de otras actividades individuales que por si solas no constituyen un comportamiento intrusivo de ningún tipo.

Así las intrusiones puede calificarse en:

- **Intrusivas pero no anómalas:** denominados falsos Negativos (el sistema erróneamente indica ausencia de intrusión). En este caso la actividad es intrusiva pero como no es anómala no es detectada. No son deseables, por que dan una falsa sensación de seguridad del sistema.
- **No intrusivas pero anómalas:** denominados. Falsos Positivos (el sistema erróneamente indica la existencia de intrusión).En este caso la actividad es no intrusiva, pero como es anómala el sistema “decide” que es intrusiva. Deben intentar minimizarse, ya que en caso contrario se ignoran los avisos del sistema, incluso cuando sean acertados.

- **No intrusiva ni anómala:** son Negativos Verdaderos, la actividad es no intrusiva y se indica como tal.
- **Intrusiva y anómala:** se denominan positivos Verdaderos, la actividad es intrusiva y es detectada.

Los detectores de intrusiones anómalas requieren mucho gasto computacional, ya que se siguen normalmente varias métricas para determinar cuanto se aleja el usuario de lo que se considera comportamiento normal.

8.5.1.1 CARACTERÍSTICAS DE IDS

Cualquier sistema de detección de intrusos debería, sea cual sea el mecanismo en que este basado, **debería** contar con las siguientes características:

- Debe funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en background dentro del equipo que esta siendo observado. Sin embargo, no debe ser una “caja negar” (debe ser examinable desde el exterior).
- Debe ser tolerante a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema.
- En relación con el punto anterior, debe ser resistente a perturbaciones. El sistema puede monitorizarse a si mismo para asegurarse de que no ha sido perturbado.
- Debe imponer mínima sobre descarga sobre el sistema. Un sistema que ralentiza la maquina simplemente no será utilizado.
- Debe observar desviaciones sobre comportamiento estándar.
- Debe ser fácilmente adaptable al sistema ya instalado. Cada sistema tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones.
- Debe hacer frente a los cambios de comportamiento del sistema según añaden nuevas aplicaciones al mismo.
- Debe ser difícil de “engañar”.

8.5.1.2 FORTALEZAS DE IDS

- Suministra información muy interesante sobre el tráfico malicioso de la red.
- Poder de reacción para prevenir el daño.
- Es una herramienta útil como arma de seguridad de la red.
- Ayuda a identificar de donde provienen los ataques que se sufren.
- Recoge evidencias que pueden ser usadas para identificar intrusos
- Es una “cámara” de seguridad y una “alarma” contra ladrones.
- Funciona como “disuasor de intrusos”.
- Alerta al personal de seguridad de que alguien esta tratando de entrar.
- Protege contra la invasión de la red
- Suministra cierta tranquilidad.

- Es una parte de la infraestructura para la estrategia global de defensa.
- La posibilidad de detectar intrusiones desconocidas e impresivas. Pueden incluso contribuir (parcialmente) al descubrimiento automático de esos nuevos ataques.
- Son medios dependientes de los mecanismos específicos de cada sistema operativo. Pueden ayudar a detectar ataques del tipo "abuso de privilegios" que no implica realmente vulnerabilidad de seguridad. En pocas palabras, se trata de una aproximación a la paranoia : " todo aquello que no se ha visto previamente es peligroso"
- Menor costo de implementación y mantenimiento al ubicarse en puntos estratégicos de la red.
- Dificulta el trabajo del intruso de eliminar sus huellas.

8.5.1.3 DEBILIDADES DE IDS

- No existe un parche para la mayoría de bugs de seguridad.
- Se producen falsas alarmas.
- Se producen fallos en las alarmas.
- No es sustituí ahora un buen Firewalluna auditoria de seguridad regular y una fuerte y estricta política de seguridad.

8.5.1.4 INCONVENIENTES DE IDS

- La alta tasa de falsas alarmas dado que no es posible cubrir todo el ámbito del comportamiento de un sistema de información durante la fase de aprendizaje.
- El comportamiento puede cambiar con el tiempo, haciendo necesario un reentrenamiento periódico del perfil, lo que da lugar a la no disponibilidad del sistema o la generación de falsas alarmas adicionales.
- El sistema puede sufrir ataques durante la fase de aprendizaje, con lo que el perfil de comportamiento contendrá un comportamiento intrusivo el cual no será considerado anómalo.

8.6 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 parar por el usuario, la llamada se devolverá al usuario legal no al del intruso, siendo este desconectado. Como precaución adicional, el usuario deberá verificar que la llamada-retorno proceda del número a donde llamo previamente.

8.7 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 la red, para detectar el modo en el cual esta actuando (recordar que un Sniffer la coloca en modo promiscuo), y el tráfico de datos en ella.

8.8 GESTIÓN DE CLAVES "SEGURAS"

Si se utiliza una clave de 8 caracteres de longitud, con los 96 caracteres de longitud, con los 96 caracteres posibles, puede tardarse 2.288 años en descifrarla (analizando 100.000 palabras por segundo). Esto se obtiene a partir de las 96 (7.213.895.789.838.340) claves posibles de generar con esos caracteres.

Partiendo de la premisa en que no se disponen de esa cantidad de años para analizarlas por fuerza bruta, se deberá comenzar a probar con las claves más posibles Débiles.

Según demuestra el análisis de +NetBull realizado sobre 2-134 cuentas y probando 227.000 palabras por segundo:

- Con un diccionario 2.030 palabras (el original de Jhon de Ripper 1.04), se obtuvieron 36 cuentas en solo 19 segundos (1,77%).
- Con un diccionario de 250.000 palabras, se obtuvieron 64 cuentas en 36:18 minutos (3.15%).

Otro estudio muestra el resultado obtenido al aplicar un ataque, mediante un diccionario de 62.727 palabras, a 13.794 cuentas:

- En un año se obtuvieron 3.340 contraseñas (24,22 %).
- En la primera semana se descubrieron 3,000 claves (21,74%)
- En los primeros 15 minutos se descubrieron 368 palabras claves (2.66%).

Según los grandes números vistos, seria valido afirmar que: es imposible encontrar ¡36 cuentas en 19 segundos!. También debe observarse, en el segundo estudio que el porcentaje de hallazgos casi no varía entre un año y una semana.

Tal vez, ¿esto sucedió porque existían claves nulas; que corresponde al nombre del usuario; a consecuencias alfabéticas tipo: abad; a consecuencias numéricas tipo "1,2,3,4, a secuencias observadas en el teclado tipo "qwer" ; a palabras que existen en un diccionario el lenguaje del usuario, si estas, claves (las mas débiles) son las primeras en ser analizadas y los tiempos obtenidos confirman la hipótesis.

Este simple estudio confirma nuestra mala elección de contraseñas y el riesgo se incrementa si el atacante conoce algo sobre la victima (Ingeniería Social) ya que podrá probar palabras relacionadas a su persona o diccionarios orientados.

8.8.1 NORMAS DE ELECCIÓN DE CLAVES

Se debe tener en cuenta los siguientes consejos:

1. No utilizar contraseñas que sean palabras (aunque sean extranjeras? O nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
2. No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I, fecha de nacimiento patente del automóvil,etc.)
3. Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
4. Deben ser largas, de 8 caracteres o más.
5. Tener contraseñas diferentes en maquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas maquinas.
6. Deben ser fáciles de recordar para no verse obligado a recibirlas. Algunos ejemplos son:

    - Combinar palabras cortas con algún numero o carácter de puntuación: soy2_yo3
    - Usar un acrónimo para mayor seguridad: A9r7R5G3d1P
    - Mejor incluso si la frase no es conocida: Hasta ahora no he Olvidado mi Contraseña – aHoelLo
    - Elegir una palabra sin sentido, aunque pronunciable: taChunda72, Ataju1H, Wen2Mar.
    - Realizar reemplazos de letras por signos o números: En seguridad Mas vale Prevenir que Curar – 35M//Pq

8.8.2 NORMAS PARA PROTEGER UNA CLAVE

La protección de la contraseña recae tanto sobre el administrador del sistema como sobre el usuario. Al comprometer una cuenta se puede estar comprometiendo todo el sistema.

La siguiente frase difundida en UseNet resume alguna de las reglas básicas de uso de la contraseña “Un password debe ser como un cepillo de dientes. Úsalo cada día: cámbialo regularmente; y NO lo compartas con tus amigos”.

Algunos consejos a seguir:

1. No permitir ninguna cuenta sin contraseña. Si es administrador del sistema, repasar este echo periódicamente.
2. No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas del Root, System, Test, Demo, Guest, etc.
3. Nunca compartir con nadie la contraseña. Si se hace, cambiarla inmediatamente.
4. No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.
5. No teclear la contraseña si hay alguien mirando. Es una norma táctica de buen usuario no mirar el teclado mientras alguien teclee su contraseña.

6. No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si se debe mencionar no hacerlo explícitamente diciendo: “mi clave es”:
7. No mantener una contraseña indefinidamente. Cambiarla regularmente. Disponer de una lista de contraseñas que puedan usarse clínicamente (por lo menos 5).

Muchos sistemas incorporan ya algunas medidas de gestión y protección de las contraseñas. Entre ellas podemos citar las siguientes:

1. Numero de intentos limitado. Tras un numero de intentos fallidos, pueden tomarse distintas medidas:

    1. Obligar a reescribir el nombre de usuario (lo más común).
    2. Bloquear el acceso durante un tiempo.
    3. Enviar un mensaje al administrador y/o mantener un registro especial.

    1. Longitud mínima. Las contraseñas deben tener un numero mínimo de caracteres (se recomienda 7 u 8 como mínimo).
    2. Restricciones de formato. Las contraseñas deben cambiar un mínimo de letras y números, no pueden contener el nombre del usuario ni ser un blanco.
    3. Envejecimiento y expiración de contraseñas. Cada cierto tiempo se fuerza a cambiar la contraseña. Se obliga a no repetir ciertas cantidad de las anteriores. Se mantiene un periodo forzoso entre cambios, para evitar que se vuelva a cambiar inmediatamente y se repita la anterior.
    4. Ataque preventivo. Muchos administradores utilizan crackeadores para intentar atacar las contraseñas de su propio sistema en busca de debilidades.

8.8.3 CONTRASEÑAS DE UN SOLO USO

Las contraseñas de un solo uso (One Time Password) son uno de los mecanismos de autentificación más seguros, debido a que su descubrimiento tan solo permite acceder al sistema una vez. Además, en muchas ocasiones se suelen utilizar dispositivos hardware para su generación, lo que las hace mucho más difíciles de descubrir.

Ejemplos de este tipo de contraseñas serian las basadas en funciones unidireccionales (sencillas de evaluar en un sentido pero imposible o muy costoso de evaluar en un sentido contrario) y en listas de contraseñas.

Se distinguen tres tipos de contraseñas de un solo uso:

1. Las que requieren algún dispositivo hardware para su generación, tales como calculadoras especiales tarjetas inteligentes (Token Cards).
2. Las que requieren algún tipo de software de cifrado especial.
3. Las que se basan en una lista de contraseñas sobre papel.

La tarjeta genera periódicamente valores mediante a una función secreta y unidireccional, basada en el tiempo y el número de identificación de la misma.

El usuario combina el número generado por la tarjeta con su palabra de paso para obtener el password de entrada, lo que protege en caso de robo o perdida.

8.9 SEGURIDAD EN PROTOCOLOS Y SERVICIOS

Se ha visto en capítulos anteriores la variedad de protocolos de comunicaciones existentes, sus objetivos y su funcionamiento. Como puede preveerse todos estos protocolos tienen su debilidad ya sea en su implementación o en su uso. A continuación se describe los problemas de seguridad más comunes y sus formas de prevención.

Nuevamente no se verán los detalles sobre el funcionamiento de cada uno de ellos, simplemente se ofrecerá las potenciales puertas de entrada como fuentes de ataques que ni siquiera tienen por que proporcionar acceso a la maquina (como las DoS por ejemplo).

De esta forma, si cada servicio ofreciendo es un posible problema para la seguridad, parece claro que lo ideal seria no ofrecer ninguno, poseer una maquina completamente aislada de resto, evidentemente, hoy en día no es posible en la mayor parte de los sistemas.

Por lo tanto, ya que es necesaria la conectividad entre equipos, se ha de ofrecer los mínimos servicios necesarios para que todo funcione correctamente, esto choca frontalmente con las políticas de la mayoría de fabricantes y empresas, que por defecto mantienen la mayoría de servicios abiertos al instalar un equipo nuevo: es responsabilidad del administrador preocuparse de cerrar los que no sean estrictamente necesarios.

8.9.1 NETBIOS

Estos puertos (137-139 en TCP y UDP) son empleados en las redes Microsoft para la autentificación de usuarios y la compartición de recursos. Como primera medida debe minimizarse la cantidad de recursos compartidos y luego debe evitarse permitir el acceso global a esos dispositivos, ya que es posible el acceso de intrusos desde cualquier lugar externo a la red.

8.9.2 ICMP

A fin de prevenir los ataques basados en bombas ICMP, se debe filtrar todos los paquetes de redirección y los paquetes inalcanzables.

8.9.3 FINGER

Típicamente el servicio Finger (puerto 79 en TCP) ha sido una de las principales fuentes de problemas. Este protocolo proporciona información detallada de los usuarios de una estación de trabajo, estén o no conectados en el momento de acceder al servicio.

La información suministrada suele ser de mucha utilidad para un atacante: datos del usuario, hábitos de conexión, cuentas inactivas. Esta claro que esto es fácilmente aprovechable por un intruso para practicar ingeniería social contra esos usuarios.

Es básico deshabilitar este servicio, restringir su acceso a unos cuantos equipos de la red local o utilizar versiones de Finger que permiten especificar la información que se muestra al acceder al servicio.

8.9.4 POP

El servicio POP (puertos 109 y 110 en TCP) utilizando para que los usuarios puedan acceder a su correo sin necesidad de montar un sistema de archivos compartidos. Se trata de un servicio que se podrá considerar peligroso, por lo que (como el resto, pero este especialmente) debemos deshabilitarlo a no ser que sea estrictamente necesario ofrecerlo; en ese caso debemos restringir al máximo los lugares y usuario desde los que se pueden acceder.

Mediante POP se genera un transito peligroso de contraseñas a traves de la red. Se ofrece tres modelos distintos de autentificación: uno basado en Kerberos: apenas utilizado, otro basado en un protocolo desafió-respuesta, y el otro basado en un simple nombre de usuario con su password correspondiente.

Este ultimo, el mas usado en todo tipo de entornos, es un excelente objetivo para un intruso con un Sniffer. Los usuarios suelen configurar sus clientes para que Chequen el buzón de correo de cada pocos minutos, con lo que a intervalos muy cortos envían su cable a un puerto conocido de una maquina conocida; al realizar esta comunicación en texto claro, un atacante no tiene mas que interceptar la sesión POP para averiguar nombres de usuario y claves (a parte de poder leer el correo).

8.9.5 NNTP

El servicio NNTP (puerto 119 en TCP) se utilizado para intercambiar mensajes de grupos de noticias entre servidores de News. Los diferentes demonios encargados de esta tarea suelen discriminar conexiones en función de la dirección o el nombre de la maquina cliente para decidir so ofrece el servicio de un determinado host, y si es así, concretar de que forma puede acceder a el (solo, lectura, solo ciertos grupos, etc.).

De esta forma los servidores NNTP son muy vulnerables a cualquier ataque que permita falsear la identidad de la maquina origen, como el IP Spoofing.

Los problemas relacionados con las News no suelen ser excesivamente graves desde un punto de vista estrictamente técnico, pero en ocasiones si que lo son aplicando una visión global. Por ejemplo, habría que evaluar el daño que le supone a la imagen de la organización el que un atacante envié mensajes insultantes o pornográficos utilizando el nombre o los recursos de la misma.

Realmente, es muy poco probable que se necesite ofrecer en servicio, por lo que más razonable es deshabilitarlo. Generalmente solo existen servidores de noticias en grandes organizaciones, y si debe administrar equipo con este servicio la mejor forma de protegerlo es utilizando un buen firewall.

8.9.6 NTP

NTP (puerto 123 en UDP y TCP) es un protocolo utilizando para sincronizar relojes de maquinas de una forma muy precisa: a pesar de su sostificacion no fue diseñado con una idea de robustez ante ataques, por lo que puede convertirse en una gran fuente de problemas si no esta correctamente configurado.

Son muchos problemas de seguridad relacionados con un tiempo correcto: el mas simple y obvio es la poca finalidad qué ofrecerá el sistema de Log a la hora de determinar cuando sucedió determinado evento.

Otro problema inerte a NTP se refiere a la plantificación de tareas: si el reloj tiene problemas, es posible que ciertas tareas no se lleguen a ejecutar, que se ejecuten varias veces, o que se ejecuten cuando no han de hacerlo; esto es especialmente peligroso para tareas de las que depende la seguridad (como los backups).
No obstante, muy pocos sistemas necesitan la precisión de NTP, por lo tanto lo que es habitual tener servicio deshabilitado. En la mayoría de ocasiones el propio reloj de la máquina, o un protocolo mucho más simple (como time), es más que suficiente para sincronizar equipos.

8.9.7 TFTP

TFTP es un protocolo de transferencias de archivos (puerto 69 basado en UDP) que no proporciona ninguna seguridad. Por tanto en la mayoría de sistemas es deseable (obligatorio) que este servicio este desactivo. Al utilizar este servicio en ningún momento se solicita un nombre de usuario o una clave, lo que da una idea de los graves problemas de seguridad que ofrece este servicio.

“Gracias” a este protocolo se han implementado algunas de las ultimas vulnerabilidades del Internet Information Server”.

