

TESIS LICENCIATURA EN SISTEMAS

UNIVERSIDAD TECNOLÓGICA NACIONAL

SEGURIDAD INFORMÁTICA

**SUS IMPLICANCIAS E
IMPLEMENTACIÓN**

AUTOR: A.S.S. BORGHELLO, CRISTIAN FABIAN

DIRECTOR DE TESIS: ING. GOTTLIEB, BERNARDO

ASESOR CIENTÍFICO: MINGO, GRACIELA

SEPTIEMBRE DE 2001

GRACIAS !!

A mis padres. Por hacer de mi lo que soy

A Evange. To Be

A mis amigos (los que estuvieron y los que están). Por hacer de lo que soy algo mejor

Al ISIPER. Por hacer de mi sueño una realidad

A mis correctoras. Por hacer legible este documento

A los virus informáticos. Por esta Tesis

A los hackers. Porque el Saber y la Libertad son su lema

A los entrevistados. Por soportar mis conocimientos básicos

Copyright © Cristian Fabian Borghello 26 de Junio de 2002

Dirección Nacional del Derecho de Autor exp. 196817

"El punto más débil del capitalismo especulativo es el sistema financiero. Mucho más peligroso que el bug del milenio, sería un virus que modificase todos los descubiertos. Un virus que alterase la titularidad de los valores bursátiles. Un virus que dirigiese los fondos de los fabricantes de armas hacia cuentas de organizaciones humanitarias. Un virus en la ruleta del sistema, la bola truncada que hiciese saltar la banca: la puerta trasera está en Wall Street. Los sicarios del imperio le llamarán criminal, pero al ser humano capaz de crear ese virus, tiene un lugar reservado en los libros de historia"

Carlos Sánchez Almeida. "Revolución", 15 de octubre de 1999

"Internet es peligrosa. Sobre todo para la salud financiera del sistema"

Carlos Sánchez Almeida. "Todo Está en venta", octubre de 2000

CAPÍTULO 1



“La seguridad absoluta tendría un costo infinito.”

Anónimo

INTRODUCCIÓN

“Ser lo que soy, no es nada sin la Seguridad”. Sin duda W. Shakespeare (1564–1616) tenía un concepto más 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 “estudiosos” como una herramienta dentro del ámbito en que se la estudia: relaciones internacionales–nacionales, estudios de riesgo, prevención de crímenes y pérdidas, etc. Muchos sostienen que es una teoría tan amplia, compleja y abstracta como la pobreza, la belleza o el amor; y ni siquiera arriesgan su definición.

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

El motivo del presente es desarrollar un estudio completo del estado actual y futuro posible de Seguridad Informática, que continuamente se pone sobre el tapete y en realidad se conoce muy poco; se suele manejar con el amarillismo de los medios no especializados, dificultando esto su accionar y colocando en tela de juicio el arduo trabajo de los especialistas. También intentaré brindar un completo plan de estrategias y metodologías, que sin bien no brindan la solución total (como muchos prometen), podrá cubrir parte del “agujero” que hoy se presenta al hablar de Seguridad Informática.

La mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesarios para prevenir, principalmente, el daño y/o pérdida de la información que, en última instancia es el Conocimiento con que se cuenta.

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

1.1 EVOLUCIÓN 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 AC) o el Hammurabi (2000 AC). También la 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 más importantes pruebas de seguridad de los antiguos: las pirámides egipcias, el palacio de Sargon, el templo Karnak en el valle del Nilo; el dios egipcio Anubi representado con una llave en su mano, etc.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales: luchando o huyendo (fight or flight), 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 pérdidas eran inaceptables contra las posibles ganancias.

La primera evidencia de una cultura y organización en seguridad “madura” aparece en los documentos de la Res Publica (estado) de Roma Imperial y Republicana.

El próximo paso de la Seguridad fue la especialización. Así nace la Seguridad Externa (aquella que se preocupa por la amenaza de entes externos hacia la organización); y la

¹ Presentación del libro “Seguridad: una Introducción”. Dr. MANUNTA, Giovanni. Consultor y Profesor de Seguridad de Cranfield University. Revista Seguridad Corporativa. <http://www.seguridadcorporativa.org>

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 XVIII, 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 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 Management, 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 felonías, 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 sería 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, está 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 conseguido 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 en manos 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 concepto a los ya conocidos en la antigüedad; los actuales sólo son perfeccionamientos de aquellos: llaves, cerraduras, cajas fuertes, puertas blindadas, trampas, vigilancia, etc.

1.2 DE QUE ESTAMOS HABLANDO

Conceptos como Seguridad son “borrosos” o su definición se maneja con cierto grado de incertidumbre teniendo distinto significado para distintas personas. Esto tiene la peligrosa consecuencia de que la función de seguridad puede ser frecuentemente etiquetada 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 se sabe los problemas nunca se resuelven: la energía del problema no desaparece, sólo se 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 figuras²:

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 delegadas a terceros por el cambio de otro valor, generalmente dinero.
4. El valor puede no ser algo concreto. Por ejemplo se podría querer cuidar el honor, la intimidad, el conocimiento, etc.
5. La situación global 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 arrebatarse 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 incluso inferiores) a la época de las cavernas en el ambiente virtual:

² Presentación del libro “Seguridad: una Introducción”. Dr. MANUNTA, Giovanni. Consultor y Profesor de Seguridad de Cranfield University. Revista Seguridad Corporativa. <http://www.seguridadcorporativa.org>

“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 particular) 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.”⁴.

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.”⁴

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 trabajos perfectamente ubicables sobre un escritorio de oficina. En este proceso de digitalización y miniaturización llamado “downsizing” la característica más 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 LA SEGURIDAD INFORMÁTICA

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

Así, definimos **Dato** como “la unidad mínima con la que compone cierta información. Datum es una palabra latina, que significa “lo que se da”⁵.

La **Información** “es una agregación de datos que tiene un significado específico más allá de cada uno de éstos”⁵, y tendrá un sentido particular según como y quien la procese.

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

⁴ ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. Argentina. 1997. Página 22.

⁵ CALVO, Rafael Fernández. Glosario Básico Inglés-Español para usuarios de Internet. 1994-2000. <http://www.ati.es/novatica/2000/145>

Ejemplo: 1, 9, 8 y 7 son datos; su agregación 1987 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 analfabetismo en un país); y aquella que **debe ser privada**: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). 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 sí misma.
3. Es Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

La **Integridad** de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o 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 sólo 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 adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- **Protección a la Réplica**: mediante 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 se recibieron múltiples peticiones del mismo remitente original.
- **No Repudio**: mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

- **Consistencia:** se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- **Aislamiento:** este aspecto, íntimamente relacionado con la **Confidencialidad**, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- **Auditoria:** es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuando las realiza.

Cabe definir **Amenaza**, en el entorno informático, como cualquier elemento que comprometa al sistema.



Gráfico 1.1 – Amenazas para la Seguridad

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.

- 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.
- La Detección (durante):** mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.
- La Recuperación (después):** mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

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 (por supuesto) pero también para la figura del protector.

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

La Seguridad indicara el índice en que un Sistema Informático 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”⁶, 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 quién 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 Riesgos, las Vulnerabilidades, Amenazas y Contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base de las necesidades de seguridad.

Es importante remarcar que cada unas de estas técnicas parten de la premisa de que **no existe el 100% de seguridad esperado o deseable en estas circunstancias** (por ejemplo: al cruzar la calle ¿estamos 100% seguros que nada nos pasará?).

1.2.2 SISTEMA 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

⁶ HUERTA, Antonio Villalón. “Seguridad en Unix y Redes”. Versión 1.2 Digital – Open Publication License v.10. 2 de Octubre de 2000. <http://www.kriptopolis.com>

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?
 - ¿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 QUIEN DEBEMOS PROTEGERNOS

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

Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita⁷ 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.

⁷ ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. <http://www.cybsec.com>

2. **Clase B:** es el 12% son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo que está usando la víctima, 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”.

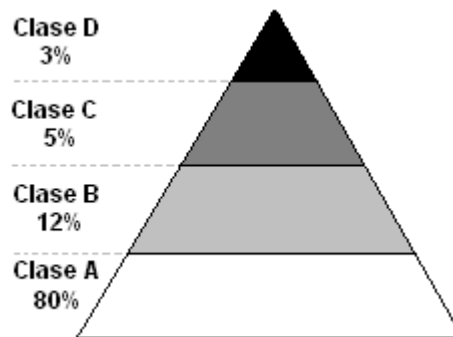


Gráfico 1.2 – Tipos de Intrusos. Fuente: CybSec S.A. <http://www.cybsec.com>

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 todos los sistemas físicos del sistema informático: CPU, cableado, impresoras, CD-ROM, cintas, componentes de comunicación.

El **software** son todos los elementos lógicos que hacen funcional al 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 **fungibles**; que son los aquellos que se gastan o desgastan con el uso continuo: papel, tonner, tinta, cintas magnéticas, disquetes.

De los cuatro, los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, 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, sino que únicamente la “escucha” o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis de tráfico. Generalmente se emplean para:

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

Es posible evitar el éxito, si bien no el ataque, mediante el cifrado de la información y otros mecanismos que se verán 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 distinguirlos entre sí.
- **Destrucción:** es una modificación que inutiliza el objeto.

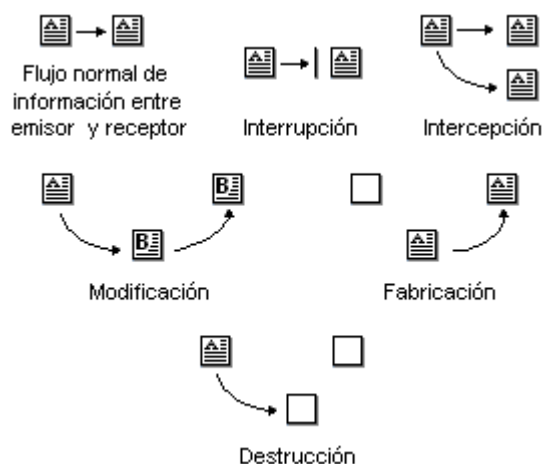


Gráfico 1.3 – Tipos de Ataques Activos. Fuente: HOWARD, John D. Thesis: An Analysis of security on the Internet 1989–1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6–Página 59.

Con demasiada frecuencia se cree que los piratas son lo 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 20 metros bajo tierra en un recinto de hormigón.
- Aislada informáticamente 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 en un sistema informático, su operatividad descende 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.

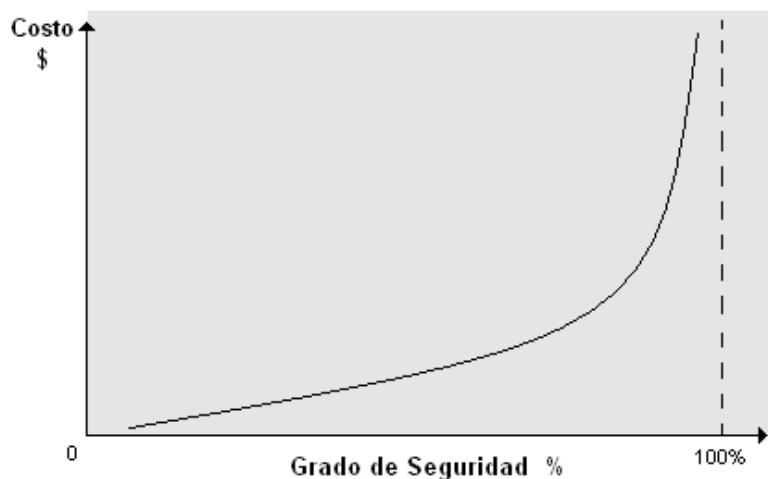


Gráfico 1.4 – Relación Operatividad–Seguridad. Fuente: ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1º Edición. Argentina. 1997. Página 26

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 marzo de 2001 por la consultora Ernst & Young⁸ sobre 273 empresas de distintos sectores de actividad y países.

- El 40% de las empresas estudiadas consideran como un problema grave la seguridad informática.
- El “gasto” en Seguridad Informática oscila entre el 4% y el 10% del gasto total informático.
- El 83% de las empresas reconoce no haber emprendido nunca acciones legales después de un ataque.
- El 72% se muestra reacia a admitir que sus sistemas han sido saboteados.
- El 79% cree que existen mayores probabilidades de sufrir un ataque informático procedente del exterior. Esto, como se verá posteriormente es un error.
- El 66% consideran a la Seguridad y Privacidad de la información el impedimento principal para el crecimiento del e-comerse.
- El 80% manifestó no haber experimentado un ataque por intrusión durante el año anterior; pero sólo el 33% indicó su capacidad para la detección de dichos ataques.
- Sólo el 39% hace uso de software estándar de seguridad y el 20% de este total hace uso avanzado de estas herramientas.

⁸ “Encuesta de Seguridad Informática 2001”. Marzo 2001. <http://www.ey.com>

CAPÍTULO 2



“Un experto es aquel que sabe cada vez más sobre menos cosas, hasta que sabe absolutamente todo sobre nada.. es la persona que evita los errores pequeños mientras sigue su avance inexorable hacia la gran falacia”

Definición de Webber—Corolario de Weinberger (Leyes de Murphy)

SEGURIDAD FÍSICA

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

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

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

Así, la **Seguridad Física** consiste en la “aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial”⁹. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

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 recomendarán pautas de aplicación general y no procedimientos específicos. Para ejemplificar esto: valdrá de poco tener en cuenta aquí, en Entre Ríos, técnicas de seguridad ante terremotos; pero sí será de máxima utilidad en Los Angeles, EE.UU.

Este tipo de seguridad está 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. 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 en un sistema informático, además de que la solución sería extremadamente cara. A veces basta recurrir al sentido común para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

A continuación se analizan los peligros más 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 de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

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

⁹ HUERTA, Antonio Villalón. “Seguridad en Unix y Redes”. Versión 1.2 Digital – Open Publication License v.10 o Later. 2 de Octubre de 2000. <http://www.kriptopolis.com>

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 incendio a los que se encuentra sometido un centro de cómputos son:

1. El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
2. El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
3. Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
4. Debe construirse un “falso piso” instalado sobre el piso real, con materiales incombustibles 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.
7. El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

2.1.1.1 SEGURIDAD DEL EQUIPAMIENTO

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

Para protegerlos se debe tener en cuenta que:

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

2.1.1.2 RECOMENDACIONES

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

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

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

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

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

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

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 pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas 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 más recientes son que las señales muy fuertes de radar pueden interferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor. Ello podría ocurrir sólo 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 que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

2.1.5.1 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 está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. 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 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 se pueden resumir en los siguientes:

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 él) por acción de campos eléctricos, que si sufren los cables metálicos.
2. Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
3. Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

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

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

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

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

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 protección en todo el sistema de cañería al interior y al 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 podrían 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 ERGOMETRÍA

“La **Ergonomía** es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible.”¹⁰

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

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 distribución ineficiente de las teclas, el diseño antinatural del teclado y la ausencia (ahora atenuada por el uso del mouse) de movimientos alternativos al de tecleado, 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 estar diseñado de manera que permita que el usuario se coloque en la posición más natural posible. Como esta posición variará 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 más afectadas por el trabajo con computadoras.

La pantalla es 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:

¹⁰ ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1º Edición. Argentina. 1997. Página 30.

1. Tener especial cuidado al elegir los monitores y placas de vídeo de las computadoras.
2. Usar de pantallas antirreflejo 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 menor esfuerzo muscular dinámico, pero aumenta, al mismo tiempo, la carga estática de acuerdo con las posturas inadecuadas asumidas.

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

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

Los efectos del estrés pueden encuadrarse dentro de varias categorías:

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

2.1.6.4 AMBIENTE LUMINOSO

Se parte de la base que las oficinas mal iluminadas son la principal causa de la pérdida de la productividad en 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 estar comprendida entre el 45% y el 65%. En todos los lugares hay que contar con sistemas que renueven 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 máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina 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, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

2.2.3 SABOTAJE

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

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

2.3 CONTROL DE ACCESOS

El control de acceso no sólo requiere la capacidad de identificación, sino 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 del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

A cualquier personal ajeno a la planta se le solicitará completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de egreso, 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 a los distintos sectores de la empresa.

En este caso la persona se identifica por **algo que posee**, por ejemplo 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 personal recién ingresado.
- Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
- Visitas.

Las personas también pueden acceder mediante **algo que saben** (por ejemplo un número de identificación o una password) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación los datos ingresados se contrastarán 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 DESVENTAJAS DE LA UTILIZACIÓN DE GUARDIAS

La principal desventaja de la aplicación de personal de guardia es que éste puede llegar a ser sobornado por un tercero para lograr el acceso a sectores donde no esté 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 accesos.

2.3.3 UTILIZACIÓN DE DETECTORES DE METALES

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 activará la alarma.

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

2.3.4 UTILIZACIÓN DE SISTEMAS BIOMÉTRICOS

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

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

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

2.3.4.1 LOS BENEFICIOS DE UNA TECNOLOGÍA BIOMÉTRICA

Pueden eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años, el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración. Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, 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 posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más 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 compara la voz (entonación, diptongos, agudeza, etc.).

Este sistema es muy sensible a factores externos como el ruido, el estado de animo y enfermedades de la persona, el envejecimiento, etc.

2.3.4.5 VERIFICACIÓN DE PATRONES OCULARES

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

Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en los mismos enfermedades que en ocasiones se prefiere mantener en secreto.

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 facsímil, 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 es ejecutada.

El equipamiento de colección de firmas es 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 la 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 emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta 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 frecuencia 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, generará una perturbación en dicho campo que accionará 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, sólo 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 golpes o manipulaciones extrañas sobre la superficie controlada.

2.3.7.4 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 estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben 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 alcance para las instalaciones de alarmas locales. Los sensores se conectan a un transmisor que envía la señal de radio a un receptor conectado a la central de control de alarmas encargada de procesar la información recibida.

2.3.7.5 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 estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está 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 enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

2.3.7.6 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 computadora, seguridad, control de

todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía.

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

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 la áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

CAPÍTULO 3



“Miro a mi alrededor veo que la tecnología ha sobrepasado nuestra humanidad, espero que algún día nuestra humanidad sobrepase la tecnología.”

Albert Einstein

SEGURIDAD LÓGICA

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

Así, la Seguridad Física, sólo 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 más importante que se posee es la **información**, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

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

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

Los objetivos que se plantean serán:

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

3.1 CONTROLES DE ACCESO

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

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

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el National Institute for Standards and Technology (NIST)¹¹ 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 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.

¹¹ <http://www.nist.gov>

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.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. 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.
2. Algo que la persona **posee**: por ejemplo una tarjeta magnética.
3. Algo que el individuo **es** y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
4. 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 dos 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 serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados 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 se denomina "single log-in" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería 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 éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a 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 habilitación 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 operativo 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 operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría 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 adecuación 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 períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.
5. Detección de actividades no autorizadas. Además de realizar auditorías o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando 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 puede 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 desvincularán 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 serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, 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 alterarla. 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 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 a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más 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 difícil recordárlas 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 passwords débiles.

Es mi deseo que después de la lectura del presente quede la idea útil de usar passwords seguras ya que aquí radican entre el 90% y 99% de los problemas de seguridad planteados.

- **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 acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún 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 cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

3.1.6.2 ENCRIPTACIÓN

La información encriptada solamente puede ser descryptada 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 Capítulo 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, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

3.1.6.4 LÍMITES SOBRE LA 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 la base de datos y límites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

3.1.6.5 ETIQUETAS DE SEGURIDAD

Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden 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 pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.

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 público 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 usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que 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 más críticas, 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 constituir un compromiso vacío, 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 pérdida 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.
3. Elección de la persona para cada puesto: requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales
4. Entrenamiento inicial y continuo del empleado: cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales para la ejecución de las tareas que se asignen, deben comunicárseles las políticas

organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.

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

Sólo 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 prioritario dentro de la organización.

3.2 NIVELES DE SEGURIDAD INFORMÁTICA

El estándar de niveles de seguridad mas utilizado internacionalmente es el TCSEC Orange Book¹², desarrollado en 1983 de acuerdo a las normas de seguridad en 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 al máximo.

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

Cabe aclarar que cada nivel requiere 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 sólo una división y está 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 autenticación 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 administración del sistema sólo pueden ser realizadas por este “super usuario”; quien tiene gran responsabilidad en la seguridad del

¹² Orange Book. Department Of Defense. Library N° S225, 711. EEUU. 1985. <http://www.doe.gov>

mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran 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 Autenticación: 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 NIVEL C2: 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 accesos e intentos fallidos de acceso a objetos. Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoría es 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 auditoría 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 ultrasecreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo 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, nóminas, 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 la propagación de derecho de accesos a los distintos objetos.

3.2.5 NIVEL B2: PROTECCIÓN ESTRUCTURADA

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior. La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior. Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

3.2.6 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 que recibe las peticiones de acceso de cada usuario y las permite o las deniega 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 terminal 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.

3.2.7 NIVEL A: PROTECCIÓN VERIFICADA

Es el nivel más 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 componentes de 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.

CAPÍTULO 4



“(...) ladrón, trabajaba para otros: ladrones más adinerados, patrones que proveían el exótico software requerido para atravesar los muros brillantes de los sistemas empresariales, abriendo ventanas hacia los ricos campos de la información. Cometió el clásico error, el que había jurado no cometer nunca. Robo a sus jefes.”

Neuromante

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 de delincuencia antes impensables. La cuantía de los perjuicios así ocasionados es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o castigarse.

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

4.1 LA INFORMACIÓN Y EL DELITO

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

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: “no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión “delitos informáticos” esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún.”¹³

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

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburg (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea 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 aquéllas”¹⁴.

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define **Delito Informático** como “cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.”¹⁵

“Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma”¹⁶.

¹³ TÉLLES VALDEZ, Julio. Derecho Informático. 2º Edición. Mc Graw Hill. México. 1996 Pág. 103–104

¹⁴ MOLINER, María. Diccionario de María Moliner Edición Digital. Copyright© 1996 Novel Inc.; Copyright© 1996 María Moliner.

¹⁵ Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.

¹⁶ CARRION, Hugo Daniel. Tesis “Presupuestos para la Punibilidad del Hacking”. Julio 2001. www.delitosinformaticos.com/tesis.htm

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, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.

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

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

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

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

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

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

Ejemplos:

- Falsificación de documentos vía computarizada: tarjetas de créditos, cheques, etc.
 - Variación de la situación contable.
 - Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.
 - Alteración el 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 siguiente características:

1. Sólo una determinada cantidad de personas (con conocimientos técnicos por encima de lo normal) pueden llegar a cometerlos.
2. Son conductas criminales del tipo “cuello blanco”: no de acuerdo al interés protegido (como en los delitos convencionales) sino 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 realizan cuando el sujeto atacado se encuentra trabajando.
4. Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
5. Provocan pérdidas económicas.
6. Ofrecen posibilidades de tiempo y espacio.
7. Son muchos los casos y pocas las denuncias, y todo ello por la falta de regulación y por miedo al descrédito de la organización atacada.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico.
9. Tienden a proliferar, por lo se requiere su urgente regulación legal.

María Luz Lima, por su parte, presenta la siguiente clasificación de “delitos electrónicos”¹⁷:

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 máquina electrónica o su material con objeto de dañarla.

4.2 TIPOS DE DELITOS INFORMÁTICOS

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

- a. Fraudes cometidos mediante manipulación de computadoras

¹⁷ LIMA de la LUZ, María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrua. México. Enero-Julio 1984.

- Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.
- La manipulación de programas: consiste en modificar los programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación.
- Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude del que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.
- Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Se basa en el principio de que 10,66 es igual a 10,65 pasando 0,01 centavos a la cuenta del ladrón n veces.

b. 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.

c. 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 acceso 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 la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, se considera, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

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

- “Fraude en el campo de la informática.

- Falsificación en materia informática.
- Sabotaje informático y daños a datos computarizados o programas informáticos.
- Acceso no autorizado.
- Intercepción sin autorización.
- Reproducción no autorizada de un programa informático protegido.
- Espionaje informático.
- Uso no autorizado de una computadora.
- Tráfico de claves informáticas obtenidas por medio ilícito.
- Distribución de virus o programas delictivos.”¹⁸

4.3 DELINCUENTE Y VICTIMA

4.3.1 SUJETO ACTIVO

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

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

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas 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 en 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 ocasionados a la sociedad. A los sujetos que cometen este tipo de delitos no se considera delincuentes, no se los segrega, no se

¹⁸ CARRION, Hugo Daniel. Tesis “Presupuestos para la Punibilidad del Hacking”. Julio 2001.
www.delitosinformaticos.com/tesis.htm

los desprecia, ni se los desvaloriza; por el contrario, es considerado y se considera a sí mismo “respetable”. Estos tipos de delitos, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

4.3.2 SUJETO PASIVO

Este, **la víctima del delito**, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, etc. que usan sistemas 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 él 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 víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada “cifra negra”.

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

En el mismo sentido, podemos decir que con:

- a. la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras;
- b. alertas a las potenciales víctimas, para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática;
- c. creación de una adecuada legislación que proteja los intereses de las víctimas;
- d. 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.

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

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

- este tipo de programas, ya sean fuente u objeto, serán protegidos como obras literarias de conformidad con el Convenio de Berna, de julio 1971, para la Protección de Obras Literarias y Artísticas;
- las compilaciones de datos posibles de ser legibles serán protegidos como creaciones de carácter intelectual y que;
- para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que, “los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias”¹⁹.

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 22.195 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 1972.

La Convención Relativa a 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 aún 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 de 1980.

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

- a. La ley 111 de Patentes de Invención regula la protección a la propiedad intelectual.

¹⁹ Artículo 61, Convenio de Berna de 1971 para la Protección de Obras Literarias y Artísticas.

- b. La ley Penal 11.723 de “Propiedad Científica, Literaria y Artística”, modificada por el decreto 165/94, ha modificado los Artículos 71, 72, 72 bis, 73 y 74 (ver Anexo I).

Por esta ley, en el país sólo 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 ítem en el concepto de propiedad intelectual, no tiene en cuenta la posibilidad de plagio ya que no hay jurisprudencia que permita establecer qué porcentaje de igualdad en la escritura de dos programas se considera plagio. Las copias ilegales de software también son penalizadas, pero por reglamentaciones comerciales.

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 afectarse una “cosa” y las leyes definen “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 disquete será penalizado: en ese caso, deberá hacerse cargo de los costos de cada elemento pero no de lo que contenían. También se especifica (art. 1109) que el damnificado no podrá reclamar indemnización si hubiera existido negligencia de su parte.

Ahora, cabe preguntarse ¿En Argentina, qué amparo judicial se tiene ante hechos electrónicos ilícitos?. La respuesta es que 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 sancionaron 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 a cometer delito (art. 209), instigación al suicidio (art. 83); hurto (art. 162), estafas (art. 172), además de los de defraudación, falsificación, tráfico de menores, narcotráfico, etc., todas conductas que pueden 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 cuál 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 dicha información tenía.

El problema surge en que los datos almacenados tienen 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 puede valorar los “unos y ceros” almacenados.

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

Hablar de estafa (contemplada en el art. 172 del código penal) no es aplicable a una máquina 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 en 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 coaxil por ejemplo) sin autorización, en forma directa o remota, no constituyen un acto penable por la justicia, aunque sí el daño del mismo.

La mayor dificultad es cuantificar el delito informático. Estos pueden ser muy variados: reducir la capacidad informativa de un sistema con 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 Internet, el problema se vuelve aún más grave ya que se caracteriza por ser algo completamente descentralizado. Desde el punto de vista del usuario esto constituye un beneficio, puesto que no tiene ningún control ni necesita autorización para acceder a los datos. Sin embargo, constituye un problema desde el punto de vista legal. Principalmente porque la leyes penales son aplicables territorialmente y no puede pasar las barreras 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 qué 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. Ardita²⁰ 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 Taiwan y de allí a otra alemana ¿Con las leyes de qué país se juzgará?.

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 así, 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 I) por la que se protege la información confidencial a través de acciones penales y civiles, considerando información confidencial aquella que cumple los siguientes puntos:

²⁰ ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. <http://www.cybsec.com>

- 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 dónde se cometió el delito y quién es el damnificado.

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

La División Computación de la Policía Federal no realiza acciones o investigaciones preventivas (a modo de las organizaciones estadounidenses) actúa en un aspecto pericial cuando el operativo ya está en marcha.

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

Estos problemas afectan mucho a la evolución del campo informático de la argentina, generando malestar en empresas, usuarios finales y toda persona que utilice 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, sino para evitar convertirse en un agente de dispersión que contribuya, por ejemplo, a que un virus informático siga extendiéndose y alcance una computadora en la que, debido a su entorno crítico, produzca un daño realmente grave e irreparable.

Desde la óptica **legal**, y ante la inexistencia de normas que tipifiquen los delitos cometidos a través de la computadora, es necesario y muy importante que la ley contemple accesos ilegales a las redes como a sus medios de transmisión. 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 paradójico (¿gracioso?) es que no existe sanción legal para la persona que destruye información almacenada en un soporte, pero si para la que destruye la misma información impresa sobre papel.

No obstante, existen en el Congreso Nacional diversos proyectos de ley que contemplan esta temática (ver Anexo II).