8.9.8 FTP

Un problema básico y grave de FTP (puerto 21 en TCP) es que ha sido diseñado para ofrecer la máxima velocidad en la conexión, pero no para ofrecer la seguridad: todo el intercambio de información, desde el login, y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto claro con lo que un atacante no tiene mas que capturar todo ese trafico y conseguir así un acceso valido al servidor. Incluso puede hacer una amenaza a la privacidad de los datos el echo de que este atacante también pueda capturar y reproducir (y modificar) los archivos trasferidos.

Para solucionar este problema es conveniente dar acceso FTP a pocos usuarios bien identificados y que necesiten utilizarlo, concientizándolos de la utilidad de aplicaciones que cifren todo el trafico de información (como SSH por ejemplo).

8.9.8.1 FTP ANÓNIMO

El servicio FTP se vuelve especialmente preocupantes cuando se trata de configurar un servidor de FTP anónimo; muchos de estas maquinas situadas en universidades y empresas se convierten en servidores de imágenes pornográficas, de Warez (copias ilegales de programas comerciales), etc. Conseguir un servidor de FTP anónimo seguro puede llegar a ser una tarea complicada.

El usuario Anónimo debe conectar a un entorno restringido del sistema y solo a ese.

8.9.8.2 FTP INVITADO

El otro tipo de acceso FTP es el dominio invitado (guest). La idea de este mecanismo es muy sencilla. Se trata de permitir que cada usuario conecte a la maquina mediante su login y su contraseña, pero evitando que tenga acceso a partes del sistema de archivos que no necesita para realizar su trabajo; se conectara a un entorno restringido de forma similar a lo que sucede en los accesos anónimos.

Para poder crear fácilmente entornos FTP restringidos a cada usuario, es conveniente instalar programas para este fin en la maquina servidor. Estos servidores permiten crear usuarios invitados configurando el entorno al que van a conectarse los usuarios, su estructura de directorios-archivo y sus permisos a los recursos.

8.9.9 TELNET

El protocolo TELNET (TCP, puerto 23), permite utilizar una maquina como Terminal virtual de otra a través de la red, de forma que se crea un canal virtual de comunicaciones similar (pero mucho mas inseguro) a utilizar una Terminal físicamente conectada a un servidor.

TELNET es el clásico servicio que hasta hace unos años no se solía deshabilitar nunca: lo mas normal es que este servicio este disponible para que los usuarios puedan trabajar remotamente, al menos desde el conjunto de maquinas determinado.

Evidentemente reducir al mínimo imprescindible el conjunto de sistemas desde donde es posible la conexión es una primera medida de seguridad: no obstante, no suele ser suficiente.

TELNET no utiliza ningún tipo de Cifrado, por lo que todo el tráfico entre equipos se realiza en texto. Cualquier intruso con Sniffer puede capturar el Login y el password utilizados en una conexión otorgado a cualquiera que lo lea esos datos un acceso total ala maquina destino. Es muy recomendable no utilizar TELNET para conexiones remotas, si no sustituirlo por aplicaciones equivalentes pero que utilizan cifrado para la transmisión de datos (SSH o SSL –Telnet por ejemplo).

8.9.10 SMTP

La mala configuración del servicio SMTP (puerto 25 en TCP) utilizado para transferir correo electrónico entre equipos remotos; suele ser causante del Mail Bombing y el Spam redirigido.

Por lo general se recibirá correo de un numero intermediario de maquinas, y no se podrá bloquear el acceso a SMTP. No obstante, en este caso podemos aplicar unas medidas de seguridad simples, como realizar una consulta inversa a DNS para asegurarnos de que solo maquinas registradas envía correo o no permitir que el sistema reenvié correo que no provenga de direcciones registradas bajo su dominio.

8.9.11 SERVIDORES WWW

Hoy en día las conexiones a servidores Web son sin duda las más extendidas entre usuarios de Internet. En la actualidad mueve a diario millones de dólares y es uno de los pilares fundamentales de muchas empresas: es por tanto un objetivo muy atractivo para cualquier intruso.

Los problemas de seguridad relacionados con el protocolo HTTP se dividen en tres grandes grupos en función de los datos a los que pueden afectar.

- **Seguridad en el servidor**: es necesario garantizar que la información almacenada en la maquina servidora no puede ser modificada sin autorización, que permanezca disponible y que solo pueda ser accedida por los usuarios a los que este legítimamente permitido.
- **Seguridad en la red**: cuando un usuario conecta a un servidor Web se produce un intercambio de información entre ambos: es vital garantizar que los datos que recibe el cliente desde el servidor sean los mismos que se están enviando (esto es, que no sufran modificaciones de terceros), y también garantizar que la información

que el usuario envía hacia el servidor no sea capturada, destruida o modificada por un atacante.

- **Seguridad en el cliente**: es necesario garantizar al usuario que descarga paginas de un servidor no va a perjudicar a la seguridad de su equipo. Se deben evitar Applets maliciosos, programas con virus o simples cuelgues al acceder a las páginas de la organización. Ante echos de esta especie seguramente la persona dejara de visitarlas, con la consecuente perdida de imagen (y posiblemente un cliente) de esa entidad.

Asegurar el servidor implica (aparte de las medidas habituales) medidas excepcionales dedicadas al servidor de Web y su entorno de trabajo.

Sea cual sea el servidor utilizado, (IIS, Apache, NCSA, Netscape, etc.), es necesario seguir un consejo básico: minimizar el numero de usuarios en la maquina y minimizar el numero de servicios ofrecidos en ella: aunque lo normal es que una maquina dedicada a cualquier tarea, sea también el servidor sea un equipo dedicado solo a esa tarea.

Los problemas relacionados con servidores Web suelen proceder de errores de programación en los CGIs ubicados en el servidor. La cantidad del GCI para comunicarse con el resto del sistema que alberga las paginas es lo que le otorga su potencia, pero también lo que causa mayores problemas de seguridad: un fallo en estos programas suele permitir a cualquier visitante" ejecutar en el sistema.

Una medida de seguridad básica es ejecutar el demonio servidor bajo la identidad de un usuario con el privilegio mínimo para que todo funcione correctamente, pero nunca como Administrador, ORT o cuenta del sistema.

Para garantizar la seguridad de los datos que circulan entre un cliente y el servidor es casi obligatorio cifrar datos (mediante SSL o utilizando Certificados Digitales por ejemplo).

8.10.1 CRIPTOLOGÍA- HISTORIA

En el año 500 a.C. los griegos utilizaron un cilindro llamado "scytale" alrededor del cual enrollaban una tira de cuero. Al escribir un mensaje sobre el cuero y desenrollarlo se veía una lista de letras sin sentido. El mensaje correcto solo podía leerse al enrollar el cuero nuevamente en un cilindro de igual diámetro.

Durante el Imperio Romano Julio Cesar empleo un sistema de cifrado consistente en sustituir la letra a encriptar por otra letra distanciada a tres posiciones mas adelante. Durante su reinado, los mensajes de Julio Cesar nunca fueron desencriptados:

En el siglo S.XII Roger Bacón y en el S. XV León Batista Albertini inventaron y publicaron sentidos algoritmos de encriptación basados en modificar del método de julio Cesar.

Durante la segunda guerra mundial en un lugar llamado Bletchley Park (70 Km.al nortede Londres) un grupo de científicos trabaja en Enigma, la maquina encargada de cifrar los mensajes secretos alemanes.

En este grupo se encontraban tres matemáticos polacos llamados Marina Rejewsky, Jerzy, Henryk Zygalsji t “un joven que se mordía siempre las pieles alrededor de las uñas, iba con ropa sin planchar y era mas bien bajito. Este joven retraído se llama Alan Turing y había sido reclutado porque unos años antes había creado un ordenador binario. Probablemente poca gente en los servicios secretos ingleses sabia lo que era un ordenador (y mucho menos binario)…. Pero no cabía duda que solo alguien realmente inteligente podía inventar algo así, cualquier cosa que no fuese…Era mucho mas abstracto que todos sus antecesores y solo utilizaba 0 y 1 como valores posibles de las variables de su de su algebra.

Seria Turing el encargado de descifrar el primer mensaje de Enigma y cambiar, el curso de la guerra, la historia y de … la Seguridad Informática actual.

8.10.2 CRIPTOGRAFÍA

La palabra **Criptografía** proviene etimológicamente del griego (Kriptos oculto) y (Grafo Escritura) y significarte parte de escribir con clave secreta o de un modo enigmático.

Apartando Luz a la definición cabe aclar que la criptografía hace años que dejo ser un Arte para convertirse en una técnica o conjunto de ellas que tratan sobre la protección (ocultamente ante personas no autorizadas) de la información: Entre las disciplinas que engloba cabe destacar la teoría de la Información, la Teoría de la información, la Matemática Discreta, la Teoría de los Grandes Números y la complejidad Algorítmica.

Es decir que la criptografía es la ciencia es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que solo el emisor y el destinatario conocen), para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

El mensaje cifrado recibe el nombre **Criptograma**

La importancia de la Criptografía radica en que es el único método actual capaz de hacer cumplir el objetivo de la Seguridad Informática "mantener la privacidad, Integridad, Autenticidad… "y hacer cumplir con el **No Rechazo,** relacionado a no poder negar la autoría y recepción de un mensaje enviado.

8.10.3 CRIPTOANALISIS

Es el arte de estudiar los mensajes ilegibles, encriptados, para transformarlos en legibles sin conocer la clave, aunque el método de cifrado empleado siempre es conocido.

8.10.4 CRIPTOSISTEMA

"Un criptosistema se define como la quíntupla (m,C,K,E,D.), donde:

- **m** representa el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.
- **C** Representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- **K** representa el conjunto de claves que se pueden emplear en el criptosistema.
- **E** es el conjunto de las transformaciones de cifrado o familia de funciones que se aplica a cada elemento de **m** para obtener un elemento de **C.** Existe una transformación diferente **Ex** cada valor posible de la clave **K**.
- **D** es el conjunto de trasformaciones de descifrado, analogo a **E.**

Todo criptosistema cumple la condición **Dk (Ek(m)) = m** es decir, que si se tiene un mensaje **m,** se cifra empleando la clave **K** y luego se descifra empleando la misma clave, se obtiene el mensaje original **m**.

Existe dos tipos fundamentales de Criptosistemas utilizados para cifrar datos de información digital y ser enviados posteriormente después por medios de trasmisión libre.

A. **Simétricos o de clave privada:** se emplea la misma clave **K** para cifrar y descifrar, por lo tanto el emisor y el receptor deben poseer la clave. El

mayor conveniente que presentan es que se debe contar con un canal seguro para la transmisión de dicha clave.

B. **Asimétricos o de llave publica:** se emplea una doble clave conocidas como **Kp** (clave privada) y **Kp** (clave publica). Una de ellas es utilizada para la transformación E de cifrado y la otra para el descifrado D. En mucho de los sistemas existentes estas clave son intercámbiales, es decir que si empleamos una para descifrar y viceversa.

Los sistemas asimétricos deben cumplir con la condición que clave Publica (al ser conocida y solo utilizada para cifrar) no debe permitir calcular la privada. Como puede observarse este sistema permite intercambiar claves en un canal inseguro de transmisión ya que lo único que se envía es la clave pública.

Los algoritmos asimétricos emplean claves de longitud mayor a los simétricos. Así, por ejemplo, suele considerarse segura una clave de 128 bits para estos últimos pero se recomienda claves de 1024 bits (como mínimo) para los algoritmos. Esto permite que los algoritmos simétricos sean considerablemente más rápidos que los asimétricos.

En la práctica actualmente se emplee una combinación de ambos sistemas ya que los asimétricos son computacionalmente más costosos (mayor tiempo de cifrado). Para realizar dicha combinación se cifra el mensaje **m** con un sistema simétrico y luego se encripta la clave **K** utilizada en el algoritmo simétrico (generalmente mas corta que el mensaje) con un sistema asimétrico.

Después estos Criptosistemas modernos podemos encontrar otros no menos importantes utilizados desde siempre para cifrar mensajes de menos importancia o domésticos, y que han ido perdiendo su eficiencia por ser fácilmente criptoanalizables y por tanto “reventables” Cada uno de los algoritmos clásicos descriptos a continuación utilizan la misma clave K para cifrar y descifrar el mensaje.

8.10.4.1 TRANSPOSICIÓN

Son aquellos que alteran el orden de los caracteres dentro del mensaje a cifrar. El algoritmo de trasposición más común consiste en colocar el texto en una tabla de **n** columnas. El texto cifrado serán los caracteres dados por columna (de arriba hacia abajo) con una clave **K** consistente en el orden en que se leen las columnas.

Ejemplo: Si en = 3 columnas, la clave (3,1,2) y el mensaje a cifrar “SEGURIDAD INFORMATICA”.

1	2	3
S	**E**	**G**
U	**R**	**I**
D	**A**	**D**
	1	**N**
F	**O**	**R**
M	**A**	**T**

I	**C**	**A**

El mensaje cifrado será: “GIDNRTASUD FMIERAIOAC”

8.10.4.2 CIFRADOS MONOALFABÉTICOS

Sin desordenar los símbolos del lenguaje, se establece una correspondencia única para todos aquellos en todo el mensaje. Es decir que si al carácter A le corresponde carácter D esta correspondencia se mantiene durante todo el mensaje.

8.10.4.2.1 Algoritmo de Cesar

Es uno de los algoritmos criptográficos más simples. Consiste en sumar 3 al número de orden de cada letra. De esta forma a la A le corresponde la D, a la B la E, y así sucesivamente. Puede observarse que este algoritmo ni siquiera posee clave, puesto que la transformación siempre en la misma. Obviamente, para descifrar basta con restar 3 al número de orden de las letras del criptograma.

Ejemplo: Si el algoritmo de cifrado es:

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

Entonces el mensaje cifrado será:

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

8.10.4.2.2 Sustitución General

Es el caso general del algoritmo de Cesar. El sistema consiste en sustituir cada letra por otra aleatoria. Esto supone un grado más de complejidad aunque como es de suponer las propiedades estadísticas del texto original se conservan en el criptograma y por lo tanto el sistema sigue siendo criptoanalizable.

8.10.5 ALGORITMOS SIMÉTRICOS MODERNOS (LLAVE PRIVADA)

La mayoría de los algoritmos simétricos actuales apoyan en los conceptos de **Confusión** y **Difusión** vertidos por Claude Shannon sobre la teoría de la Información a finales de los años cuarenta.

Estos métodos consisten en ocultar la relación entre el texto plano, el texto cifrado y la clave, (confusión); y repartir la influencia de cada bit del mensaje original lo mas posible entre el mensaje cifrado (Difusión).

El objetivo del presente no es entrar en detalles de cada uno de los muchos algoritmos existentes, por lo que solo se dará una idea de su funcionamiento y complejidad.

8.10.5.1 REDES DE FIESTEL

Este algoritmo no es un algoritmo de cifrado per se, pero muchos de los vistos a continuación lo utilizan como parte vital en su funcionamiento. Se basa en dividir un bloque de longitud n (generalmente el texto a cifrar) en dos mitades, L y R . Luego se define un cifrado de producto interactivo en el que la salida de cada ronda es la entrada de la siguiente:

8.10.5.2 DES

Data Encrytion Standard es el algoritmo simétrico mas extendido mundialmente. A mediados de los setenta fue adoptado como estándar para las comunicaciones seguras (Estándar AES) del gobierno de EE.UU. Es su principio fue diseñado por la NSA (Nacional Security Agency) para ser implementado en hardware, pero al extenderse su algoritmo se comenzó a implementar en software.

DES utiliza bloques de 64 bits, los cuales codifica empleando claves de 56 bits y aplicando permutaciones a nivel de bit en diferentes momentos (mediante tablas de permutaciones y operaciones XQR). Es una red de feistel de 16 rondas, más dos permutaciones, una que se aplica al principio y otra al final.

La flexibilidad de DES reside en que el mismo algoritmo puede ser utilizado tanto para cifrar como para descifrar, simplemente invirtiendo el orden de las 16 subclaves obtenidas a partir de clave de cifrado.

En la actualidad no se a podido romper el sistema DES criptoanaliticamente (deducir la clave simétrica a partir de la información interceptada) Sin embargo una empresa española sin fines de lucro llamado **electrónica fontier foundation (EFF)** construyo en enero de 1999 una maquina capaz de probar las 2 claves posibles en DES y romperlo solo en tres días con fuerza bruta.

A pesar de su caída DES sigue siendo utilizado por su amplia extinción de las implementaciones vía hardware existentes (en cajeros automáticos y señales de video por ejemplo) y se evita tener confiar en nuevas tecnologías no probadas. En vez de abandonar su utilización se prefiere suplantar a DES con lo que se conoce como cifrado múltiple, es decir, aplicar varias veces el mismo algoritmo para fortalecer la longitud de la clave.

8.10.5.2.1 DES MULTIPLE

Consiste en aplicar varias veces el algoritmo DES (con diferentes claves) al mensaje original. El más conocido de todos ellos él Triple – DES (T-DES), el cual consiste en aplicar 3 veces DES de la siguiente manera:

1. Se codifica con la clave K1
2. Se decodifica el resultado con la clave K2
3. Lo obtenido se vuelve a codificar con K1

La clave resultante en la concatenación de K1 y K2 con una longitud de 112 bits.

En 1988 el NIST (National Institute of Standars Technology) convoco a un concurso para poder determinar un algoritmo simétricos seguro y próximo sustituto de DES. Se aceptaron 15 candidatos y a principios del año 2000 los 5 finalistas fueron MARS, RC, - 6, Serpent y TwoFish Rijdael (que en octubre será el ganador).

8.10.5.3 IDEA

El International Data Encription Algorithm fue desarrollado en Alemania a principios de los noventa por James L. Massey y Xuejia Lai.

Trabaja con bloques de 64 bits de longitud empleando una clave de 128 bits y, como en el caso de DES, se utiliza el mismo algoritmo tanto para cifrar como para descifrar.

El proceso de encriptación consiste ocho rondas de cifrado idéntico excepto por los subclaves utilizadas (segmentos de 16 bits de los 128 de las clave), en donde se combinan diferentes operaciones matemáticas (XORs y Sumas Modulo 16) y una transformación final.

“En mi opinión, el es el mejor y mas seguro algoritmo de bloques disponibles actualmente al publico.

8.10.5.4 BLOWFISH

Este algoritmo fue desarrollado por Bruce Schnerier en 1993. Para la encriptación emplea bloques de 64 bits y permite claves de encriptación de diversas longitudes (hasta 448 bits) .

Generalmente, utiliza valores decimales de * (a que pueda cambiarse a voluntad) para obtener las funciones de encriptación y desencriptacion, estas funciones emplean operaciones lógicas simples y presentes en cualquier procesador. Esto se traduce en un algoritmo “liviano”, que permite su implementación, vía hardware, en cualquier controlador (como teléfonos celulares por ejemplo).

8.10.5.5. RC5

Este algoritmo, diseñador por RSA 15, permite definir el tamaño de bloque a encriptar, el tamaño de la clave utilizada y el número de fases de encriptación.

El algoritmo genera una tabla de encriptación y luego procede a encriptar los datos.

8.10.5.6 CAST

Es un buen sistema de cifrado en bloques con una clave de 128 bits, es muy rápido y es gratuito. Su nombre deriva de las iniciales de sus autores, Carlisle, Adams, Stafford, Travares, de la empresa Northern Telecom (NorTel).

CAST no tiene claves débiles o semidebiles y hay fuertes argumentos acerca que CAST es completamente inmune a los métodos de criptoanálisis mas potentes conocidos.

8.10.5.7 RIJNDAEL (EL NUEVO ESTANDAR AES)

Este nuevo algoritmo belga mezcla de Vicent Rijmen y Joan Daemen (sus autores) sorprende tanto por su innovador diseño como su simplicidad practica; aunque tras el se esconda un complejo trasfondo matemático.

Su algoritmo no se basa en redes de fiesel, y en su lugar se ha definido una estructura de “capas” formadas por funciones polinomicas reversibles (tiene inversa) y no lineales. Es fácil imaginar que el proceso de descifrado consiste en aplicar las funciones inversas a las aplicadas para cifrar, en el orden contrario.

Las implementaciones actuales pueden utilizar bloques de 128, 192, y 256 bits de longitud combinadas con claves de 128, 192, y 256 bits para su cifrado; aunque tanto los bloques como las claves pueden extenderse en múltiple de 32 bits.

Si bien su joven edad no permite asegurar nada, según sus autores, es altamente improbable que existan claves débiles en el nuevo AES. También se ha probado la resistencia al criptoanálisis tanto lineal como diferencial, asegurando así la desaparición de DES.

8.10.5.8 CRIPTOANÁLISIS DE ALGORITMOS SIMÉTRICOS

El criptoanálisis comenzó a extenderse a partir de la aparición de DES por sospechas (nunca confirmadas) de que el algoritmo por la NSA contenía puertas traseras. Entre los ataques mas potentes a la criptografía simétrica se encuentra:

- **Criptoanálisis Diferencial:** Ideado por Biham y Shamir en 1990, se basa en el estudio de dos textos codificados para estudiar las diferencias entre ambos mientras se los esta codificando. Luego puede asignarse probabilidades a ciertas claves de cifrado.
- **Criptoanálisis Lineal:** Ideado por Mitsuru Matsui, se basa en tomar porciones del texto cifrado y porciones de otro texto plano y efectuar operaciones sobre ellos de forma tal de obtener probabilidades de aparición de ciertas claves.

Sin embargo, estos métodos, no han podido ser más eficientes en la práctica. En el momento después de que un sistema criptográfico es publicado y se muestra inmune a estos dos tipos de ataque (y otros pocos) la mayor preocupación es la longitud de las claves.

8.10.6. ALGORITMOS ASIMÉ TRICOS (LLAVE PRIVADA PÚBLICA)

Ideado por los matemáticos Whitfield Diffe y Martín Hellman (HD) con el informático Ralph Merkle a mediados de los 70, estos algoritmos han demostrado su seguridad en comunicaciones inseguras como Internet. Su principal característica es que no se basa en una única clave sino en un par de ellas: una conocida (Publica) y otra Privada.

Actualmente existen muchos algoritmos de este tipo pero han demostrado ser un poco utilizables en la practica ya sea por la longitud de las claves, la longitud del texto encriptado generado o su velocidad de cifrado extremadamente largos.

DH esta basado en las propiedades y en el tiempo necesario para calcular el valor del logaritmo de un número extremadamente alto y primo.

8.10.6.1 RSA

Este algoritmo fue ideado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman (RSA). Es el más empleado en la actualidad, sencillo de comprender e implementar, aunque la longitud de sus claves es bastante considerable (ha pasado desde sus 200 bits originales a 2048 actualmente).

RSA es la suma de dos de los algoritmos más importantes de la historia: El Máximo Común Divisor de Euclides (Grecia 450- 377 A.C) y el último teorema de Fermat (Francia 1601-1665).

Se emplean las ventajas proporcionadas por las prioridades de los números primeros cuando se aplican sobre ellos operaciones matemáticas basadas en la función del modulo. En concreto, emplea la función exponencial discreta para cifrar y descifrar, cuya inversa, el logaritmo discreto, es muy difícil de calcular.

Los cálculos matemáticos de este algoritmo emplean un numero denominado Modulo Publico, N, que forma parte del la clave y que se obtiene a partir de la multiplicación de dos numero primos, **p** y **q**, diferentes y grandes (del orden de 512bits) y que forman parte de clave privada. La gran propiedad de RSA es que, mientras que N es público los valores de **p** y **q** se pueden mantener en secreto debido a la dificultad que entraña la factorización de un número grande.

La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presentas la factorización de

su producto, aunque el avance tecnológico hacer que cada vez sea mas rápido un posible ataque por fuerza bruta, el simple echo de aumentar la longitud de las claves empleadas supone un incremento en la carga computacional lo suficientemente grande para que este tipo de ataque sea visible.

Sin embargo, se ha de notar que, aunque el echo de aumentar la longitud delas claves RSA no supone ninguna dificultad tecnológica, las leyes de exportación de criptografía de EEUU, imponían, hasta el 20 de septiembre de 2000, un limite a dciha longitud por lo que el su uso comercial de RSA no estaba permitido, ya que la patente pertenecía a los laboratorios RSA. Desde esta fecha su uso es libre.

8.10.6.1.1 Ataques a RSA

Si un ataque quiere recuperar la clave privada a partir de la pública debe obtener **p** y **q** a partir de **N**, lo cual actualmente es un problema intratable si los números primos son lo que suficientemente grandes (alrededor de 200 dígitos).

Vale decir que a nadie ha demostrado que no pueda existir un método que permita descifrar un mensaje sin usar la clave privada y sin factorizar **N.** Asi, aunque el algoritmo es bastante seguro conceptualmente, existen algunos ataques que pueden ser efectivos al apoyarse sobre deficiencias en la implementación y uso del mismo.

El ataque que con mayores probabilidades de éxito es el **ataque de intermediario,** que en realidad puede darse sobre cualquier algoritmo de la clave publica Kb, C se interpone, obteniendo la clave publica, supongamos:

…que A quiera establecer una comunicación con B y que C quiera espirarla Cuando A le solicite a B su clave publica Kb, C se interpone poniendo, obteniendo la clave de B y enviando a A una clave falsa Kc, creada por el. Cuando A codifique el mensaje, C lo intercepta de nuevo, lo decodifica con su clave propia y emplea Kb para codificarlo y enviarlo a B… ni A ni B sospecharan nunca de lo sucedido.

La única manera de evitar esto consiste en asegurar a A que la clave publica de B es autentica. Para ello esto debería ser firmada por un amigo común que, actuando como Autoridad Certificadora, certifique su autenticidad.

Otros ataque (como el de claves débiles, es de texto plano escogido, el de modulo común, y el exponente bajo) aprovechan vulnerabilidades especificas de algunas implementaciones.

8.10.6.2 CURVAS ELÍPTICAS (CEE)

Las curvas elípticas fueron propuestas por primera vez para ser usadas en aplicaciones criptográficas en 1985 de forma independiente por Miller y Koblitz. Las curvas elípticas en si llevan estudiándose de la teoría de los números

La eficiencia de este algoritmo radica en la longitud reducida de las claves, lo cual permite su implementación en sistemas de bajos recursos como teléfonos celulares y Smart Cards. Puede hacerse la siguiente comparación con RSA obteniendo el mismo nivel de seguridad:

- CCE de 163 bits = RSA de 1024 bits.
- CCE de 224 bits = RSA DE 2048 bits.

Otros algoritmos asimétricos conocidos son **ElGamal** (basado en el problema de los Logaritmos Discretos de Diffie-Hellman DH), **Rabin** (basado en el problema de calculo de raíces cuadradas modulo un numero compuesto), **DDS y LUC.**

8.10.7 AUTENTIFICACIÓN

Es de destacar que muchas de estas definiciones, pueden ser encontradas en el texto del Proyecto de “ley de firma Digital” (ver anexo Leyes) actualmente con media sanción.

Se entiende por autentificación cualquier método que permita garantizar alguna característica sobre un objeto dado. Interesa comprobar la autentificación de:

a) Un Mensaje mediante una firma: se debe caracterizar la procedencia de un mensaje conocido, de forma de poder asegurar que no es una falsificación. A este mecanismo se le conoce como **Firma Digital** y consiste en asegurar que el mensaje **m** proviene del emisor **E** y no de otro.
b) Un usuario mediante una contraseña: se debe garantizar la presencia de un usuario autorizado mediante una contraseña secreta.
c) Un Dispositivo: se debe garantizar la presencia de un dispositivo valido en el sistema, por ejemplo una llave electrónica.

8.10.7.1 FIRMA DIGITAL

Una firma digital se logra mediante una Función Hash de Resumen. Esta función se encarga de obtener una “muestra única” del mensaje original. Dicha muestra es más que pequeña y es muy difícil encontrar otro mensaje que tenga la misma firma. Suponiendo que B envía un mensaje m a A el procedimiento es:

a) B genera un resumen del mensaje (m) y lo cifra con su clave privada.
b) B envía el criptograma.

c) A genera su propia copia de r (m) usando la clave publica de B asociada a la privada.
d) A compra su criptograma con el recibido y si coincide el mensaje es autentico.

Cabe destacar que:

1. Cualquiera que posea la clave pública de B puede contrastar que el mensaje proviene realmente de B.
2. La firma digital es distinta en todos los documentos: si A firma dos documentos produce dos criptogramas distintos y ; si A y B firma el mismo documento m también se producen de criptogramas diferentes.

Las funciones Hash están basadas en que un mensaje de longitud arbitraria se transforma en un mensaje de longitud constante dividiendo el mensaje en partes iguales, aplicando la función de transformación a cada parte y sumando todos los resultados obtenidos.

Actualmente se recomienda utilizar firmas de al menos 128 bits (38 dígitos) siendo 160 bits (48 dígitos) el valor mas utilizado.

8.10.7.1.1 MD5

El Message Diggest 5 (resultado mejorado sobre el MD4 original de Ron Rivest) procesa los mensajes de entrada en bloques de 512, y que produce una salida de 128 bits.

Siendo **m** un mensaje de **b** bits de longitud, se alarga **m** hasta que su longitud sea 64 bits inferior a un múltiplo de 512. Esto se realiza agregando un 1 y tantos ceros como sea necesario. A continuación se agregan 64 bits con el valor b comenzando por el byte menos significativo.

A continuación se realiza 64 operaciones divididas en 4 rondas sobre estos bloque de 512 bits. Finalmente, se suman y concatenan los bloques obteniendo la firma deseada de **m**.

8.10.7.1.2 SHA – 1

El Secure Hash Algorithm fue desarrollado por la NSA, y genera firmas de 160 bits a partir de bloques de 512 bits del mensaje original. S u funcionamiento es similar al MD5, solo variando la longitud de los bloques y la cantidad de operaciones realizadas en las 5 rondas en las que se divide el proceso.

Otros algoritmos utilizados para ofrecer firmas digitales son: DSA (Digital Signatura Logarithm) y el RIPE-MD 160.

8.10.8 PGP (PRETTY GOOD PRIVANCY)

8.10.8.1.1 ANILLOS DE CLAVES

Un anillo es una colección de claves almacenadas en un archivo, cada usuario tiene dos anillos, una para las claves públicas y otro para las 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.

8.10.8.1.2 CODIFICACIÓN DE MENSAJES

Como ya se sabe, los algoritmos simétricos de cifrado son más rápidos que los asimétricos. Por esta razón PGP cifra primero el mensaje empleando un algoritmo simétrico con una clave generada aleatoriamente (clave de pensión) y posteriormente codifica la clave haciendo uso de la llave pública del destinatario. Dicha clave es extraída convenientemente del anillo de claves públicas correspondientes.

8.10.8.1.3 DECODIFICACIÓN DE MENSAJES

Cuando se trata de decodificar el mensaje, PGP simplemente busca en 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 permita decodificar el mensaje.

Nótese que siempre que siempre que se quiere hacer uso de una clave privada, habrá que suministrar la contraseña correspondiente, por lo que si este anillo quedara comprometido, el atacante tendría que averiguar dicha contraseña para descifrar los mensajes.

No obstante, si el anillo de claves privadas quedara comprometido, es recomendable revocar todas las claves almacenadas y generar otras nuevas.

8.10.8.1.4 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 de cifrado ante el criptoanálisis que explotan las redundancias del texto plano.

PGP utiliza rutinas de comprensión de dominio publico creadas por Gaily – Adler-Wales (basadas en los algoritmos de Liv-Zemple) funcionalmente semejantes a las utilizadas en los software comerciales de ese tipo.

8.10.8.1.5 Algoritmos Utilizados por PGP

Las diferentes versiones de PGP han ido adoptando diferentes combinación de algoritmos de signatura y cifrado eligiendo entre los estudios. 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 Ganal.

8.10.9 ESTEGANOGRAFÍA

Consiste en ocultar en el interior de información aparentemente inocua, otro tipo de información (citada o no). El texto se envía como texto plano, pero entre mezclado con mucha cantidad de “basura” que sirve de camuflaje al mensaje enviado. El método de recuperación y lectura solo es conocido por el destinatario del mensaje y se conoce como “separar el grano de paja”.

Los mensajes suelen ir ocultos entre archivos de sonido o imágenes y ser enormemente grandes por la cantidad extra de información enviada (la comparación del mensaje original).

8.11 COMERCIO ELECTRÓNICO

El comercio eléctrico abarca todos los conceptos relacionados con procesos de mercado entre entidades físicas o jurídicas pero a través de redes de telecomunicaciones.

El principal requisito que debe tener una transacción electrónica es la **Seguridad** además de:

- **Confidencial (anonimato)** la identidad del comprador no es conocida como el vendedor, nadie excepto en banco debería ignorar la naturaleza de la compra Y :) la identidad del comprador; el banco debería ignorar la naturaleza de la compra y, un tercero no debería poder acceder a la información enviada.
- **Autenticación:** permite a cada lado de la comunicación asegurarse de que el otro es quien dice ser.
- **Integridad:** evita que un tercero pueda modificar la información enviada por cualquiera de las partes.
- **No Repudio o Irrefuntabilidad:** permite a cada lado de la comunicación, probar fehacientemente que el otro lado ha participado: el origen no puede negar haberlo enviado y el destino no puede negar haberlo recibido.

- **Flexibilidad:** aceptar todas las posibilidades formas de pagos existentes.
- **Eficiencia:** el costo del servicio no debe ser mayor que el precio del producto o servicio.

8.11.1 DINERO ELECTRÓNICO

Como ya se menciono, si alguna desea verificar la clave pública del emisor. Es decir que una persona que se dedique a autentificar documentos debería poseer cantidad considerable de claves almacenadas.

Este problema se soluciona aplicando un Certificado Digital (CD) emitido y firmado por una Autoridad Certificadora (AC).

El CD es un documento firmado digitalmente por la AC y establece una relación entre una persona y su llave pública.

La idea es que cualquiera que conozca la llave pública de la AC puede autentificar un CD de la misma manera que se autentifica cualquier documento físico. Si se confía en la AC, entonces se puede confiar que la clave publica que figura en el Certificado es de la persona que dice ser.

Luego, si una persona firma un documento y anexa su CD, cualquiera que conozca la clave publica de la AC (una única clave) podrá verificar la autenticidad del documento.

El Estándar internacional para CD mas aceptado y extendido en la actualidad es el denominado X.509.

8.11.1.1 CERTIFICADOS X.509

Este certificado se basa en la Recomendación X.509 de CCITT llamada “The Directory – Autentication Framework”, que data de 1988 y actualmente se encuentra en su versión 3.

Un Certificado es esencialmente una clave pública un identificador, firmados digitalmente por una autoridad de certificación, y su utilidad es demostrar que una clave publica pertenece a un usuario concreto.

El estándar X.509 solo define la sintaxis de los certificados por lo que no esta atado a ningún algoritmo en particular, y completa los siguientes campos:

1. **Versión:** indica si la versión del certificado X.509 es la 1 (defecto), 2 o 3.

2. **Numero de serie:** Es un numero entero asignado por la AC emisora y que identifica unívocamente al certificado dentro del conjunto de certificados emitidos.
3. **Firma:** Identifica al algoritmo utilizado por la AC para firmar el certificado.
4. **Emisor:** El nombre del emisor identifica a la entidad que ha firmado a certificado.
5. **Validez:** Indica el intervalo de tiempo en el que el certificado es valido.
6. **Usuario o Sujeto:** Es un nombre distinguible X.500 que identifica de forma univoca al poseedor del certificado; y la nomenclatura de nombres distinguibles (DN:DistinguisehdNames).
7. **Clave publica del usuario:** Contiene la clave pública del usuario junto con el identificador del algoritmo con el que se ha de utilizar.
8. **Identificadores únicos de emisor y de usuario:** Es una cadena de bits opcional que identifica al emisor o al usuario en el caso de que su DN sea reutilizado con el paso del tiempo.
9. **Campos de extensión:** Permite la adición de nuevos campos a la estructura sin que por ello se tenga que modificar la definición del certificado.