4.5 LEGISLACIÓN INTERNACIONAL

4.5.1 ALEMANIA

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra 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 en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, 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 de 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 de datos incorrectos o incompletos, mediante 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 sino 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 automática a través de la confección del programa, por la introducción, cancelación o alteración 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 en sancionar una Ley contra Delitos Informáticos. La ley 19223 publicada 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 encuadrarse 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 en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

Dar a conocer la información almacenada en 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 castigará 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 extrema: secretos de alta seguridad, los secretos estatales y aquella información que dañe seriamente la seguridad estatal y sus intereses. Se consideran actividades ilegales la infiltración de documentos relacionados con el Estado, la defensa, las tecnologías de punta, o la difusión de virus informático.

El Tribunal ha hecho especial énfasis al apartado 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 quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa.

Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) aprobada el 15 de diciembre de 1999, la cual reemplaza 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, agravándolas cuando existe una intención dolosa 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 ESTADO 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 datos de un banco de Mineapolis. 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 más 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 blanco 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 entrenamiento para sus agentes acerca de 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, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica, anticipándose un año al dictado de la Computer Fraud y Abuse Act de 1986.

Este se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en casos en los 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 contaminant) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino 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 en la cantidad de casos de 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 Mitnick y los de “ShadowHawk” Herbert Zinn hijo (ver Anexo II).

El FCIC (Federal Computers Investigation Committee), 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 el 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 él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos 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 informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

4.5.8 HOLANDA

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

El mero hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si se usó esa 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 máquina 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 interés público es legal.

El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años, aunque el máximo está reservado para quienes causaron la

muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos 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 “escapó”, la pena no superará el mes.

El usar el servicio telefónico mediante un truco técnico (Phreaking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres años de prisión. La venta de elementos que permitan el Phreaking 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 está 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 Misuse 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: hackear (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 un backdoor), la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del 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 CONCLUSIÓN

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

Desde la Criminología debemos señalar que el anonimato, sumado a la inexistencia de una norma que tipifique los delitos señalados, son un factor criminógeno que favorece la

multiplicación de autores que utilicen los medios electrónicos para cometer delitos a sabiendas que no serán alcanzados por la ley.

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

“Al final, la gente se dará cuenta de que no tiene ningún sentido escribir leyes específicas para la tecnología. El fraude es el fraude, se realice mediante el correo postal, el teléfono o Internet. Un delito no es más o menos delito si se utilizó criptografía (...). Y el chantaje no es mejor o peor si se utilizaron virus informáticos o fotos comprometedoras, a la antigua usanza. Las buenas leyes son escritas para ser independientes de la tecnología. En un mundo donde la tecnología avanza mucho más deprisa que las sesiones del Congreso, eso es lo único que puede funcionar hoy en día. Mejores y más rápidos mecanismos de legislación, juicios y sentencias...quizás algún día.”²¹.

²¹ SCHNEIER, Bruce. *Secrets & Lies*. Página 28-29.

CAPÍTULO 5



“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Art. 12 Declaración Universal de Derechos Humanos, 1948

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 primeros albores del hacking siempre se ha mantenido una extraña relación entre estos particulares personajes, lo legal, lo ético y lo moral, siendo estas característica, lo

que intentan resaltar para esclarecer la diferencia entre cada uno de los clanes existentes en la ReD (como se la llama comúnmente en la jerga).

En el presente sólo se tratará de exponer el perfil de la persona encargada de una de las principales, (publicitariamente), si bien no la mayor amenaza que asechan nuestro sistema informático; para luego sí entrar en las formas de ataques propiamente dichos.

5.1 PATAS DE PALO Y PARCHES

5.1.1 CARTA DE PRESENTACIÓN²²

"Hola, soy Cybor. Probablemente no me conozcan. Tampoco pretendo salir en la prensa. Eso no me importa, sin embargo si hay otras cosas que me interesan mas que mi identidad. Por ejemplo, me interesan las aperturas de sistemas cifrados. Pero eso es algo que nadie te enseña. Eso tienes que aprenderlo por ti mismo. También me interesa que todos sepáis quienes somos y que no estamos solos en este peculiar mundo. Me interesa que sepan que no todos los Hackers somos iguales. También me interesa saber que la palabra Hacker tiene un significado muy curioso. En un artículo reciente se publicó que se nos conocían como piratas informáticos; es probable, pero creo que están tremendamente equivocados. Quiero reivindicar mi posición. Pero lo cierto es que cada vez que hablan de nosotros es para decir que hemos reventado el ordenador de tal multinacional con grandes perdidas o que hemos robado cierta información. Estas cosas suceden, y particularmente tengo que decir que estas cosas están al alcance de otros personajes más peligrosos que nosotros. En nuestro mundo habitan los Crackers y los Phreakers... para la mayoría todos somos iguales y todos somos piratas informáticos. Pero quiero ir por pasos. ¿Que te parece saber de donde procede la palabra Hacker?.

En el origen de esta palabra esta el término Hack –algo así como golpear con un hacha en inglés– que se usaba como forma familiar para describir como los técnicos telefónicos arreglaban las cajas defectuosas, asestándoles un golpe seco... Quien hacia esto era un Hacker. Otra historia relata como los primeros ordenadores grandes y defectuosos, se fallaban continuamente. Los que las manejaban se devanaban los sesos creando rutas para aumentar la velocidad y cosas parecidas. Estas cosas se denominaban Hacks y a los que lo hacían se les llamaban Hackers. Otra denominación se le hacia a aquel experto en cualquier campo que disfrutaba modificando el orden de funcionamiento del aparato. De esta forma siempre superaba las limitaciones y esto le producía una alta satisfacción. A estas personas también se les llamaban Hackers.

Pero pronto surgieron otros acrónimos como Crackers. Fue inventado por los propios Hackers para diferenciar a aquel que fisgaba en un ordenador con aquel que creaba un virus dañino o copiaba un software. Así, frente a un ordenador ajeno un Hacker y un Cracker no son la misma cosa. Por otro lado en algunas ocasiones un Hacker es muy útil porque siempre detecta un agujero en cualquier programa nuevo... El Cracker aprovecharía este error para entrar en el programa y copiarlo.

Aparte del Cracking existen otras formas de vandalismo tecnológico. Así, el Phreaking, por ejemplo es la manipulación de las redes telefónicas para no pagar las llamadas. El Carding se refiere al uso ilegal de las tarjetas de crédito. Y el Trashing consiste en rastrear la basura o residuos de los sistemas informáticos en busca de información como contraseñas.

Pero, volviendo a los Hackers. ¿Cómo son?. ¿Qué aspecto tienen?. Cuando alguien oye mencionar la palabra Hacker rápidamente se le viene a la cabeza un adolescente ojoso, con los ojos inyectados en sangre que ha pasado las últimas 24 horas delante del ordenador. Esta imagen esta estereotipada. No es así. Un Hacker puede ser cualquier estudiante de informática o electrónica, que sale con los amigos y que tiene novia. Un Hacker es una persona normal como tu. Los Hackers son casi siempre gente joven. Quizás somos los que más nos interesamos por la tecnología. Un Hacker normalmente despierta el gusanillo a temprana edad. Y no se hace de la noche a la mañana. Cuando logra serlo después de realizar un Hack, se busca un apodo y no da la cara por cuestión de seguridad... Normalmente al final de todo somos contratados por empresas importantes para ayudarles en su trabajo. Y otra cosa que hacemos es contar como funciona la tecnología que se nos oculta. Este método se llama enseñar y creo que no es nada malo. De modo que si un Hacker escribe un libro es porque tiene algo que enseñar y nada más... Y sobre todo quiero que quede buena constancia de lo que somos.

Cybor, Bangor Diciembre del 96 Maine"

²² HERNÁNDEZ, Claudio. Los Clanes de la Red. Publicación Virtual – Revisión 1. España 1999.

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 llama piratas y delincuentes. Ellos reivindican su situación e intentan aclarar las diferencias entre los distintos clanes del Underground asegurando 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 sea 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 acción 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...”²³.

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 “jergon”²⁴ (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 estos técnicos eran “Hackers” y se dedicaban a “hackear” 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 acné 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 hacker al igual que un chico curioso; y hace que cada uno de nosotros sea un pirata al fotocopiar un libro o copiar el último procesador de palabras del mercado.

En el MIT (Massachusetts Institute of 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 (Tech Model Railroad Club) tenía instalada en el

²³ STERLING, Bruce. La Caza de Hackers. Freeware Literario – Traducción de la versión en Original en Ingles por el grupo kriptopolis.com. España. 1999. <http://www.kriptopolis.com>

²⁴ Jergon File de Eric Raymond: <http://murrow.journalism.wisc.edu/jargon/jargon.html>

Edificio 20 del Instituto, y se quedó inmediatamente prendado de la parte técnica de la instalación.

En el TMRC existían dos facciones 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, hacía 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 en las instalaciones, y Samson obtuvo la suya en un fin de semana.

Los miembros del Subcomité de Señales y Energía no se limitaban a trabajar en las instalaciones del TMRC, sino que no era extraño encontrarlos a altas horas de la madrugada recorriendo edificios y túneles de servicio intentando averiguar cómo 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. Samson y otros miembros del TMRC estaban en él (...).

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

El TX-0 no usaba tarjetas sino 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 sentar en la consola del TX-0 e intentar corregir el problema directamente usando una serie de interruptores y controles.

Dado que sólo se disponía un equivalente a 9 KB de memoria, era fundamental optimizar al máximo los programas que se hacían, por lo que una de las obsesiones fundamentales de los que lo usaban y se consideraban 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 llamaba “hacks” y de ahí es de dónde viene el término “Hacker”, denominación que uno recibía de sus compañeros (...).

De esta historia podemos obtener el perfil principal:

- Un hacker es a todas luces, alguien con profundos conocimientos sobre la tecnología.
- Tiene 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 estudiado, 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 del orden y por multinacionales que desean contratarlos.

La policía compara su incursión en una computadora ajena con la de un ladrón en un domicilio privado; pero para ellos la definición válida 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 al decir: "... si un Hacker entra en un sistema, sin romper puertas y sin modificar los contenidos no se puede penalizar su actuación" y va más allá al afirmar: "...que tampoco sería delito hacerse con contraseñas, siempre y cuando se demuestre que éstas no han sido utilizadas... pero 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..."²⁵.

5.1.2 LA ACTITUD DEL HACKER

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

Se deberá aprender a puntuarse, principalmente, en función de lo que los otros hackers piensan acerca de las habilidades obtenidas (éste es el motivo por el cual no se puede ser un hacker de verdad hasta que otros hackers lo denominen así de manera consistente). Este hecho está 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 fuerte) que impide que se admita al ego o la validación externa como elementos involucrados en la propia motivación.

El status 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, sino 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 de largo alcance, y los donan, de tal manera que cualquiera pueda utilizarlos (free).
2. Ayudar a probar y depurar software libre. Son reconocidas aquellas personas que depuran los errores del software libre. Es considerado un buen Beta-Tester aquel

²⁵ Extraído de <http://www.kriptopolis.com>

que sabe cómo describir claramente los síntomas, que puede localizar correctamente los problemas, que tolera los errores en una entrega apurada, y que está dispuesto a aplicar unas cuantas rutinas sencillas de diagnóstico.

3. Recolectar y filtrar información útil e interesante y construir páginas Web o documentos como FAQs y ponerlos a disposición de los demás.
4. Ayudar a mantener en funcionamiento la infraestructura. La cultura hacker funciona gracias al trabajo voluntario. Los administradores de listas de correo, moderadores de foros 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 “divertidos”. 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 tribales y voceros. La búsqueda visible de esa clase de fama es peligrosa, por lo que la modestia es siempre recomendada.

5.1.3 DEFINICIÓN DE HACKER

Un **Hacker** es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información (Free Information), 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 obtienen, 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 Cracker²⁶.

Pero entonces veamos que **sí** es un **Hacker**²⁷:

1. Un verdadero Hacker es curioso y paciente. Si no fuera así terminarían por hartarse en el intento de entrar en el mismo sistema una y otra vez, abandonando el objetivo.
2. 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

²⁶ Crack (en inglés) Grieta. La traducción del término Cracker al español es “el que produce una grieta”

²⁷ Definición extraída y traducida del Jargon File de Eric Raymond.
<http://murrow.journalism.wisc.edu/jargon/jargon.html>

conocen y que les aburre. ¿Porqué destruir algo y perderse el placer de decir a los demás que hemos estado en un lugar donde ellos no han estado?.

3. Un Hacker es inconformista, ¿porqué pagar por una conexión que actualmente cuesta mucho dinero, y además es limitada? ¿Porqué pagar por una información que solo van a utilizar una vez?.
4. Un Hacker es discreto, es decir que cuando entra en un sistema es para su propia satisfacción, no van por ahí cantándolo a los cuatro vientos. La mayoría de los casos de “Hackers” escuchados son en realidad “Fantasming”. Esto quiere decir, que si un amigo se entera que se ha entrado en cierto sistema; “el ruido de los canales de comunicación” hará que se termine sabiendo que se ha entrado en un sistema cinco veces mayor, que había destruido miles de ficheros y que había inutilizado el sistema.
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 sólo lo imprescindible.
6. Un Hacker programa de forma entusiasta (incluso obsesiva), rápido y bien.
7. Un Hacker es experto en un programa en particular, o realiza trabajos frecuentemente usando cierto programa. Por ejemplo “un Hacker 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 del reto intelectual de superar o 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 término 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 tecnología. En el peor, los Hackers pueden ser traviesos perversos o exploradores curiosos. 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”²⁸.

En el presente se usará la palabra Intruso para definir a las personas que ingresan a un sistema sin autorización y preservará la palabra Hacker; evitando producir falsos conceptos que contribuyan a la confusión aportada por el amarillismo de la prensa, la mitología y la mitomanía de algunas personas.

²⁸ Rich Crash Lewis, Hacker Test, 1992. Texto extraído y traducido de Electronic Frontier of Compuserve. <http://www2.vo.lu/homepages/phahn/humor/hacker30.txt>

5.1.4 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 hackear.

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

5.1.5 CRACKERS

Los **Crackers**, en realidad, son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de la 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”.

5.1.6 PHREAKERS

Otro personaje en el Underground es el conocido como **Phreaker**²⁹. 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 éstas no cobren las llamadas que se hacen.

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

Se dice que el Phreaking es el antecesor del Hacking 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 Bell³⁰ basaba en la utilización de los mecanismos para la realización de llamadas gratuitas. Lo que Bernay descubrió, fue que dentro de Bell existían unos números de prueba que servían para que los operarios comprobaran las conexiones. Hasta aquí todos eran simples adolescentes que hacían llamadas gratuitas a sus padres en otro estado.

La situación cambió cuando se descubrió que MamaBell (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 “Boxes” (cajas). La primera fue la “Blue Box” que fue hallada en 1961 en el Washington State College, y 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

²⁹ Fusión de las palabras Freak, Phone y Free: Mounstruo de los Teléfonos Libres (intento de traducción literal)

³⁰ Compañía telefónica fundada por Alexander Graham Bell

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 pretendían y creían los directivos de Bell).

El cómo los Phreakers llegaron a enterarse del funcionamiento de estos tonos fue algo muy simple: Bell, orgullosa de su nuevo sistema, lo publicó 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 Red Box y Black Box, la cuales permitían realizar llamadas gratis desde teléfonos públicos.

Las Blue Boxes no solo servían para realizar llamadas gratuitas, sino que proporcionaban a sus usuarios los mismos privilegios que los operadores de Bell.

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

El primer Phreaker que utilizó este método fue Joe Engressia, quien era ciego. A los 8 años, y por azar, silbó por el auricular de su teléfono cuando escuchaba un mensaje pregrabado y la llamada se cortó. Realizo esto varias veces y en todas se le cortaba. La razón es un fenómeno llamado Talk-Off, que consiste en que cuando alguien silba y alcanza casualmente los 2600 Hz, la llamada se corta, como si fuera una Blue Box orgánica. Joe aprendió como potenciar su habilidad para silbar 2600 Hz y ya con 20 años era capaz de producir los 2600 Hz con su boca y silbar los tonos del número con el que quería conectarse.

Otro Phreaker que utilizaba el método de Engressia, fue John Draper, más conocido por 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 Engressia: soplabla su silbato y la línea se quedaba libre.

Muchos Phreakers evolucionaron mas tarde al Hacking, como es el caso del pionero Mark Bernay, que bajo el nick de The Midnight Skulker (El Vigilante de Medianoche) se rió de todos los fallos de seguridad de muchas empresas.

Hoy, el Hacking y el Phreaking 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 Phreaking si desea utilizar la línea telefónica mucho tiempo en forma gratuita y; de la misma forma un Phreaker necesitará del Hacking si desea conocer en profundidad cualquier sistema de comunicaciones.

5.1.7 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 trabajaba para conseguir una tarjeta de crédito ajena. Así nació:

1. El **Carding**, es el uso (o generación) ilegítimo 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 Hacking 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 DESAFÍOS DE UN HACKER

1. El mundo está 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 sí mismos más allá de sus propios límites físicos. De manera similar, un hacker 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 deben 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 órdenes, puede hacer que deba dejar de resolver ese problema con el cual está fascinado.
9. La actitud no es sustituto para la competencia.
10. Tener la actitud para ser hacker no alcanza, como tampoco 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 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 Assembler, 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 del hacker. Se deberá aprender como pensar en los problemas de programación de una manera general, independiente de cualquier lenguaje. Se debe llegar al punto en el cual se pueda aprender un lenguaje nuevo en días, relacionando lo que está en el manual con lo que ya sabe de antes. Se debe aprender varios lenguajes muy diferentes entre sí. Es una habilidad compleja y la mayoría de los mejores hackers lo hacen de forma autodidacta.

2. Aprender Unix. El paso más importante es obtener un Unix libre, instalarlo en una máquina personal, y hacerlo funcionar. Si bien se puede aprender a usar Internet sin saber Unix, nunca se podrá ser hacker en Internet sin conocerlo. Por este motivo, la cultura hacker actual está 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 (ver Anexo I).

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

En capítulos posteriores se analizarán 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 LA ÉTICA DEL HACKER³¹

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 los algunos “Mandamientos” en los cuales se basa un hacker a la hora de actuar sobre los sistemas que ataca:

- I. Nunca destruyas nada intencionadamente en la PC que estés hackeando.
- 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. A ser posible no 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 al SysOp, déjale un mensaje con la lista de gente que pueda responder por tí.
- VI. Nunca hackees en computadoras del 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

³¹ Maximum Security. A Hacker's guide to protecting your Internet Site and Network. Macmillan Computer Publishing©. 1999. EE.UU. <http://sams.net>
<http://www.itlibrary.com/reference/library/1575212684/ewtoc.html>

abusa de la Blue Box, puedes ser cazado.

- VIII. No dejes en mucha información del sistema que estas hackeando. Di sencillamente "estoy trabajando en ..." pero no digas a quien pertenece, ni el número de 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 hackeando, no sabrás que es...

5.1.12 MANIFIESTO HACKER³²

En los principios, un grupo hackers llamado Legión 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”:

(...) "Hoy he hecho un descubrimiento. He encontrado una computadora. Esperad, esto es lo mejor. La computadora hacía lo que yo quería. Si cometía un error era porque yo me equivocaba. No porque yo no le gustara... Y entonces ocurrió... una puerta se abrió al mundo, surcando la línea telefónica igual que la heroína surca las venas del adicto, el impulso eléctrico te envía a un refugio a salvo de las incompetencias del día a día... la BBS ha sido encontrada. Es... es a donde pertenezco. Conozco a todo el mundo aquí, incluso sin haberlos visto antes, sin haber hablado con ellos y puede que a algunos no vuelva a verlos jamás... Os conozco a todos... Éste es nuestro mundo... el mundo del electrón y el conmutador, la belleza del budio. Hacemos uso de un servicio ya existente sin pagar por lo que podría ser gratis si no estuviera en manos de unos glotones aprovechados, y tú nos llamas a nosotros criminales. Nosotros exploramos... y tú nos llamas criminales. Existimos sin color de piel, sin nacionalidad, sin inclinaciones religiosas... y tú nos llamas criminales. Tú que construyes bombas atómicas, tú que haces la guerra, tú asesino, nos engañas y mientes intentando hacernos creer que es por nuestro propio bien, sin embargo somos criminales. Si, soy un criminal. Mi crimen es la curiosidad. Mi crimen es juzgar a la gente por que lo que ellos dicen y piensan, no por como ellos aparentan ser exteriormente. Mi crimen es ser más inteligente que tú, algo por lo que nunca me perdonarás." (...)

+++ The Mentor +++

Fermín (alias) es un estudiante universitario español, trabaja en una empresa de seguridad informática ganando un sueldo impactante. Este trabajo lo consiguió siendo hacker y según dice él por “... nacer y ser curioso, por hacer del 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 él que los utilizan para delinquir e incluso son buscados y pagados para ello, “... pero este no es un hacker.”³³

Un ejemplo de este 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”.

³² La Conciencia de un Hacker escrito por The Mentor Volumen 1–Capítulo 7–3º Párrafo.

³³ Declaraciones de Fermín para <http://www.kriptopolis.com>

5.1.13 OTROS HABITANTES DEL CIBERESPACIO

5.1.13.1 GURÚS

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 sólo enseñan las técnicas básicas.

5.1.13.2 LAMERS O SCRIPT–KIDDERS

Son aficionados jactosos. Prueban todos los programas (con el título “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 sólo 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 aprovechando los conocimientos del hacker y lo ponen en práctica sin saber.

5.1.13.3 COPYHACKERS

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 del hacker. Se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, 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 difícilmente 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 cómo 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 basan en el principio de que cualquiera puede ser atacado y sabotado, 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, cassettes, DVD, etc.) y los vende ilegalmente.

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 sí mismos desarrolladores de software; y los que infectan los sistemas con los virus creados. Sin embargo es difícil imaginar que cualquier “desarrollador” no se vea complacido al ver que su “creación” ha sido ampliamente “adquirida por el público”.

5.2 PERSONAL (INSIDERS)

Hasta aquí se ha presentado al personal como víctima de atacantes externos; sin embargo, de los robos, sabotajes o accidentes relacionados con los sistemas informáticos, el 70%³⁴ son causados por el propio personal de la organización propietaria de dichos sistemas (“Inside Factor”).

Hablando de los Insiders Julio C. Ardita³⁵ explica que “(...) desde mitad de 1996 hasta 1999 la empresa tuvo dos casos de intrusiones pero en el 2000 registramos siete, de las cuales 5 eran intrusos internos o ex-empleados (...)”.

El siguiente gráfico detalla los porcentajes de intrusiones clasificando a los atacantes en internos y externos.

³⁴ Fuente: Cybsec S.A. <http://www.cybsec.com>

³⁵ ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. <http://www.cybsec.com>

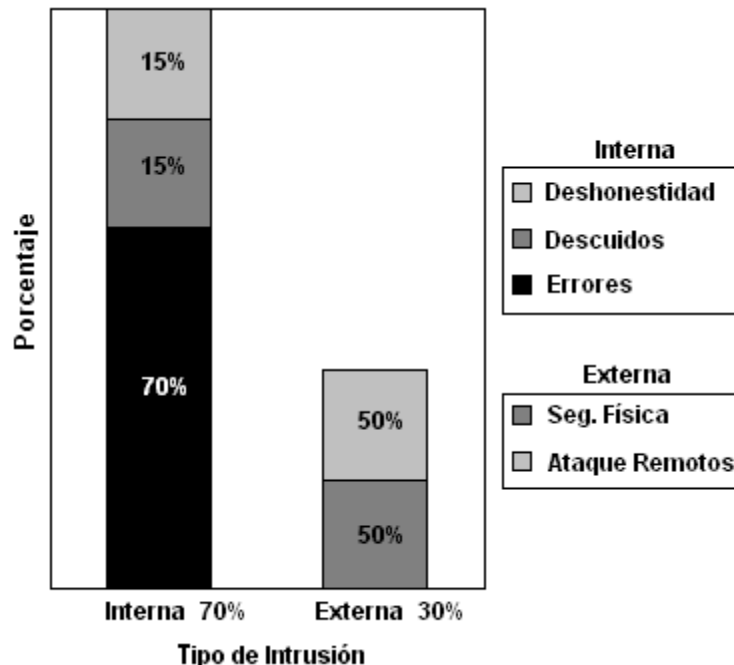


Gráfico 5.1 – Intrusiones. Fuente: <http://www.cybsec.com>

Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de una máquina conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el que un atacante 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 del tipo pasivos o 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 verá que aquí el daño no es intencionado pero ello no está en discusión; el daño existió y esto 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 conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño. También han existido casos donde el ex-empleado deja Bombas Lógicas que “explotan” tiempo 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 aún no tienen los conocimientos ni experiencia básicos para considerarlos hackers o crackers (podrían ser Newbies). En la mayoría de los casos son estudiantes intentando penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para él 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 él; y no sólo a la persona que coloca bombas o quema automóviles. Son ejemplos concretos de este tipo, ataque de modificación³⁶ de los datos de clientes entre empresa competidoras, o de servidores que albergan páginas web, bases de datos entre partidos políticos contrarios, etc.

5.2.5 INTRUSOS REMUNERADOS

Este es, sin duda, el grupo de atacantes más peligroso, aunque también el menos habitual. Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar “secretos” (código fuente de programas, bases de datos de clientes, información confidencial de satélites, diseño de un nuevo producto, etc.) o simplemente para dañar, de alguna manera la imagen de la entidad atacada.

Suele darse, sólo, en grandes multinacionales donde la competencia puede darse el lujo de un gran gasto para realizar este tipo de contratos y contar con los medios necesarios para realizar el ataque.

5.2.6 RECOMENDACIONES

Una norma básica, sería verificar cada aspirante a ser nuevo empleado; aunque tampoco debemos olvidar que el hecho de que alguien entre “limpio” a la organización no

³⁶ Por **Modificación** se entiende cualquier cambio de los datos incluyendo su borrado.

implica que vaya 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 mínimo privilegio que necesite para desempeñar correctamente su función, es decir, que sólo se le debe permitir que sepa lo necesario para realizar su trabajo.
- **Conocimiento parcial (dual control):** las actividades más 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 aplicable 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 retiró.
- **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 último punto sea el más difícil de implementar debido a la gran cantidad de usuarios que se deben informar de los nuevos accesos y de la movilidad de alguno de ellos.

En estos puntos se encuentran las mayores 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 podrá verificarse los antecedentes de miles de alumnos (y tampoco ético prohibir su acceso por ser estos dudosos). De esta forma, en las redes de Investigación y Desarrollo (I+D) 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.

CAPÍTULO 6



“Ningún problema verdadero tiene solución. En cada problema grande hay un problema pequeño que lucha por salir. Y... En cada problema pequeño hay un problema grande que lucha por salir.”

Leyes de Smith–Hoare–Schainker (Leyes de Murphy)

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 de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de las computadoras, así como a la puesta en órbita 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, almacenamiento y procesamiento 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 más 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 cálculo de una organización se está reemplazando por otro que considera un número 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 hacer que todos los programas, datos y equipos estén disponibles para cualquier usuario de la red que así 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 éste los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. La presencia de múltiples CPUs 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 máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario y con los datos guardados en una o más máquinas que funcionan como servidor de archivo compartido.

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

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

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

Una forma que muestra el amplio potencial del uso de redes como medio de comunicación es Internet y el uso del correo electrónico (e-mail), que se envía 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 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, archivos, datos, etc.).

Desde una perspectiva más 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 mantiene los servicios). Así, a una **Red** más que varias computadoras conectadas, la constituyen personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.

Las redes deberían ser lo más 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 rigen la transmisión de datos. El primer factor se llama nivel físico y el segundo protocolo.

En el 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 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** sólo permiten 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 de 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 (grupos de entidades afines que les ayudan a realizarlo). El efecto final es que sean capaces de “hablar” entre sí.

El objetivo último de todo el esfuerzo invertido 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 sí y las haga funcionar como una máquina compuesta, capaz de sacar provecho de las conexiones de alta velocidad.

Parece lógico suponer que las computadoras podrán trabajar en conjunto cuando dispongan de una conexión entre ellas. Pero ¿Cómo conseguir, sin embargo, que computadoras de diferentes fabricantes en 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 Interconnection) es utilizado por, prácticamente, la totalidad de las redes del mundo. Este modelo fue creado por el ISO (International Standard Organization), y consiste en siete niveles o capas donde cada una de ellas define las funciones que deben 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 él, y a su vez proporciona alguna funcionalidad a los niveles superiores.

Los siete niveles del modelo OSI son los siguientes:

1. **Capa Física:** esta capa tiene que ver con el envío de bits en un medio físico de transmisión y asegura que si de 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.
Capa de Enlace: en esta capa se toman los bits que entrega la Capa Física y se agrupan para formar marcos de bits (Frames). Se realiza un chequeo de errores sobre cada frame. Si un marco se pierde o se daña en el medio físico esta 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 cómo acceder al medio físico.
2. **Capa de Red:** se encarga de controlar la operación de la subred (medios físicos y dispositivos de enrutado). Una tarea primordial es decidir cómo 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 registra el tipo y cantidad de paquetes que circulan.

3. **Capa de Transporte:** el objetivo de esta capa es el de tomar datos de la Capa de Sesión y asegurarse que dichos datos lleguen a su destino. En ocasiones los datos que vienen de la Capa de Sesión exceden el tamaño máximo de transmisión (MTU Maximum Transmission Unit) de la interfaz de red, por lo cual es necesario particionarlos y enviarlos en unidades más pequeñas, lo cual da origen a la fragmentación y ensamblado de paquetes cuyo control se realiza en esta capa.
La última labor importante de la Capa de Transporte es ofrecer un mecanismo de nombrado que sirva para identificar y diferenciar las múltiples conexiones existentes, así como determinar en qué 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 nodo (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).
4. **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 transferir un archivo muy grande entre dos nodos que tienen una alta probabilidad de sufrir una caída, es lógico pensar que una transmisión ordinaria nunca terminaría porque algún interlocutor perderá la conexión. La solución es que se establezcan puntos de chequeo cada pocos minutos de manera que, si la conexión se rompe, más tarde se pueda reiniciar a partir del punto de chequeo, lo cual ahorra tiempo y permite la finalización de la transferencia.
5. **Capa de Presentación:** esta 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 en la transmisión.
6. **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 permiten desplegar en la terminal local los resultados, aún cuando éstos 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 conversiones necesarias de manera que el archivo puede usarse inmediatamente bajo alguna aplicación.