La firma, realizada por la AC emisora, permite que aquellas entidades que deseen realizar comunicaciones con la persona poseedora del certificado, puedan comprobar que la información que este contiene es autentica (suponiendo que confíen en la AC emisora).

Una vez que los certificados han sido firmados, se almacenan en servidores de directorios y/o transmitidos por cualquier medio (seguros o no) para que estén disponibles públicamente.

Los certificados tienen un periodo de vida limitado, el cual esta especificado en el campo Validez, y que suene determinado por la política de la AC emisora. Sin embargo, en algunas ocasiones especiales la seguridad de la clave privada asociada puede verse comprometida, por lo que la utilización de la correspondiente clave publica ha de ser evitada.
En tal caso, la AC emisora puede revocar el certificado para prevenir su uso.

8.11.1.2 SSL

Secure Sockets Layers es un protocolo seguro de Internet diseñado en 1994 por Netscape Communication Corporation y posteriormente adoptado por otros navegadores. Es utilizado para cualquier comunicación donde deba establecerse un canal seguro (al solicitarse clave o número de tarjeta de crédito por ejemplo).

En la pipila TCP/IP, se ubica entre la capa TCP (Trasnporte) y de Aplicación, por lo que es muy flexible ya que puede ser utilizado en cualquier aplicación que utilice TCP/IP (Mail, HTTP, FTP, News, etc.) aunque actualmente solo se implementa sobre HTTP. Para diferenciar las páginas más comunes HTTP de

las protegidas se utiliza la denominación HTTPS conectado mediante el puerto 443.

SSLv3 supera algunas limitaciones de sus versiones anteriores y ofrece esas características:

- **Cifrado de datos:** los datos viajan cifrados mediante algunos de los algoritmos vistos. Para el intercambio de datos entre servidor y cliente se utilizan algoritmos simétricos (DES-TDES, RC4, IDEA) y para la clave de sesión (utilizada para los algoritmos anteriores) cifrado asimétrico (típicamente RSA).
- **Fragmentación de datos:** en el emisor se fragmentan los datos en los bloques para volver a reemplazarlos en el receptor.
- **Comprensión de datos:** se puede aplicar un algoritmo de compresión a los datos.
- **Autentificación de servidores:** el usuario puede verificar la identidad del servidor al que se conecta y al que puede mandar datos confidenciales.
- **Integridad de mensajes:** las modificaciones intencionales o accidentales, de la información en el viaje por el canal inseguro son detectadas.
- **Autentificación del cliente:** permite al servidor conocer la identidad del usuario, con el fin de decidir si este puede acceder a cierta información protegida. Esta autentificación no siempre debe darse.

Al reunir estas características, la comunicación se divide en dos frases:

- **Saludo (HandsHaking):** los interlocutores se identifican mutuamente empleando, habitualmente, certificados X509. Tras el intercambio de claves, los dos escogen una clave de sesión simétrica para el intercambio de datos.
- **Comunicación:** se produce el intercambio de información propiamente dicho, que se codifica mediante las claves de sesión ya establecidas.

De aquí en adelante, durante la sesión segura abierta, SSL proporciona un canal de comunicaciones seguro entre el servidor y el cliente a través del cual se intercambiara cifrada la siguiente información:

- La URL del documento solicitado.
- El contenido del documento solicitado. Los contenidos de cualquier formulario enviado desde el navegador.
- Los contenidos de cualquier formulario enviado desde el navegador.
- Los contenidos de las cabeceras HTTP.

8.11.1.2.1 LIMITACIONES Y PROBLEMAS DE SSL

1. Debido a la limitación de exportación del gobierno de los EEUU sobre los productos criptográficos, las versiones de los navegadores

distribuidas legalmente más allá de sus fronteras operan con nada mas que 40 bits de longitud de clave, frente a los 128 o 256 bits de las versiones fuertes.

2. Claves tan cortas facilitan los ataques de fuerza bruta, dependiendo de los recursos informáticos disponibles. Este serio problema gano notoriedad en los medios de comunicación cuando en 1995 un estudiante francés, Damián Doliguez, fue capaz de descifrar un mensaje cifrado con SSL en pocos días utilizando la red de computadoras de su universidad.

3. SSL solo garantiza la confidencialidad e integridad de los datos de transito, pero nunca antes ni después, Por lo tanto, si se envían datos personales al servidor, SSL solamente asegura que no serán modificados ni espiados mientras viajan desde el navegador hasta el servidor. Lo que el servidor haga con ellos, están mas allá que la competencia de este protocolo.

4. SSL no garantiza la identidad del servidor al que se conecta el usuario. Podría suceder que el servidor seguro contase con un certificado perfectamente valido y que estuviera suplantado la identidad de algún otro servidor seguro bien conocido. Por consiguiente es de extrema importancia que se compruebe siempre el certificado del sitio Web para cerciorarse de que no se están conectado a un Web falsificado.

5. El servidor identifica al navegador incluso aunque este no se autentique mediante certificados. Cuando un usuario se conecta a un servidor, rutinariamente le comunica ciertos datos como su dirección IP, tipo y versión de navegador, sistema operativo, y otros.

6. Actualmente SSL solamente se utiliza para comunicaciones Web seguras, por lo que otros servicios de Internet, como el correo electrónico, no Irán cifrados a pesar de utilizar SSL para el envió de formularios o la recuperación de paginas web. Por esto, se debe usar S/MIME, PGP o algún otro software criptográfico para correo.

7.

8.11.1.2.2 VENTAJAS DE SSL

1. SSL v3.0 goza de gran popularidad y se encuentra ampliamente extendido en Internet, ya que viene soportado por los dos principales navegadores del mercado, Netscape Navigator e Internet Explorer.
2. SSL proporciona un canal de comunicaciones seguro entre los servidores Web y los clientes (los navegadores), pero su uso no se limita a la transmisión de páginas Web. Al encontrarse entre los niveles de transporte y de aplicación, potencialmente; SSL puede servir para securizar otros servicios como FTP, correo, telnet, etc.

3. El usuario no necesita realizar ninguna acción especial para invocar el protocolo SSL, basta con seguir un enlace o abrir una pagina cuya dirección empieza por http://. El navegador se encarga del resto.

8.11.1.3 TLS

Trasnport Layer Security es un protocolo estandarizado por el IETF. Esta basado en SSL v3 (y es totalmente compatible) pero incorpora algunas mejoras y se destaca por no ser de una empresa privada.

8.11.1.4 SET

Secure Electronic Transaction es un protocolo definido por las empresas VISA, Mastercard, Microsoft, IBM, Netscape, Verising, GTE y otras, exclusivamente para realizar comercio electrónico con tarjetas de crédito.

SET es un conjunto de protocolos, normas, y especificaciones de seguridad, que constituyen una forma estándar para la realización de transacciones, reproduciendo en un entorno electrónico el pago con tarjeta de crédito física.

Además de poseer todas las características de SSL, el sistema autentifica los titulares de las tarjetas, los comerciantes y los bancos, garantiza la confidencialidad de la información de pago y asegura que los mensajes no sean manipulados.

La diferencia fundamental entre SSL y SET es que este ultimo establece diferentes entidades (Cliente, Vendedor, Banco) y un protocolo de comunicaciones entre el Vendedor y el banco. Cada una de estas entidades debe certificarse previo realizar cualquier transacción y cada mensaje queda firmado para evitar modificaciones y repudio posteriores.

Esta diferencia puede apreciarse cuando se piensa que SSL solo protege un numero de tarjeta de crédito por ejemplo cuando se envía del cliente al comerciante sin embargo no hace nada para la validación de ese numero, no chequea la autorización, permite que el comerciante lo almacene, etc. SET cubre todas estas debilidades ofreciendo seguridad a las entidades intervinientes.

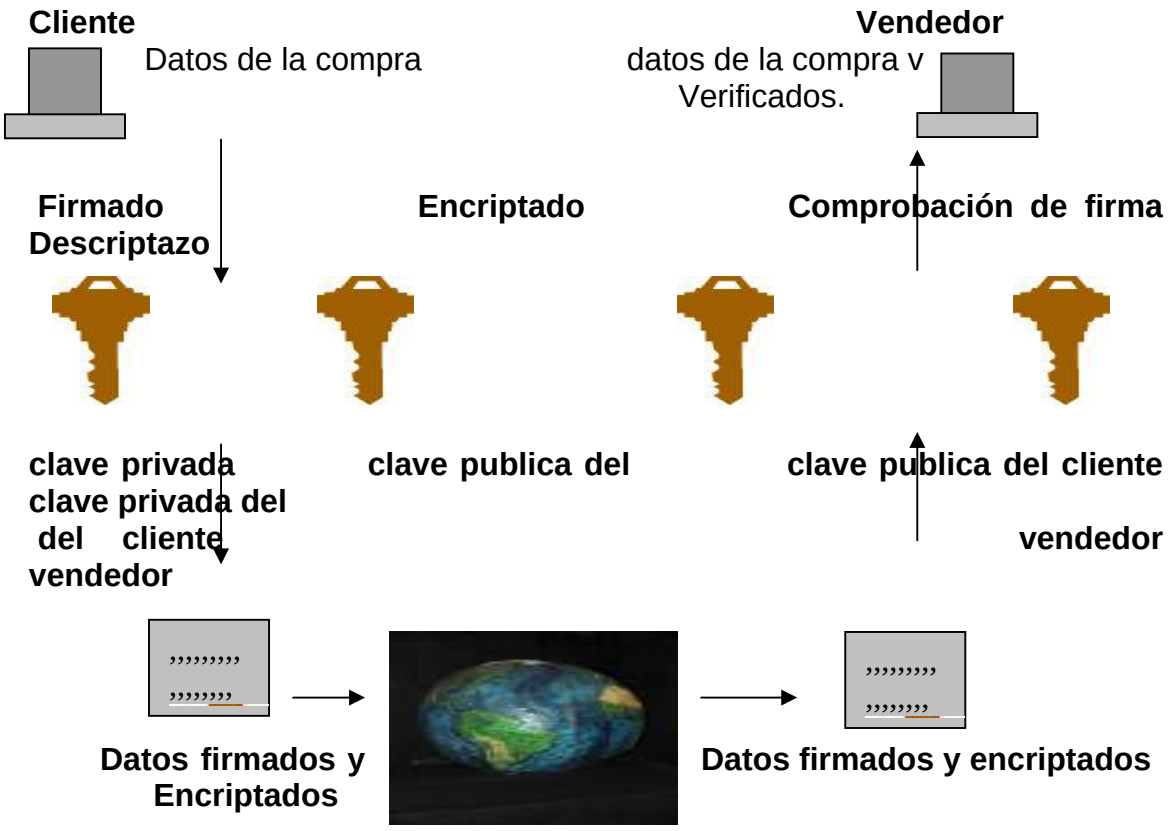
La implantación de protocolo SET aporta una serie de beneficios:

- Autentifica los titulares de las tarjetas de crédito, los comerciantes y los bancos que intervienen en la operación La autentificación asegura que los participantes en la operación comercial sean quienes dicen ser: el consumidor sabe que en que comercio esta comprando y; el comercio esta seguro de que quien esta comprando es realmente el titular de instrumento de pago. La autentificación se realiza a través de certificados digitales que tanto el comerciante como el comprador poseen.

- Garantiza la máxima confidencialidad de la información del pago. Toda la información que viaja por la red, durante el intercambio de identidades y datos, esta protegida contra cualquier intromisión o captura con métodos criptográficos.
- Asegura que los mensajes financieros no sean manipulados dentro del circuito del proceso de pago. La integridad y la autenticidad se basan en la generación de firmas digitales.

La utilización de un documento firmado con clave pública del receptor puede apreciarse en el Grafico.

1. El Cliente Firma el documento de compra, mediante su Clave Privada.
2. El Cliente Encripta los datos, mediante, la Clave Publica del Vendedor.
3. El Vendedor descifra, mediante su Clave Privada, los datos encriptados por el Cliente.
4. El Vendedor compraba la integridad y autenticidad de los datos (firma del cliente), mediante la Clave Publica del mismo.



Proceso Encriptado

SET se utiliza algoritmos de encriptación como SHA-1, DES, Y RSA ya que estos son compatibles con los certificados existentes, aunque en próxima versiones se piensa dar soporte a algoritmos de curvas elípticas.

8.12 OTROS PROTOCOLOS DE SEGURIDAD

8.12.1 SSH

El protocolo Secure SHell fue desarrollado en 1995 por Tatu Ylonen para permitir un longueo seguro en terminales remotas, evitando el viaje de password es claro por redes inseguras; mediante del uso de comunicaciones cifradas. El protocolo SSH se establece en tres niveles:

1. **Nivel de transporte:** en este nivel se procede a la autentificación del servidor, el establecimiento de un canal cifrado (confidencialidad), chequeo de integridad de los mensajes, y un identificador único de sesión. Típicamente esta conexión se realiza mediante TCP/IP.

   En cuanto a los algoritmos empleados:

   a. Para el intercambio de claves: Diffie – Hellman.
   b. Algoritmos de clave publica para encriptación y autentificación del servidor: DSA, Certificado X.509 y Certificados PGP.
   c. Algoritmos de la clave simétrica: 3DES, BlowFish e IDEA.
   d. Algoritmos de integridad: SHA1 y MD5.

Todos estos son utilizados con claves de 128 bits.

2. **Nivel de Autentificación del Usuario:** En este nivel se supone establecida la encriptación e integridad del canal y la autentificación del servidor. Para la autentificación del usuario de SSH ofrece varias posibilidades:

   - Autentificación del usuario basada en claves Publica-Privada: la autentificación del usuario se establece en base a la posesión de la clave privada. El servidor SSH conoce la clave pública del usuario. Este es el modo recomendado por los fabricantes que implementan SSH.
   - Autentificación del usuario basada en passwords. Hay que señalar que el password no viaja encriptado, si no el canal por el que va el password es el que se mantiene encriptado (el nivel de Transporte es un túnel). Es tarea del servidor la validación del password según su base de datos.
   - Autentificación del usuario basada en procedencia del Host, en esta situación hay que proteger las claves privadas del Host por parte del usuario. Es una autentificación parecida a la ofrecida por otros sistemas de longueo por lo que es completamente desaconsejable.

3. **Nivel de Conexión:**Es el protocolo encargado de multiplexar el “túnel encriptado” en varios canales lógicos; de forma de obtener múltiples sesiones para la ejecución de canales remotos.

8.12.2 S/MIME

El protocolo MIME seguro fue propuesto por la empresa RSA y después de su aparición fue propuesto como estándar por la IETF pero por problemas de derechos y restricciones de patentes no pudo ser posible.

S/MIME utiliza técnicas similares a PGP e incorpora certificados X.509. Aunque no cuente con el apoyo necesario para ser considerado un estándar, esta implementado en muchos programas de correo electrónico. Tiene la ventaja sobre PGP, que al utilizar Autoridades de Certificación, es ideal para ser utilizado por empresas y para el comercio electrónico.

8.12.3 SOCKS

En Sus orígenes este protocolo fue aprobado por el IETF como un estándar para la autentificación ante un Firewalls. Actualmente, y combinado con SSL provee las bases para construir VPN altamente seguras.

Socks permite la conexión de equipos situados tras un Firewall. Inicialmente fue pensado para permitir el acceso desde una red interna a servicios disponibles en el exterior, sin embargo puede emplearse en sentido contrario, para el acceso desde el exterior de la organización (protegida con un firewall).

La conexión es valida por el sistema de autentificación y después del servidor Socks actúa de intermediario con la aplicación situada en el servidor destino.

Socks actúa de “envoltura “sobre el protocolo UDP-TCP permitiendo que los equipos protegidos por el firewall puedan conectarse a una red insegura, utilizando su propia dirección y devolviendo los resultados al cliente.

8.12.4 KERBEROS

En 1993 el MIT creas el proyecto Athena y basándose en la mitología griega con su perro de tres cabezas una cola de serpiente vigilando la entrada a Hades (el infierno), nace Cerberos.

Cerberos 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**:el usuario indica el recurso al que desea acceder mediante un cliente verificado.
- **Usuario**:El usuario se ve obligado a verificar su autenticidad cada cierto tiempo.

En estos sistemas se tiene una dificultad esencial: la pass Word viaje en forma permanente por la red estando a merced de cualquier tipo de ataque que se desee realizar.

Kerberos fue creado para mitigar este problema de forma tal que el usuario necesita autorización para comunicarse con el servidor (y esta es confiable) se elimina la necesidad de demostrar el conocimiento de información privada y de que esta viaje a través de la red.

Kerberos provee un servidor de autentificación centralizado, cuya función es autentifcicar a los usuarios frente a servidores y a estos frente a los usuarios. La tecnología Kerberos esta basado en tres objetivos de seguridad (tres cabezas):

- **Autentificación Service (AS):** Autentifica los usuarios y les proporciona un ticket para realizar la comunicación con el servidor de Tickets.
- **Tickets Gratis Service (TGS):** proporciona las credenciales necesarias para la comunicación con el servidor que proporciona los servicios.
- **Autenticador:**es un certificado testigo construido por el cliente o el servidor para probar las identidades y la actualidad de la comunicación, solo puede ser utilizado una vez.