Gráficamente:

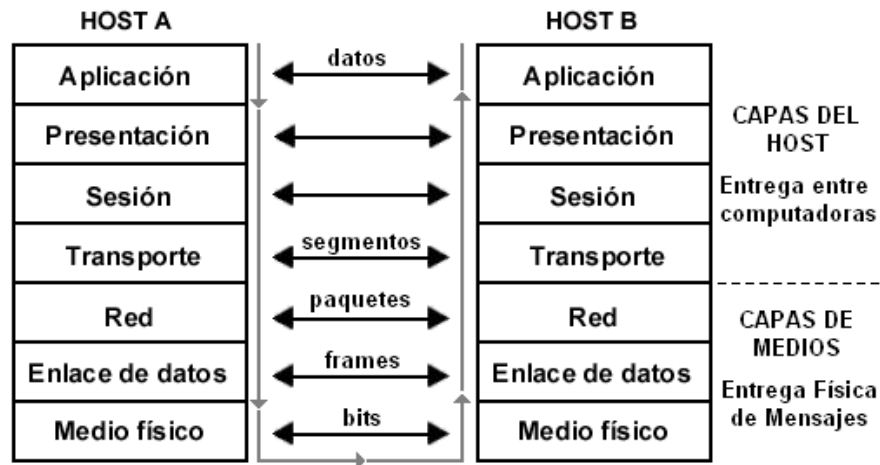


Gráfico 6.1 – Modelo OSI. Fuente: CISCO Networking Academies. Curriculum Online Versión 1.1.

6.1.1.5.1 Transmisión de Datos en el Modelo OSI

Un envío 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.

1. La Capa de Aplicación toma los datos y los encapsula añadiendo un encabezado que puede contener información de control o estar vacío. Envía el paquete resultante a la Capa de Presentación.
2. La Capa de Presentación recibe el paquete y no intenta decodificarlo o separar sus componentes, sino que lo toma como datos y le añade un encabezado con información de control de esta capa.
3. Las Capa de Sesión y de Transporte reciben el paquete, que también son sólo datos para ellas y le añaden un encabezado de control. El resultado es enviado a la capa inferior.
4. La Capa de Red se encarga de enrutar el paquete a su destino.
5. Las Capas de Red, Enlace de datos y Física toman, respectivamente, el paquete que les envía la capa superior y añaden a éste un encabezado definido por el protocolo que corresponde a cada capa y pasan el resultado a la capa inferior.
6. La Capa Física, por último, traducirá el último paquete a las señales apropiadas para que viajen por el medio físico hasta el nodo destino.
7. 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 el nodo destino.

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

6.2 PROTOCOLOS DE RED

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

En 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 placas. Este lenguaje es lo que se 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 el producto de una sociedad cada vez más intercomunicada y relacionada, en donde lo importante es que la información llegue a su destino sí, pero también lo es que llegue en las mismas condiciones en que ha sido enviada y en el tiempo previsto.

Algunos de los protocolos mas conocidos y ampliamente difundidos son:

6.2.1 NETBIOS–NETBEUI–NWLINK–WINS

Network Basic Input Output System, es el protocolo más sencillo. Está 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 Interface) pero continúa utilizando el juego de comandos del NetBIOS y luego para hacerlo compatible con otros protocolos (como IPX–SPX) se amplió nuevamente recibiendo el nombre de NWLink (NetWare Link).

NetBIOS toma el puerto 137–139 en computadoras que utiliza el sistema operativo Windows[®] de la empresa Microsoft[®]. Está considerado el protocolo más fácilmente vulnerable de los existentes, a punto tal que cualquier 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 cómo conectar computadoras entre sí para lograr el intercambio de información.

Actualmente TCP/IP se utiliza ampliamente en la versión 4 (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 datagramas

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

6.2.2.1 LAS CAPAS DEL MODELO TCP/IP

El Transmission Communication Protocol/Internet Protocol es actualmente el protocolo más ampliamente utilizado por su independencia del Sistema Operativo y hardware utilizado. 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 un 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 (Transmission 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 gráfico 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 está implantada por dos protocolos: el Transmission Control Protocol (TCP) y el User Datagram Protocol (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 UDP 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 esta 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 Host, como 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 enviar datos por cable coaxial delgado (10Base2), cable coaxial grueso (10Base5), par trenzado (10Base-T), fibra óptica (10Base-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, ésta 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 "Datagrama" (datagram), y son conjuntos de datos que se envían como mensajes independientes.

6.2.2.2 FUNCIONAMIENTO

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

Luego, 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 reenvío de los faltantes. Por último TCP se encarga de reensamblar los paquetes en el orden correcto, basándose en los números asignados previamente.

6.2.2.3 COMPARACIÓN CON EL MODELO OSI

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

El modelo TCP/IP no tiene bien divididas 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 Transporte. 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.

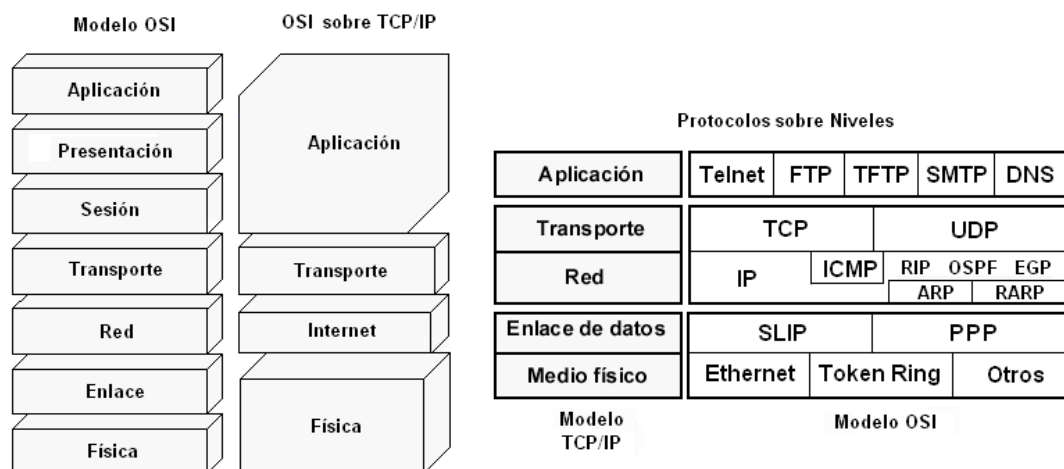


Gráfico 6.2 – Comparación Modelo OSI–TCP

6.2.3 NIVEL FÍSICO DEL MODELO TCP/IP

6.2.3.1 ARP

El Address Resolution 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 transmitirá 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 Resolution 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 simultáneas 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 Point to Point Protocol fue desarrollado por el IETF (Internet Engineering Task Force) en 1993 para mejorar algunas deficiencias 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 datagramas 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 ni el sistema operativo.

Sus principales características son:

1. Es transparente a las capas superiores.
2. Transmite protocolos IP, IPX, Apple Talk, etc.
3. Es ampliable ya que no fue pensando para solucionar un problema en concreto.

PPP esta dividido en dos subprotocolos:

1. **LCP (Link Control Protocol):** 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 Protocol):** se encarga de negociar y configura 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 transportará los correspondientes paquetes. Cualquier paquete recibido mientras su NCP no esté en el estado abierto es descartado.

6.2.5 NIVEL DE RED DEL MODELO TCP/IP

6.2.5.1 IPX–SPX

El Internetwork Packet Exchange–Sequenced Packet Exchange 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 datagrama, sin comprobar la integridad de la información que contiene. Para ello se utiliza una nueva cabecera que se antepone al datagrama que se está tratando.

La cabecera IP tiene un tamaño de 160 bits y está formada por varios campos de distinto significado entre los que se destaca el tipo de protocolo de transporte del datagrama, el número 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 esté preparado (no existe una conexión directa emisor–receptor). De hecho, muchas veces se mandan paquetes a un destino inexistente 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: 205.025.076.223)

En el nivel IP se definen los siguientes aspectos de intercambio de información:

1. Un mecanismo de direcciones que permite identificar de manera unívoca 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 universalidad de la red.
2. Un concepto relativo al transporte 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 esté conectado con otra computadora en otra red en el exterior. Los routers reconocen un paquete y comprueban que no sea para alguna máquina conectada a su red y entonces lo mandan a otra, más 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.
3. 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 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 las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno 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 las 126 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 primeros 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 bytes de la dirección constituyen el

identificador de la computadora permitiendo, por consiguiente, un número máximo de 64.516 ordenadores en 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 192 y 223, 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 Host, 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 *209.89.67.156* se creó 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 al nivel de aplicaciones no sirve simplemente indicar la dirección IP; se necesitarán mas especificaciones para que el Host de destino pueda escoger la aplicación correcta. 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 Socket, 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 existe miles de puertos ocupados de los $2^{16} = 65535$ posibles, de los cuales apenas unos cuantos son los más utilizados y se encuentran divididos en tres rangos:

- 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 | FTP–Data | TCP/UDP | Transferencia archivos |
| 21 | FTP | TCP | Control Transferencia Archivos |
| 23 | TELNET | TCP/UDP | Servicio Remoto |

| | | | |
|-------------|---------------------------|---------|--------------------------------|
| 25 | SMTP | TCP/UDP | Envío de mails |
| 43 | Whois | TCP/UDP | Servicio de Nombre de Dominios |
| 53 | DNS | TCP/UDP | |
| 70 | Gopher | TCP/UDP | |
| 79 | Finger | TCP/UDP | |
| 80 | WWW-HTTP | TCP/UDP | |
| 110 | POP3 (PostOffice) | TCP/UDP | World Wide Web |
| 119 | UseNet | TCP | Recepción de mail |
| 137 | NetBIOS | UDP | Newsgroups de usuarios |
| 194 | IRC (Internet Relay Chat) | TCP/UDP | Chat |
| 443 | HTTPS | TCP | HTTP Seguro vía SSL |
| 750 | Kerberos | TCP/UDP | Chat |
| 6667 | IRC (Internet Relay Chat) | TCP | |

Tabla 6.1 – Fuente: <http://www.isi.edu/in-notes/iana/assignments/port-numbers> según RFC 768, RFC 793 y RFC 1060

6.2.5.3 APPLETALK

Este protocolo (de nivel de red) está incluido en el Sistema Operativo de Apple Macintosh desde su aparición, permite interconectar computadoras y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte.

6.2.6 NIVEL DE TRANSPORTE 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. Así, las aplicaciones pueden encargarse de su tarea sin preocuparse de la seguridad en la comunicación.

TCP divide el mensaje original en datagramas de menor tamaño (múltiplo de 32 bits), y por lo tanto, mucho más manejables. Los datagramas serán dirigidos 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 datagramas (cabecera). Luego, se ocupa de que los datos sean entregados y que los paquetes sean reensamblados correctamente asegurando así que lo que se recibe sea efectivamente lo enviado.

Si ocurriera algún error en la transmisión, TCP se encargará 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 envío) en donde indica si faltan paquetes, tamaños o datos erróneos, etc.

Las principales características de este protocolo 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 máquinas 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 envío, o bien, forzar la transferencia dividiendo el paquete de la aplicación en datagramas más pequeños.
4. **Flujo no estructurado:** se refiere a la posibilidad de envío de información de control de estado junto a los datos propiamente dichos.
5. **Conexión full duplex:** permite la transferencia concurrente en ambas direcciones, sin ninguna interacción. La ventaja es evidente: el protocolo puede enviar datagramas desde el origen al receptor e información de control en sentido opuesto, reduciendo el tráfico en la red.

El Gráfico 6.3 detalla la constitución de cada datagrama del protocolo TCP (160–192 bits = 20–24 bytes). Comprender este diagrama es de especial interés para cualquiera que desee manipular datos en una comunicación actual.

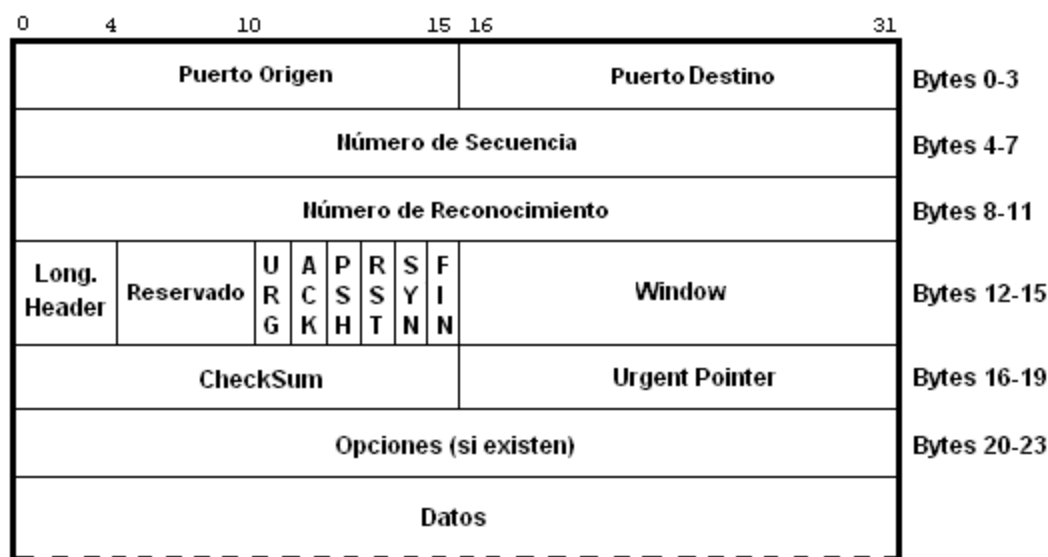


Gráfico 6.3 – Constitución de un datagrama TCP

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 esta distinción. Además, el programa cliente que realiza la petición también debe conocer el número de puerto en el que se encuentra el servidor adecuado. Mientras que el programa del usuario utiliza números prácticamente aleatorios, el servidor debe tener asignado un número estándar para que pueda ser utilizado por el cliente (ver Tabla 6.1). 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** (4 bits) contiene la longitud total de la cabecera TCP expresada en el número de palabras de 32 bits que ocupa (el tamaño real dividido 4). Esto permite determinar el lugar donde comienzan los **Datos**.

En la transmisión de datos a través del protocolo TCP la fiabilidad es un factor muy importante. Para poder detectar los errores y pérdida de información en los datagramas, es necesario que el cliente envíe de nuevo al servidor unas **Señales de Confirmación** (32 bits) una vez que se ha recibido y comprobado la información satisfactoriamente. Si el servidor no obtiene la señal de confirmación adecuada transcurrido un período de tiempo razonable, el datagrama completo se volverá a enviar.

Por razones de eficiencia los datagramas se envían continuamente sin esperar la confirmación, haciéndose 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 datagrama llegue con errores a su destino. Para poder detectarlos, cuando sucede esto, se incluye un **Checksum** (16 bits), el cual contiene un valor calculado a partir de la información del datagrama completo. En el otro extremo el receptor vuelve a calcular este valor, comprobando que es el mismo que el suministrado en la cabecera. Si el valor es distinto significará que el datagrama es incorrecto.

La forma en que TCP numera los datagramas es contando los bytes de datos que contiene cada uno de ellos y añadiendo esta información al campo correspondiente de la cabecera del datagrama siguiente.

De esta manera el primero empezará en cero; el segundo contendrá el tamaño de la parte de datos; el tercero contendrá la suma de ese número más el tamaño de los datos del segundo datagrama; y así sucesivamente. Por ejemplo, para un tamaño fijo de 500 bytes de datos en cada datagrama, la numeración sería la siguiente: 0 para el primero, 500 para el segundo, 1000 para el tercero, etc.

Existe otro factor más a tener en cuenta durante la transmisión de información, y es la potencia y velocidad con que cada computadora puede procesar los 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 éste no pueda procesarla. Este inconveniente se soluciona mediante un campo **Window** (16 bits), en el cual se introduce un valor indicando la cantidad de información que el receptor está preparado para procesar en un momento dado.

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

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

- Bit 5 (URGent): Identifica datos urgentes.
- Bit 4 (ACKnowledge): Indica que el campo de confirmación es válido.
- Bit 3 (PuSH): Aunque el buffer de datos no este lleno, se fuerza el envío.
- Bit 2 (ReSeT): Abortar la conexión. Todos los buffers asociados se vacían.

- Bit 1 (SYnchronize sequence Number): Sincronizar los números de secuencia.
- Bit 0 (FINish): Se solicita el cerrado de la conexión.

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

6.2.6.2 UDP

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

Cuando se utiliza UDP la garantía de que 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 la cabecera del 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 Message Protocol es de características similares al UDP, pero con un formato aún más simple. Su utilidad no está en el transporte de datos "de usuario", sino en los mensajes de error y de control necesarios para los sistemas de la red.

6.2.7.2 FTP

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

FTP utiliza dos canales 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:

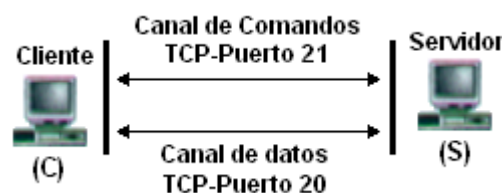


Gráfico 6.4 – Conexión FTP

El FTP permite 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 o 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 estas 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 esté 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 en los permisos, siendo normal en estos casos que no se permita realizar acciones tales como añadir archivos o modificar los existentes.

El FTP proporciona dos modos de transferencia de archivos: ASCII y binario. El modo de transferencia 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 HyperText Transfer Protocol es la base de toda comunicación desarrollada en la Web. Utilizado 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 hipermediático. Es un protocolo genérico, sin estado, orientado a objetos, que se puede 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:

1. Protocolo de Aplicación: aunque generalmente se implementa sobre el TCP/IP, también es capaz de hacerlo sobre otros protocolos de capas más bajas. HTTP presupone únicamente un transporte fiable, así que puede utilizar cualquier protocolo que garantice este requisito mínimo.
2. Sistemas de información distribuidos, colaboradores, de hipermedios: HTTP soporta sistemas de información distribuidos es decir, sistemas esparcidos por múltiples servidores.
3. 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.
4. Sin estado: HTTP no mantiene un estado. Cuando se solicita una transferencia a través de HTTP, se crea la conexión, se produce la transferencia y se termina la conexión. Esta es una de las debilidades de HTTP; sin información de estado, cada página Web está sola. Por ejemplo, es difícil desarrollar una aplicación basada en la

Web que permita que un usuario se conecte en una página y que mantenga esta información de conexión durante todo el tiempo que el usuario esté 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 él.

5. Orientado a objetos, escritura y negociación de la representación de los datos: HTTP no está orientado a objetos en el mismo sentido que un lenguaje de programación. Esta descripción significa simplemente que 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 indican qué debe transferirse.
6. Sistema creado independientemente de los datos que se transfieren: Debido a que HTTP sólo mueve datos, no necesita tener información sobre cada uno de los tipos a transferir. Por ejemplo, un servidor Web no necesita un conocimiento específico sobre el funcionamiento interno del formato de un archivo de vídeo para hacer el envío.

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.

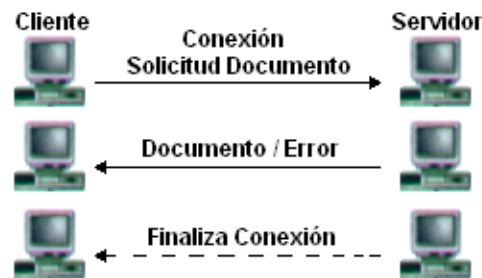


Gráfico 6.5 – Conexión HTTP

El protocolo HTTP en su estructura, divide el mensaje en encabezado (Header) y en cuerpo (Entity), separados entre sí por una línea en blanco.

6.2.7.4 SMTP

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

Generalmente los mensajes de correo electrónico no se envían directamente a las computadoras personales de cada usuario, sino 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 e-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.



Gráfico 6.6 – Conexión SMTP

6.2.7.5 POP

El servidor POP (Post Office Protocol) fue diseñado para la recuperación 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 se hallan enviado cada uno de los mails que se almacenaban en el servidor.

Actualmente el protocolo POP se encuentran en su tercera implementación por lo que generalmente se escuchará sobre POP3.

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

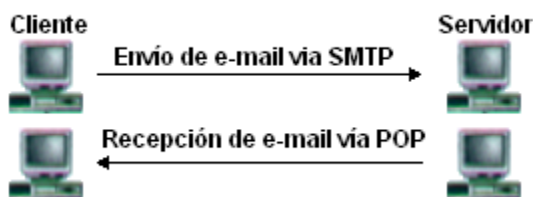


Gráfico 6.7 – Relación SMTP-POP

6.2.7.6 MIME

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

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

1. MIME–Versión: especifica la versión de MIME utilizado para codificar el mensaje.
2. Content–Type: especifica el tipo y subtipo de los datos no ASCII.
3. Content–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 envío de noticias (News). NNTP está basado en las especificaciones de UseNet (tratado también en este capítulo) pero con algunas modificaciones en su estructura que le permiten ser adaptables a otros grupos de noticias no UseNet.

6.2.7.8 SNMP

El Simple Network Management 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 World 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 más extendidas entre usuarios de Internet, hasta el punto tal de que muchas personas piensan que este servicio es el único existente, junto al IRC. Inicialmente se ideó para que unos cuantos físicos intercambiaban 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 (URL) que a su vez está relacionado unívocamente con una dirección IP.

El tipo más común de datos transportado a través de HTTP es HTML (HyperText 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 línea. Los recursos hiperenlazados y los archivos de imágenes en línea están identificados con los URL intercalados dentro del documento HTML.

A pesar de que algunos servidores Web personales de gama baja sólo pueden enviar páginas estáticas, la mayoría de los servidores HTTP admiten la CGI (Common Gateway Interface). Con CGI se pueden escribir programas que se integran en la Web y que realizan tareas tales como el proceso de formularios y las búsquedas en bases de datos, las cuales HTML no puede ejecutar.

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

6.3.1 SERVICIOS DE INTERNET

Como sabemos, Internet es en la actualidad, la red de computadoras más grande del mundo. Sin embargo la importancia de Internet no reside solamente en el número de máquinas interconectadas sino en los servicios que brinda.

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

A través de Telnet o e-mail, el servicio presenta una interface ANSI (sin gráficos), sólo con caracteres alfanuméricos. Con un programa cliente, la gestión es más sencilla, visual y agradable, como sucede en la WWW donde se presentan cada una de las páginas en formato gráfico.

6.3.1.1 TELNET

Este protocolo 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 sistema 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 de usuario.

El sistema local que utiliza el usuario se convierte en una terminal "no inteligente" donde todos los caracteres pulsados y las acciones que se realicen se envían al Host 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 específico (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 para diversos servicios de Internet, como Gopher, Wais, FTP o cualquier otro programa–cliente disponible en el Server. Estas conexiones suelen ser más económicas (pero más lentas) y están restringidas a los servicios que brinda el servidor.

6.3.1.2 IRC

El Internet Relay 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 sí. El manejo del sistema es muy simple. El IRC está organizado por redes, cada una de las cuales está 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 programa cliente, siendo los cuatro más populares el mIRC, Pirch, Ichat y Microsoft Chat.

Cada servidor IRC está conectado a los servidores más cercanos. De esta manera, todos los servidores IRC están conectados (al menos indirectamente) unos con otros.

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 “#”. 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 se desea no existe y esperar que otras personas ingresen en él. Se suele entrar en las charlas con apodos (nick), sin dar el nombre real, de manera que los usuarios conserven el anonimato. Cuando la última persona abandona un canal, IRC lo elimina.

6.3.1.3 USENET

Una de las áreas más populares de Internet son los grupos de discusión o NewGroups. El término UseNet 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 dos 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, sino 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 enviar cualquier mensaje al mismo, y cualquiera dentro de 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 relevantes son:

| Tema | Descripción |
|-------------------|------------------|
| alt (alternative) | Diferentes temas |

| | |
|------------------|--|
| Bionet | Biología |
| biz (business) | Negocios |
| comp (computer) | Computadoras e Informática |
| Ddn | Red de datos del departamento de defensa |
| News | Grupos sobre UseNet |
| rec (recreative) | Ocio |
| sci (science) | Ciencias |
| soc | Ciencias sociales |
| talk | Debates |

Tabla 6.2 – Jerarquías más comunes en UseNet

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

Tiene una gran utilidad práctica, ya que si un usuario determinado tiene algún comentario o duda acerca de un tema, puede acudir al grupo temático indicado, dejar un 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 tienen una utilidad que permite buscar información sobre un usuario particular. Este servicio es conocido como Finger (dedo).

En Internet los usuarios se conocen por su identificador. 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:

1. Información pública sobre cualquier usuario.
2. Comprobación de si un usuario está utilizando actualmente un Host determinado en Internet, pudiendo ver un resumen de información para cada usuario que está conectado.
3. Conectar con determinado Host, que se han configurado para ofrecer otros 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 una empresa).

El servicio WhoIs 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 *whois Harvard* 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 día muchas organizaciones corren este servicio que proporciona información sobre los usuarios de una organización. Uno de los servidores WhoIs más conocido es *whois.internic.net* que contiene nombres y direcciones de Internet.

Es de remarcar que servicios como Telnet, Finger, Archie, Gopher, WhoIs y Ping están cayendo en desuso a favor de las cada vez más perfeccionadas herramientas basadas en la World Wide Web. De todas maneras (como se verá en capítulos posteriores) siguen brindando gran utilidad a administradores de sistemas y usuarios avanzados, sobre todo en temas de seguridad.

CAPÍTULO 7



“La seguridad de un sistema es tan fuerte como su punto más débil... La seguridad total no existe pero si la mínima inseguridad”

infohack.org

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 el uso** de un recurso.
- Cuando un **atacante** tiene **acceso desautorizado** está 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. Howard³⁷ en su tesis estudia la cantidad de ataques que puede tener un incidente. Al concluir dicho estudio y basado en su experiencia en los laboratorios del CERT³⁸ afirma que esta cantidad varía entre 10 y 1.000 y estima que un número razonable para estudios es de 100 ataques por incidentes.

7.2 DETECCIÓN DE INTRUSOS

A finales de 1996, Dan Farmer (creador de una de las herramientas más útiles en la detección de intrusos: SATAN) realizó un estudio sobre seguridad analizando 2.203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron Web Sites orientados al comercio y con contenidos específicos, además de un conjunto de sistemas informáticos aleatorios con los que realizar comparaciones.

³⁷ HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 12–Página 165

³⁸ CERT: Computer Emergency Response Team. Grupo de Seguridad Internacional especializado en dar respuesta a las empresas y organizaciones que denuncian ataques informáticos a sus sistemas de información. <http://www.cert.org>

El estudio se realizó empleando técnicas sencillas y no intrusivas. Se dividieron los problemas potenciales de seguridad en dos grupos: rojos (red) y amarillos (yellow). Los problemas del grupo rojo son los más serios y suponen que el sistema está abierto a un atacante potencial, es decir, posee problemas de seguridad conocidos en disposición de ser explotados. Así por ejemplo, un problema de seguridad del grupo rojo es un equipo que tiene el servicio de FTP anónimo mal configurado.

Los problemas de seguridad del grupo amarillo son menos serios pero también reseñables. Implican que el problema detectado no compromete inmediatamente al sistema pero puede causarle serios daños o bien, que es necesario realizar tests más intrusivos para determinar si existe o no un problema del grupo rojo.

La tabla 7.1 resume los sistemas evaluados, el número de equipos en cada categoría y los porcentajes de vulnerabilidad para cada uno. Aunque los resultados son límites superiores, no dejan de ser... escandalosos.

| Tipo de sitio | # Total sitios testeados | % Total Vulnerables | % Yellow | % Red |
|------------------------|--------------------------|---------------------|--------------|--------------|
| Bancos | 660 | 68,34 | 32,73 | 35,61 |
| Créditos | 274 | 51,1 | 30,66 | 20,44 |
| Sitios Federales US | 47 | 61,7 | 23,4 | 38,3 |
| News | 312 | 69,55 | 30,77 | 38,78 |
| Sexo | 451 | 66,08 | 40,58 | 25,5 |
| Totales | 1.734 | 64,93 | 33,85 | 31,08 |
| Grupo aleatorio | 469 | 33,05 | 15,78 | 17,27 |

Tabla 7.1 – Porcentaje de Vulnerabilidades por tipo de sitio. Fuente: <http://www.trouble.org/survey>

Como puede observarse, cerca de los dos tercios de los sistemas analizados tenían serios problemas de seguridad y Farmer destaca que casi un tercio de ellos podían ser atacados con un mínimo esfuerzo.

7.3 IDENTIFICACIÓN DE LAS AMENAZAS

La identificación de 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 podrían 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.

La Tabla 7.2 detalla el tipo de atacante, las herramientas utilizadas, en que fase se realiza el ataque, los tipos de procesos atacados, los resultados esperados y/u obtenidos y los objetivos perseguidos por los intrusos³⁹.

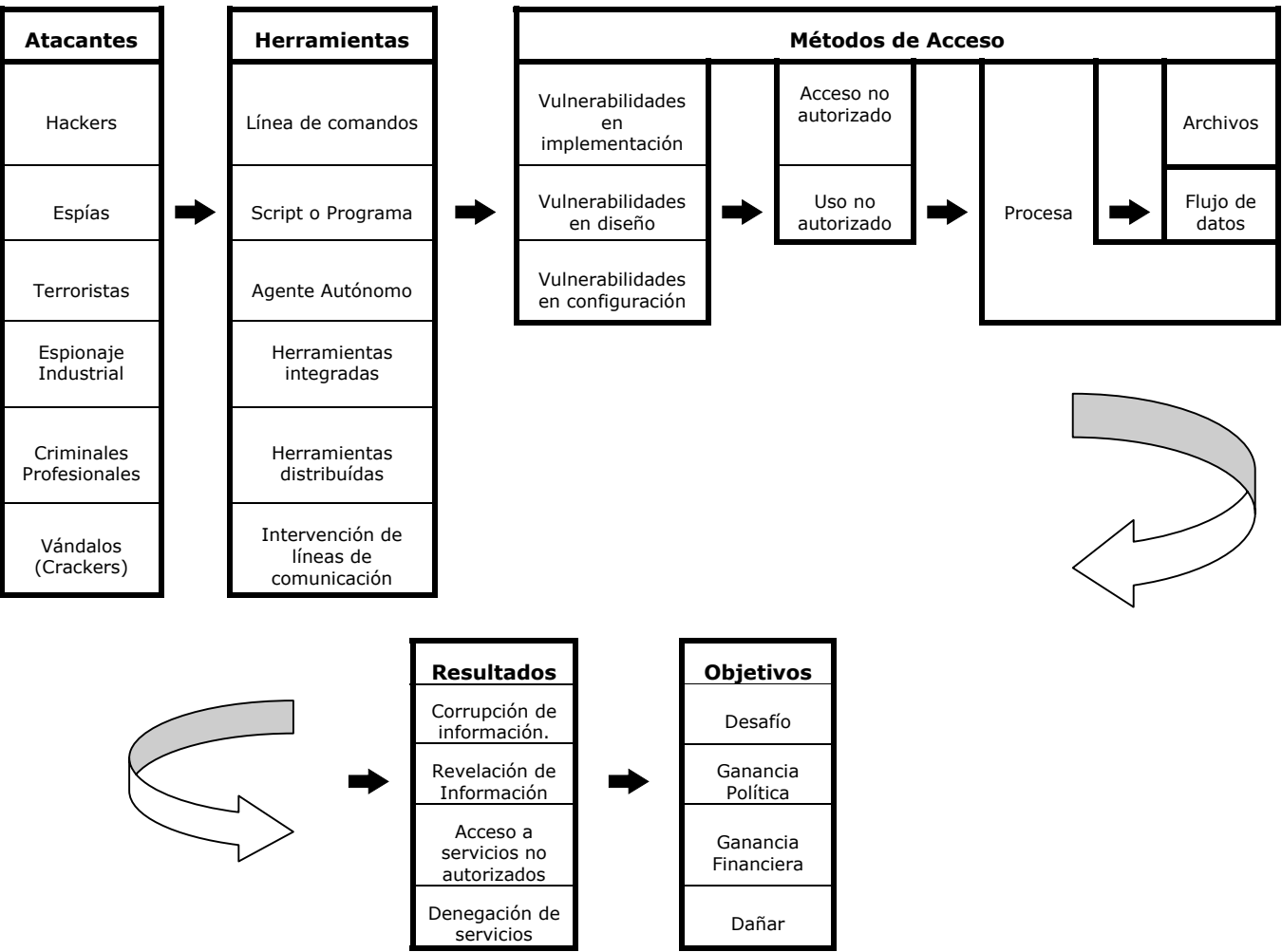


Tabla 7.2. Detalle de Ataques. Fuente: HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6–Página 71

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 cualquier servidor de información de cualquier organismo en Internet, simplemente siguiendo las instrucciones que acompañan la herramienta.

Los número que siguen no pretenden alarmar a nadie ni sembrar la semilla del futuro Hacker. Evidentemente la información puede ser aprovechada para fines menos lícitos que para los cuales fue pensada, pero esto es algo ciertamente difícil de evitar.

| Año | Incidentes Reportados | Vulnerabilidades Reportadas | Mensajes Recibidos |
|------|-----------------------|-----------------------------|--------------------|
| 1988 | 6 | | 539 |

³⁹ HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6–Página 71

| | | | |
|-----------------------|---------------|--------------|----------------|
| 1989 | 132 | | 2.868 |
| 1990 | 252 | | 4.448 |
| 1991 | 406 | | 9.629 |
| 1992 | 773 | | 14.463 |
| 1993 | 1.334 | | 21.267 |
| 1994 | 2.340 | | 29.580 |
| 1995 | 2.412 | 171 | 32.084 |
| 1996 | 2.573 | 345 | 31.268 |
| 1997 | 2.134 | 311 | 39.626 |
| 1998 | 3.734 | 262 | 41.871 |
| 1999 | 9.859 | 417 | 34.612 |
| 2000 | 21.756 | 1.090 | 56.365 |
| 2001 (4 meses) | 15.476 | 1.151 | 39.181 |
| Total | 63.187 | 3.747 | 357.802 |

Tabla 7.3 – Vulnerabilidades Reportadas al CERT 1988–2001. Fuente: CERT Internacional.
<http://www.cert.org/statistics>

Nota I: Estos incidentes sólo representan el 30% correspondientes a los Hackers.

Nota II: En 1992 el DISA⁴⁰ realizó un estudio durante el cual se llevaron a cabo 38.000 ataques a distintas sitios de organizaciones gubernamentales (muchas de ellas militares). El resultado de los ataques desde 1992 a 1995 se resumen en el siguiente cuadro⁴¹:

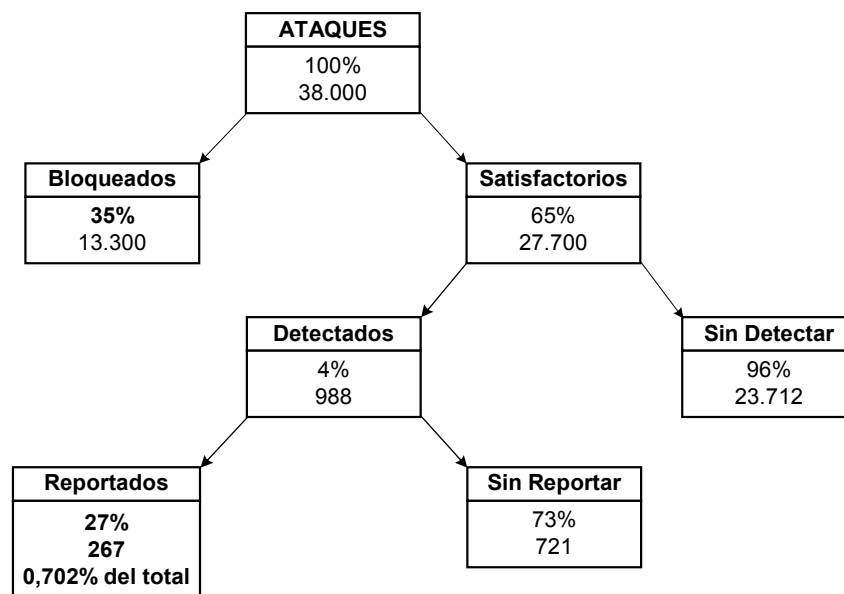


Gráfico 7.1 – Porcentaje de Ataques. Fuente: <http://www.disa.mil>

Puede observarse que solo el 0,70% (267) de los incidentes fueron reportados. Luego, si en el año 2000 se denunciaron 21.756 casos eso arroja 3.064.225 incidentes en ese año.

⁴⁰ DISA (Defense Information System Agency). <http://www.disa.mil>

⁴¹ HOWARD, John D. Thesis. An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 12–Página 168.

Nota III: Puede observarse que los incidente reportados en 1997 con respecto al año anterior es menor. Esto puede deberse a diversas causas:

- Las empresas u organizaciones no se pueden permitir el lujo de denunciar ataques a sus sistemas, pues el nivel de confianza de los clientes (ciudadanos) bajaría enormemente.
- Los administradores tienen cada vez mayor conciencia respecto de la seguridad de sus sistemas y arreglan por sí mismos las deficiencias detectadas. A esto hay que añadir las nuevas herramientas de seguridad disponibles en el mercado.
- Los “Advisories” (documentos explicativos) sobre los nuevos agujeros de seguridad detectados y la forma de solucionarlos, lanzados por el CERT, han dado sus frutos.

7.4 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. Ante la diversificación de clasificaciones de amenazas y la inminente aparición de nuevas técnicas, para la realización del presente los ataques serán clasificados y categorizados según mi experiencia y conocimiento de cada caso.

Otra lista de términos asociada con los ataques puede ser la siguiente⁴²:

| | | | | |
|--------------------------|--------------------------|--------------------------------|------------------------------------|--------------------------|
| <i>Trojan horses</i> | <i>Fraud networks</i> | <i>Fictitious people</i> | <i>Infrastructure observation</i> | <i>e-mail overflow</i> |
| <i>Time bombs</i> | <i>Get a job</i> | <i>Protection limit poke</i> | <i>Infrastructure interference</i> | <i>Human engineering</i> |
| <i>Bribes</i> | <i>Dumpster diving</i> | <i>Sympathetic vibration</i> | <i>Password guessing</i> | <i>Packet insertion</i> |
| <i>Data diddling</i> | <i>Computer viruses</i> | <i>Invalid values on calls</i> | <i>Van Eck bugging</i> | <i>Packet watching</i> |
| <i>Login spoofing</i> | <i>Data diddling</i> | <i>Wiretapping</i> | <i>Combined attacks</i> | <i>e-mail spoofing</i> |
| <i>Scanning</i> | <i>Dumpster diving</i> | <i>Eavesdropping</i> | <i>Denial-of-service</i> | <i>Harassment</i> |
| <i>Masquerading</i> | <i>Software piracy</i> | <i>Data copying</i> | <i>Degradation of service</i> | <i>Traffic analysis</i> |
| <i>Trap doors</i> | <i>Covert channels</i> | <i>Viruses and worms</i> | <i>Session hijacking</i> | <i>Timing attacks</i> |
| <i>Tunneling</i> | <i>Trojan horses</i> | <i>IP spoofing</i> | <i>Logic bombs</i> | <i>Salamis</i> |
| <i>Password sniffing</i> | <i>Excess privileges</i> | | | |

⁴² HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6-Página 52. Se conserva el idioma original (inglés) para no falsear información con respecto a los términos empleados.

Al describirlos no se pretende dar una guía exacta ni las especificaciones técnicas necesarias para su uso. Sólo se pretende dar una idea de la cantidad y variabilidad de los mismos, así como que su adaptación (y aparición de nuevos) continúa paralela a la creación de nuevas tecnologías.

Cabe destacar que para la utilización de estas técnicas no será necesario contar con grandes centros de cómputos, lo que queda fehacientemente demostrado al saber que algunos Hackers más famosos de la historia hackeaban con computadoras (incluso armadas con partes encontradas en basureros) desde la habitación de su hogar (ver Anexo II).

Cada uno de los ataques abajo descriptos serán dirigidos remotamente. Se define **Ataque Remoto** como “un ataque iniciado contra una maquina sobre la cual el atacante no tiene control físico”⁴³. Esta máquina es distinta a la usada por el atacante y será llamada **Víctima**.

7.4.1 INGENIERA SOCIAL

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 (generalmente es así), 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 convincente. O bien, podría enviarse 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 técnico 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 de Internet lo mejor es cortar y devolver la llamada a forma de confirmación.

7.4.2 INGENIERÍA SOCIAL INVERSA

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

⁴³ Maximum Security. A Hacker's guide to protecting your Internet Site and Network. Macmillan Computer Publishing®. 1999. EE.UU. Capítulo 25.
<http://sams.net>. <http://www.itlibrary.com/reference/library/1575212684/ewtoc.html>

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 llevara 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.

7.4.3 TRASHING (CARTONEO)

Generalmente, un usuario anota su login y password en un papelito y luego, cuando lo 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 (como el caso descripto) 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.

7.4.4 ATAQUES DE MONITORIZACIÓN

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

7.4.4.1 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 (generalmente en post-it adheridos al monitos 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.

7.4.4.2 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.

7.4.4.3 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 números de teléfono 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 módem 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:

7.4.4.3.1 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 máquina, que lanza el scanner, y también se verá su inmediata desconexión.

7.4.4.3.2 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 del 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 máquinas. 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:

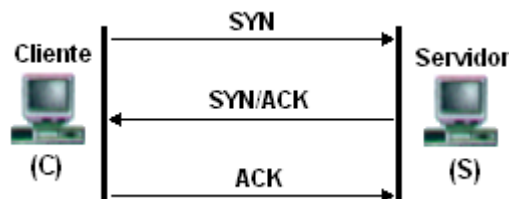


Gráfico 7.2 – Conexión en Tres Pasos.

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 está abierto y escuchando) al recibir este segmento SYN (activa el indicador) y envía una autenticación ACK de manera de acuse de recibo a C. Si S está cerrado envía un indicador RST.
3. C entonces ACKea (autentifica) a S. Ahora ya puede tener lugar la transferencia de datos.

Cuando las aplicaciones conectadas terminan la transferencia, realizan 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.

7.4.4.3.3 TCP FIN Scanning– Stealth Port Scanning

Hay veces en que incluso 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 aplicación de tecnologías (en este caso el protocolo TCP nacido 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”⁴⁴.

7.4.4.3.4 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 un 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.

7.4.4.4 EAVESDROPPING–PACKET SNIFFING

Muchas redes son vulnerables al Eavesdropping, o a la pasiva interceptación (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 Sniffers 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 ha ingresado por otras vías.

⁴⁴ GONCALVES, Marcus. Firewalls Complete. Beta Book. McGraw Hill. 1997. EE.UU. Página 25

Cada maquina 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 Sniffers 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 recurso 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 pueden ser detectados con algunos trucos.

7.4.4.5 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 a continuación 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 o 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.

Muchos ataques de este tipo comienzan con Ingeniería Social, y los usuarios, por falta de cultura, facilitan a extraños sus identificaciones dentro del sistema usualmente través de una simple llamada telefónica.

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

7.4.5.2.1 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:

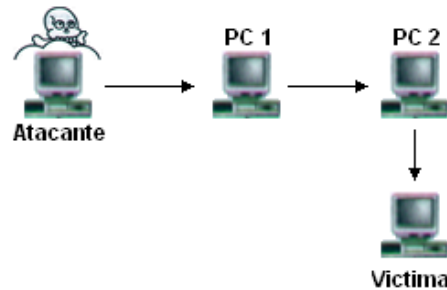


Gráfico 7.3 – Ataque Spoofing

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 (ver Anexo II).

7.4.5.2.2 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.

7.4.5.3 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.

7.4.5.4 IP SPLICING–HIJACKING

Se produce cuando un atacante consigue interceptar una sesión ya establecida. El atacante espera a que la víctima 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 autenticación 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 = F454FDF5
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 = F454FDF5 (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 : 195.1.1.1 Puerto 1025
IP Destino: 195.1.1.2 Puerto 23
SEQ = 3DF454E4 (ACK enviado por el servidor)
ACK = F454FDFF
Datos: Confirmación de Recepción (ACK)

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:

1° Paquete ACK Cliente = F454FDF5
2° Paquete ACK Cliente = F454FDFF
Tamaño del campo datos = F454FDFF - F454FDF5 = **0A**

5. Hecho esto el atacante envía un paquete con la 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 + 0A)

El servidor al recibir estos datos no detectará el cambio de origen ya que los campos que ha recibido como secuencia y ACK son los 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 descrito.

7.4.5.5 UTILIZACIÓN DE BACKDOORS

“Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autenticación para realizar ciertas tareas.

Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo”⁴⁵.

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 control normales.

7.4.5.6 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 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 hallado 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.

7.4.5.7 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 esta 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 capítulos posteriores.

7.4.5.7.1 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 hallada.

⁴⁵ HUERTA, Antonio Villalón. “Seguridad en Unix y redes”. Versión 1.2 Digital – Open Publication License v.10 o Later. 2 de Octubre de 2000. Capítulo 5–Página 81. <http://www.kriptopolis.com>

Actualmente es posible encontrar diccionarios de gran tamaño orientados, incluso, a un área específico de acuerdo al tipo de organización que se este atacando.

En la tabla 7.4 podemos observar el tiempo de búsqueda de una clave de acuerdo a su longitud y tipo de caracteres utilizados. La velocidad de búsqueda se supone en 100.000 passwords por segundo, aunque este número suele ser mucho mayor dependiendo del programa utilizado.

| Cantidad de Caracteres | 26–Letras minúsculas | 36–Letras y dígitos | 52–Mayúsculas y minúsculas | 96–Todos los caracteres |
|-------------------------------|-----------------------------|----------------------------|-----------------------------------|--------------------------------|
| 6 | 51 minutos | 6 horas | 2,3 días | 3 meses |
| 7 | 22,3 horas | 9 días | 4 meses | 24 años |
| 8 | 24 días | 10,5 meses | 17 años | 2.288 años |
| 9 | 21 meses | 32,6 años | 890 años | 219.601 años |
| 10 | 45 años | 1.160 años | 45.840 años | 21.081.705 años |

Tabla 7.4 – Cantidad de claves generadas según el número de caracteres empleado

Aquí puede observarse la importancia de la utilización de passwords con al menos 8 caracteres de longitud y combinando todos los caracteres disponibles. En el siguiente Capítulo podrá estudiarse las normas de claves relativamente seguras y resistentes.

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, existen 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 o 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 más 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, acumula 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 está 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 un 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 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 máquina, 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 mas 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 sino 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 simultaneas. 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 con 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 máquina 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 hosts mandarán una respuesta a la víctima cuya dirección IP figura en el paquete ICMP.

Gráficamente:

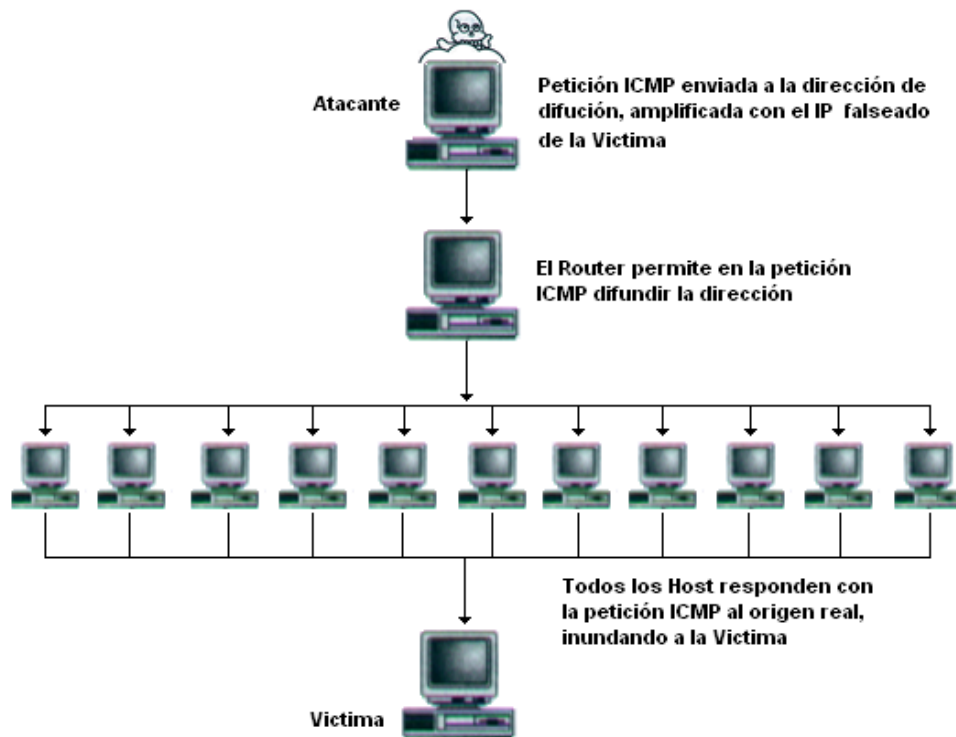


Gráfico 7.4 – Ataque Smurf

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 está 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 son las máquinas/redes que puedan actuar de intermediarias (inocentes) en el ataque y no 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 OOB, SUPERNUKE O WINNUKE

Un ataque característico, y quizás el más común, de los equipos con 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 a un 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 suministrado 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 superponen, haciendo que el sistema se cuelgue. Windows NT[®] 4.0 de Microsoft[®] es especialmente vulnerable a este ataque. Aunque existen Patches (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 solicitados el mensaje o no. Es muy utilizado por las empresas para publicitar 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 DIDDLE

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 o 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 manifiestos) terroristas o humorísticos, como el ataque de The Mentor, ya visto, a la NASA; o la reciente modificación del Web Site del CERT (mayo de 2001).

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

El 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 la 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 que 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 expertos⁴⁶ especializados en descubrir fallas de seguridad⁴⁷ 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 mucho 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 ACTIVEX

ActiveX es una de las tecnologías más potentes que ha desarrollado Microsoft[®]. Mediante ActiveX es posible reutilizar código, descargar código totalmente funcional de un sitio remoto, etc. Esta tecnología es considerada la respuesta de Microsoft[®] a Java.

ActiveX soluciona los problemas de seguridad mediante certificados y firmas digitales. Una Autoridad Certificadora (AC) expende un certificado que acompaña a los controles activos y a una firma digital del programador.

Cuando un usuario descarga una página con un control, se le preguntará si confía en la AC que expendió el certificado y/o en el control ActiveX. 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 acarrear la acción o un perfecto novato en la materia.

Esta última característica es el mayor punto débil de los controles ActiveX 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.

⁴⁶ Safe Internet Programming: Creadores sobre seguridad en Java <http://www.cs.princeton.edu/sip>

⁴⁷ Hostile Applets Home Page (HAHP): Seguridad en Java. Dr. Mark D. LaDue.
<http://www.rstcorp.com/hostile-applets>

La filosofía ActiveX 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 alemanes⁴⁸, desarrolló un control ActiveX 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 víctima se conectara a su banco, se iniciara automáticamente una transferencia a una cuenta del grupo alemán .

Otro control ActiveX muy especialmente “malévolo” es aquel que manipula 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 autenticación de usuarios mediante Certificados y las Autoridades Certificadoras será abordada con profundidad en capítulos posteriores.

7.4.7.6 VULNERABILIDADES EN LOS NAVEGADORES

Generalmente los navegadores no fallan por fallos intrínsecos, sino que fallan las tecnologías que implementan, aunque en este punto analizaremos realmente fallos intrínsecos de los navegadores, como pueden ser los “Buffer Overflow”⁴⁹.

Los “Buffer Overflows” consisten en explotar una debilidad relacionada con los buffers que la aplicación usa para almacenar las entradas de usuario. Por 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 protocolo usado puede 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.

Además la reciente aparición (octubre de 2000) de vulnerabilidades del tipo Transversal en el servidor Web Internet Information Server[©] de la empresa Microsoft[®], explotando fallas en la traducción de caracteres Unicode, puso de manifiesto cuan fácil puede resultar explotar una cadena no validada. Por ejemplo:

```
www.servidor.com/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
```

devuelve el directorio de la unidad c: del servidor deseado.

Para poder lanzar este tipo de ataques hay que tener un buen conocimiento de lenguaje Assembler y de la estructura interna de la memoria del sistema operativo utilizado o bien, leer la documentación de sitios web donde explican estas fallas.

⁴⁸ Computers Chaos Club. <http://www.ccc.de>

⁴⁹ http://www.newhackcity.net/win_buff_overflow

También se puede citar el fallo de seguridad descubierto por Cybersnot Industries[®] relativo a los archivos “.lnk” y “.url” de Windows 95[®] y NT[®] respectivamente. Algunas versiones de Microsoft Internet Explorer[®] podían ser utilizadas para ejecutar la aplicación que se deseara siempre que existiera en la computadora de la víctima (por ejemplo el tan conocido y temido *format.com*).

Para más información relacionada con los ataques intrínsecos a los navegadores, se aconsejan las páginas no oficiales de seguridad tanto en Internet Explorer^{®50} como en Netscape Communicator^{®51}.

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 variadas 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 clase de servicios informáticos disponibles.

Los Sistemas operativos abiertos (como Unix y Linux) tienen agujeros mas conocidos y controlados que aquellos que existen en sistemas operativos cerrados (como 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 IMPLEMENTACIÓN DE ESTAS TÉCNICAS

A lo largo de mi investigación he recopilando distinto tipos de programas que son la aplicación de las distintas técnicas enumeradas anteriormente. La mayoría de las mismos son encontrados fácilmente en Internet en versiones ejecutables, y de otros se encuentra el código fuente, generalmente en lenguaje C, Java y Perl.

Cada una de las técnicas explicadas pueden ser utilizadas 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.

⁵⁰ <http://www.nwnetworks.com/iesf.html>

⁵¹ <http://hplyot.obspm.fr/~dl/netscapesec>

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 identificarán 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 propiamente dicha: 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 administrados 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.

El anexo III se brinda una lista de herramientas disponibles, las cuales son la implementación de las técnicas estudiadas.

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 todos 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. Medidas 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. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.
8. Por último, pero quizás lo más importante, **la capacitación continua 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.

Pero como siempre en esta oscura realidad existe una parte que es cierta y otra que no lo es tanto. Para aclarar este enigma veamos porque se eligió la palabra 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 con exactitud 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).⁵²

“Un virus responde al modelo DAS: Dañino, Autorreplicante y Subrepticio.”⁵³

Virus Biológico (VB): Fragmentos de ADN o ARN cubiertos de una capa proteica. Se reproducen solo en el interior de células vivas, para lo cual toman el control de sus enzimas y metabolismo. Sin esto son tan inertes como cualquier otra macromolécula.⁵⁴

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 sí 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 que esta dentro de un cajón.
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.

¹⁶⁻¹⁸ Revista Virus Reports. Ediciones Ubik Número 16–Página 2.

⁵³ Dr Fred Cohen. Considerado el padre de los VI y de sus técnicas de defensa: <http://all.net>

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 replicación 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 diversa 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 está!); o viceversa: de RAM infectada a un disquete sano; o directamente aprovechando un flujo de 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 más las analogías que pueden encontrarse haciendo un análisis más exhaustivo de ambas entidades, pero que trascenderían 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 e intenciones apropiadas del caso.

7.5.2 ORIGEN

Los orígenes de los VI se puede 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 Hupp 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, Viernes 13, 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 Cohen⁵⁵:

“El 3 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 ocho horas de trabajo sobre un VAX 11/750 ejecutando Unix, el primer virus estuvo listo para la demostración. En esa semana fueron obtenidos los permisos y cinco experimentos fueron realizados. El 10 de noviembre el virus fue mostrado. La infección inicial fue realizada en “vd” (un programa que mostraba la estructura de archivos 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 qué podía hacer 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 fue el 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 usuarios de ordenadores personales, aunque en cierto modo también sirvió para concientizar 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.

⁵⁵ Dr Fred Cohen. Considerado el padre de los VI y de sus técnicas de defensa: <http://all.net>

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 en circulación hasta límites insospechados. Si a finales de 1994 el número de virus, según la International Computer Security Association (ICSA), rondaba los cuatro mil, 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 NCSA⁵⁶ es el principal organismo dedicado al seguimiento del fenómeno de los 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 alguno 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%.

Existen virus adscritos a programa y también a documentos, los conocidos como Macrovirus. Estos últimos, concretamente los que utilizan documentos de MS-Word[®] para la infección comenzaron su propagación en 1995, cuando Microsoft[®] lanza su nueva versión de este popular procesador de texto.

Aprovechando esta innovación tecnológica (las macros), han aparecido más de 1.900 virus diferentes, registrados y catalogados, que utilizan este medio para infectar los documentos. Tal ha sido su crecimiento y extensión, que los principales responsables de la lucha antivirus llegaron a recomendar que no se enviaran ni se aceptaran documentos de MS-Word[®] enviados por Internet, lo que supone una fuerte limitación al uso del correo electrónico. Entre los diez virus más importantes de 1997, cuatro eran macros de Word.

Según la NCSA, si sólo un 30% de todos las PCs del mundo utilizaran un antivirus actualizado y activo de forma permanente, se cortaría la cadena de contagio y se acabaría con el fenómeno de los virus en todo el mundo.

Sin embargo, no todos los usuarios, bien sean de carácter empresarial o doméstico, son conscientes del riesgo que corren. Hace un tiempo bastaba con chequear los nuevos programas o archivos que se introducían en la computadora, teniendo especial cuidado con el software pirateado (principal forma de contagio) y con los disquetes usados provenientes de otras personas. De alguna manera, las vías de transmisión eran menores y estaban más controladas. Pero con Internet, las posibilidades de infección se han multiplicado con creces.

Desde el 17 al 31 de julio del año 2000 el Ministerio de Ciencia y Tecnología de España, la empresa antivirus Panda Software y otras organizaciones montaron la Primera Campaña Nacional Antivirus Informáticos⁵⁷. El propósito de la campaña era ofrecer al usuario

⁵⁶ NCSA: National Computer Security Association. <http://www.ncsa.com>

⁵⁷ Campaña Nacional Antivirus Informáticos. <http://www.sinvirus.com>

la posibilidad de búsqueda de virus en su sistema (en forma on-line) y desinfección del mismo.