Un servidor KDC (Kerberos Distribution Center) alojado en el AS mantiene una base de datos de sus clientes (usuarios y servicios) y sus respectivas claves simétricas privadas utilizando DES (aunque actualmente se encuentra en desarrollo versiones de hebreos empleando RSA):

- **La clave Secreta del Usuario:** esta clave es conocida únicamente por el usuario por kebreos y tiene la finalidad de autentificar al usuario frente a kebreos. El AS comparte una única clave secreta con cada servidor, las cuales fueron distribuidas físicamente o de otra de forma segura.
- **La clave de Sesión:** clave secreta generada por Kebreos luego de verificar al usuario y expedida al mismo con el objetivo te autentificar el intercambio de un par de usuario que define una sesión. Esta clave tiene un tiempo de vida predeterminado y conocida únicamente por aquellos para los cuales fue generada.

Existen dos tipos de credenciales utilizadas por el modelo:

- **Ticket:** es un certificado testigo expedido a un cliente para solicitar los servicios de un servidor. Este ticket contiene el ID del usuario y su dirección en la red y es encriptado usando la clave secreta

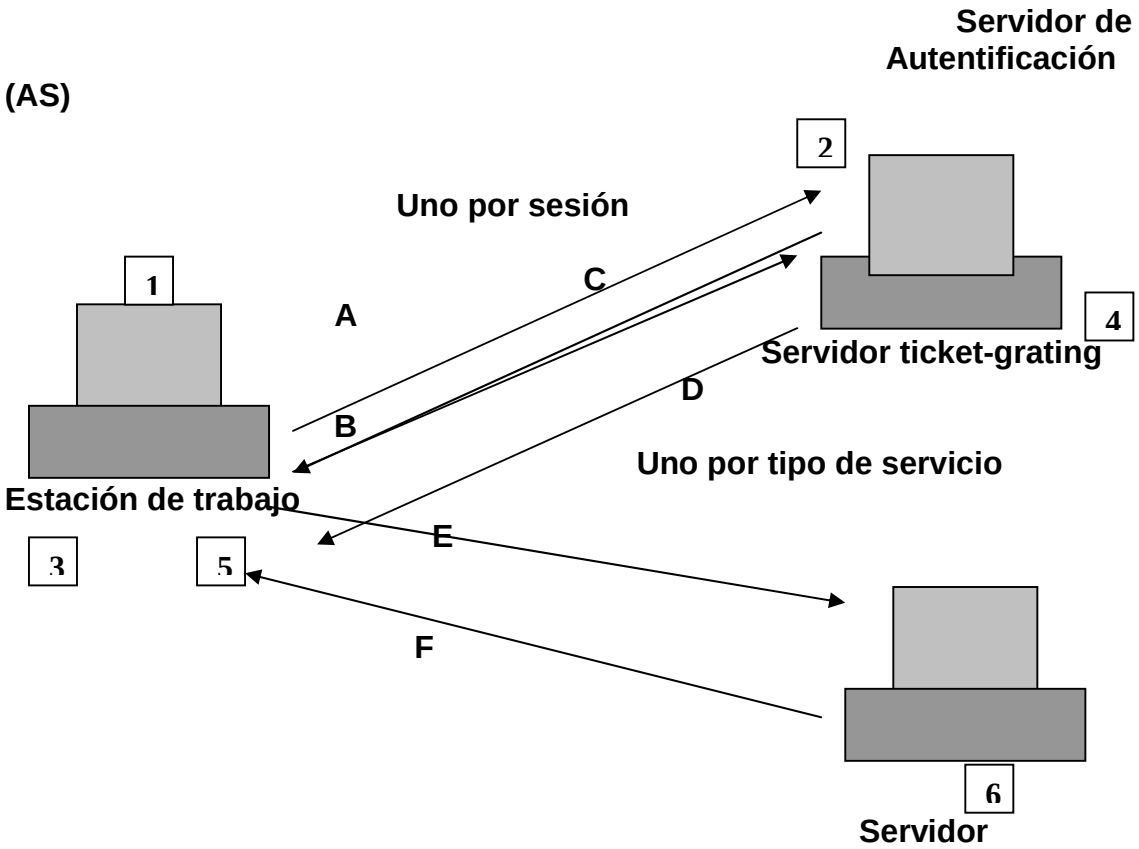
compartida por el AS y el cliente, garantizado que este ha sido autentificado recientemente (el mismo tiene un periodo de validez).

- **Autentificador:** Es un testigo construido por el cliente y enviado al AS para probar su identidad. Solo cuando el servidor desencripta el Ticket, y verifica que el ID del usuario es autentico, otrorga el servicio requerido.

8.12.4.1 RESUMEN DE KERBEROS

En el grafico 8.7 puede apreciarse el funcionamiento de las distintas entidades intervinentes en Kebreos y su función:

a. Solicitud de un ticket de acceso.
b. Ticket + Clave de Sesión.
c. Solicitud de un ticket de acceso de servicio.
d. Ticket + Clave de sesión.
e. Solicitud de Servicio.
f. Autenticador de servicio. .



El proceso de autentificación se divide en dos etapas:

- autentificación de Usuario

1. Un usuario desde una Estación de trabajo requiere un servicio.

2. AS verifica el correcto acceso del usuario a la base de datos, crean un ticket y una clave de sesión. Los resultados son encriptados usándola clave derivada de la password del usuario.

- Autentificación de servicio

1. La estación solicita la password al usuario y la utiliza para desencriptar el mensaje, luego envía al TGS y el autentificador que contiene el nombre del usuario, la dirección de red y el tiempo de vida.
2. El TGS desencripta el ticket y el autenticados, verifica la solicitud y crea un ticket y el Autenticados, verifica la solicitud y crea un ticket para ser enviado al Servidor.
3. La estación de trabajo envía el Ticket y el Autenticador al Servidor.
4. El servidor verifica que el ticket y el Autenticador coincidan, luego permite el servicio.

8.12.4.2 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 este 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 sistema 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 esque casi toda la seguridad reside en el servidor que mantiene la base de dos claves, por lo que este se ve comprometido, toda la red estará amenazada.

Por ultimo, la implementación de Kebreos, actualmente acarrea algunos inconvenientes ya que se debe realizar un proceso de “Kerberizacion” sobre cada programa que se desee utilizar, suponiendo esto un conocimiento y tiempo considerable no siempre disponible. Si bien este conveniente esta siendo subsanado en diversas versiones aun no se cuentan con la estandarización suficiente para extinción masiva.

8.13 VPN – REDES PRIVADAS VIRTUALES

La tecnología de VPN proporciona un medio para usar el canal público del Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privado a través de una red insegura. Es decir que la red pública solo proporciona la infraestructura para enviar los datos.

El objetivo fundamental de una VPN es proteger los datos durante la transmisión a través de la red, permitiendo el uso de redes públicas como si

fueran privadas (virtualmente privadas). Esta protección previene el mal uso, modificación, uso no autorizado e interrupciones de acceso a la información mientras atraviesa los distintos segmentos de la red (o redes).

Una VPN no protege la información mientras esta alojada en el origen, o cuando llega y se aloja en su destino. También puede dejar expuesto los datos durante alguno de los procesos de encriptación en la red (redes internas antes de la encriptación o redes externas después de la encriptación). Una VPN solo protege los aspectos de protección en la comunicación, no protege la información alojada en el disco, en pantallas o impresas.

8.13.1 REQUERIMIENTOS DE UNA VPN

- **Escalabilidad:** esto significa poder decidir cuanta información puede manejarse al mismo tiempo, y efectivamente poder hacerlo.
- **Performance:** este uno de los puntos críticos, la VPN debe estar preparada para manejar una gran cantidad de trafico si esque va a trabajar en un ambiente corporativo.
- **Disponibilidad:** Las soluciones VPN están siendo adoptadas estratégicamente por las organizaciones para proveer accesos externos y eliminar altos costos de conectividad, por lo que su disponibilidad debe estar asegurada en todo momento.
- **Transparencia:** La VPN necesita ser fácil de usar y entender para el usuario, que lo utilizara sin saber como exactamente trabaja, una vez que han sido definidos los “túneles” de protección de la información. Una buena política de distribución debe permitir a la VPN determinar cuando encriptar y cuando enviar texto claro, pidiéndole al usuario únicamente su autentificación para proveer el acceso
- **Fácil de Administrar:** una VPN que se instale en una mediana o gran empresa debe ser fácil de administrar, como todo producto de seguridad, donde la administración y el control centralizado de la solución es clave. El modulo de control debe tener una simple vía de diseñar la política de seguridad, y una fácil distribución de esa política en todos los puntos de la empresa.
- **Interoperatividad:** Una completa VPN debe poder comunicarse con otros productos VPN.
- **Encriptación:** La solución VPN debería ofrecer distintos tipos de encriptación, que se utilizaran de acuerdo a las necesidades de cada segmento de la red. El estándar actúa para la encriptación comercial de DES o 3DES, pero existen otras alternativas como BlowFish o CAST (168 bit).
- **Seguridad:** Uno de los requerimientos más importantes antes de implementar la VPN, es contar en políticas y procedimientos de seguridad definidos. La red virtual solo resuelve un problema específico y su configuración debe estar basada en una política que haya contemplado el análisis del riego que debemos atacar con la instalación de esta herramienta. Esto hace que sea atractivo combinar la flexibilidad de los protocolos VPN con la seguridad por IPSEC.

8.13.2 L2TP

Layer To Tunneling Protocoles un protocolo estándares del IETF que ha sido ampliamente implementado. L2TP encapsula las tramas del protocolo punto a punto (PPP Point to Point Protocol) que van a enviarse a través de redes.

Cuando esta configurado para utilizar IP como su transporte, L2TP, se puede utilizar como protocolo de túnel VPN en Internet. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparece con paquetes IP, aprovecha la seguridad IPSecestandar para obtener una fuerte protección de integridad, reproducción, autenticidad, y privacidad. L2TP se diseño específicamente para conexiones Cliente – Servidor de acceso a redes y para conexiones Gateway a Gateway.

8.13.3 PPTP

Point to Point Tunneling Protocol (antecesor de L2TP) fue diseñado para proporcionar comunicaciones autenticadas y cifradas entre un cliente y un Gateway o entre dos Gateways (sin necesitar una infraestructura de clave publica) utilizando un ID de usuario y una contraseña. Apareció por primera vez en 1996, dos años antes la disponibilidad de IPSec y L2TP y su objetivo era simplicidad en su diseño, la compatibilidad multiprotocolo y la capacidad de cruzar una amplia gama de redes IP.

8.13.4 IPSEC

El IETF ha desarrollado, en principios de 1995, un conjunto de estándares para la seguridad de protocolo IPSec. Este estándar es valido para IPv4 y IPv6, y provee un marco que permite a dos o más partes el uso de distintos algoritmos de encriptación métodos de autentificación en una misma sesión de comunicación. Esta flexibilidad permite incorporar esta tecnología para integrar distintos participantes a bajo costo. Sin necesidad de dispositivos adicionales.

Por primera vez el protocolo IP (capa de red y superiores) se modifica para proporcionar seguridad. IPSec proporciona autenticación de origen, comprobación de integridad y opcionalmente, confidencialidad de contenido.

El equipo emisor protege los datos antes de la transmisión y el equipo receptor los descodifica una vez que los ha recibido. IPSec se basa en claves criptográficas (independientes de los algoritmos utilizados)y se puede utilizar para proteger equipos, sitios, dominios, comunicaciones de aplicaciones, usuario de acceso telefónico. Como parte de un completo plan de seguridad que utiliza controles rigurosos y seguridad periférica, IPSec asegura la protección de los datos que transmita.

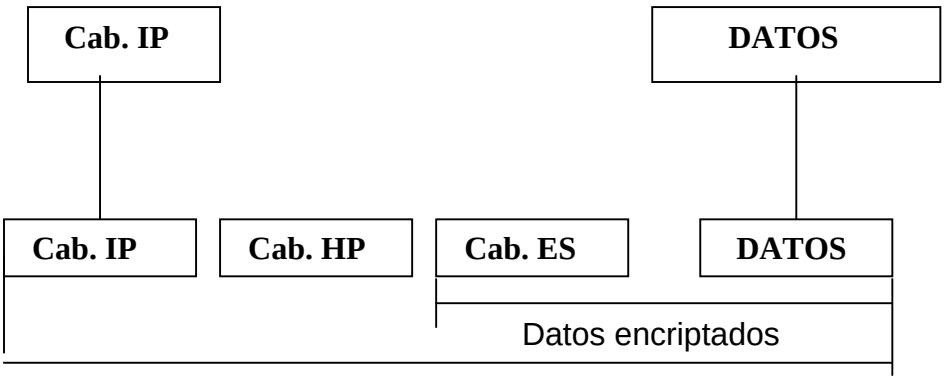
IPSec elimina el requisito de la implementación de seguridad de la aplicación bajando la seguridad al nivel de red. Esto permite a las aplicaciones permanecer independientes de la infraestructura de seguridad subyacente. Los datagramas IP se protegen sin tener en cuenta la aplicación que inicialmente genero tráfico.

En otras palabras, las aplicaciones no son compatibles con IPSec. Las reglas de seguridad las define el administrador sin tener en cuenta que aplicación se ejecuta; IPSec es transparente para las aplicaciones.

IPSec define una familia de protocolos diseñados para ser empleados con los datagramas IP.

- Authentication Header (AH)- Protocolo IP 51 : utilizado para garantizar la integridad de los datos, proporciona protección antirreproduccion y protege la autenticación de Host, AH provee autenticacion, integridad y protección a la replica (una transacción solo debe llevarse a cabo una vez) asegurado partes de la cabecera IP del paquete.
- Encapsulating Security Payload (ESP)-Protocolo IP 50: incluye las características de AH y agrega, opcionalmente, la confidencialidad de los datos asegurando los paquetes IP que siguen a la cabecera.

La aplicación de estos dos protocolos puede verse en el siguiente grafico:



Es importante tener en cuenta que ni AH ni ESP proporcionan los algoritmos criptográficos reales para implementar las características especificadas anteriormente, solo aprovechan los algoritmos croptologicos y de autentificación existentes.

Los servicios proporcionados por IPSec pueden aplicarse en dos modos a los datagramas IP:

- **Modo normal:** empleado para realizar comunicaciones entre equipos finales (punto a punto). En este caso toda la comunicación es encriptada y los equipos intermediarios no pueden desecriptar el contenido de los datagramas. Este método permite la total confidencialidad de la comunicación.
- **Modo Túnel:** los datagramas son enviados en claro hacia equipos intermediarios (Router y Firewall), este encripta los datos y los envía al exterior. En el otro extremo del túnel se realiza el proceso de desencriptado y se envia el data grama en claro hacia el equipo destino.

Esto permite a los equipos de la red intensa visualizar los datos y solo encriptar los que salen al exterior.

8.14 INVERSIÓN

Los costos de las diferentes herramientas de protección se están haciendo accesibles, en general, incluso para las organizaciones más pequeñas. Esto hace que la implementación de mecanismos de seguridad se de prácticamente en todos los niveles: empresas grandes, medianas, chicas, y usuarios finales. Todos pueden acceder a las herramientas que lo necesitan y los costos (la inversión que cada uno debe realizar) va de acuerdo con el tamaño y pontecialidades de la herramienta.

Pero no es solo una cuestión de costos, los constantes cambios de la tecnología hacen que para mantener un nivel parejo de seguridad, se debe actualizar permanentemente las herramientas con las que se cuenta. Como los intrusos mejoras sus armas y metodologías de penetración de forma incesante, el recambio y la versión constantes en los mecanismos de seguridad se convierten en imprescindibles .Y este es un verdadero punto critico.

Según Testers, “Esto es tan importante como el tipo de elementos que se usen”. Sin duda, éstos deben ser las que mejor se adapten al tipo de organización. Pero tan importante como eso es el hecho de conocer exactamente cómo funciona y que se puede hacer con ellos.

CAPITULO 9

9.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las políticas de seguridad informática [1]representan un tipo especial de reglas de negocios documentadas. Su auge ha sido estimulado por la explosión de tecnologías de manejo de información, incluyendo a los teléfonos celulares, los buscapersonas y los computadores. Los que trabajan en el ambiente empresarial deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información generada en el complejo mundo de los negocios. Definitivamente, es imprescindible mantener reglas claras que enmarquen el desarrollo de las actividades en cualquier actividad comercial, los sistemas de información no escapan de este tipo de documentación.

En general, la seguridad informática depende de la articulación eficiente de varios factores, uno de los cuales es ese conjunto de políticas de seguridad informática, las cuales representan el marco normativo para el establecimiento de cualquier solución de seguridad para las organizaciones.

El ofrecer productos o servicios a través de Internet sin tomar en cuenta la seguridad informática no sólo denota negligencia, sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente la reputación de la organización. Para todos nuestros proyectos, las políticas de seguridad informática proporcionan delimitaciones claras que definen un dominio donde se puede encontrar una solución aceptable.

Algunos dicen que la seguridad informática es un problema de personas, mientras que otros dicen que es un problema de tecnología, y podría decirse que ambos tienen razón. Pero antes de que se pueda hacer algo al respecto, la gerencia debe involucrarse en la seguridad informática, asignar suficientes recursos y comunicar claramente a todos los integrantes de su equipo que la seguridad informática realmente sí es importante. Muchas encuestas indican que aquéllos que ejercen la seguridad informática piensan que la llave para alcanzar el éxito de la seguridad informática es la participación de la alta gerencia.

Las políticas son instrucciones gerenciales que trazan una dirección predeterminada o describen la manera de manejar un problema o situación. Las políticas con planteamientos de alto nivel que transmiten a los trabajadores la orientación que necesitan para tomar decisiones presentes y futuras. Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro, y en algunos casos fuera de la organización. Las políticas también pueden considerarse como reglas de negocio. Aunque los documentos de políticas de seguridad informática varían de una organización a otra, un típico documento de este tipo incluye una exposición de motivos, la descripción de las personas a quienes se dirigen las políticas, el historial de las modificaciones efectuadas, unas cuantas definiciones de términos especiales y las instrucciones gerenciales específicas sobre el tratamiento de las políticas.

---

[1] José Torres (jtorres@scientech.com.ve)
Director de Tecnología e Información
Scientech de Venezuela
www.scientech.com.ve

Las políticas son obligatorias y pueden considerarse el equivalente de una ley propia de la organización. Se requiere una autorización especial cuando un empleado desea irse por un camino que no está contemplado en la política. Debido a que el cumplimiento es obligatorio, las políticas utilizan palabras como "no se debe hacer" o "se tiene que hacer", ya que estas estructuras semánticas transmiten certeza e indispensabilidad.

Las políticas representan declaraciones instruccionales de más alto nivel que las normas, aunque ambas son de obligatorio cumplimiento. Las políticas proporcionan las instrucciones generales, mientras que las normas indican requisitos técnicos específicos. Las normas cubren detalles como, por ejemplo, los pasos a seguir para lograr alguna implementación, los conceptos del diseño de los sistemas, las especificaciones de las interfaces del software, los algoritmos y otros. Las normas, por ejemplo, definirían la cantidad de bits de la llave secreta que se requieren en un algoritmo de cifrado. Por otro lado, las políticas simplemente definirían la necesidad de utilizar un proceso de cifrado autorizado cuando se envíe información confidencial a través de redes públicas, tales como Internet.

Las políticas están diseñadas para durar hasta cinco años, mientras que las normas sólo unos pocos. Las normas necesitan modificarse más a menudo debido al cambio incesante en los procedimientos manuales, en las estructuras organizacionales, en los procedimientos empresariales y en la tecnología de sistemas informáticos.

Las políticas generalmente van dirigidas a un público más amplio que las normas. Por ejemplo, una política que exija la utilización de paquetes antivirus se aplicaría a todos los usuarios de computadores personales, pero la norma que requiera el uso de certificados digitales de clave pública sólo podría ser dirigida al personal que realice operaciones a través de Internet.

Las políticas no sólo son distintas, sino que se encuentran a un nivel mucho más alto que los procedimientos. La declaración de una política describe los lineamientos generales que deben seguirse para atender un problema específico, mientras que los procedimientos dictan los pasos operativos específicos o los métodos manuales que los trabajadores deben emplear para lograr un objetivo dado. Por ejemplo, en muchos departamentos de tecnología informática existen procedimientos específicos para realizar los respaldos de los discos duros de los servidores. En este ejemplo, la política podría plantear o describir la necesidad de realizar respaldos, de tener almacenaje fuera de la sede y de salvaguardar los medios de respaldo. La norma podría definir el software a utilizar para hacer los respaldos y cómo configurar dicho software. El procedimiento podría describir cómo usar el software de respaldo, cómo y cuándo sincronizar dichos respaldos y otros detalles.

Por ejemplo, una política puede establecer el uso de aquel software antivirus autorizado por la gerencia de Seguridad Informática y ningún otro. El nombre del proveedor y el del producto pueden cambiar de mes a mes sin necesidad de cambiar la política. Esos detalles podrán aparecer en la norma, pero no en la política.

Algunas personas, particularmente los usuarios y personal del departamento de Tecnología de Información, frecuentemente dicen, "Cuando me digan algo, me ocupo de la Seguridad Informática". Esta actitud no es sorprendente cuando se aprecia en la mayoría

de la gente una falta de conciencia sobre la magnitud de los riesgos que enfrentan en materia de Seguridad Informática, así como que tampoco tienen la disposición de tomarse un tiempo para analizar seriamente dichos riesgos. Aparte de esto, por no contar con la pericia requerida, la mayoría de las personas no puede estimar la necesidad de establecer ciertas medidas de control.

Por ello, las políticas representan la manera más definitiva que la gerencia puede utilizar para demostrar la importancia de la Seguridad Informática y que los trabajadores tienen la obligación de prestar atención a la Seguridad Informática. Las políticas pueden compensar aquellas influencias que, de otra manera, evitarían que se prestara suficiente protección a los recursos informáticos. Un ejemplo frecuente es el de los gerentes de mediano nivel que, en repetidas ocasiones, se niegan a asignar recursos en sus presupuestos a la Seguridad Informática. En este caso, la otra influencia es el bono que frecuentemente reciben como recompensa por mantener los costos bajos. Pero los gerentes de mediano nivel no pueden seguir negando las solicitudes de fondos para la Seguridad Informática si el apoyo es exigido por la alta gerencia.

La gerencia en toda organización tiene que aclarar sus intenciones con respecto a la operación de los computadores y las redes. Si la gerencia dedica tiempo a preparar una política de seguridad informática y su correspondiente documentación, entonces al presentarse el momento que sea necesaria la acción disciplinaria, la demanda o la litigación, la organización no estará sujeta a estos mismos problemas legales. Las políticas además representan para la gerencia una manera relativamente barata y directa de definir el comportamiento correcto.

Uno de los problemas más graves del campo de la seguridad informática tiene que ver con los esfuerzos fragmentados e inconsistentes que al respecto abundan. Demasiadas veces un departamento estará feliz de prestar su colaboración en materia de seguridad informática, mientras que otro de la misma organización se mostrará reacio. Dependiendo de los recursos computacionales que compartan estos departamentos, como la intranet, el departamento reacio crea peligros informáticos para el otro departamento. Esto podría suceder, por ejemplo, si un hacker obtuviera acceso a la intranet a través de un descuidado proceso de autentificación de usuario dentro del departamento reacio, y luego utilizara esta invasión para destruir información del departamento que sí presta atención a su seguridad. Aunque no es ni posible ni deseable que todas las personas de la organización estén familiarizadas con las complejidades de la seguridad informática, sí es importante que todos se suscriban a un nivel mínimo de protección. En términos de alto nivel, las políticas se utilizan para definir dicho nivel mínimo de protección, que algunos llaman línea de base.

Utilizar terceros, contratistas, consultores y personal temporal ya se ha convertido en una necesidad de las organizaciones, que a su vez deben establecer nexos empresariales cercanos con otras organizaciones, incluso cuando éstas representan competencia. La enorme cantidad de entes empresariales existentes ha dificultado el manejo de cosas como el control del acceso, la protección de la propiedad intelectual y todo lo relativo a la seguridad informática. Debido a que tanta gente está involucrada, existe la necesidad apremiante de coordinar consistentemente las actividades de los grupos internos y externos. Y allí es exactamente donde las políticas de seguridad informática pueden prestar gran ayuda. Por ejemplo, una política puede definir cuándo y dónde se requiere la firma de un acuerdo de confidencialidad, e igualmente definir cuándo no.

Supervisar directamente a toda esta gente no es práctico, necesitan aprender a auto-gestionarse, pero necesitan las instrucciones adecuadas para poder hacerlo bien. Así que la herramienta Nº 1 para el manejo de la conducta de la gente en el área de seguridad informática lo constituye el documento de políticas de seguridad informática.

9.2 EVALUACIÓN DE RIESGO DE SEGURIDAD

9.2.1 OBJETIVOS

- Resaltar la necesidad de contar con seguridad informática en las instrucciones para la protección y resguardo de sus activos.
- Promover la realización de análisis de riesgo continuos como elementos para determinar requerimientos e incrementar el nivel de seguridad.

9.2.2 DEFINICIÓN

RIESGO: Es la posibilidad de sufrir algún daño o pérdida.

ACTIVO: datos, infraestructura, hardware, software, personal y su experiencia, información, servicios.

SEGURIDAD INFORMÁTICA: determina qué necesita ser protegido y por qué, de qué necesita protegerse, y cómo protegerlo mientras exista.

ANALISIS DE RIESGO: Proceso mediante el cual se identifican las amenazas y las vulnerabilidades en una organización, se valora su impacto y la probabilidad de que ocurran.

Es un proceso para asegurar que los controles de seguridad de un sistema se adapten según la proporción de sus riesgos.

9.2.3 FACES DEL ANÁLISIS DE RIESGO

FACE 1: Construir perfiles de amenazas basados en activos. Activos críticos, requerimientos de seguridad para los activos críticos, prácticas de seguridad actuales, vulnerabilidades actuales de la organización.

FACE2: Identificar vulnerabilidades de infraestructura. Componentes clave, vulnerabilidades actuales de la tecnología.

FACE3. Desarrollar planes y estrategias de seguridad. Riegos de los activos críticos, medidas de riesgo, estrategias de protección, planes de mitigación de riesgos.

9.2.4 BENEFICIOS

- Costos de seguridad justificados

- Análisis desde el interior (selft-analysis).
- Permite que la seguridad se convierta en parte de la cultura de la organización.
- Apoya la comunicación y facilita la toma de decisiones.
- Certeza económica/financiera.
- Permite determinar las necesidades de acción correctivas.
- Incrementa la consciencia de seguridad en todos los niveles.
- Brinda criterios para el diseño y evaluación de planes de contingencia.
- Mayor productividad del grupo de seguridad.

9.2.5 LIMITANTES

- Es un proceso analítico con un gran número de variables.
- Una sola metodología no es aplicable a todos los ambientes.
- Inversión de tiempo y recursos dedicados a las actividades.
- Las soluciones al problema de seguridad no son instantáneas.

9.3 ESTRATEGIA DE SEGURIDAD

Es de interés para los administradores de recursos de información, los directores de seguridad informática y los administradores, y tiene un valor especial para todos aquellos que intentan establecer directivas de seguridad. La metodología ofrece un acercamiento sistemático a esta importante tarea y, como precaución final, también implica el establecimiento de planes de contingencia en caso de desastre.

Los datos de los sistemas informáticos están en constante peligro por varias causas: errores de los usuarios o ataques intencionados o fortuitos. Pueden producirse accidentes y ciertas personas con intención de atacar el sistema pueden obtener acceso al mismo e interrumpir los servicios, inutilizar los sistemas o alterar, suprimir o robar información.

Los sistemas informáticos pueden necesitar protección en algunos de los siguientes aspectos de la información:

- *Confidencialidad.* El sistema contiene información que requiere protección contra la divulgación no autorizada. Por ejemplo, datos que se van a difundir en un momento determinado (como, información parcial de informes), información personal e información comercial patentada.
- *Integridad.* El sistema contiene información que debe protegerse de modificaciones no autorizadas, imprevistas o accidentales. Por ejemplo, información de censos, indicadores económicos o sistemas de transacciones financieras.
- *Disponibilidad.* El sistema contiene información o proporciona servicios que deben estar disponibles puntualmente para satisfacer requisitos o evitar pérdidas importantes. Por ejemplo, sistemas esenciales de seguridad, protección de la vida y predicción de huracanes.

Los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados. Cada organización debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación. Cada sistema informático, entorno y directiva organizativa es distinta, lo que hace que cada servicio y cada estrategia de seguridad sean únicos. Sin embargo, los fundamentos de una buena seguridad siguen siendo los mismos y este documento se centra en dichos principios.

Aunque una estrategia de seguridad puede ahorrar mucho tiempo a la organización y proporcionar importantes recomendaciones de lo que se debe hacer, la seguridad no es una actividad puntual. Es una parte integrante del ciclo vital de los sistemas. Las actividades que se describen en este documento suelen requerir actualizaciones periódicas o las revisiones correspondientes. Estos cambios se realizan cuando las configuraciones y otras condiciones y circunstancias cambian considerablemente o cuando hay que modificar las leyes y normas organizativas. Éste es un proceso iterativo. Nunca termina y debe revisarse y probarse con periodicidad.

9.3.1 INTRODUCCIÓN A LA COMPILACIÓN DE UNA ESTRATEGIA DE SEGURIDAD

El establecimiento de un conjunto eficaz de directivas y controles de seguridad requiere el uso de un método para determinar los puntos vulnerables que existen en nuestros sistemas y en las directivas y controles de seguridad que los protegen. El estado actual de las directivas de seguridad informática se puede determinar mediante la revisión de la siguiente lista de documentación. La revisión debe tomar nota de las áreas en las que las directivas son deficitarias y examinar los documentos que haya:

- Directiva de seguridad informática física, como los controles de acceso físico.
- Directivas de seguridad de la red (por ejemplo, las referentes al correo electrónico y a Internet).
- Directivas de seguridad de los datos (control de acceso y controles de integridad).
- Planes y pruebas de contingencias y de recuperación de desastres.
- Conocimiento y formación en seguridad informática..
- Directivas de administración y coordinación de la seguridad informática.

Otros documentos que contienen información importante como:

- Contraseñas del BIOS de los equipos.
- Contraseñas para la configuración de enrutadores.
- Documentos de control de acceso.
- Otras contraseñas de administración de dispositivos.

9.3.2 ESTABLECER ESTRATEGIAS PROACTIVAS Y REACTIVAS

En cada método, el plan de seguridad debe incluir una estrategia *proactiva* y otra *reactiva*.

La estrategia *proactiva* o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar la estrategia proactiva.

La estrategia *reactiva* o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible

9.3.3 PRUEBAS

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

Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso. La carencia de laboratorios y equipos de pruebas a causa de restricciones presupuestarias puede imposibilitar la realización de ataques simulados. Para asegurar los fondos necesarios para las pruebas, es importante que los directivos sean conscientes de los riesgos y consecuencias de los ataques, así como de las medidas de seguridad que se pueden adoptar para proteger al sistema, incluidos los procedimientos de las pruebas. Si es posible, se deben probar físicamente y documentar todos los casos de ataque para determinar las mejores directivas y controles de seguridad posibles que se van a implementar.

Determinados ataques, por ejemplo desastres naturales como inundaciones y rayos, no se pueden probar, aunque una simulación servirá de gran ayuda. Por ejemplo, se puede simular un incendio en la sala de servidores en el que todos los servidores hayan resultado dañados y hayan quedado inutilizables. Este caso puede ser útil para probar la respuesta de los administradores y del personal de seguridad, y para determinar el tiempo que se tardará en volver a poner la organización en funcionamiento.

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

9.3.4 EQUIPOS DE RESPUESTA A INCIDENTES

Es aconsejable formar un equipo de respuesta a incidentes. Este equipo debe estar implicado en los trabajos proactivos del profesional de la seguridad. Entre éstos se incluyen:

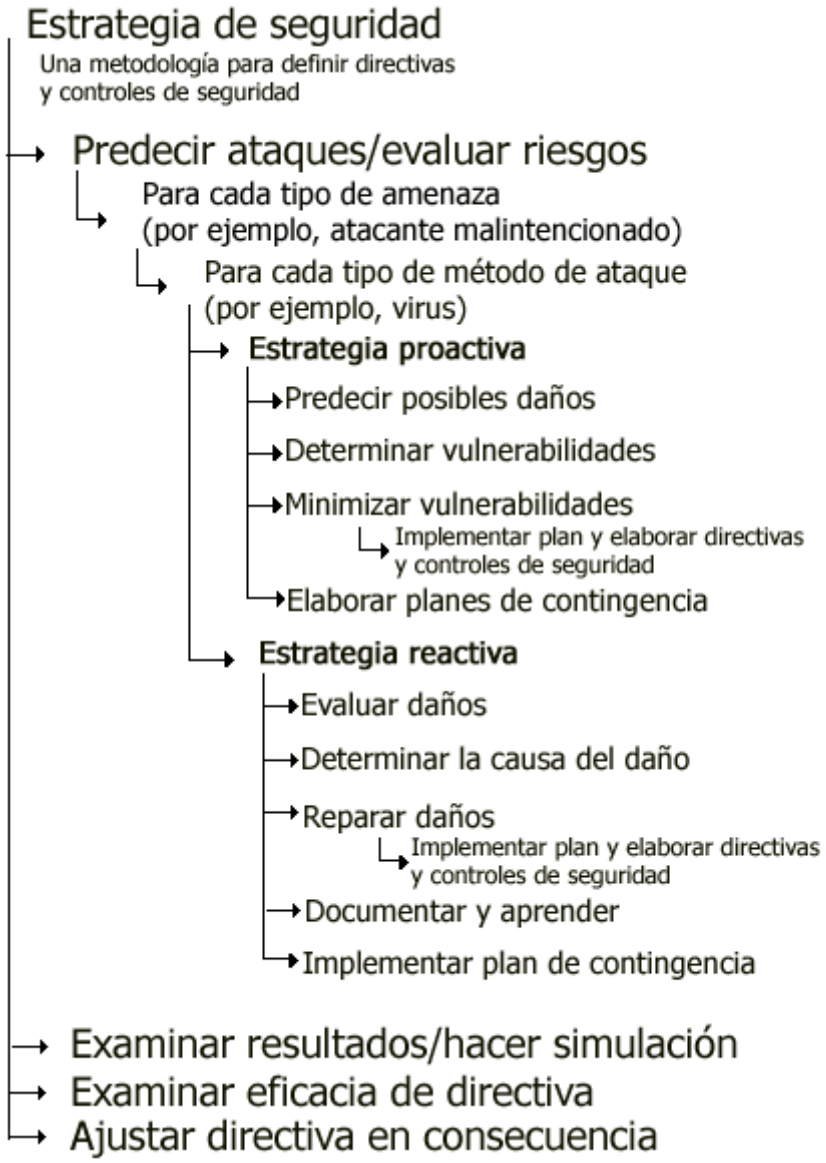
- El desarrollo de instrucciones para controlar incidentes.
- La identificación de las herramientas de software para responder a incidentes y eventos.
- La investigación y desarrollo de otras herramientas de seguridad informática.
- La realización de actividades formativas y de motivación.
- La realización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

Estos trabajos proporcionarán los conocimientos que la organización puede utilizar y la información que hay que distribuir antes y durante los incidentes.

Una vez que el administrador de seguridad y el equipo de respuesta a incidentes han realizado estas funciones proactivas, el administrador debe delegar la responsabilidad del control de incidentes al equipo de respuesta a incidentes. Esto no significa que el administrador no deba seguir implicado o formar parte del equipo, sino que no tenga que estar siempre disponible, necesariamente, y que el equipo debe ser capaz de controlar los incidentes por sí mismo. El equipo será el responsable de responder a incidentes como virus, gusanos o cualquier otro código dañino; invasión; engaños; desastres naturales y ataques del personal interno. El equipo también debe participar en el análisis de cualquier evento inusual que pueda estar implicado en la seguridad de los equipos o de la red.