Al finalizar la campaña, se obtuvieron 516.122 visitas al sitio y se eliminaron 348.195 virus. Las vías de infección informadas fueron el 56% vía e-mail, el 31% vía disquete y el 5% vía CD-ROM.

A nivel mundial, en el ámbito de las medianas y grandes empresas, históricamente, la mayor causa de pérdidas de información fue el sabotaje, seguido por los virus informáticos y por último por otras causas como fallas e impericias. Durante 1993 y 1994 las pérdidas por virus superaron las ocasionadas por sabotaje, pero a partir de 1995 el sabotaje volvió a ocupar el primer lugar debido a la utilización de virus específicos.

Según la NCSA en 1995 el volumen de pérdidas causadas en los Estados Unidos por VI era similar al de las pérdidas por Hacking y alcanzaban los US\$1.000 millones. En 1996 las pérdidas por VI aumentaron en mayor proporción que las causadas por intrusos informáticos alcanzando los US\$5.000 millones y US\$6.000 millones respectivamente

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 dependen de un sistema operativo en particular, ya que un documento puede ser procesado tanto en Windows® 95/98/NT/2000®, como en una Macintosh u otras.

7.5.4.1 TÉCNICAS DE PROPAGACIÓN

Actualmente las técnicas utilizadas por los virus para logra 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 la computadora del usuario. En las últimas 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. **Páginas web y transferencia 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 lo 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 que su “programa” pudiera ejecutarse. Estas son diversas y algunas de lo más ingeniosas:

7.5.4.2.1 Archivos Ejecutable (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.

Ejemplos: Chernovil, Darth Vader, PHX

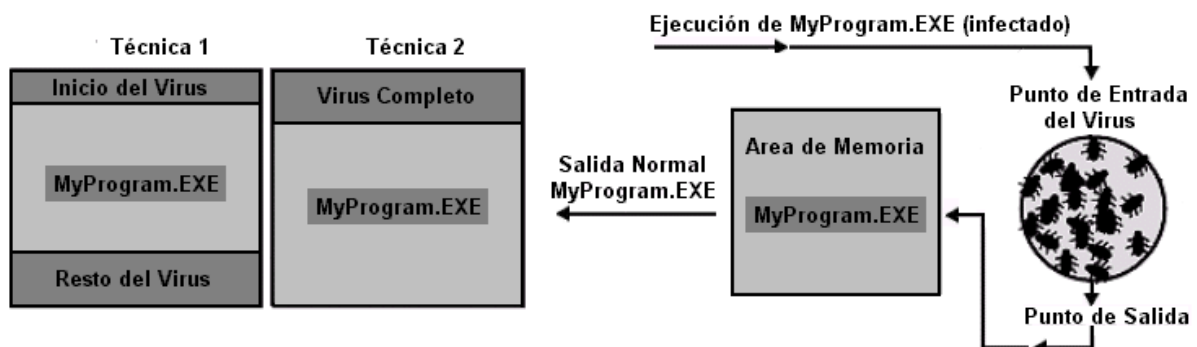


Gráfico 7.5 – Técnicas de Infección en Archivos Ejecutables

7.5.4.2.2 Virus en el Sector de Arranque (Virus ACSO 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 o los 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.

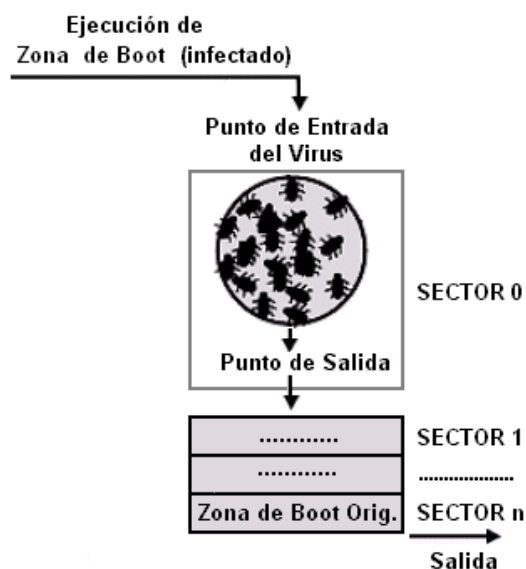


Gráfico 7.6 – Técnica de infección en Zona de Booteo

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 está 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.

Ejemplos: 512, Avispa, Michelangelo, DIR II.

7.5.4.2.4 Macrovirus

Estos virus infectan archivos de información generados por aplicaciones de oficina que cuentan con lenguajes de programación de macros. Últimamente son 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 para el procesador 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

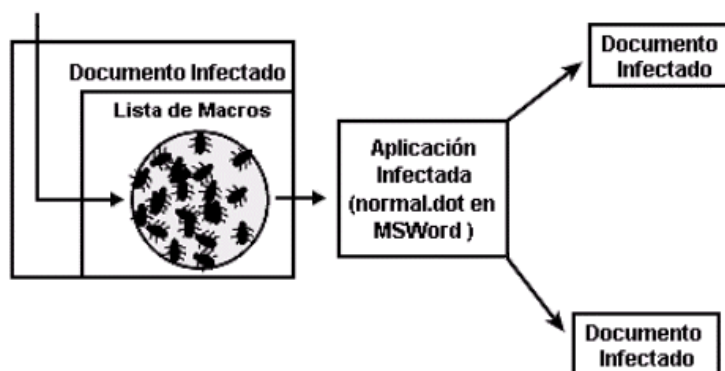


Gráfico 7.7 – Infección de múltiples Documentos

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 y I Love You. 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 contruidos para sabotear un sistema o entorno específico. 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 Fantasma

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 solidarias, 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 consecuentes 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 sí 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 desconocía, 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 las características 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 Orifice 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 mas 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 la información o provoca la baja del 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. **Módulo de Reproducción:** es el encargado de manejar las rutinas de parasitación de entidades ejecutables con el fin de que el virus pueda ejecutarse subrepticamente, 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. **Módulo 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.



Gráfico 7.8 – Módulos de los Virus Informáticos

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 desenvuelve el virus ya que el consumo de ciclos de reloj en un medio delicado (como un aparato biomédico) puede causar un gran daño.

- b. **Daño Explícito:** 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. Deshacerse 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 utilizar la 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 también infectadas. Puede que se llegue a encontrar una copia 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:** los 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 hay 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 ¡18 meses! de prisión al autor de SMEG. Sin embargo, el autor del virus Loverletter no fue sentenciado porque 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 informática 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, sólo aparecen unos cinco totalmente novedosos al año.

Debe tenerse en cuenta que:

- Un programa antivirus forma parte del sistema y por lo tanto funcionará correctamente si es adecuado y está bien configurado.
- 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 esta acción:
 - 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 controlada por el usuario (MBR, Boot Sector, FAT, y otras). Su principal ventaja reside en que es capaz de detectar virus que no han sido agregados a las base de datos de los antivirus (técnica proactiva). Su desventaja radica en que puede “sospechar” de demasiadas cosas y el usuario debe ser medianamente capaz de identificar falsas alarmas.
3. **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.



Gráfico 7.9 – Modelo de un Antivirus

- **Módulo de Control:** Este módulo posee la técnica de Verificación de Integridad que posibilita el registro de posibles cambios en las zonas y archivos considerados de riesgo.
- **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 sea 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 desinstalación desde la misma. 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 la 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”.

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 causar 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 diseminador 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 previo puede ser calificado 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 basta con tener un antivirus, sino 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.

En la Campaña Nacional Antivirus Informáticos se proponen 15 consejos para evitar el contagio de virus⁵⁸. A continuación se resumen todas ellas:

- VII. Instalar un buen antivirus para la detección y eliminación de nuevos virus. Además es necesario actualizarlo frecuentemente. Como ya se ha explicado la efectividad de un programa antivirus reside, en gran medida, en su capacidad de actualización (preferentemente diaria).
- VIII. Comprobar que el antivirus elegido incluye soporte técnico, resolución urgente de nuevos virus y servicios de alerta, bien a través de correo electrónico, por teléfono o fax.
- IX. Asegurarse que el antivirus esté siempre activo vigilando constantemente todas las operaciones realizadas en el sistema.
- X. Verificar, antes de abrir, cada nuevo mensaje de correo electrónico recibido. Este medio es el medio de transmisión preferido por los diseminadores de virus. Cualquier correo puede contener virus, aunque no este acompañado de archivos adjuntos. Además no es necesario ejecutar el archivo adjunto de un mensaje de correo para ser infectado, en algunos sistemas basta únicamente con abrir el mensaje. Para prevenir esto, lo mejor es verificar los mensajes inesperados o que provengan de una fuente poco habitual.
- XI. Evitar la descarga de programas de lugares no seguros o pocos fiables de Internet. Muchas páginas web permiten la descarga de programas y archivos cabiendo la posibilidad que estos archivos estén infectados. Son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen.
- XII. Rechazar archivos que no se hayan solicitado cuando se esté en chats o grupos de noticias. Hay que tener especial cuidado y aceptar sólo lo que llegue de un remitente conocido y de confianza.
- XIII. Analizar siempre con un buen antivirus los disquetes que entran y salen de la computadora. Si se utilizan disquetes propios en otros lugares es aconsejable protegerlos contra escritura.
- XIV. Retirar los disquetes de las disqueteras al apagar o reiniciar el ordenador. Esta tarea es para evitar que se activen los virus de arranque.
- XV. Analizar el contenido de los archivos comprimidos. El antivirus deberá de contar con una funcionalidad que permita detectar el mayor número de formatos comprimidos posibles. Además, antes de abrir uno de estos archivos, es aconsejable guardarlos en carpetas temporales.
- XVI. Mantenerse alerta ante acciones sospechosas de posibles virus. Hay varios síntomas que pueden delatar la presencia de nuevos virus: aumento del tamaño de los archivos, aviso de macros en documentos, ralentización en ciertos procesos, etc. Como mejor solución a estas sospechas de posibles infecciones, se debe recurrir al servicio de resolución urgente de nuevos virus de la compañía antivirus.

⁵⁸ Para más información referirse a <http://www.sinvirus.com>

- XVII. Añadir las opciones de seguridad de las aplicaciones que se utilizan normalmente en la política de protección antivirus, ya que los programas informáticos más utilizados se convierten, precisamente por esta razón, en blanco de los autores de virus.
- XVIII. Realizar copias de seguridad frecuentes y periódicas de la información más importante. Esta es una muy buena forma de minimizar el impacto de un virus. De esta manera, una pérdida de datos, causada por un virus, puede ser superada mediante la restauración de la última copia.
- XIX. Ante la gran cantidad de información recibida por diferentes medios, es aconsejable contrastar estos datos con la información completa, actualizada y experta difundida por determinadas compañías y organismos confiables.
- XX. A la hora de instalar nuevos programas, el riesgo de infección es menor (aunque no nulo) si se trata de software legal. Si el software ha llegado de fuentes piratas nadie puede asegurar que esté libre de virus.
- XXI. Exigir a los fabricantes de software, proveedores de acceso a Internet y editores de publicaciones, que se impliquen en la lucha contra los virus. En la lucha contra los virus es precisa la participación de todos los agentes implicados en el sector informático para minimizar el problema de las infecciones provocadas.

CAPÍTULO 8



“Esto es lo que llamamos Criptograma, en el cual el sentido está oculto bajo letras embarulladas a propósito y que, convenientemente dispuestas, formarían una frase inteligible —dijo el profesor—

Viaje al centro de la tierra. Julio Verne

PROTECCIÓN

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

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

En el presente capítulo, después de lo 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 representarán el 100% de la seguridad deseado, aunque muchas parezcan la panacea, será la suma 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 esto. En lo que sí 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. Ardita⁵⁹: “(...) 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 y los sistemas de rastreo de intrusiones”.

Al conjunto de técnicas que se utilizan para evaluar y probar la seguridad de una red se lo conoce como Penetration Testing, uno de los recursos más poderosos con los que se cuenta hoy para generar barreras cada vez más eficaces.

Un test está totalmente relacionado con el tipo de información que se maneja en cada organización. Por consiguiente, según la información que deba ser protegida, se determinan la estructura y las herramientas de seguridad; no a la inversa

El software y el Hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina “políticas de seguridad internas” 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.
- **Auditoría:** se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

⁵⁹ ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. <http://www.cybsec.com>

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su “voluntad de hacer algo” que permita detener un posible ataque antes de que éste suceda (proactividad). A continuación se citan algunos de los métodos de protección más comúnmente empleados.

1. **Sistemas de detección de intrusos:** son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.
2. **Sistemas orientados a conexión de red:** monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (Firewalls) y los Wrappers.
3. **Sistemas de análisis de vulnerabilidades:** analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La “desventaja” de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.
4. **Sistemas de protección a la integridad de información:** sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger. Algunos ejemplos son los programas que implementan algoritmos como Message Digest (MD5) o Secure Hash Algorithm (SHA), o bien sistemas que utilizan varios de ellos como PGP, Tripwire y DozeCrypt.
5. **Sistemas de protección a la privacidad de la información:** herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos entidades. Dentro de este tipo de herramientas se pueden 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 capas que pueden ser incorporadas de manera progresiva al modelo global de seguridad en la organización, logrando así el método más efectivo para disuadir el uso no autorizado de sistemas y servicios de red. Podemos considerar que estas capas son:

1. Política de seguridad de la organización.
2. Auditoría.
3. Sistemas de seguridad a nivel de Router–Firewall.
4. Sistemas 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 existan, tanto internos como remotos.”⁶⁰

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

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

- **Penetration Test Externo:** el objetivo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde fuera del Firewall y consisten en penetrar la Zona Desmilitarizada para luego acceder a la red interna. Se compone de un elevado número de pruebas, entre las que se puede nombrar:
 - Pruebas de usuarios y la “fuerza” de sus passwords.
 - 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 de realización del Test.
 - Prueba de ataques de Denegación de Servicio.
- **Penetration 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 un 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.

⁶⁰ ARDITA, Julio Cesar. “Prueba de Vulnerabilidad”. ©1996–2001 CYBSEC S.A.
<http://www.cybsec.com/0302.htm>

- 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 HONEYPOTS–HONEYNETS

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

Actualmente un equipo de Honeynet Project⁶¹ 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 Honeynets dan a los crackers un gran espacio para recorrer. Presentan obstáculos que poseen el nivel de complejidad suficiente para atraerlos, pero sin irse al extremo para no desalentarlos (...). Ellos juegan con los archivos y conversan animadamente entre ellos sobre todos los ‘fascinantes programas’ que encuentran, mientras el personal de seguridad observa con deleite cada movimiento que hacen”, dijo Dan Adams. “Francamente, siento una combinación de sentimientos con respecto a espiar a la gente, aunque no sean buenas personas”⁶².

Esta última frase se está presentando a menudo en el tema de la investigación (y vigilancia) electrónica. Este es el caso del ex–director del proyecto Honeynet J. D. Glaser, quien renunció a su puesto después de aclarar que está convencido “que la vigilancia electrónica no es correcta, aunque se utilice en aras de la investigación (...). Ampliar un Honeynet es parecido a entrapar los derechos de otros, aunque sean los derechos de un delincuente.”

Con respecto a algunos de los resultados obtenidos por el grupo de investigación puede observarse el siguiente ejemplo:

A un intruso le tomo menos de un minuto irrumpir en la computadora de su universidad a través de Internet, estuvo dentro menos de media hora y a los investigadores le tomo 34 horas descubrir todo lo que hizo.

Se estima que esas 34 horas de limpieza pueden costar U\$2.000 a una organización y U\$22.000 si se debiera tratar con un consultor especializado.

⁶¹ Honeynet Project: <http://project.honeynet.org>

⁶² ADAMS, Dan. Administrador de los sistemas London SecTech, quien sigue de cerca el proyecto Honeynet.

8.2 FIREWALLS

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar 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 la Ingeniería Social y el ataque de Insiders.

Un **Firewall** es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

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

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

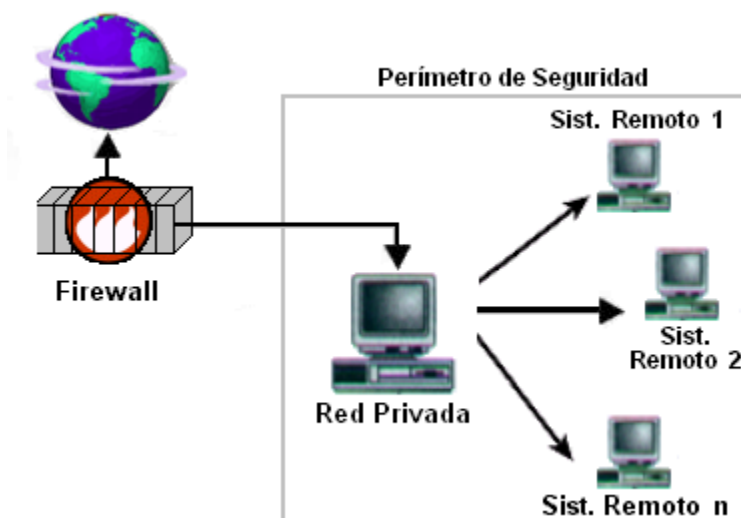


Gráfico 8.1 – Firewall

Como puede observarse, el Muro Cortafuegos, sólo 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–desencriptación 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 Routers (enrutadores a nivel de Red).

Los Routers son dispositivos electrónicos encargados de establecer comunicaciones externas y de convertir los protocolos utilizados en las LAN en protocolos de WAN y viceversa.

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

La evolución tecnológica les ha permitido transformarse en computadoras muy especializadas capaz de determinar, si el paquete tiene un destino externo y el camino más corto y más 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 máquina correspondiente o devuelve el paquete a su origen en caso de que él 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 más 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 máquinas la comunicación está 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 80 abierto) 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 en 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, por lo que exponen la red al mundo exterior.

4. Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.
5. No soportan políticas de seguridad complejas como autenticación 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 máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma. Gráficamente:



Gráfico 8.2 – Bastión Host

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 desactivado”.

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 de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior.

Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior.

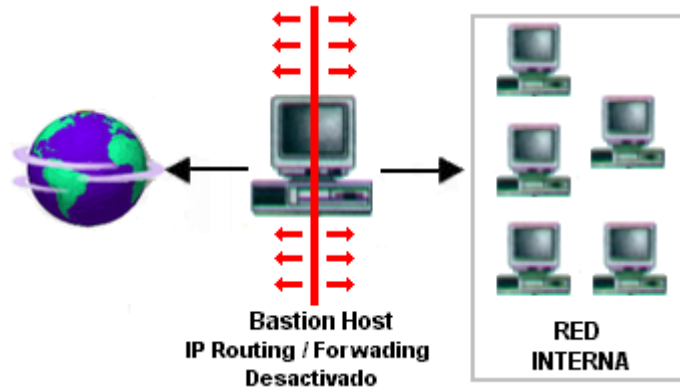


Gráfico 8.3 – Dual-Homed Host

8.2.2.4 SCREENED HOST

En este caso se combina un Router con un host bastión 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 sólo se permiten un número reducido de servicios.



Gráfico 8.4 – Screened Host

8.2.2.5 SCREENED SUBNET

En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga 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 hacia la red externa. El Router interior hace lo mismo con 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 simplificarían a uno solo.

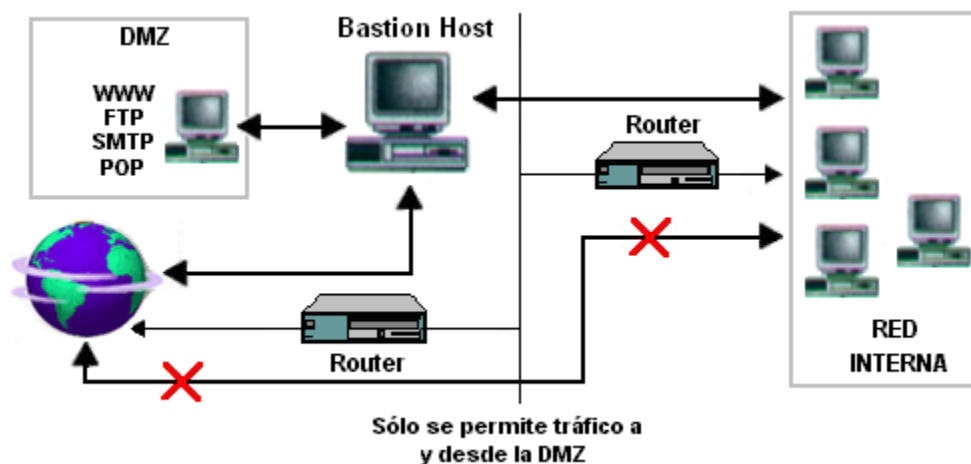


Gráfico 8.5 – Screened Hosted

Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separados de los servicios públicos. Además, no existe una conexión directa entre la red interna y la externa.

Los sistemas Dual-Homed Host y Screened 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 grado 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 solicitada 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 del filtrado de los paquetes por parte del Router serán menos compleja dado a que él sólo debe atender las solicitudes del Gateway.

Así mismo tiene la desventaja de ser intrusivos 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 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 se 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 a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple “cuelgue” o infección de virus hasta la pérdida de toda su información almacenada.

8.2.3 POLÍTICAS DE DISEÑO DE FIREWALLS

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

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

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

- ¿Qué se debe proteger?. Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).
- ¿De quién protegerse?. De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir.

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

- ¿Cómo protegerse?. Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:

c. 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.

d. Estrategias de seguridad

- Paranoica: se controla todo, no se permite nada.
- Prudente: se controla y se conoce todo lo que sucede.
- Permisiva: se controla pero se permite demasiado.
- Promiscua: no se controla (o se hace poco) y se permite todo.

- ¿Cuánto costará?. Estimando en función de lo que se desea proteger se debe decidir cuanto es conveniente invertir.

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:** este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

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

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 expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada maquina interna.

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

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

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

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

8.2.6 LIMITACIONES DE UN FIREWALL

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

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

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

Finalmente, un Firewall es vulnerable, él NO protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna. Como moraleja: “cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menor será la resistencia contra los paquetes externos. El único Firewall seguro (100%) es aquel que se mantiene apagado”⁶³

8.3 ACCESS CONTROL LISTS (ACL)

Las Listas de Control de Accesos proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

8.4 WRAPPERS

Un Wrapper es un programa que controla el acceso a un segundo programa. El Wrapper literalmente cubre la identidad de este segundo programa, obteniendo con esto un más alto nivel de seguridad. Los Wrappers son usados dentro de la seguridad en sistemas UNIXs. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento.

Los Wrappers son ampliamente utilizados, y han llegado a formar parte de herramientas de seguridad por las siguientes razones:

- Debido a que la seguridad lógica esta concentrada en un solo programa, los Wrappers son fáciles y simples de validar.

⁶³ HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet. Boletín de Política Informática N° 2. Página 7. España. 2000.

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

El paquete Wrapper más ampliamente utilizado es el TCP-Wrappers, el cual es un conjunto de utilidades de distribución libre, escrito por Wietse Venema (co-autor de SATAN, con Dan Farmer, y considerado el padre de los sistemas Firewalls) en 1990.

Consiste en un programa que es ejecutado cuando llega una petición a un puerto específico. Este, una vez comprobada la dirección de origen de la petición, la verifica contra las reglas almacenadas, y en función de ellas, decide o no dar paso al servicio. Adicionalmente, registra estas actividades del sistema, su petición y su resolución.

Algunas configuraciones avanzadas de este paquete, permiten 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 máquina atacante, en el caso de un intento de conexión, para tener más 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 pensarse 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 máquina y los servicios accedidos. Así, estos controles son el complemento perfecto de un Firewall y la instalación de uno no está supeditada a la del otro.

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 abordados, si bien son eficaces, distan mucho de ser la protección ideal.

Así, debe estar fuera de toda discusión la conveniencia 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 sospechosas (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 él, 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 a 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 él mayor seguridad.

8.5.1 INTRUSIÓN DETECTION 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 anómala desde el exterior–interior de un sistema informático.

Los sistemas de detección de intrusos pueden clasificarse, según su función y comportamiento en:

- **Host–Based IDS:** operan 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 esperado 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 actuará como un usuario comprometido; su comportamiento se alejará 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 sí solas no constituyen un comportamiento intrusivo de ningún tipo. Así las intrusiones pueden clasificarse 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, porque 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 ignorarán 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 cuánto 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 esté 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 está siendo observado. Sin embargo, no debe ser una “caja negra” (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 sí mismo para asegurarse de que no ha sido perturbado.
- Debe imponer mínima sobrecarga sobre el sistema. Un sistema que relentiza la máquina, simplemente no será utilizado.
- Debe observar desviaciones sobre el 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 se 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 dónde 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 está 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 imprevistas. Pueden incluso contribuir (parcialmente) al descubrimiento automático de esos nuevos ataques.
- Son menos dependientes de los mecanismos específicos de cada sistema operativo.
- Pueden ayudar a detectar ataques del tipo “abuso de privilegios” que no implica realmente ninguna 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 sustituto para un buen Firewall, una auditoría 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 re-entrenamiento 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 pasar por el usuario, la llamada se devolverá al usuario legal y no al del intruso, siendo este desconectado. Como precaución adicional, el usuario deberá verificar que la llamada-retorno proceda del número a donde llamó previamente.

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 red, para detectar el modo en el cual está actuando (recordar que un Sniffer la coloca en Modo Promiscuo), y el tráfico de datos en ella.

8.8 GESTION DE CLAVES “SEGURAS”

Como ya se vio en el capítulo anterior (ver Tabla 7.4), si se utiliza una clave de 8 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 96^8 (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, comúnmente llamadas Claves Débiles.

Según demuestra el análisis de +NetBul⁶⁴ realizado sobre 2.134 cuentas y probando 227.000 palabras por segundo:

- Con un diccionario 2.030 palabras (el original de John 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 estudio⁶⁵ 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, sería válido 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 secuencias alfabéticas tipo ‘abcd’; a secuencias numéricas tipo ‘1234’; a secuencias observadas en el teclado tipo ‘qwer’; a palabras que existen en un diccionario del lenguaje del usuario?. Sí, estas claves (las más 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 víctima (Ingeniería Social) ya que podrá probar palabras relacionadas a su persona o diccionarios orientados.

⁶⁴ +NetBul. Tabla de Tiempos del John the Ripper 1.4. SET N°15-0x07. Junio de 1998.
<http://www.vanhackez.co/set> – <http://www.thepentagon.com/paseante>

⁶⁵ KLEIN, Daniel V. Foiling the Cracker: A Survey of, and Improvement to, Password Security.

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 máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.
6. Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:
 - Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3
 - Usar un acrónimo de alguna frase fácil de recordar: A rio Revuelto Ganancia de Pescadores → ArRGdP
 - Añadir un número al acrónimo para mayor seguridad: A9r7R5G3d1P
 - Mejor incluso si la frase no es conocida: Hasta Ahora no he Olvidado mi Contraseña → aHoelIo
 - Elegir una palabra sin sentido, aunque pronunciable: taChunda72, AtajulH, Wen2Mar
 - Realizar reemplazos de letras por signos o números: En Seguridad Más 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 algunas 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 se es administrador del sistema, repasar este hecho periódicamente.
2. No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas de 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 tácita de buen usuario no mirar el teclado mientras alguien teclea 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 cíclicamente (por lo menos 5).

Muchos sistemas incorporan ya algunas medidas de gestión y protección de las contraseñas. Entre ellas podemos citar las siguientes:

1. Número de intentos limitado. Tras un número de intentos fallidos, pueden tomarse distintas medidas:
 - Obligar a reescribir el nombre de usuario (lo más común).
 - Bloquear el acceso durante un tiempo.
 - Enviar un mensaje al administrador y/o mantener un registro especial.
2. Longitud mínima. Las contraseñas deben tener un número mínimo de caracteres (se recomienda 7 u 8 como mínimo).
3. Restricciones de formato. Las contraseñas deben combinar un mínimo de letras y números, no pueden contener el nombre del usuario ni ser un blanco.
4. Envejecimiento y expiración de contraseñas. Cada cierto tiempo se fuerza a cambiar la contraseña. Se obliga a no repetir ciertas cantidad de las anterior. Se mantiene un periodo forzoso entre cambios, para evitar que se vuelva a cambiar inmediatamente y se repita la anterior.
5. 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 SÓLO USO

Las contraseñas de un solo uso (One–Time Passwords) son uno de los mecanismos de autenticación 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 serían las basadas en funciones unidireccionales (sencillas de evaluar en un sentido pero imposible o muy costoso de evaluar en 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 o 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 en 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 le protege en caso de robo o pérdida.

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 preverse todos estos protocolos tienen su debilidad ya sea en su implementación o en su uso. A continuación se describen 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 ofrecerán las potenciales puertas de entrada como fuentes de ataques que ni siquiera tienen por qué proporcionar acceso a la máquina (como las DoS por ejemplo).

De esta forma, si cada servicio ofrecido es un posible problema para la seguridad, parece claro que lo ideal sería no ofrecer ninguno, poseer una máquina completamente aislada del 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 empleado en las redes Microsoft® para la autenticación 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 deben 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. Está claro que esto es fácilmente aprovechable por un intruso para practicar ingeniería social contra esos usuarios.

Es básico deshabilitar este servicio, restringir su acceso a unos cuantos equipos de la red local o utilizar versiones de Finger que permiten especificar la información que se muestra al acceder al servicio.

8.9.4 POP

El servicio POP (puertos 109 y 110 en TCP) utilizado para que los usuarios puedan acceder a su correo sin necesidad de montar un sistemas de archivos compartidos. Se trata de un servicio que se podría 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 puede acceder.