9.3.5 METODOLOGÍA PARA LA DEFINICIÓN DE ESTRATEGIAS DE SEGURIDAD

La siguiente sección explica una metodología para definir una estrategia de seguridad informática que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los métodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales, y, por consiguiente, se puedan volver a utilizar en distintos casos de ataque. La metodología se basa en los distintos tipos de amenazas, métodos de ataque y puntos vulnerables explicados en "Amenazas a la seguridad". El siguiente diagrama de flujo describe la metodología.



9.3.5.1 **PREDECIR POSIBLES ATAQUES Y ANALIZAR RIESGOS**

La primera fase de la metodología esquematizada en el diagrama de flujo es determinar los ataques que se pueden esperar y las formas de defenderse contra ellos. Es imposible estar preparado contra todos los ataques; por lo tanto, hay que prepararse para los que tiene más probabilidad de sufrir la organización. Siempre es mejor prevenir o aminorar los ataques que reparar el daño que han causado.

Para mitigar los ataques es necesario conocer las distintas amenazas que ponen en peligro los sistemas, las técnicas correspondientes que se pueden utilizar para comprometer los controles de seguridad y los puntos vulnerables que existen en las directivas de seguridad. El conocimiento de estos tres elementos de los ataques ayuda a predecir su aparición e, incluso, su duración o ubicación. La predicción de

los ataques trata de pronosticar su probabilidad, lo que depende del conocimiento de sus distintos aspectos. Los diferentes aspectos de un ataque se pueden mostrar en la siguiente ecuación:

Amenazas+ Motivos + Herramientas y técnicas + Puntos vulnerables = Ataque

9.3.5.2 PARA CADA TIPO DE AMENAZA

Considere todas las amenazas posibles que causan ataques en los sistemas. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales. La siguiente ilustración clasifica las distintas amenazas a los sistemas.

Diagrama 1 Amenazas a sistemas

Amenazas como empleados ignorantes o descuidados, y los desastres naturales no implican motivos u objetivos; por lo tanto, no se utilizan métodos, herramientas o técnicas predeterminadas para iniciar los ataques. Casi todos estos ataques o infiltraciones en la seguridad se generan internamente; raras veces los va a iniciar alguien ajeno a la organización.

Para estos tipos de amenazas, el personal de seguridad necesita implementar estrategias proactivas o reactivas siguiendo las instrucciones del diagrama 1.

9.3.5.2.1 PARA CADA TIPO DE MÉTODO DE ATAQUE

Para iniciar un ataque, se necesita un método, una herramienta o una técnica para explotar los distintos puntos vulnerables de los sistemas, de las directivas de seguridad y de los controles. Los agresores pueden utilizar varios métodos para iniciar el mismo ataque. Por lo tanto, la estrategia defensiva debe personalizarse para cada tipo de método utilizado en cada tipo de amenaza. De nuevo, es importante que los profesionales de la seguridad estén al día en los diferentes métodos, herramientas y técnicas que utilizan los agresores. Puede encontrar una explicación detallada al respecto en "Amenazas a la seguridad". La siguiente es una lista breve de estas técnicas:

- Ataques de denegación de servicio
- Ataques de invasión
- Ingeniería social
- Virus
- Gusanos
- Caballos de Troya
- Modificación de paquetes
- Repetición de paquetes
- Adivinación de contraseñas
- Interceptación de correo electrónico

9.5.3.2.2 ESTRATEGIA PROACTIVA

La estrategia proactiva es un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran. Entre estos pasos se incluye observar cómo podría afectar o dañar el sistema, y los puntos vulnerables que explota (pasos 1 y 2). Los conocimientos adquiridos en estas evaluaciones pueden ayudar a implementar las directivas de seguridad que controlarán o aminorarán los ataques. Éstos son los tres pasos de la estrategia proactiva:

1. Determinar el daño que causará el ataque.
2. Establecer los puntos vulnerables y las debilidades que explotará el ataque.
3. Reducir los puntos vulnerables y las debilidades que se ha determinado en el sistema para ese tipo de ataque específico.

El seguimiento de estos pasos para analizar los distintos tipos de ataques tiene una ventaja adicional: comenzará a emerger un modelo, ya que en los diferentes factores se superponen para diferentes ataques. Este modelo puede ser útil al determinar las áreas de vulnerabilidad que plantean el mayor riesgo para la empresa. También es necesario tomar nota del costo que supone la pérdida de los datos frente al de la implementación de controles de seguridad. La ponderación de los riesgos y los costos forma parte de un análisis de riesgos del sistema que se explica en el documento técnico acerca del diseño de la seguridad.

Las directivas y controles de seguridad no serán, en ningún caso, totalmente eficaces al eliminar los ataques. Éste es el motivo por el que es necesario desarrollar planes de recuperación y de contingencia en caso de que se quebranten los controles de seguridad.

DETERMINAR EL DAÑO POSIBLE QUE PUEDE CAUSAR UN ATAQUE

Los daños posibles pueden oscilar entre pequeños fallos del equipo y la pérdida, catastrófica, de los datos. El daño causado al sistema dependerá del tipo de ataque. Si es posible, utilice un entorno de prueba o de laboratorio para clarificar los daños que provocan los diferentes tipos de ataques. Ello permitirá al personal de seguridad ver el daño físico que causan los ataques experimentales. No todos los ataques causan el mismo daño. Éstos son algunos ejemplos de las pruebas que hay que ejecutar:

- Simular un ataque con virus a través de correo electrónico en el sistema del laboratorio y ver el daño que ha provocado y cómo recuperarse de la situación.
- Utilizar la ingeniería social para adquirir un nombre de usuario y una contraseña de algún empleado ingenuo y observar cómo se comporta.
- Simular lo que ocurriría ante un incendio en la sala de servidores. Mida el tiempo de producción perdido y el tiempo necesario para la recuperación.
- Simular un ataque de virus dañino. Anote el tiempo necesario para recuperar un equipo y multiplique ese tiempo por el número de equipos del sistema infectados para averiguar el tiempo de inactividad y la pérdida de productividad.

También es aconsejable implicar al equipo de respuesta a incidentes ya mencionado, ya que es más probable que un equipo, en lugar de una sola persona, consiga localizar todos los tipos distintos de daños que se han producido.

DETERMINAR LOS PUNTOS VULNERABLES O LAS DEBILIDADES QUE PUEDEN EXPLOTAR LOS ATAQUES

Si se pueden descubrir los puntos vulnerables que explota un ataque específico, se pueden modificar las directivas y los controles de seguridad actuales o implementar otras nuevas para reducir estos puntos vulnerables. La determinación del tipo de ataque, amenaza y método facilita el descubrimiento de los puntos vulnerables existentes. Esto se puede reconocer por medio de una prueba real.

A continuación encontrará una lista de los posibles puntos vulnerables. Éstos representan solamente unos pocos de los muchos que existen e incluyen ejemplos en las áreas de seguridad física, de datos y de red.

Seguridad física:

- ¿Hay bloqueos y procedimientos de entrada para obtener acceso a los servidores?
- ¿Es suficiente el aire acondicionado y se limpian regularmente los filtros? ¿Están protegidos los conductos de aire acondicionado contra robos?
- ¿Hay sistemas de alimentación ininterrumpida y generadores, y se comprueban en los procedimientos de mantenimiento?
- ¿Hay equipo para la extinción de incendios y procedimientos de mantenimiento apropiados para el equipo?
- ¿Hay protección contra el robo de hardware y software? ¿Se guardan los paquetes y licencias de software y las copias de seguridad en lugares seguros?
- ¿Hay procedimientos para almacenar los datos, copias de seguridad y software con licencia en las instalaciones y fuera de ellas?

Seguridad de datos:

- ¿Qué controles de acceso, controles de integridad y procedimientos de copias de seguridad existen para limitar los ataques?
- ¿Hay directivas de privacidad y procedimientos que deban cumplir los usuarios?
- ¿Qué controles de acceso a los datos (autorización, autenticación e implementación) hay?
- ¿Qué responsabilidades tienen los usuarios en la administración de los datos y las aplicaciones?
- ¿Se han definido técnicas de administración de los dispositivos de almacenamiento con acceso directo? ¿Cuál es su efecto en la integridad de los archivos de los usuarios?
- ¿Hay procedimientos para controlar los datos importantes?

Seguridad de la red:

- ¿Qué tipos de controles de acceso (Internet, conexiones de la red de área extensa, etc.) existen?
- ¿Hay procedimientos de autenticación? ¿Qué protocolos de autenticación se utilizan en las redes de área local, redes de área extensa y servidores de acceso telefónico? ¿Quién tiene la responsabilidad de la administración de la seguridad?
- ¿Qué tipo de medios de red, por ejemplo, cables, conmutadores y enrutadores, se utilizan? ¿Qué tipo de seguridad tienen?
- ¿Se ha implementado la seguridad en los servidores de archivos y de impresoras?
- ¿Hace uso la organización del cifrado y la criptografía en Internet, redes privadas virtuales (VPN), sistemas de correo electrónico y acceso remoto?
- ¿Se ajusta la organización a las normas de redes?

Reducir los puntos vulnerables y debilidades que puede explotar un posible ataque

La reducción de los puntos vulnerables y las debilidades del sistema de seguridad que se determinaron en la evaluación anterior es el primer paso para desarrollar directivas y controles de seguridad eficaces. Ésta es la compensación de la estrategia proactiva. Mediante la reducción de los puntos vulnerables, el personal de seguridad puede hacer disminuir tanto la probabilidad de un ataque como su eficacia, si se produce alguno. Tenga cuidado de no implementar controles demasiado estrictos, ya que la disponibilidad de la información se convertiría en un problema. Debe haber un cuidado equilibrio entre los controles de seguridad y el acceso a la información. Los usuarios deben tener la mayor libertad posible para tener acceso a la información.

Elaborar planes de contingencia

Un plan de contingencia es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. El plan se

sigue si el sistema no se puede restaurar a tiempo. Su objetivo final es mantener la disponibilidad, integridad y confidencialidad de los datos (es el proverbial "Plan B").

Debe haber un plan para cada tipo de ataque y tipo de amenaza. Cada plan consta de un conjunto de pasos que se han de emprender en el caso de que un ataque logre pasar las directivas de seguridad. El plan de contingencia debe:

- Determinar quién debe hacer qué, en qué momento y en qué lugar para que la organización siga funcionando.
- Ensayarse periódicamente para mantener al personal informado de los pasos de la contingencia actual.
- Abarcar la restauración de las copias de seguridad.
- Explicar la actualización del software antivirus.
- Abarcar el traspaso de la producción a otra ubicación o sitio.

Los siguientes puntos resaltan las distintas tareas que deben evaluarse para desarrollar un plan de contingencia:

- Evaluar las directivas y controles de seguridad de la organización para utilizar todas las oportunidades destinadas a reducir los puntos vulnerables. La evaluación debe tratar el plan y los procedimientos de emergencia actuales de la organización y su integración en el plan de contingencia.
- Evaluar los procedimientos actuales de respuesta ante emergencias y su efecto en el funcionamiento continuo de la organización.
- Desarrollar respuestas planeadas a ataques, integrarlas en el plan de contingencia y anotar hasta qué punto son adecuadas para limitar el daño y reducir el impacto del ataque en las operaciones de procesamiento.
- Evaluar procedimientos de copia de seguridad, que incluyan la documentación más reciente y pruebas de recuperación de desastres, para evaluar su adecuación e integrarlos en el plan de contingencia.
- Evaluar planes de recuperación de desastres para determinar su adecuación con el fin de proporcionar un entorno operativo temporal o a largo plazo. Los planes de recuperación de desastres deben incluir la prueba de los niveles de seguridad necesarios, con el fin de que el personal de seguridad pueda ver si siguen exigiendo la seguridad en todo el proceso de recuperación o en operaciones temporales y el traspaso de la organización otra vez a su sitio de procesamiento original o a un sitio nuevo.

Redactar un documento detallado que describa los distintos descubrimientos en las tareas anteriores. El documento debe mostrar:

- Todos los casos para probar el plan de contingencia.
- El impacto de las dependencias y de la ayuda planeada de fuera de la organización, y las dificultades que la obtención de los recursos esenciales tendrán en el plan.
- Una lista de prioridades observadas en las operaciones de recuperación y el fundamento para establecerlas.

9.5.3.2.3 ESTRATEGIA REACTIVA

La estrategia reactiva se implementa cuando ha fallado la estrategia proactiva y define los pasos que deben adoptarse después o durante un ataque. Ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar por qué tuvo lugar, a reparar el daño que causó y a implementar un plan de contingencia, si existe. Tanto la estrategia reactiva como la proactiva funcionan conjuntamente para desarrollar directivas y controles de seguridad con el fin de reducir los ataques y el daño que causan.

El equipo de respuesta a incidentes debe incluirse en los pasos adoptados durante o después del ataque para ayudar a evaluarlo, a documentar el evento y a aprender de él.

Evaluar el daño

Determine el daño causado durante el ataque. Esto debe hacerse lo antes posible para que puedan comenzar las operaciones de restauración. Si no se puede evaluar el daño a tiempo, debe implementarse un plan de contingencia para que puedan proseguir las operaciones comerciales y la productividad normales.

Determinar la causa del daño

Para determinar la causa del daño, es necesario saber a qué recursos iba dirigido el ataque y qué puntos vulnerables se explotaron para obtener acceso o perturbar los servicios. Revise los registros del sistema, los registros de auditoría y las pistas de auditoría. Estas revisiones suelen ayudar a descubrir el lugar del sistema en el que se originó el ataque y qué otros recursos resultaron afectados.

Reparar el daño

Es muy importante que el daño se repare lo antes posible para restaurar las operaciones comerciales normales y todos los datos perdidos durante el ataque. Los planes y procedimientos para la recuperación de desastres de la organización (que se tratan en el documento acerca del diseño de la seguridad) deben cubrir la estrategia de restauración. El equipo de respuesta a incidentes también debe poder controlar el proceso de restauración y recuperación, y ayudar en este último.

Documentar y aprender

Es importante documentar el ataque una vez que se ha producido. La documentación debe abarcar todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado (en hardware y software, pérdida de datos o pérdida de productividad), los puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos tomados para reparar el daño. La documentación ayudará a modificar las estrategias proactivas para evitar ataques futuros o mermar los daños.

Implementar un plan de contingencia

Si ya existe algún plan de contingencia, se puede implementar para ahorrar tiempo y mantener el buen funcionamiento de las operaciones comerciales. Si no hay ningún plan de contingencia, desarrolle un plan apropiado basado de la documentación del paso anterior.

9.5.3.2.4 REVISAR EL RESULTADO Y HACER SIMULACIONES

El segundo paso importante en la estrategia de seguridad es revisar los descubrimientos establecidos en el primer paso (predicción del ataque). Tras el ataque o tras defenderse de él, revise su resultado con respecto al sistema. La revisión debe incluir la pérdida de productividad, la pérdida de datos o de hardware, y el tiempo que se tarda en recuperarlos. Documente también el ataque y, si es posible, haga un seguimiento del lugar en el que se originó, qué métodos se utilizaron para iniciarlo y qué puntos vulnerables se explotaron. Para obtener los mejores resultados posibles, realice simulaciones en un entorno de prueba.

9.5.3.2.5 REVISAR LA EFICACIA DE LAS DIRECTIVAS

Si hay directivas para defenderse de un ataque que se ha producido, hay que revisar y comprobar su eficacia. Si no hay directivas, se deben redactar para aminorar o impedir ataques futuros.

9.5.3.2.6 AJUSTAR LA DIRECTIVA EN CONSECUENCIA

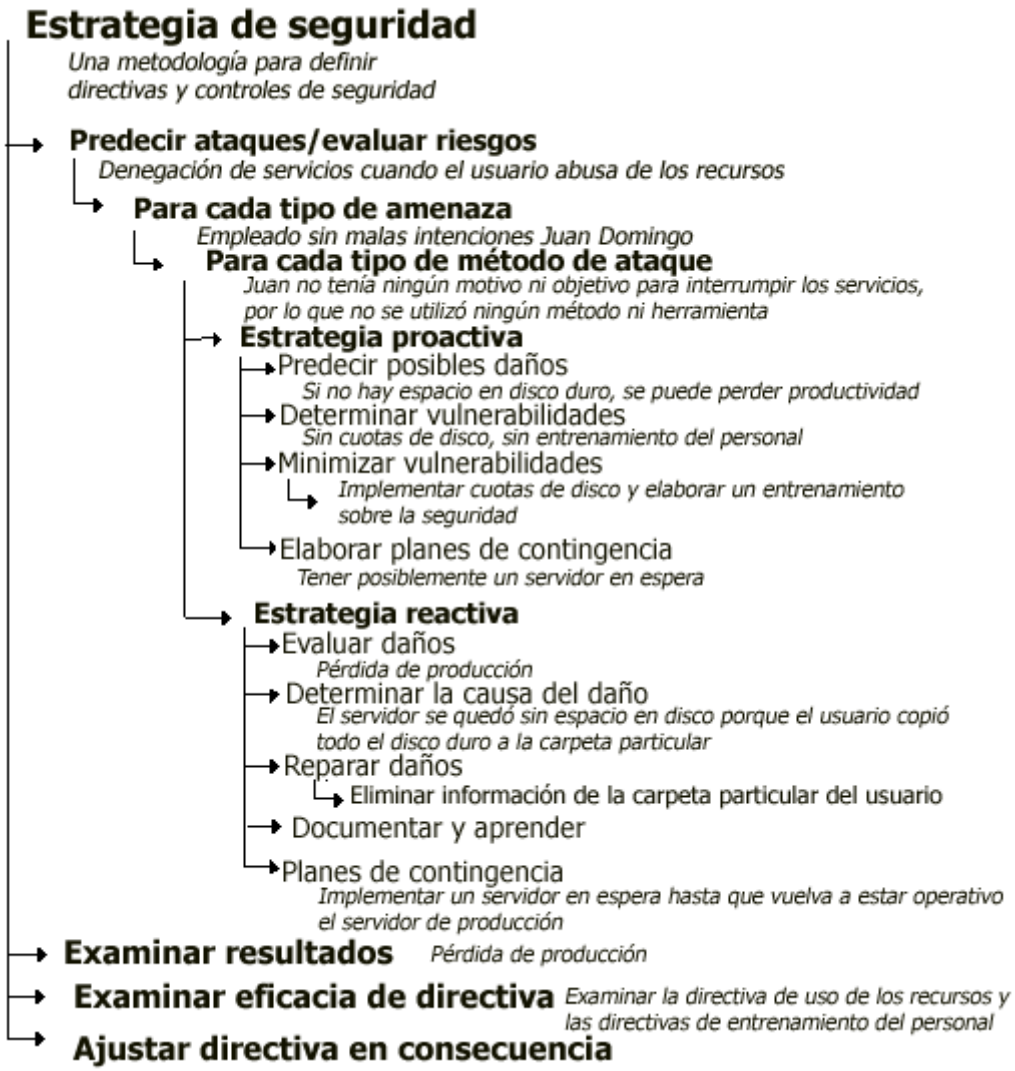
Si la eficacia de la directiva no llega al estándar, hay que ajustarla en consecuencia. Las actualizaciones de las directivas debe realizarlas el personal directivo relevante, los responsables de seguridad, los administradores y el equipo de respuesta a incidentes. Todas las directivas deben seguir las reglas e instrucciones generales de la organización. Por ejemplo, el horario laboral puede ser de 8 a.m. a 6 p.m. Podría existir o crearse una directiva de seguridad que permita a los usuarios conectarse al sistema solamente durante este horario.

9.3.6 EJEMPLOS

Ejemplo 1: amenaza no intencionada

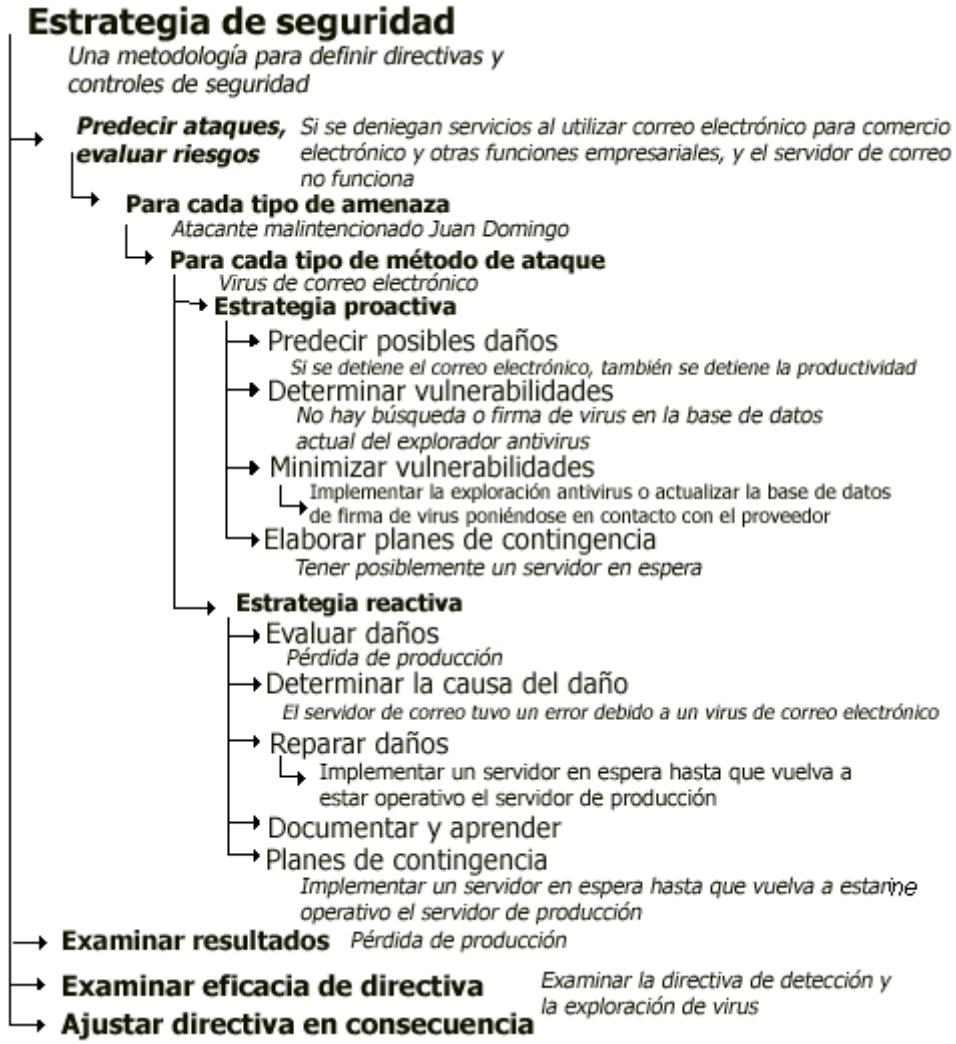
Un empleado, Juan Domingo, no desea perder la información que ha guardado en el disco duro. Desea hacer una copia de seguridad de esta información, así que la copia a su carpeta particular del servidor que resulta ser también el servidor principal de aplicaciones de la organización. No se han definido cuotas de disco para las carpetas particulares de los usuarios que hay en el servidor. El disco duro de Juan tiene 6,4 GB de información y el servidor tiene 6,5 GB de espacio libre. El servidor de aplicaciones deja de responder a las actualizaciones y peticiones porque se ha quedado sin espacio en el disco. El resultado es que se deniega a los usuarios los servicios del servidor de aplicaciones y la productividad se interrumpe. A continuación, se explica la metodología que se debería haber adoptado antes de que

Juan decidiera hacer una copia de seguridad de su disco duro en su carpeta particular.



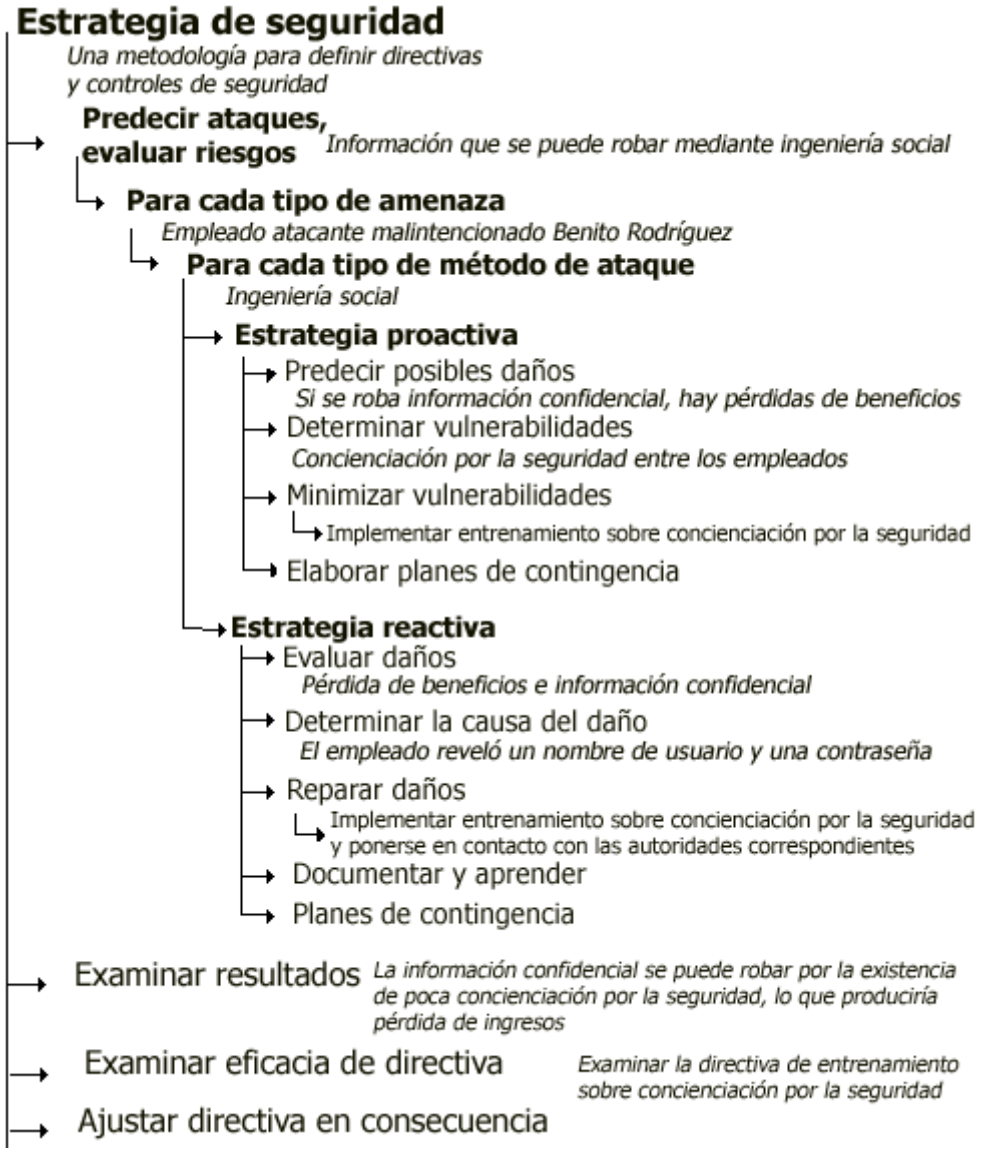
Ejemplo 2: amenaza malintencionada (agresor externo)

Juan es aficionado a crear virus y entrar ilegalmente en sistemas. Cristina crea un virus nuevo que altera los sistemas de correo electrónico de todo el mundo.



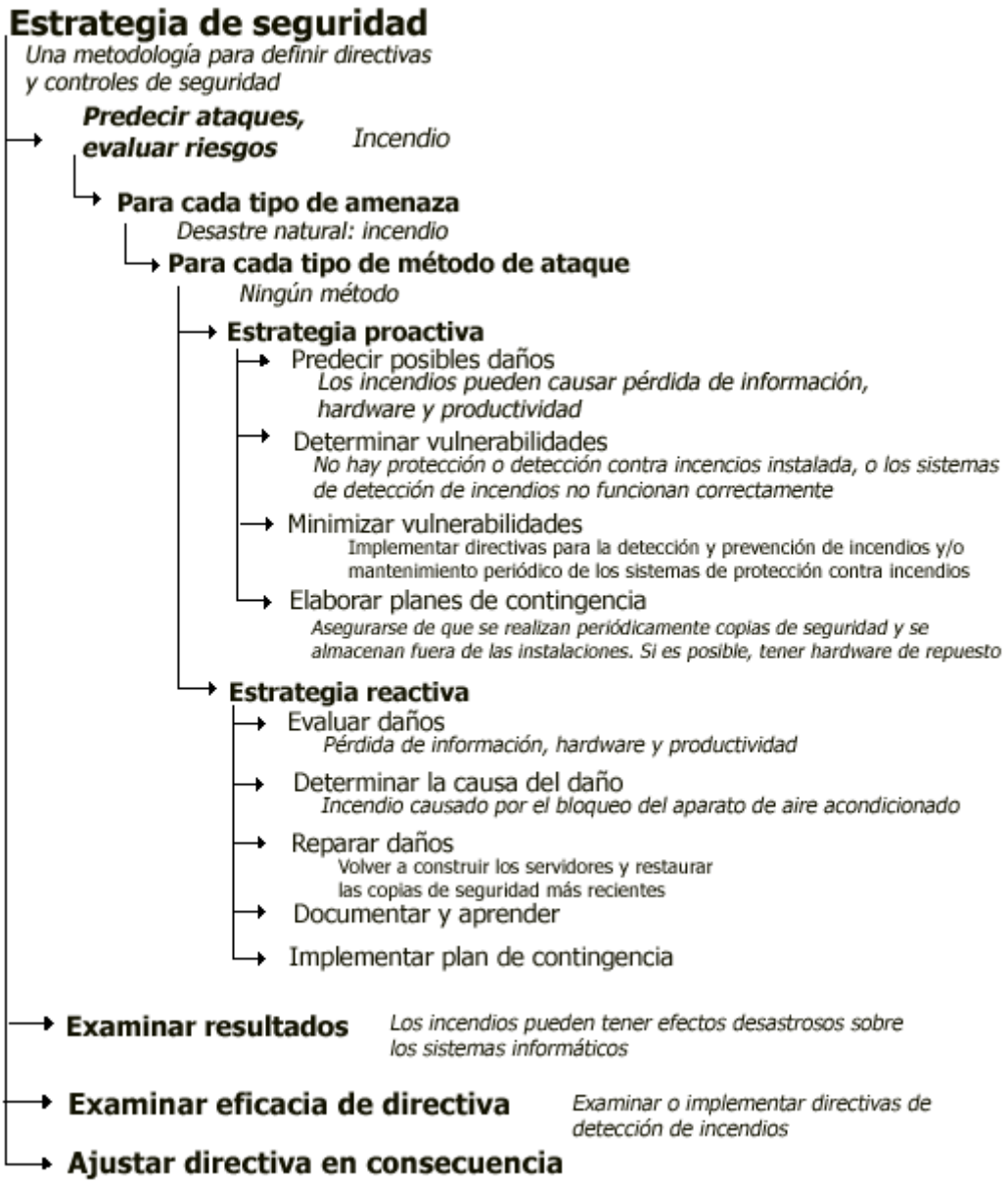
Ejemplo 3: amenaza malintencionada (agresor interno)

Un empleado, Enrique Barrera, trabaja para una empresa que diseña naves espaciales. Una organización competidora se pone en contacto con Enrique para ofrecerle una gran suma de dinero por robar información del diseño de la organización más reciente, el "Flingbot 2000". Enrique no tiene los derechos necesarios para tener acceso a la información. En una conversación telefónica con un empleado que tiene derechos de acceso, simula que es uno de los administradores. Enrique dice al empleado que está realizando un trabajo administrativo habitual y le solicita su nombre de usuario y contraseña para comprobarlos con los registros del servidor. El empleado accede a dar a Enrique dicha información.



Ejemplo 4: amenaza no intencionada (desastre natural)

La organización x no tiene sistemas de detección y protección contra incendios en la sala de servidores. Un administrador de los sistemas de la organización deja un par de manuales encima del aparato de aire acondicionado. Durante la noche el acondicionador de aire se caliente y comienza un incendio que arrasa la sala de servidores y un par de despachos.


Estrategia de seguridad
Una metodología para definir directivas y controles de seguridad
Predecir ataques, evaluar riesgos
Incendio
Para cada tipo de amenaza
Desastre natural: incendio
Para cada tipo de método de ataque
Ningún método
Estrategia proactiva
Predecir posibles daños
Los incendios pueden causar pérdida de información, hardware y productividad
Determinar vulnerabilidades
No hay protección o detección contra incencios instalada, o los sistemas de detección de incendios no funcionan correctamente
Minimizar vulnerabilidades
Implementar directivas para la detección y prevención de incendios y/o mantenimiento periódico de los sistemas de protección contra incendios
Elaborar planes de contingencia
Asegurarse de que se realizan periódicamente copias de seguridad y se almacenan fuera de las instalaciones. Si es posible, tener hardware de repuesto
Estrategia reactiva
Evaluar daños
Pérdida de información, hardware y productividad
Determinar la causa del daño
Incendio causado por el bloqueo del aparato de aire acondicionado
Reparar daños
Volver a construir los servidores y restaurar las copias de seguridad más recientes
Documentar y aprender
Implementar plan de contingencia
Examinar resultados
Los incendios pueden tener efectos desastrosos sobre los sistemas informáticos
Examinar eficacia de directiva
Examinar o implementar directivas de detección de incendios
Ajustar directiva en consecuencia

CONCLUSIONES

En la actualidad la prioridad hacia la seguridad informática es muy alta las firmas más poderosas del planeta tierra gastan millones de dólares, para que sus datos confidenciales no se vean afectados por el ingenio y/o curiosidad de un pirata informático o un fenómeno natural los destruya.

La meta final de este proyecto no solo es buscar una solución al problema que enfrenta la empresa El Hilo Negro SA de CV en cuanto a la seguridad informática de su departamento de sistemas, si no que también sea de utilidad para que otras empresas contemplen la necesidad de tener dentro de su esquema administrativo un área especial de sistemas con personal capacitado con los conocimientos necesarios para planear, organizar, dirigir y controlar todos aquellos sucesos que tengan que ver con uno de los recursos más importante de toda organización, la Información.

Se detallaron muchos temas importantes como el aspecto legal que tiene un delito informático y como puede ser tratado ante una corte de ciertos países, cabe señalar que muchos de esos delitos son cometidos por medio del internet y que son pocos los casos en que se puede dar con el paradero del delincuente informático. En forma general se contemplo la seguridad física en la que no intervienen las herramientas informáticas pero que es necesaria para que no se hagan mal uso de los equipos.

En México nos falta mucho en cuanto a cultura informática, esperemos que en un futuro no muy lejano las empresas mexicanas tomen con más seriedad todo lo que implica un área de sistemas. Para que sus actividades sean mas rápidas al momento de procesarlas y la seguridad informática este ahí presente para crear un ambiente de confianza y seguridad de que la información estará protegida ante cualquier suceso imprevisto que la ponga en riesgo ya sea cometida por humanos o fenómenos en el que no interviene la inteligencia del hombre.