Mediante POP se genera un tránsito peligroso de contraseñas a través de la red. Se ofrece tres modelos distintos de autenticación: uno basado en Kerberos, apenas utilizado, otro basado en un protocolo desafío–respuesta, y el otro basado en un simple nombre de usuario con su password correspondiente.

Este último, el más usado en todo tipo de entornos, es un excelente objetivo para un intruso con un Sniffer. Los usuarios suelen configurar sus clientes para que chequeen el buzón de correo cada pocos minutos, con lo que a intervalos muy cortos envían su clave a un puerto conocido de una máquina conocida; al realizar toda esta comunicación en texto claro, un atacante no tiene más que interceptar la sesión POP para averiguar nombres de usuario y claves (a parte de poder leer el correo).

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 máquina cliente para decidir si ofrece el servicio a un determinado host, y si es así, concretar de que forma puede acceder a él (sólo lectura, sólo ciertos grupos, etc.).

De esta forma, los servidores NNTP son muy vulnerables a cualquier ataque que permita falsear la identidad de la máquina origen, como el IP Spoofing.

Los problemas relacionados con las News no suelen ser excesivamente graves desde un punto de vista estrictamente técnico, pero en ocasiones sí 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 envíe mensajes insultantes o pornográficos utilizando el nombre o los recursos de la misma.

Realmente, es muy poco probable que se necesite ofrecer este servicio, por lo que lo más razonable es deshabilitarlo. Generalmente sólo existen servidores de noticias en grandes organizaciones, y si se 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 utilizado para sincronizar relojes de máquinas de una forma muy precisa; a pesar de su sofisticación no fue diseñado con una idea de robustez ante ataques, por lo que puede convertirse en una gran fuente de problemas si no está correctamente configurado.

Son muchos los problemas de seguridad relacionados con un tiempo correcto; el más simple y obvio es la poca fiabilidad que ofrecerá el sistema de Log a la hora de determinar cuándo sucedió determinado evento.

Otro problema inherente a NTP se refiere a la planificación 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 que es habitual tener este 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 transferencia de archivos (puerto 69 basado en UDP) que no proporciona ninguna seguridad. Por tanto en la mayoría de sistemas es deseable (obligatorio) que este servicio esté desactivado. Al utilizar este servicio en ningún momento se solicita un nombre de usuario o una clave, lo que da una idea de los graves problemas de seguridad que ofrece este servicio.

“Gracias” a este protocolo se han implementado algunas de las últimas 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 más que capturar todo ese tráfico y conseguir así un acceso válido al servidor. Incluso puede ser una amenaza a la privacidad de los datos el hecho de que ese atacante también pueda capturar y reproducir (y modificar) los archivos transferidos.

Para solucionar este problema es conveniente dar acceso FTP a pocos usuarios bien identificados y que necesiten utilizarlo, concientizándolos de la utilidad de aplicaciones que cifren todo el tráfico de información (como SSH por ejemplo).

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 máquinas 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 sólo a ese.

8.9.8.2 FTP INVITADO

El otro tipo de acceso FTP es el denominado invitado (guest). La idea de este mecanismo es muy sencilla: se trata de permitir que cada usuario conecte a la máquina 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 conectará 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 máquina servidor. Estos servidores permiten crear usuarios invitados configurando el entorno al que van a conectarse los usuarios, su estructura de directorios–archivos y sus permisos a los recursos.

8.9.9 TELNET

El protocolo TELNET (TCP, puerto 23) permite utilizar una máquina como terminal virtual de otra a través de la red, de forma que se crea un canal virtual de comunicaciones similar (pero mucho más inseguro) a utilizar una terminal físicamente conectada a un servidor.

TELNET es el clásico servicio que hasta hace unos años no se solía deshabilitar nunca: lo más normal es que este servicio esté disponible para que los usuarios puedan trabajar remotamente, al menos desde un conjunto de máquinas determinado.

Evidentemente, reducir al mínimo 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 claro. Cualquier intruso con un Sniffer puede capturar el Login y el password utilizados en una conexión otorgando a cualquiera que lea esos datos un acceso total a la máquina destino. Es muy recomendable no utilizar TELNET para conexiones remotas, sino sustituirlo por aplicaciones equivalentes pero que utilizan cifrado para 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 número indeterminado de máquinas, 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 sólo máquinas registradas envían correo o no permitir que el sistema reenvíe 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:⁶⁶

- **Seguridad en el servidor:** es necesario garantizar que la información almacenada en la máquina servidora no pueda ser modificada sin autorización, que permanezca disponible y que sólo pueda ser accedida por los usuarios a los que les esté legítimamente permitido.
- **Seguridad en la red:** cuando un usuario conecta a un servidor web se produce un intercambio de información entre ambos; es vital garantizar que los datos que recibe el cliente desde el servidor sean los mismos que se están enviando (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 páginas 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 hechos de esta especie seguramente la persona dejará de visitarlas, con la consecuente pérdida 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 número de usuarios en la máquina y minimizar el

⁶⁶ HUERTA, Antonio Villalón. Seguridad en Unix y redes. (Versión 1.2)–Digital Open Publication License v.10 o Later. 2 de Octubre de 2000. Capítulo 11–Página 190. <http://www.kriptopolis.com>.

número de servicios ofrecidos en ella; aunque lo normal es que una máquina dedicada a cualquier tarea, sea también el servidor Web, es recomendable que dicho servidor sea un equipo dedicado sólo a esa tarea.

Los problemas relacionados con servidores Web suelen proceder de errores de programación en los CGIs ubicados en el servidor. La capacidad del CGI para comunicarse con el resto del sistema que alberga las páginas es lo que le otorga su potencia, pero también lo que causa mayores problemas de seguridad: un fallo en estos programas suele permitir a cualquier “visitante” ejecutar órdenes en el sistema.

Una medida de seguridad básica es ejecutar el demonio servidor bajo la identidad de un usuario con privilegios mínimos para que todo funcione correctamente, pero nunca como Administrador, Root o cuenta del sistema.

Para garantizar la seguridad de los datos que circulan entre un cliente y el servidor es casi obligatorio cifrar dichos datos (mediante SSL o utilizando Certificados Digitales por ejemplo).

8.10 CRIPTOLOGÍA

8.10.1 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 sólo 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 más adelante. Durante su reinado, los mensajes de Julio Cesar nunca fueron descifrados.

En el S. XII Roger Bacon y en el S. XV León Batista Alberti inventaron y publicaron sendos algoritmos de encriptación basados en modificaciones del método de Julio César.

Durante la segunda guerra mundial en un lugar llamado Bletchley Park (70 Km al norte de Londres) un grupo de científicos trabajaba en Enigma, la máquina encargada de cifrar los mensajes secretos alemanes.

En este grupo se encontraban tres matemáticos polacos llamados Marian Rejewski, Jerzy Rozycki, Henryk Zygalski y “un joven que se mordía siempre las pieles alrededor de las uñas, iba con ropa sin planchar y era más bien bajito. Este joven retraído se llamaba Alan Turing y había sido reclutado porque unos años antes había creado un ordenador binario. Probablemente poca gente en los servicios secretos ingleses sabía lo que era un ordenador (y mucho menos binario)... pero no cabía duda que sólo alguien realmente inteligente podía inventar algo así, cualquier cosa que eso fuese... Era mucho más abstracto que todos sus antecesores y sólo utilizaba 0 y 1 como valores posibles de las variables de su álgebra.”⁶⁷.

Sería 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 Κρυπτοζ (Kriptos–Oculto) y Γραφειν (Grafo–Escritura) y significa “arte de escribir con clave secreta o de un modo enigmático”⁶⁸.

Aportando luz a la definición cabe aclarar que la Criptografía hace años que dejó de ser un arte para convertirse en una técnica (o conjunto de ellas) que tratan sobre la protección (ocultamiento ante personas no autorizadas) de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Matemática Discreta, la Teoría de los Grandes Números y la Complejidad Algorítmica.

⁶⁷ Extraído de <http://www.kriptopolis.com>

⁶⁸ LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadores. Dpto. de Informática Universidad de Jaén. Edición virtual. España. 1999. <http://www.kriptopolis.com>. Capítulo 2–Página 23.

Es decir que la **Criptografía** es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que sólo 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**



Gráfico 8.6 – 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 CRIPTOANÁLISIS

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 quintupla **(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 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 **E_K** para cada valor posible de la clave **K**.
- **D** es el conjunto de transformaciones de descifrado, análogo a **E**.

Todo Criptosistema cumple la condición **D_K(E_K(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**.⁶⁹

⁶⁹ LUCENA LÓPEZ, Manuel José. Criptografía y Seguridad en Computadores. Dpto. de Informática Universidad de Jaén. Edición virtual. España. 1999. <http://www.kriptopolis.com>. Capítulo 2–Página 24.

Existen dos tipos fundamentales de Criptosistemas utilizados para cifrar datos e información digital y ser enviados posteriormente después por medios de transmisión 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 inconveniente que presentan es que se debe contar con un canal seguro para la transmisión de dicha clave.
- b. **Asimétricos o de llave pública:** se emplea una doble clave conocidas como **K_p** (clave privada) y **K_P** (clave Pública). Una de ellas es utilizada para la transformación E de cifrado y la otra para el descifrado D. En muchos de los sistemas existentes estas clave son intercambiables, es decir que si empleamos una para cifrar se utiliza la otra para descifrar y viceversa.

Los sistemas asimétricos deben cumplir con la condición que la clave Publica (al ser conocida y sólo 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 asimétricos. Esto permite que los algoritmos simétricos sean considerablemente más rápidos que los asimétricos.

En la práctica actualmente se emplea 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 más corta que el mensaje) con un sistema asimétrico.

Después de 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 eficacia por ser fácilmente criptoanalizables y por tanto “reventables”. Cada uno de los algoritmos clásicos descritos 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 transposición 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 $n = 3$ columnas, la clave **K** es (3,1,2) y el mensaje a cifrar “SEGURIDAD INFORMATICA”.

| 1 | 2 | 3 |
|---|---|---|
| S | E | G |
| U | R | I |
| D | A | D |
| | I | 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 ellos 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 César

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 es 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 César. 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 se 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 más 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 sólo se dará una idea de su funcionamiento y complejidad.

8.10.5.1 REDES DE FEISTEL

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 Encryption Standard es el algoritmo simétrico más extendido mundialmente. A mediados de los setenta fue adoptado como estándar para las comunicaciones seguras (Estándar AES) del gobierno de EE.UU. En su principio fue diseñado por la NSA (National Security Agency)⁷⁰ 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 XOR). 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 la clave de cifrado.

En la actualidad no se ha podido romper el sistema DES criptoanalíticamente (deducir la clave simétrica a partir de la información interceptada). Sin embargo una empresa española sin fines de lucro llamado Electronic Frontier Foundation (EFF)⁷¹ construyo en Enero de 1999 una máquina capaz de probar las 2^{56} claves posibles en DES y romperlo sólo en tres días con fuerza bruta.

A pesar de su caída DES sigue siendo utilizado por su amplia extensión de las implementaciones vía hardware existentes (en cajeros automáticos y señales de video por ejemplo) y se evita tener que 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 Múltiple

Consiste en aplicar varias veces el algoritmo DES (con diferentes claves) al mensaje original. El más conocidos de todos ellos el Triple-DES (T-DES), el cual consiste en aplicar 3 veces DES de la siguiente manera:

1. Se codifica con la clave K_1 .
2. Se decodifica el resultado con la clave K_2 .
3. Lo obtenido se vuelve a codificar con K_1 .

⁷⁰ National Security Agency (NSA): <http://www.nsa.gov:8080>

⁷¹ Electronic Frontier Foundation (EFF) actualmente ya no se encuentra trabajando pero puede visitarse su sitio en <http://www.eff.com>

La clave resultante es la concatenación de K_1 y K_2 con una longitud de 112 bits.

En 1998 el NIST (National Institute of Standards Technology) convocó a un concurso para poder determinar un algoritmo simétrico 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 y Rijndael (que en octubre sería el ganador).

8.10.5.3 IDEA

El International Data Encryption 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 en ocho rondas de cifrado idéntico, excepto por las subclaves utilizadas (segmentos de 16 bits de los 128 de la clave), en donde se combinan diferentes operaciones matemáticas (XORs y Sumas Módulo 16) y una transformación final.

“En mi opinión, él es el mejor y más seguro algoritmo de bloques disponible actualmente al público.”⁷²

8.10.5.4 BLOWFISH

Este algoritmo fue desarrollado por Bruce Schneier 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 π (aunque puede cambiarse a voluntad) para obtener las funciones de encriptación y desencriptación. 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, diseñado por RSA⁷³, permite definir el tamaño del 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 o desencriptar 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 Tavares, de la empresa Northern Telecom (NorTel).

⁷² SCHNEIER, Bruce. Applied Cryptography. Segunda Edición. EE.UU. 1996

⁷³ RSA Labs: <http://www.rsa.com>. No confundir con el algoritmo de clave pública del mismo nombre RSA (Rivest-Shamir-Adleman)

CAST no tiene claves débiles o semidébiles y hay fuertes argumentos acerca que CAST es completamente inmune a los métodos de criptoanálisis más potentes conocidos.

8.10.5.7 RIJNDAEL (EL NUEVO ESTÁNDAR AES)

Este nuevo algoritmo belga mezcla de Vincent Rijmen y Joan Daemen (sus autores) sorprende tanto por su innovador diseño como por su simplicidad práctica; aunque tras él se esconda un complejo trasfondo matemático.

Su algoritmo no se basa en redes de Feistel, y en su lugar se ha definido una estructura de “capas” formadas por funciones polinómicas reversibles (tienen 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 múltiplo 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 propuesto por la NSA contenía puertas traseras. Entre los ataques más potentes a la criptografía simétrica se encuentran:

- **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 está 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 muy eficientes en la práctica. En el momento después de que un sistema criptográfico es publicado y se muestra inmune a estos dos tipos de ataques (y otros pocos) la mayor preocupación es la longitud de las claves.

8.10.6 ALGORITMOS ASIMÉTRICOS (LLAVE PRIVADA—PÚBLICA)

Ideado por los matemáticos Whitfield Diffie y Martín Hellman (DH) 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 (Pública) y otra Privada.

Actualmente existen muchos algoritmos de este tipo pero han demostrado ser poco utilizables en la práctica ya sea por la longitud de las clave, la longitud del texto encriptado generado o su velocidad de cifrado extremadamente largos.

DH está 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 mas 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 propiedades de los números primos cuando se aplican sobre ellos operaciones matemáticas basadas en la función módulo. En concreto, emplea la función exponencial discreta para cifrar y descifrar, y cuya inversa, el logaritmo discreto, es muy difícil de calcular.

Los cálculos matemáticos de este algoritmo emplean un número denominado Módulo Público, N , que forma parte de la clave pública y que se obtiene a partir de la multiplicación de dos números primos, p y q , diferentes y grandes (del orden de 512 bits) y que forman parte de la 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 presenta la factorización de su producto. Aunque el avance tecnológico hace que cada vez sea más rápido un posible ataque por fuerza bruta, el simple hecho 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 inviable.

Sin embargo, se ha de notar que, aunque el hecho de aumentar la longitud de las claves RSA no supone ninguna dificultad tecnológica, las leyes de exportación de criptografía de EE.UU. imponían, hasta el 20 de septiembre de 2000, un límite a dicha 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 atacante 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 suficientemente grandes (alrededor de 200 dígitos).

Vale decir que nadie ha demostrado que no pueda existir un método que permita descifrar un mensaje sin usar la clave privada y sin factorizar N . Así, 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 clave pública. Supongamos:

... que A quiere establecer una comunicación con B, y que C quiere espiarla. Cuando A le solicite a B su clave pública K_B , C se interpone, obteniendo la clave de B y enviado a A una clave falsa K_C , creada por él. Cuando A codifique el mensaje, C lo intercepta de nuevo, lo decodifica con su clave propia y emplea K_B para codificarlo y enviarlo a B... ni A ni B sospecharán nunca de lo sucedido.

La única manera de evitar esto consiste en asegurar a A que la clave pública de B es auténtica. Para ello esta debería ser firmada por un amigo común que, actuando como Autoridad Certificadora, certifique su autenticidad.

Otros ataques (como el de claves débiles, el de texto plano escogido, el de módulo común, y el de exponente bajo) aprovechan vulnerabilidades específicas 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 sí llevan estudiándose durante muchos siglos y están entre los objetos más ricamente estructurados y estudiados de la teoría de 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 del cálculo de raíces cuadradas módulo un número compuesto), **DSS** 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 garantizar la procedencia de un mensaje conocido, de forma de poder asegurar que no es una falsificación. A este mecanismo se lo 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 válido 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 pequeña y es muy difícil encontrar otro mensaje que tenga la misma firma. Suponiendo que B envía un mensaje m firmado a A, el procedimiento es:

- a. B genera un resumen del mensaje $r(m)$ y lo cifra con su clave privada.
- b. B envía el criptograma.
- c. A genera su propia copia de $r(m)$ usando la clave pública de B asociada a la privada.
- d. A compara su criptograma con el recibido y si coinciden el mensaje es auténtico.

Cabe destacar que:

- 1. Cualquiera que posea la clave pública de B puede constatar 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 firman el mismo documento m también se producen dos 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 más utilizado.

8.10.7.1.1 MD5

El Message Digest 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 de b comenzando por el byte menos significativo.

A continuación se realizan 64 operaciones divididas en 4 rondas sobre estos bloques 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.

Su 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 obtener firmas digitales son: DSA (Digital Signature Algorithm) y el RIPE–MD160.

8.10.8 PGP (PRETTY GOOD PRIVACY)

Este proyecto de “Seguridad Bastante Buena” pertenece a Phill Zimmerman quien decidió crearlo en 1991 “por falta de herramientas criptográficas sencillas, potentes, baratas y al alcance del usuario común. Es personal. Es privado. Y no es de interés para nadie más que no sea usted... Existe una necesidad social en crecimiento para esto. Es por eso que lo creé.”⁷⁴

Actualmente PGP es la herramienta más popular y fiable para mantener la seguridad y privacidad en las comunicaciones tanto para pequeños usuarios como para grandes empresas.

8.10.8.1 FUNCIONAMIENTO DE PGP

8.10.8.1.1 Anillos de Claves

Un anillo es una colección de claves almacenadas en un archivo. Cada usuario tiene dos anillos, uno 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 sesión) y posteriormente codifica la clave haciendo uso de la llave pública del destinatario. Dicha clave es extraída convenientemente del anillo de claves públicas a partir del identificador suministrado por el usuario

Nótese que para que el mensaje pueda ser leído por múltiples destinatarios basta con que se incluya en la cabecera cada una de las 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 públicas con las que está codificado, pide una contraseña para abrir el anillo de claves privadas y comprueba si se tiene una clave que permita decodificar el mensaje.

⁷⁴ “Porque escribí PGP”. Declaraciones de Phill Zimmerman. <http://www.pgpi.com> – <http://pgp.org>

Nótese 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 descryptarlo) para disminuir el tiempo de cifrado, de transmisión y de alguna manera fortalecer la seguridad del cifrado ante el criptoanálisis que explotan las redundancias del texto plano.

PGP utiliza rutinas de compresión de dominio público creadas por Gailly–Adler–Wales (basadas en los algoritmos de Liv–Zemple) funcionalmente semejantes a las utilizadas en los softwares comerciales de este 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 estudiados. Las signatura 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 ElGamal.

8.10.9 ESTEGANOGRAFÍA

Consiste en ocultar en el interior de información aparentemente inocua, otro tipo de información (cifrada o no). El texto se envía como texto plano, pero entremezclado con mucha cantidad de “basura” que sirve de camuflaje al mensaje enviado. El método de recuperación y lectura sólo es conocido por el destinatario del mensaje y se conoce como “separar el grano de la paja”.

Los mensajes suelen ir ocultos entre archivos de sonido o imágenes y ser enormemente grandes por la cantidad extra de información enviada (a comparación del mensaje original).

8.11 COMERCIO ELECTRÓNICO

El comercio electrónico 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:

- **Confidencialidad (anonimato):** la identidad del comprador no es conocida por el vendedor; nadie, excepto el banco, debería conocer 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 Irrefutabilidad:** 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 posibles formas de pago 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 mencionó, si alguien desea verificar la autenticidad de un mensaje (un banco por ejemplo) debe poseer la clave pública del emisor. Es decir que una persona que se dedique a autenticar documentos deberá poseer una 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 autenticar 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 pública 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 pública de la AC (una única clave) podrá verificar la autenticidad del documento.

El Estándar internacional para CD más 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 y un Identificador, firmados digitalmente por una autoridad de certificación, y su utilidad es demostrar que una clave pública pertenece a un usuario concreto.

El estándar X.509 sólo define la sintaxis de los certificados, por lo que no está atado a ningún algoritmo en particular, y contempla los siguientes campos:

1. **Versión:** Indica si la versión del certificado X.509 es la 1 (defecto), 2 ó 3.
2. **Número de serie:** Es un número 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 el certificado.
5. **Validez:** Indica el intervalo de tiempo en el que el certificado es válido.
6. **Usuario o Sujeto:** Es un nombre distinguible X.500 que identifica de forma unívoca al poseedor del certificado; y la nomenclatura de nombres distinguibles (DN: Distinguished Names).
7. **Clave pública 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:** Permiten 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 éste contiene es auténtica (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 está especificado en el campo Validez, y que viene 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 pública 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 pila TCP/IP, se ubica entre la capa TCP (Transporte) y la 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 sólo se implementa sobre HTTP. Para diferenciar las páginas 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 estas 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 bloques para volver a reensamblarlos en el receptor.
- **Compresión de datos:** se puede aplicar un algoritmo de compresión a los datos.
- **Autenticación 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.
- **Autenticación del cliente:** permite al servidor conocer la identidad del usuario, con el fin de decidir si este puede acceder a cierta información protegida. Esta autenticación no siempre debe darse.

Al reunir estas características, la comunicación se realiza en dos fases:

- **Saludo (Handshaking):** los interlocutores se identifican mutuamente empleando, habitualmente, certificados X.509. Tras el intercambio de claves públicas, 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 clientes a través del cual se intercambiará cifrada la siguiente información:

- La URL del documento solicitado.
- El contenido del documento solicitado.
- Los contenidos de cualquier formulario enviado desde el navegador.
- Las cookies enviadas desde el navegador al servidor y viceversa.
- 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 EE.UU. sobre los productos criptográficos, las versiones de los navegadores distribuidas legalmente más allá de sus fronteras operan con nada más que 40 bits de longitud de clave, frente a los 128 ó 256 bits de las versiones fuertes.

Claves tan cortas facilitan los ataques de fuerza bruta, dependiendo de los recursos informáticos disponibles. Este serio problema ganó notoriedad en los medios de comunicación cuando en 1995 un estudiante francés, Damien Doligez, fue capaz de descifrar un mensaje cifrado con SSL en pocos días utilizando la red de computadoras de su Universidad.

2. SSL **sólo** garantiza la confidencialidad e integridad de los datos en tránsito, 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, está más allá de la competencia de este protocolo.

3. SSL **no** garantiza la identidad del servidor al que se conecta el usuario. Podría suceder que el servidor seguro contase con un certificado perfectamente válido y que estuviera suplantando 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 está conectando a un web falsificado.
4. El servidor identifica al navegador incluso aunque éste 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.
5. 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 envío de formularios o la recuperación de páginas web. Por esto, se debe usar S/MIME, PGP o algún otro software criptográfico para correo.

8.12.1.2.2 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 página cuya dirección empieza por *https://*. El navegador se encarga del resto.

8.11.1.3 TLS

Transport Layer Security es un protocolo estandarizado por el IETF⁷⁵. Está 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, Verisign, 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.

⁷⁵ IETF: Internet Engineering Task Force. <http://www.ietf.org>

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 último 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 sólo protege un número de tarjeta de crédito, por ejemplo, cuando se envía del cliente al comerciante, sin embargo no hace nada para la validación de ese número, no chequea su autorización, permite que el comerciante lo almacene, etc. SET cubre todas estas debilidades ofreciendo seguridad a las entidades intervinientes.

La implantación del 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 autenticación asegura que los participantes en la operación comercial sean quienes dicen ser: el consumidor sabe en qué comercio está comprando y; el comercio está seguro de que quien está comprando es realmente el titular del instrumento de pago. La autenticación 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, está 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 la clave privada del cliente y encriptada con la clave pública del receptor puede apreciarse en el Gráfico 8.7.

1. El Cliente Firma el documento de compra, mediante su Clave Privada.
2. El Cliente Encripta los datos, mediante la Clave Pública del Vendedor.
3. El Vendedor descifra, mediante su Clave Privada, los datos encriptados por el Cliente.
4. El Vendedor comprueba la integridad y autenticidad de los datos (Firma del Cliente), mediante la Clave Pública del mismo.

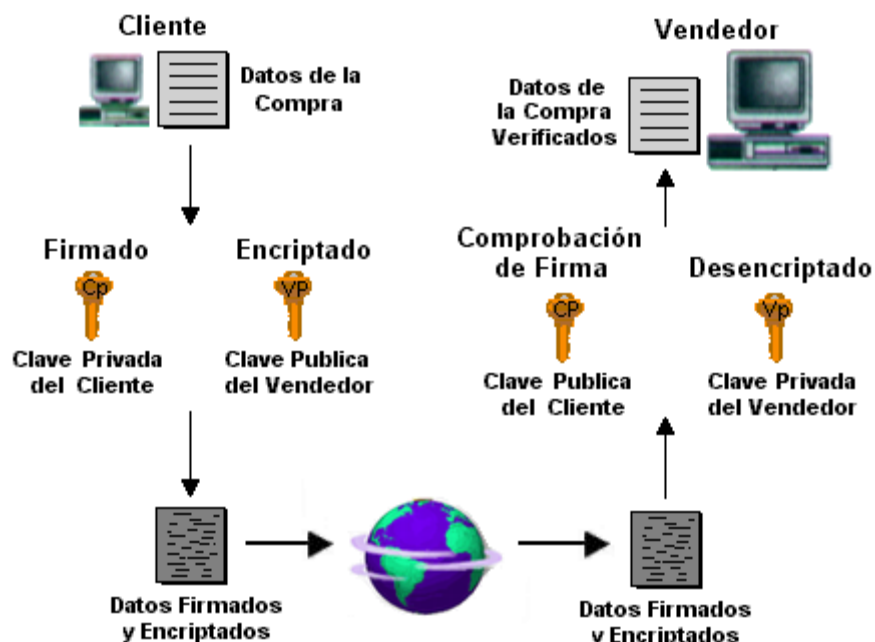


Gráfico 8.7 – Proceso Encriptado–Firmado de SET

SET utiliza algoritmos de encriptación como SHA-1, DES y RSA ya que estos son compatibles con los certificados existentes, aunque en próximas 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 logueo seguro en terminales remotas, evitando el viaje de passwords en claro por redes inseguras; mediante el uso de comunicaciones cifradas. El protocolo SSH se establece en tres niveles:

1. **Nivel de Transporte:** En este nivel se procede a la autenticación 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 pública para encriptación y autenticación del servidor: DSA, Certificados X.509 y Certificados PGP.
- c. Algoritmos de 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 Autenticación del Usuario:** En este nivel se supone establecida la encriptación e integridad del canal y la autenticación del servidor. Para la autenticación del usuario el SSH ofrece varias posibilidades:
 - Autenticación del usuario basada en claves Pública–Privada: la autenticación 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 recomendando por los fabricantes que implementan SSH.
 - Autenticación del usuario basada en passwords. Hay que señalar que el password no viaja encriptado, sino 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.
 - Autenticación del usuario basada en procedencia del Host: en esta situación hay que proteger las claves privadas del Host por parte del usuario. Es una autenticación parecida a la ofrecida por otros sistemas de logueo 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 cuenta con el apoyo necesario para ser considerado un estándar, está 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 autenticación ante un Firewall. 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 validada por el sistema de autenticación y después el 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.

Debe notarse que Socks sólo autentifica las conexiones pero no produce ningún tipo de cifrado de los datos por lo que se hace necesario combinarlo con algún algoritmo que si lo haga (SSH, SSL, PPTP, IPSec, etc).

8.12.4 KERBEROS

En 1993 el MIT crea el proyecto Athena, y basándose en la mitología griega con su perro de tres cabezas y una cola de serpiente vigilando la entrada a Hades (el infierno), nace Kerberos.

Kerberos es un sistema de seguridad que provee autenticación a través de redes inseguras. Su objetivo es restringir los accesos sólo a usuarios autorizados y poder autenticar 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 autenticación 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 password viaja 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 autenticación centralizado, cuya función es autenticar a los usuarios frente a servidores y a estos frente a los usuarios. La tecnología Kerberos está basado en tres objetos de seguridad (tres cabezas):

- **Autenticación Service (AS):** Autentifica los usuarios y les proporciona un ticket para realizar la comunicación con el servidor de Tickets.
- **Tickets Gratin 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 Kerberos empleando RSA):

- **La Clave Secreta del Usuario:** esta clave es conocida únicamente por el usuario y por Kerberos y tiene la finalidad de autenticar al usuario frente a Kerberos. 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 Kerberos luego de verificar al usuario y expedida al mismo con el objetivo de autenticar el intercambio de un par de usuarios que definen 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, garantizando que este ha sido autenticado recientemente (el mismo tiene un período de validez).
- **Autenticador:** Es un testigo construido por el cliente y enviado al AS para probar su identidad. Sólo cuando el servidor descifra el Ticket, y verifica que el ID del usuario es auténtico, otorga el servicio requerido.

8.12.4.1 RESUMEN DE KERBEROS

En el Gráfico 8.7 puede apreciarse el funcionamiento de las distintas entidades intervinientes en Kerberos y su función:

- Solicitud de un Ticket de acceso.**
- Ticket + Clave de Sesión.**
- Solicitud de un Ticket de acceso al servicio.**
- Ticket + Clave de Sesión.**
- Solicitud de Servicio.**
- Autenticador del Servidor.**

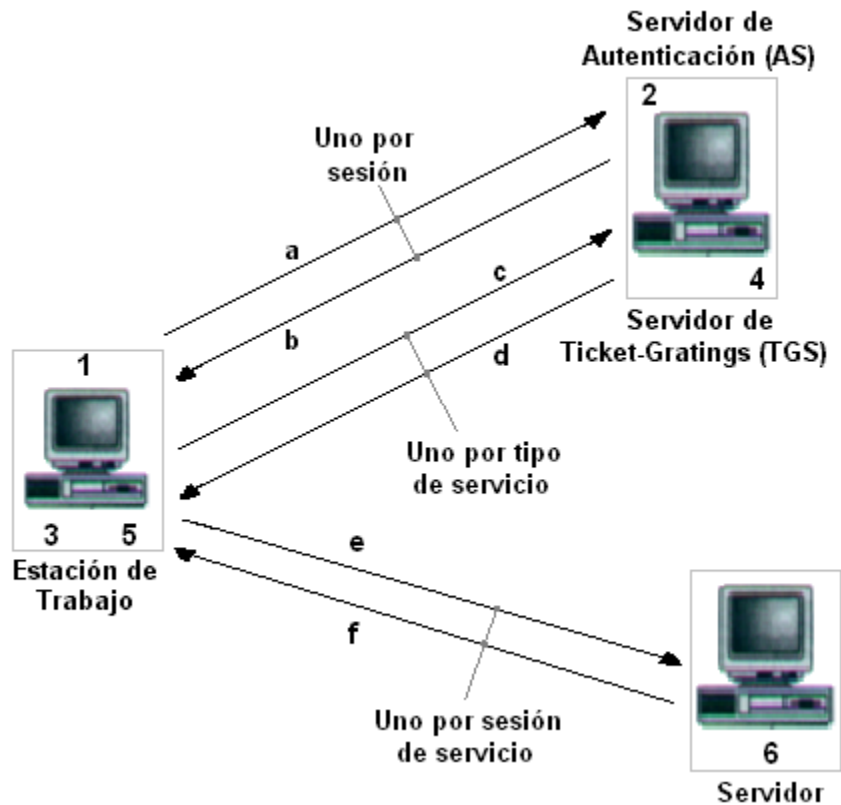


Gráfico 8.8 – Proceso de Kerberos

El proceso de Autenticación se divide en dos etapas:

- Autenticación 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, crea un Ticket y una Clave de Sesión. Los resultados son encriptados usando la clave derivada de la password del usuario.
- Autenticación de Servicio
 3. La Estación solicita la password al usuario y la utiliza para descryptar el mensaje, luego envía al TGS el Ticket y el Autenticador que contienen el Nombre de Usuario, la Dirección de red y el Tiempo de Vida.
 4. El TGS descrypta el Ticket y el Autenticador, verifica la solicitud y crea un Ticket para ser enviado al Servidor.
 5. La Estación de Trabajo envía el Ticket y el Autenticador al Servidor.
 6. El Servidor verifica que el Ticket y el Autenticador coincidan, luego permite al Servicio.

8.12.4.2 PROBLEMAS DE KERBEROS

La filosofía de Kerberos está 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 descryptar los mensajes que circulan por ella. Este concepto es una contradicción a la teoría de sistemas

distribuidos, sobre el que se basa el modelo que rige cualquier red (si una máquina falla el resto puede seguir su funcionamiento, sino a pleno, al menos correctamente).

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

Por último, la implementación de Kerberos, actualmente, acarrea algunos inconvenientes ya que se debe realizar un proceso de “Kerberización” sobre cada programa que se desee utilizar, suponiendo esto un conocimiento y tiempo considerable no siempre disponible. Si bien este inconveniente está siendo subsanado en diversas versiones aún no se cuenta con la standardización suficiente para su extensión masiva.

8.13 VPN–REDES PRIVADAS VIRTUALES

La tecnología de VPN proporciona un medio para usar el canal público de 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 sólo 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 está 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 desencriptación). Una VPN solo protege los aspectos de protección en la comunicación, no protege la información alojada en el disco, en pantalla, 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 tráfico si es que 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 utilizará 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 autenticación 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 módulo de control debe tener una simple vía para 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 utilizarán de acuerdo a las necesidades de cada segmento de la red. El estándar actual para la encriptación comercial es 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 con políticas y procedimientos de seguridad definidos. La red virtual sólo resuelve un problema específico, y su configuración debe estar basada en una política que haya contemplado el análisis del riesgo que debemos atacar con la instalación de esta herramienta. Esto hace que sea atractivo combinar la flexibilidad de los protocolos VPN con la seguridad proporcionada por IPSEC.

8.13.2 L2TP

Layer To Tunneling Protocol es 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 está 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 aparecen como paquetes IP, aprovechan la seguridad IPsec estándar para obtener una fuerte protección de integridad, reproducción, autenticidad y privacidad. L2TP se diseñó 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 pública) utilizando un ID de usuario y una contraseña. Apareció por primera vez en 1996, dos años antes de la disponibilidad de IPsec y L2TP y su objetivo era la 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 del protocolo IP conocida como IPsec. Este estándar es válido para IPv4 y IPv6, y provee un marco que permite a dos o más partes el uso de distintos algoritmos de encriptación

y métodos de autenticación 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, usuarios 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 transmite.

IPSec elimina el requisito de la implementación de seguridad en 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 generó el tráfico.

En otras palabras, las aplicaciones no son compatibles con IPSec. Las reglas de seguridad las define el administrador sin tener en cuenta qué 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 antirreproducción y protege la autenticación del Host. AH provee autenticación, integridad y protección a la replica (una transacción sólo debe llevarse a cabo una vez) asegurando 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 gráfico:

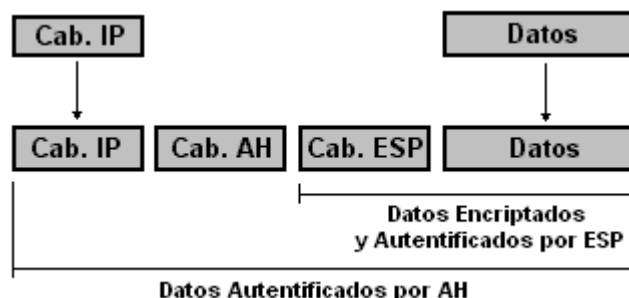


Gráfico 8.9 – Fuente: MONSERRAT COLL, Francisco Jesús. Seguridad en los protocolos TCP/IP. Página 30.
<http://www.rediris.es/ftp>

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 criptográficos y de autenticación 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 intermedios no pueden desencriptar el contenido de los datagramas. Este modo permite la total confidencialidad de la comunicación.
- **Modo Túnel:** los datagramas son enviados en claro hacia equipos intermedios (Router o Firewall), este encripta los datos y los envía al exterior. En el otro extremo del túnel se realiza el proceso de desencriptado y se envía el datagrama en claro hacia el equipo destino. Esto permite a los equipos de la red interna visualizar los datos y sólo 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 dé prácticamente en todos los niveles: empresas grandes, medianas, chicas y usuarios finales. Todos pueden acceder a las herramientas que necesitan y los costos (la inversión que cada uno debe realizar) va de acuerdo con el tamaño y potencialidades de la herramienta .

Pero no es sólo una cuestión de costos, los constantes cambios de la tecnología hacen que para mantener un nivel parejo de seguridad, se deba actualizar permanentemente las herramientas con las que se cuenta. Como los intrusos mejoran sus armas y metodologías de penetración de forma incesante, el recambio y la revisión constantes en los mecanismos de seguridad se convierten en imprescindibles. Y éste es un verdadero punto crítico.

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 funcionan y qué se puede hacer con ellos. “Es prioritario saber los riesgos que una nueva tecnología trae aparejados”.

CAPÍTULO 9



“Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más... Más vale dedicar recursos a la seguridad que convertirse en una estadística.”

POLÍTICAS DE SEGURIDAD

Hoy es imposible hablar de un sistema cien por cien seguro, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas.

La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios. “Si un Hacker quiere gastar cien mil dólares en equipos para descifrar una encriptación, lo puede hacer porque es imposible de controlarlo. Y en tratar de evitarlo se podrían gastar millones de dólares”.

La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un

conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

9.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA

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

Está lejos de mi intención (y del alcance del presente) proponer un documento estableciendo lo que debe hacer un usuario o una organización para lograr la mayor Seguridad Informática posible. Sí está dentro de mis objetivos proponer los lineamientos generales que se deben seguir para lograr (si así se pretendiese) un documento con estas características.

El presente es el resultado de la investigación, pero sobre todo de mi experiencia viendo como muchos documentos son ignorados por contener planes y políticas difíciles de lograr, o peor aún, de entender.

Esto adquiere mayor importancia aún cuando el tema abordado por estas políticas es la Seguridad Informática. Extensos manuales explicando como debe protegerse una computadora o una red con un simple Firewall, un programa antivirus o un monitor de sucesos. Falacias altamente remuneradas que ofrecen la mayor “Protección” = “Aceite de Serpiente” del mundo.

He intentado dejar en claro que la Seguridad Informática no tiene una solución definitiva aquí y ahora, sino que es y será (a mi entender) el resultado de la innovación tecnológica, a la par del avance tecnológico, por parte de aquellos que son los responsables de nuestros sistemas.

En palabras de Julio C. Ardita: “Una política de seguridad funciona muy bien en EE.UU. pero cuando estos manuales se trajeron a América Latina fue un fiasco... Armar una política de procedimientos de seguridad en una empresa está costando entre 150–350 mil dólares y el resultado es ninguno... Es un manual que llevado a la implementación nunca se realiza... Es muy difícil armar algo global, por lo que siempre se trabaja en un plan de seguridad real: las políticas y procedimientos por un lado y la parte física por otra.”⁷⁶

⁷⁶ ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. <http://www.cybsec.com>

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

Decisión: elección de un curso de acción determinado entre varios posibles.

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

Estrategia: conjunto de decisiones que se toman para determinar políticas, metas y programas.

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

Meta: objetivo cuantificado a valores predeterminados.

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

Norma: forma en que realiza un procedimiento o proceso.

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

Proyección: predicción del comportamiento futuro, basándose en el pasado sin el agregado de apreciaciones subjetivas.

Pronóstico: predicción del comportamiento futuro, con el agregado de hechos concretos y conocidos que se prevé influirán en los acontecimientos futuros.

Control: capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho. Es una acción tomada para hacer un hecho conforme a un plan.⁷⁷

Riesgo: proximidad o posibilidad de un daño, peligro. Cada uno de los imprevistos, hechos desafortunados, etc., que puede tener un efecto adverso. Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

Ahora, “una **Política de Seguridad** es un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema.”⁷⁸

La RFC 1244 define **Política de Seguridad** como: “una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán.”⁷⁹

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, donde se definen las medidas a tomar para proteger la seguridad del sistema; pero... ante todo, “(...) una política de seguridad es una forma de comunicarse con los usuarios... Siempre hay que tener en cuenta que la seguridad comienza y termina con personas.”⁸⁰ y debe:

⁷⁷ FERNANDEZ, Carlos M. Seguridad en sistemas informáticos. Ediciones Díaz de Santos S.A.. España. 1988. Página 105.

⁷⁸ HUERTA, Antonio Villalón. Seguridad en Unix y redes. (Versión 1.2). Capítulo 16–Página 259

⁷⁹ RFC 1244: Site Security Handbook. J. Reynolds – P. Holbrook. Julio 1991

⁸⁰ SPAFFORD, Gene. “Manual de seguridad en redes”. ArCERT. Argentina. 2000.
<http://www.arcert.gov.ar>

- Ser holística (cubrir todos los aspectos relacionados con la misma). No tiene sentido proteger el acceso con una puerta blindada si a esta no se la ha cerrado con llave.
- Adecuarse a las necesidades y recursos. No tiene sentido adquirir una caja fuerte para proteger un lápiz.
- Ser atemporal. El tiempo en el que se aplica no debe influir en su eficacia y eficiencia.
- Definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas.

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

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

9.2 EVALUACIÓN DE RIESGOS

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

- Se debe poder obtener una evaluación económica del impacto de estos sucesos. Este valor se podrá utilizar para contrastar el costo de la protección de la información en análisis, versus el costo de volverla a producir (reproducir).
- Se debe tener en cuenta la probabilidad que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.
- Se debe conocer qué se quiere proteger, dónde y cómo, asegurando que con los costos en los que se incurren se obtengan beneficios efectivos. Para esto se deberá identificar los recursos (hardware, software, información, personal, accesorios, etc.) con que se cuenta y las amenazas a las que se está expuesto.

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización; pero se puede presuponer algunas preguntas que ayudan en la identificación de lo anteriormente expuesto⁸¹:

- “¿Qué puede ir mal?”
- “¿Con qué frecuencia puede ocurrir?”
- “¿Cuáles serían sus consecuencias?”
- “¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?”
- “¿Se está preparado para abrir las puertas del negocio sin sistemas, por un día, una semana, cuanto tiempo?”

⁸¹ RFC 1244: Site Security Handbook. J. Reynolds – P. Holbrook. Julio 1991

- “¿Cuál es el costo de una hora sin procesar, un día, una semana...?”
- “¿Cuánto, tiempo se puede estar off-line sin que los clientes se vayan a la competencia?”
- “¿Se tiene forma de detectar a un empleado deshonesto en el sistema?”
- “¿Se tiene control sobre las operaciones de los distintos sistemas?”
- “¿Cuántas personas dentro de la empresa, (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?”
- “¿A que se llama información confidencial y/o sensitiva?”
- “¿La información confidencial y sensitiva permanece así en los sistemas?”
- “¿La seguridad actual cubre los tipos de ataques existentes y está preparada para adecuarse a los avances tecnológicos esperados?”
- “¿A quien se le permite usar que recurso?”
- “¿Quién es el propietario del recurso? y ¿quién es el usuario con mayores privilegios sobre ese recurso?”
- “¿Cuáles serán los privilegios y responsabilidades del Administrador vs. la del usuario?”
- “¿Cómo se actuará si la seguridad es violada?”

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

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

Tabla 9.1 – Tipo de Riesgo-Factor

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

9.2.1 NIVELES DE RIESGO

Como puede apreciarse en la Tabla 9.1, los riesgos se clasifican por su nivel de importancia y por la severidad de su pérdida:

1. Estimación del riesgo de pérdida del recurso (R_i)
2. Estimación de la importancia del recurso (I_i)

Para la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico de 0 a 10, tanto a la importancia del recurso (10 es el recurso de mayor importancia) como al riesgo de perderlo (10 es el riesgo más alto).

El riesgo de un recurso será el producto de su importancia por el riesgo de perderlo⁸²:

$$WR_i = R_i * I_i$$

Luego, con la siguiente fórmula es posible calcular el riesgo general de los recursos de la red:

$$W_R = \frac{(WR_1 * I_1 + WR_2 * I_2 + ... + WR_n * I_n)}{I_1 + I_2 + ... + I_n}$$

Otros factores que debe considerar para el análisis de riesgo de un recurso de red son su disponibilidad, su integridad y su carácter confidencial, los cuales pueden incorporarse a la fórmula para ser evaluados.

Ejemplo: el Administrador de una red ha estimado los siguientes riesgos y su importancia para los elementos de la red que administra:

| Recurso | Riesgo (R _i) | Importancia (I _i) | Riesgo Evaluado (R _i *I _i) |
|----------|--------------------------|-------------------------------|---|
| Router | 6 | 7 | 42 |
| Gateway | 6 | 5 | 30 |
| Servidor | 10 | 10 | 100 |
| PC's | 9 | 2 | 18 |

Tabla 9.2 – Valuación de Riesgos

Aquí ya puede apreciarse que el recurso que más debe protegerse es el servidor. Para la obtención del riesgo total de la red calculamos:

$$W_R = \frac{42 + 30 + 100 + 18}{7 + 5 + 10 + 2} = 7,92$$

Al ver que el riesgo total de la red es de casi 8 puntos sobre 10 debería pensarse seriamente en buscar las probables causas que pueden provocar problemas a los servicios brindados por los elementos evaluados.

9.2.2 IDENTIFICACIÓN DE AMENAZA

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

Se suele dividir las amenazas existentes según su ámbito de acción:

- Desastre del entorno (Seguridad Física).
- Amenazas del sistema (Seguridad Lógica).
- Amenazas en la red (Comunicaciones).
- Amenazas de personas (Insiders–Outsiders).

⁸² "Manual de seguridad en redes". ArCERT. Argentina. 2000. Página 3–1.
<http://www.arcert.gov.ar>

Se debería disponer de una lista de amenazas (actualizadas) para ayudar a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar. Es importante que los Administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

En la siguiente sección se 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.

La metodología se basa en los distintos ejemplos (uno para cada tipo de amenaza) y contempla como hubiera ayudado una política de seguridad en caso de haber existido.

9.2.3 EVALUACIÓN DE COSTOS

Desde un punto de vista oficial, el desafío de responder la pregunta del valor de la información ha sido siempre difícil, y más difícil aún hacer estos costos justificables, siguiendo el principio que “si desea justificarlo, debe darle un valor”⁸³.

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

Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea. Por eso es importante entender que los esfuerzos invertidos en la seguridad son costeables.

La evaluación de costos más ampliamente aceptada consiste en cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades. Un planteamiento posible para desarrollar esta política es el análisis de lo siguiente:

- ¿Qué recursos se quieren proteger?
- ¿De qué personas necesita proteger los recursos?
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?

Con esas sencillas preguntas (más la evaluación de riesgo) se debería conocer cuáles recursos vale la pena (y justifican su costo) proteger, y entender que algunos son más importantes que otros.

El objetivo que se persigue es lograr que un ataque a los bienes sea más costoso que su valor, invirtiendo menos de lo que vale. Para esto se define tres costos fundamentales:

⁸³ STRASSMANN, Paul A. “El arte de presupuestar: como justificar los fondos para Seguridad Informática”. <http://www.nextvision.com>

- **CP:** Valor de los bienes y recursos protegidos.
- **CR:** Costo de los medios necesarios para romper las medidas de seguridad establecidas.
- **CS:** Costo de las medidas de seguridad.

Para que la política de seguridad sea lógica y consistente se debe cumplir que:

- **CR > CP:** o sea que un ataque para obtener los bienes debe ser más costoso que el valor de los mismos. Los beneficios obtenidos de romper las medidas de seguridad no deben compensar el costo de desarrollo del ataque.
- **CP > CS:** o sea que el costo de los bienes protegidos debe ser mayor que el costo de la protección.

Luego, **CR > CP > CS** y lo que se busca es:

- “**Minimizar** el costo de la protección manteniéndolo por debajo del de los bienes protegidos”⁸⁴. Si proteger los bienes es más caro de lo que valen (el lápiz dentro de la caja fuerte), entonces resulta más conveniente obtenerlos de nuevo en vez de protegerlo.
- “**Maximizar** el costo de los ataques manteniéndolo por encima del de los bienes protegidos”⁸⁵. Si atacar el bien es más caro de lo que valen, al atacante le conviene más obtenerlo de otra forma menos costosa.

Se debe tratar de valorar los costos en que se puede incurrir en el peor de los casos contrastando con el costo de las medidas de seguridad adoptadas. Se debe poner especial énfasis en esta etapa para no incurrir en el error de no considerar costos, muchas veces, ocultos y no obvios (costos derivados).

9.2.3.1 VALOR INTRÍNSECO

Es el más fácil de calcular (pero no fácil) ya que solo consiste en otorgar un valor a la información contestando preguntas como las mencionadas y examinando minuciosamente todos los componentes a proteger.

9.2.3.2 COSTOS DERIVADOS DE LA PERDIDA

Una vez más deben abarcarse todas las posibilidades, intentando descubrir todos los valores derivados de la pérdida de algún componente del sistema. Muchas veces se trata del valor añadido que gana un atacante y la repercusión de esa ganancia para el entorno, además del costo del elemento perdido. Deben considerarse elementos como:

- Información aparentemente inocua como datos personales, que pueden permitir a alguien suplantar identidades.

⁸⁴ POYATO, Chelo-COLL, Francisco-MORENO David. Definición de una política de seguridad. España. 2000. <http://www.rediris.es/cert>

⁸⁵ RFC 1244: Site Security Handbook. J. Reynolds – P. Holbrook. Julio 1991

- Datos confidenciales de acuerdos y contratos que un atacante podría usar para su beneficio.
- Tiempos necesarios para obtener ciertos bienes. Un atacante podría acceder a ellos para ahorrarse el costo (y tiempo) necesario para su desarrollo.

9.2.3.3 PUNTO DE EQUILIBRIO

Una vez evaluados los riesgos y los costos en los que se está dispuesto a incurrir y decidido el nivel de seguridad a adoptar, podrá obtenerse un punto de equilibrio entre estas magnitudes:

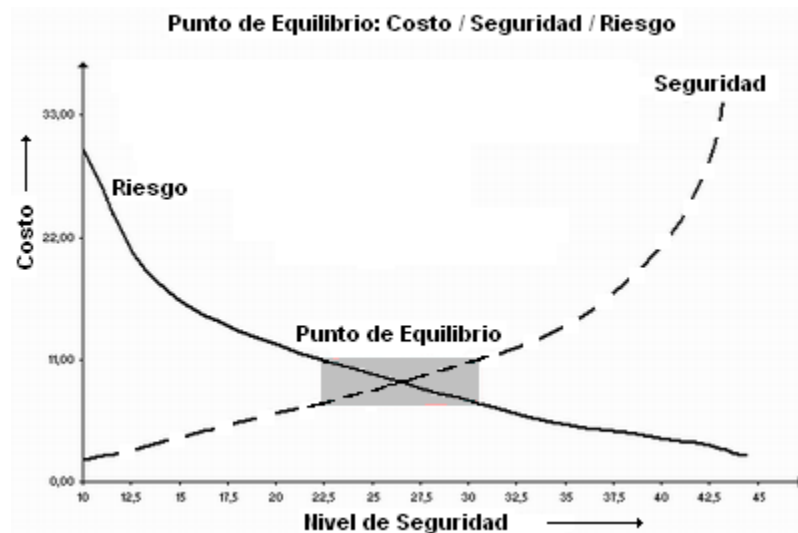


Gráfico 9.1 – Punto de equilibrio Costo/Seguridad

Como puede apreciarse los riesgos disminuyen al aumentar la seguridad (y los costos en los que incurre) pero como ya se sabe los costos tenderán al infinito sin lograr el 100% de seguridad y por supuesto nunca se logrará no correr algún tipo de riesgo. Lo importante es lograr conocer cuan seguro se estará conociendo los costos y los riesgos que se corren (Punto de Equilibrio).

9.3 ESTRATEGIA DE SEGURIDAD

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

En cada caso considerado, el plan de seguridad debe incluir una estrategia Proactiva y otra Reactiva⁸⁶.

La **Estrategia Proactiva** (proteger y proceder) o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes

⁸⁶ BENSON, Christopher. Estrategias de Seguridad. Inobis Consulting Pty Ltd. Microsoft® Solutions. <http://www.microsoft.com/latam/technet/articulos/200011>

en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar esta estrategia.

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

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

- **Lo que no se permite expresamente está prohibido:** significa que la organización proporciona una serie de servicios bien determinados y documentados, y cualquier otra cosa está prohibida.
- **Lo que no se prohíbe expresamente está permitido:** significa que, a menos que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estarán.

Estas posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no.

Actualmente, y “gracias” a las, cada día más repetitivas y eficaces, acciones que atentan contra los sistemas informáticos los expertos se inclinan por recomendar la primera política mencionada.

9.3.1 IMPLEMENTACIÓN

La implementación de medidas de seguridad, es un proceso Técnico–Administrativo. Como este proceso debe abarcar TODA la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

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

Por esto, será necesario sopesar cuidadosamente la ganancia en seguridad respecto de los costos administrativos y técnicos que se generen.

Es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

Una PSI informática deberá abarcar:

- Alcance de la política, incluyendo sistemas y personal sobre el cual se aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.

- Responsabilidad de cada uno de los servicios, recurso y responsables en todos los niveles de la organización.
- Responsabilidades de los usuarios con respecto a la información que generan y a la que tienen acceso.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas al alcance de la política.
- Definición de violaciones y las consecuencias del no cumplimiento de la política.
- Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Pero, no debe especificar con exactitud qué pasara o cuándo algo sucederá; ya que no es una sentencia obligatoria de la ley.
- Explicaciones comprensibles (libre de tecnicismos y términos legales pero sin sacrificar su precisión) sobre el porque de las decisiones tomadas.
- Finalmente, como documento dinámico de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta y rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios, etc.

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

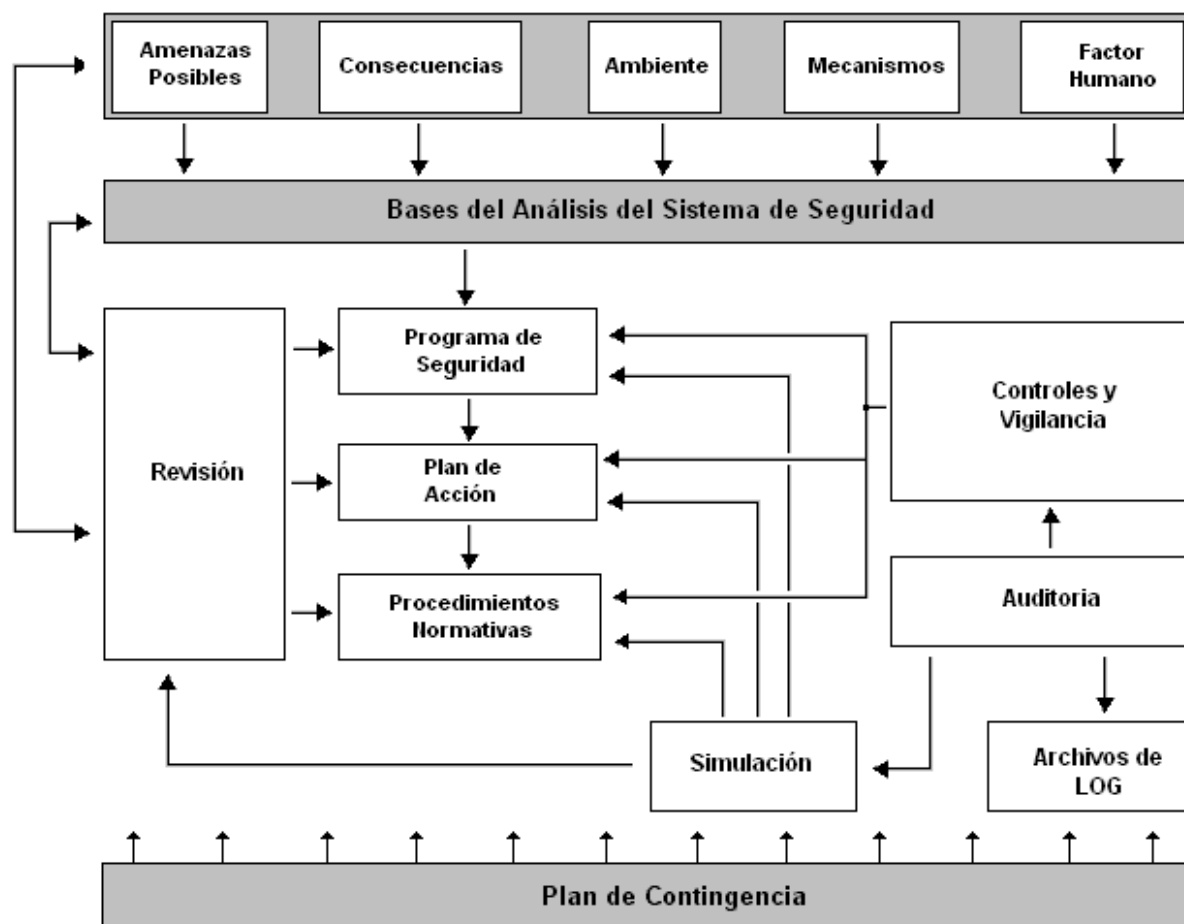


Gráfico 9.2 – Fuente: Manual de Seguridad en Redes. <http://www.arcert.gov.ar>

Se comienza realizando una evaluación del factor humano, el medio en donde se desempeña, los mecanismos con los cuales se cuenta para llevar a cabo la tarea encomendada, las amenazas posibles y sus posibles consecuencias.

Luego de evaluar estos elementos y establecida la base del análisis, se originan un programa de seguridad, el plan de acción y las normas y procedimientos a llevar a cabo.

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

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

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

Es importante destacar que la Seguridad debe ser considerada desde la fase de diseño de un sistema. Si la seguridad es contemplada luego de la implementación del mismo, el personal se enfrentará con problemas técnicos, humanos y administrativos muchos mayores

que implicaran mayores costos para lograr, en la mayoría de los casos, un menor grado de seguridad.

“Construya la seguridad desde el principio. La máxima de que es más caro añadir después de la implementación es cierta.”⁸⁷

Julio C. Ardita menciona: “Muchas veces nos llaman cuando está todo listo, faltan dos semanas y quieren que lo aseguremos (...) llegamos, miramos y vemos que la seguridad es imposible de implementar. Últimamente nos llaman en el diseño y nosotros los orientamos y proponemos las soluciones que se pueden adoptar (...)”⁸⁸

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

9.3.2 AUDITORÍA Y CONTROL

Se considera que la Auditoría son los “ojos y oídos” de la dirección, que generalmente no puede, no sabe o no debe realizar las verificaciones y evaluaciones.

La Auditoría consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno y cuando lo hace.

En cuanto al objetivo del Control es contrastar el resultado final obtenido contra el deseado a fin de incorporar las correcciones necesarias para alcanzarlo, o bien verificar la efectividad de lo obtenido.

9.3.3 PLAN DE CONTINGENCIA

Pese a todas las medidas de seguridad puede (va a) ocurrir un desastre. De hecho los expertos en seguridad afirman “sutilmente” que hay que definir un plan de recuperación de desastres “para cuando falle el sistema”, no “por si falla el sistema”⁸⁹.

Por tanto, es necesario que el Plan de Contingencias que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo y global posible.

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

⁸⁷ “Encuesta de Seguridad Informática 2001”. Marzo de 2001. Ernst & Young. <http://www.ey.com>

⁸⁸ ARDITA, Julio César. Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. <http://www.cybsec.com>

⁸⁹ POYATO, Chelo. COLL, Francisco. MORENO, David. Recomendaciones de Seguridad. Definición de una Política de Seguridad. <http://www.rediris.es/cert>

Se entiende por **Recuperación**, “tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información”⁹⁰.

Se dice que el Plan de Contingencias es el encargado de sostener el modelo de Seguridad Informática planteado y de levantarlo cuando se vea afectado.

La recuperación de la información se basa en el uso de una política de copias de seguridad (Backup) adecuada.

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.
- Creación del sector o determinación del responsable: usualmente la designación del Administrador de seguridad.
- La identificación de las herramientas de software para responder a incidentes y eventos.
- La investigación y desarrollo de otras herramientas de Seguridad Informática.
- La realización de actividades formativas 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. 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, 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.

⁹⁰ POYATO, Chelo. COLL, Francisco. MORENO, David. Recomendaciones de Seguridad. Definición de una Política de Seguridad. <http://www.rediris.es/cert>

9.3.5 BACKUPS

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

Como siempre, será necesario realizar un análisis Costo/Beneficio para determinar qué información será almacenada, los espacios de almacenamiento destinados a tal fin, la forma de realización, las estaciones de trabajo que cubrirá el backup, etc.

Para una correcta realización y seguridad de backups se deberán tener en cuenta estos puntos:

1. Se debe de contar con un procedimiento de respaldo de los sistemas operativos y de la información de los usuarios, para poder reinstalar fácilmente en caso de sufrir un accidente.
2. Se debe determinar el medio y las herramientas correctas para realizar las copias, basándose en análisis de espacios, tiempos de lectura/escritura, tipo de backup a realizar, etc.
3. El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.
4. Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenados, etc.
5. Se debe de contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.
6. Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento secundarios. Por ejemplo, la información se debe encriptar antes de respaldarse.
7. Se debe de contar con un procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
8. Mantener equipos de hardware, de características similares a los utilizados para el proceso normal, en condiciones para comenzar a procesar en caso de desastres físicos. Puede optarse por:
 - **Modalidad Externa:** otra organización tiene los equipos similares que brindan la seguridad de poder procesar la información, al ocurrir una contingencia, mientras se busca una solución definitiva al siniestro producido.
 - **Modalidad Interna:** se tiene más de un local, en donde uno es espejo del otro en cuanto a equipamiento, características técnicas y capacidades físicas. Ambos son susceptibles de ser usados como equipos de emergencia.

Se debe asegurar reproducir toda la información necesaria para la posterior recuperación sin pasos secundarios. Por ejemplo, existe información que es función de otra (checksums). Si sólo se almacenara la información principal, sin sus checksums, esto puede derivar en la inutilización de la misma cuando se recupere el backup.

9.3.6 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 (Ethical Hacking) 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 de aprendizaje. Nunca termina, ya que debe evaluarse y revisarse de forma periódica para poder implementar mejoras.

9.4 LA POLÍTICA

Después de nueve capítulos de detalles técnicos, legales, administrativos y humanos ha llegado la hora esperada por mí y espero por el lector. Las páginas que siguen tienen la intención de ofrecer un acercamiento a una metodología sistemática en la importante tarea de administrar la Seguridad Informática.

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

9.4.1 NIVEL FÍSICO

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

La defensa contra agentes nocivos conlleva tanto medidas proactivas (limitar el acceso) como normativas de contingencia (que hacer en caso de incendio) o medidas de recuperación (realizar copias de seguridad). El grado de seguridad solicitado establecerá las necesidades: desde el evitar el café y el tabaco en las proximidades de equipos electrónicos, hasta el establecimiento de controles de acceso a la sala de equipos.

Lo más importante es recordar que quien tiene acceso físico a un equipo tiene control absoluto del mismo. Por ello sólo deberían accederlo aquellas personas que sea estrictamente necesario.

9.4.1.1 AMENAZA NO INTENCIONADA (DESASTRE NATURAL)

El siguiente ejemplo ilustra una posible situación:

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

Directivas:

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

9.4.2 NIVEL HUMANO

9.4.2.1 EL USUARIO

Estas son algunos de las consideraciones que se deberían tener en cuenta para la protección de la información:

1. Quizás el usuario contempla todas las noticias de seguridad con escepticismo, piensan que los Administradores son paranoicos y se aprovechan de las contadas situaciones dadas. Quizás tengan razón, pero se debe recordar que el mundo virtual no es más que una pequeña muestra del mundo físico, con el agregado que es el campo ideal de impunidad y anonimidad.

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

Ejemplo: Se instaló un Firewall personal en dos usuarios normales de Internet, utilizando modems y Windows 98 como sistema operativo. Los resultados obtenidos en los archivos de Logs de estos usuarios fueron los siguientes:

Usuario 1 ubicado en Paraná (Entre Ríos-Argentina): 49 scaneos de puertos y 14 intentos de instalación de troyanos en 10 días.

Usuario 2 ubicado en Buenos Aires (Argentina): 28 scaneos de puertos en 8 días.

La pregunta ya no es ¿seré atacado?; a cambiando a ¿cuándo seré atacado?.

3. Generalmente se sobrevalora la capacidad de un atacante. Al contrario de la creencia popular no se necesita ser un Gurú para ingresar en una computadora y generalmente quienes lo hace son Script-Kiddies en busca de “diversión”. De hecho un Gurú siempre tendrá “mejores cosas que hacer”.
4. Convencerse de que TODOS los programas existentes tienen vulnerabilidades conocidas y desconocidas es muy bueno. Esta idea permite no sobrevalorar la seguridad de su sistema.
Ejemplo: Un usuario dice a otro: “Yo utilizo Linux porque es más seguro que Windows”. Esto es una falacia disfrazada: el usuario debería decir que Linux PUEDE ser más seguro que Windows. De hecho cualquier sistema bien configurado puede ser más seguro que uno que no lo está.
5. La Regla de Oro que todo usuario debe tomar como obligación (y su responsabilidad) es tomar la seguridad de su computadora en serio. Recordar que el eslabón más débil de una cadena equivale a la resistencia de la misma es muy bueno en este momento.

Ningún usuario inocente estará contento si su nombre aparece en la lista de posibles intruso en una red, nada más que porque alguien decidió utilizarlo para tales fines. Tampoco es bueno ser acusado de expandir un virus por el simple hecho de enviar mails sin comprobarlos anteriormente.

Los procedimientos simples mencionados pueden evitar grandes dolores de cabezas.

9.4.2.1.1 Amenaza no Intencionada (Empleado)

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

Un empleado, no desea perder la información que ha guardado en su disco rígido, así que la copia (el disco completo) a su carpeta particular del servidor, que resulta ser también el servidor principal de aplicaciones de la organización. No se han definido cuotas de disco para las carpetas particulares de los usuarios que hay en el servidor. El disco rígido del usuario tiene 6 GB de información y el servidor tiene 6,5 GB de espacio libre. El servidor de aplicaciones deja de responder a las actualizaciones y peticiones porque se ha quedado sin espacio en el disco. El resultado es que se deniega a los usuarios los servicios del servidor de aplicaciones y la productividad se interrumpe.

A continuación, se explica la metodología que se debería haber adoptado antes de que el usuario decida realizar su copia de seguridad:

Directivas:

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

9.4.2.1.2 Amenaza Malintencionada (Insider)

Una empresa competidora ofrece a un usuario cierta suma de dinero para obtener el diseño del último producto desarrollado por su empresa. Como este usuario carece de los permisos necesarios para obtener el diseño se hace pasar como un Administrador, y usando ingeniería social, consigue el nombre de usuario y password de un usuario con los permisos que él necesita.

La política de seguridad asociada a este evento debería haber contemplado:

Directivas:

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

9.4.1.2 PERSONAS AJENAS AL SISTEMA

9.4.1.2.1 Amenaza No Intencionada

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

Directivas:

1. **Predecir Ataque/Riesgo:** Negación de servicio del servidor de correo electrónico por gran la cantidad de mensajes enviados/recibidos.
2. **Amenaza:** Virus.
3. **Ataque:** Virus de correo electrónico.
4. **Estrategia Proactiva:**
 - a. Predecir posibles daños: pérdida de productividad por negación de servicio.
 - b. Determinar y minimizar vulnerabilidades: actualización de antivirus y concientización de usuarios en el manejo del correo electrónico.
 - c. Evaluar planes de contingencia: evaluar la importancia de un servidor backup. Antivirus.
5. **Estrategia Reactiva:**
 - a. Evaluar daños: pérdida de producción.
 - b. Determinar su origen: caída del servidor por overflow de mensajes.
 - c. Reparación de daños: implementar el servidor backup. Eliminación del virus causante del problema.
 - d. Documentar y aprender.
 - e. Implementar plan de contingencia: servidor backup.
6. **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

9.4.1.2.2 Amenaza Malintencionada (Out-Sider)

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

Directivas:

7. **Predecir Ataque/Riesgo:** Ingreso al sistema por vulnerabilidades en los sistemas o política de claves ineficiente.
8. **Amenaza:** Outsider recopilando información significativa.
9. **Ataque:** Ingreso al sistema.
10. **Estrategia Proactiva:**
 - a. Predecir posibles daños: Robo y venta de información. Daño a la imagen de la empresa.
 - b. Determinar y minimizar vulnerabilidades: actualización de sistemas vulnerables. Concientización a los usuarios en el manejo de contraseñas fuertes.
 - c. Evaluar planes de contingencia: implementación de servidor backup para casos de daño de la información. Recuperación de imagen. Evaluar formas de minimizar el daño por la información robada.
11. **Estrategia Reactiva:**
 - f. Evaluar daños: información susceptible robada.
 - g. Determinar su origen: ingreso al sistema.
 - h. Reparación de daños.
 - i. Documentar y aprender.
 - j. Implementar plan de contingencia: servidor backup.
12. **Examinar resultados y eficacia de la directiva:** Ajustar la directiva con los nuevos conceptos incorporados.

CONCLUSIONES



“Un largo camino comienza con su primer paso”

Proverbio Chino

AISLAMIENTO VS GLOBALIZACIÓN

Abierta, Universal, Económica y Segura. Esas son las propiedades que adjudican algunos a la información. Lograr estándares en el mundo altamente tecnificado de hoy es quizás la principal barrera con las que chocan los profesionales para “asegurar la Seguridad”.

Por otro lado, la situación internacional actual exige una concientización, por parte de todos, que la información es conocimiento y como tal debemos atribuirle la importancia que merece. Esta importancia incluye estudiar y lograr la forma de protegerla.

Esto plantea una paradoja:

- si sumamos seguridad, bajan las posibilidades de acceder a la información, lo que es igual al Aislamiento y la Marginación.
- si sumamos información, lo hacemos de forma insegura, lo que nos hace Globalmente Vulnerables.

La convergencia de los sistemas multiplica exponencialmente los problemas de seguridad planteados. El equilibrio es difícil, el espectro a cubrir es amplio y, como dificultad

extra, el campo de trabajo es intangible. Esto hace necesario desarrollar técnicas y/o adaptar las existentes de forma tal de circunscribir nuestro trabajo de conseguir información–conocimiento dentro de un marco de seguridad.

DISEÑO SEGURO REQUERIDO

Cuando se diseña un sistema se lo hace pensando en su Operatividad–Funcionalidad dejando de lado la Seguridad

Será necesario establecer una correspondencia y pertenencia entre las técnicas adoptadas conformando un sistema de seguridad; y no procedimientos aislados que contribuyan al caos general existente. Esto sólo puede lograrse al integrar la seguridad desde el comienzo, desde el diseño, desde el desarrollo.

LEGISLACIÓN VIGENTE

Las tecnologías involucradas en estos procesos condicionan las técnicas empleadas, los tiempos condicionan esas tecnologías y, paradójicamente, las legislaciones deben adaptarse a los rápidos cambios producidos. Esto hace obligatorio no legislar sobre tecnologías actuales, sino sobre conceptos y abstracciones que podrán ser implementados con distintas tecnologías en el presente y el futuro.

Es urgente legislar un marco legal adecuado, no solo que castigue a los culpables sino que desaliente acciones hostiles futuras.

TECNOLOGÍA EXISTENTE

Existen infinidad de métodos (muchas veces plasmados en herramientas) que permiten violar un sistema.

El profesional cuenta con la misma tecnología para la evaluación de la seguridad del bien a proteger y otras pensadas para la protección como fin. Esto hace que muchas veces, la seguridad, sea asunto de la idoneidad del profesional.

En algunos campos, la Tecnología deberá ampararnos ante la desaparición de elementos naturales. Por mencionar un ejemplo: la firma digital (Tecnología Criptográfica) debe cubrir la brecha que deja la inexistencia de la firma caligráfica en archivos de información.

DAÑOS MINIMIZABLES

Algunos pocos métodos realmente novedosos de infiltración ponen en jaque los sistemas de seguridad. Aquí, se prueba la incapacidad de lograr 100% de seguridad, pero también es hora de probar que los riesgos, la amenaza, y por ende los daños pueden ser llevados a su mínima expresión.

Muchas veces basta con restringir accesos a información no utilizada o que no corresponde a los fines planteados. Otras veces la capacitación será la mejor herramienta para disminuir drásticamente los daños.

RIESGOS MANEJABLES

He probado (me he probado) que: La Seguridad Perfecta requiere un nivel de perfección que realmente no existe, y de hecho dudo que algún día exista, pero los riesgos deben y pueden ser manejables.

COSTOS

El costo en el que se incurre suele ser una fruslería comparados con aquellos luego de producido un daño. El desconocimiento y la falta de información son el principal inconveniente cuando se evalúa la inclusión de seguridad como parte de un sistema.

PERSONAS INVOLUCRADAS

El desarrollo de software es una “ciencia” imperfecta; y como tal es vulnerable. Es una realidad, y espero haberlo demostrado en el extenso capítulo de “Amenazas Humanas”, que la Seguridad involucra manipulación de naturaleza humana.

Es importante comprender que:

1. La Seguridad consiste en Tecnología y Política. Es decir que la combinación de la Tecnología y su forma de utilización determina cuan seguros son los sistemas.
2. El problema de la Seguridad no puede ser resuelto por única vez. Es decir que constituye un viaje permanente y no un destino.
3. En última instancia la Seguridad es una serie de movimientos entre “buenos” y “malos”.

A manera de despedida deseo dejar un resumen realizado por el equipo de Microsoft Security Response Center sobre la forma y el cuándo nuestra computadora deja de ser nuestra.

Las 10 Leyes Inmutables de la (in)seguridad

- XXII. Si una mala persona puede persuadirlo para ejecutar su programa en SU computadora, esta deja de ser suya.
- XXIII. Si una mala persona puede alterar el sistema operativo en SU computadora, esta deja de ser suya.
- XXIV. Si una mala persona tiene acceso físico sin restricción a SU computadora, esta deja de ser suya.
- XXV. Si usted permite a una mala persona, subir un programa a SU sitio web, este deja de ser suyo.
- XXVI. Las contraseñas débiles constituyen un atentado a la seguridad.
- XXVII. Una sola máquina es segura en la medida que el Administrador es fidedigno.
- XVIII. Los datos encriptados son seguros en la misma medida que la clave de desencriptación lo sea.
- XXIX. Un antivirus desactualizado sólo es parcialmente mejor que ninguno.
- XXX. La anonimidad absoluta no es práctica, ni en la vida real ni en la web.
- XXXI. La tecnología no es una panacea.

ANEXO I



LEYES

LEYES ARGENTINAS VIGENTES

LEY 11.723

Sancionada el 26 de Septiembre de 1933.

Art. 1: A los efectos de la presente ley, las obras científicas, literarias y artísticas, comprenden los escritos de toda naturaleza y extensión; las obras dramáticas, composiciones musicales, dramático–musicales; las cinematográficas, coreográficas y pantomímicas; las obras de dibujo, pintura, escultura, arquitectura; modelos y obras de arte o ciencia aplicadas al comercio o a la industria; los impresos, planos y mapas; los plásticos, fotografías, grabados y fonogramas, en fin; toda producción científica, literaria, artística o didáctica sea cual fuere el procedimiento de reproducción.

Art. 2: El derecho de propiedad de una obra científica, literaria o artística, comprende para su autor la facultad de disponer de ella, de publicarla, de ejecutarla, de representarla, y

exponerla en público, de enajenarla, de traducirla, de adaptarla o de autorizar su traducción y de reproducirla en cualquier forma.

Art. 3: Al editor de una obra anónima o seudónima corresponderán con relación a ella los derechos y las obligaciones del autor, quien podrá recabarlos para sí, justificando su personalidad. Los autores que emplean seudónimos podrán registrarlos adquiriendo la propiedad de los mismos.

Art. 4: Son titulares del derecho de propiedad intelectual:

- a) el autor de la obra;
- b) sus herederos o derechohabientes;
- c) los que con permiso del autor la traducen, refunden, adaptan, modifican o transportan sobre la nueva obra intelectual resultante.

Art. 5: La propiedad intelectual corresponde a los autores durante su vida y a sus herederos o derechohabientes durante setenta años contados a partir del 1º de enero del año siguiente al de la muerte del autor.

En los casos de obras en colaboración, este término comenzará a contarse desde el 1º de enero del año siguiente al de la muerte del último colaborador. Para las obras póstumas, el término de setenta años comenzará a correr a partir del 1º de enero del año siguiente al de la muerte del autor.

En el caso de que un autor falleciera sin dejar herederos, y se declarase vacante su herencia, los derechos que a aquél correspondiesen sobre sus obras pasarán al Estado por todo el término de la ley, sin perjuicio de los derechos de terceros.

Art. 6: Los herederos o derechohabientes no podrán oponerse a que terceros reediten las obras del causante cuando dejen transcurrir más de diez años sin disponer su publicación.

Tampoco podrán oponerse los herederos o derechohabientes a que terceros traduzcan las obras del causante después de diez años de su fallecimiento.

En estos casos, si entre el tercero editor y los herederos o derechohabientes no hubiera acuerdo sobre las condiciones de impresión o la retribución pecuniaria, ambas serán fijadas por árbitros.

Art. 7: Se consideran obras póstumas, además de las no publicadas en vida del autor, las que lo hubieran sido durante ésta, si el mismo autor a su fallecimiento las deja refundidas, adicionadas, anotadas o corregidas de una manera tal que merezcan reputarse como obras nuevas.

Art. 8: La propiedad intelectual de las obras anónimas pertenecientes a instituciones, corporaciones o personas jurídicas, durará cincuenta años contados desde su publicación.

Art. 9: Nadie tiene derecho a publicar, sin permiso de los autores o de sus derechohabientes, una producción científica, literaria, artística o musical que se haya anotado o copiado durante su lectura, ejecución o exposición pública o privada.

Art. 10: Cualquiera puede publicar con fines didácticos o científicos, comentarios, críticas o notas referentes a las obras intelectuales, incluyendo hasta mil palabras de obras literarias o científicas u ocho compases en las musicales y en todos los casos sólo las partes del texto indispensable a ese efecto.

Quedan comprendidas en esta disposición las obras docentes, de enseñanza, colecciones, antologías y otros semejantes.

Cuando las inclusiones de obras ajenas sean la parte principal de la nueva obra, podrán los tribunales fijar equitativamente en juicio sumario la cantidad proporcional que les corresponde a los titulares de los derechos de las obras incluidas.

Art. 11: Cuando las partes o los tomos de una misma obra hayan sido publicados por separado en años distintos, los plazos establecidos por la presente ley corren para cada tomo o cada parte, desde el año de la publicación. Tratándose de obras publicadas parcial o periódicamente por entregas o folletines, los plazos establecidos en la presente ley corren a partir de la fecha de la última entrega de la obra.

Art. 12: La propiedad intelectual se regirá por las disposiciones del derecho común, bajo las condiciones y limitaciones establecidas en la presente ley.

DE LAS OBRAS EXTRANJERAS

Art. 13: Todas las disposiciones de esta ley salvo las del art. 57, son igualmente aplicables a las obras científicas, artísticas y literarias, publicadas en países extranjeros, sea cual fuere la nacionalidad de sus autores, siempre que pertenezcan a naciones que reconozcan el derecho de propiedad intelectual.

Art. 14: Para asegurar la protección de la ley argentina, el autor de una obra extranjera sólo necesita acreditar el cumplimiento de las formalidades establecidas para su protección por las leyes del país en que se haya hecho la publicación, salvo lo dispuesto en el art. 23, sobre contratos de traducción.

Art. 15: La protección que la ley argentina acuerda a los autores extranjeros no se extenderá a un período mayor que el reconocido por las leyes del país donde se hubiere publicado la obra. Si tales leyes acuerdan una protección mayor regirán los términos de la presente ley.

DE LA COLABORACIÓN

Art. 16: Salvo convenios especiales los colaboradores de una obra disfrutan derechos iguales; los colaboradores anónimos de una compilación colectiva no conservan derecho de propiedad sobre su contribución de encargo y tendrán por representante legal al editor.

Art. 17: No se considera colaboración la mera pluralidad de autores, sino en el caso en que la propiedad no pueda dividirse sin alterar la naturaleza de la obra. En las composiciones musicales con palabras, la música y la letra se consideran como dos obras distintas.

Art. 18: El autor de un libreto o composición cualquiera puesta en música, será dueño exclusivo de vender o imprimir su obra literaria separadamente de la música, autorizando o prohibiendo la ejecución o representación pública de su libreto y el compositor podrá hacerlo igualmente con su obra musical, con independencia del autor del libreto.

Art. 19: En caso de que dos o varios autores hayan colaborado en una obra dramática o lírica, bastará para su representación pública la autorización concedida por uno de ellos, sin perjuicio de las acciones personales a las que hubiera lugar.

Art. 20: Salvo convenios especiales, los colaboradores en una obra cinematográfica tienen iguales derechos, considerándose tales al autor del argumento y el productor de la

película. Cuando se trate de una obra cinematográfica musical, en que haya colaborado un compositor, éste tiene iguales derechos que el autor del argumento y el productor de la película.

Art. 21: Salvo convenios especiales:

El productor de la película cinematográfica, tiene facultad para proyectarla, aun sin el consentimiento del autor del argumento o del compositor, sin perjuicio de los derechos que surgen de la colaboración.

El autor del argumento tiene la facultad exclusiva de publicarlo separadamente y sacar de él una obra literaria o artística de otra especie. El compositor tiene la facultad exclusiva de publicar y ejecutar separadamente la música.

Art. 22: El productor de la película cinematográfica, al exhibirla en público, debe mencionar su propio nombre, el del autor de la acción o argumento o el de los autores de las obras originales de las cuales haya tomado el argumento de la obra cinematográfica, el del compositor, el del director o adaptador y el de los intérpretes principales.

Art. 23: El titular de un derecho de traducción tiene sobre ella el derecho de propiedad intelectual en las condiciones convenidas con el autor, siempre que los contratos de traducción se inscriban en el Registro Nacional de la Propiedad Intelectual dentro del año de la publicación de la obra traducida.

La falta de inscripción del contrato de traducción trae como consecuencia la suspensión del derecho de autor o sus derechohabientes hasta el momento en que la efectúe, recuperándose dichos derechos en el acto mismo de la inscripción, por el término y condiciones que correspondan, sin perjuicio de la validez de las traducciones hechas durante el tiempo en que el contrato no estuvo inscripto.

Art. 24: El traductor de una obra que no pertenece al dominio privado sólo tiene propiedad sobre su versión y no podrá oponerse a que otros la traduzcan de nuevo.

Art. 25: El que adapte, transporte, modifique o parodie una obra con la autorización del autor, tiene sobre su adaptación, transporte, modificación o parodia, el derecho de coautor, salvo convenio en contrario.

Art. 26: El que adapte, transporte, modifique o parodie una obra que no pertenezca al dominio privado, será dueño exclusivo de su adaptación, transporte, modificación o parodia, y no podrá oponerse a que otros adapten, transporten, modifiquen o parodien la misma obra.

DISPOSICIONES ESPECIALES

Art. 27: Los discursos políticos o literarios y en general las conferencias sobre temas intelectuales, no podrán ser publicados si el autor no lo hubiere expresamente autorizado. Los discursos parlamentarios no podrán ser publicados con fines de lucro, sin la autorización del autor. Exceptúase la información periodística.

Art. 28: Los artículos no firmados, colaboraciones anónimas, reportajes, dibujos, grabados o informaciones en general que tengan un carácter original y propio, publicados por un diario, revista u otras publicaciones periódicas por haber sido adquiridos u obtenidos por éste o por una agencia de informaciones con carácter de exclusividad, serán considerados como de propiedad del diario, revista, u otras publicaciones periódicas, o de la agencia.

Las noticias de interés general podrán ser utilizadas, transmitidas o retransmitidas; pero cuando se publiquen en su versión original será necesario expresar la fuente de ellas.

Art. 29: Los autores de colaboraciones firmadas en diarios, revistas y otras publicaciones periódicas son propietarios de su colaboración. Si las colaboraciones no estuvieren firmadas, sus autores sólo tienen derecho a publicarlas en colección, salvo pacto en contrario con el propietario del diario, revista o periódico.

Art. 30: Los propietarios de las publicaciones periodísticas deberán inscribirlas en el Registro Nacional de la Propiedad Intelectual. La inscripción del periódico protege a las obras intelectuales publicadas en él y sus autores podrán solicitar al Registro una certificación que acredite aquella circunstancia. Para inscribir una publicación periódica deberá presentarse al Registro Nacional de la Propiedad Intelectual un ejemplar de la última edición acompañado del correspondiente formulario.

La inscripción deberá renovarse anualmente y para mantener su vigencia se declarará mensualmente ante el Registro, en los formularios que correspondan, la numeración y fecha de la autenticidad de las mismas.

El incumplimiento de esta obligación, sin perjuicio de las responsabilidades que puedan resultar para con terceros, será penado con multa de hasta cinco mil pesos moneda nacional que aplicará el director del Registro Nacional de la Propiedad Intelectual. El monto de la multa podrá apelarse ante el Ministerio de Justicia.

El Registro podrá requerir en cualquier momento la presentación de ejemplares de esta colección e inspeccionar la editorial para comprobar el cumplimiento de la obligación establecida en el párrafo anterior.

Si la publicación dejase de aparecer definitivamente deberá comunicarse al Registro y remitirse la colección sellada a la Biblioteca Nacional, dentro de los seis meses subsiguientes al vencimiento de la última inscripción.

El incumplimiento de esta última obligación, será penada con una multa de cinco mil pesos moneda nacional (texto ordenado por Dec. Ley 12.063/57).

Art. 31: El retrato fotográfico de una persona no puede ser puesto en el comercio sin el consentimiento expreso de la persona misma, y muerta ésta, de su cónyuge e hijos o descendientes directos de éstos, o en su defecto del padre o de la madre. Faltando el cónyuge, los hijos, el padre o la madre, o los descendientes directos de los hijos, la publicación es libre. La persona que haya dado su consentimiento puede revocarlo resarciendo daños y perjuicios. Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubieran desarrollado en público.

Art. 32 : El derecho de publicar las cartas pertenece al autor. Después de la muerte del autor es necesario el consentimiento de las personas mencionadas en el artículo que antecede y en el orden allí indicado.

Art. 33: Cuando las personas cuyo consentimiento sea necesario para la publicación del retrato fotográfico o de las cartas, sean varias y haya desacuerdo entre ellas, resolverá la autoridad competente.

Art. 34: Para las obras fotográficas, la duración del derecho de propiedad es de 20 años desde la primera publicación. Sin perjuicio de las condiciones y protección de las obras originales reproducidas o adaptadas a películas, para las obras cinematográficas la duración del derecho de propiedad es de 30 años desde la fecha de la primera publicación. La fecha y el lugar de la publicación y el nombre o la marca del autor o del editor debe estar inscrita sobre la obra fotográfica o sobre la película, de lo contrario la reproducción de la obra fotográfica o audiovisual no podrá ser motivo de la acción penal establecida en esta ley.

Art. 35: El consentimiento a que se refiere el art. 31 para la publicación del retrato no es necesario después de transcurridos 20 años de la muerte de la persona retratada. Para la publicación de una carta, el consentimiento no es necesario después de transcurridos 20 años de la muerte del autor de la carta. Esto aun en el caso de que la carta sea objeto de protección como obra, en virtud de la presente ley.

Art. 36: Los autores de obras literarias, dramáticas, dramático-musicales y musicales, gozan del derecho exclusivo de autorizar:

- a) La recitación, la representación y la ejecución pública de sus obras;
- b) La difusión pública por cualquier medio de la recitación, la representación y la ejecución de sus obras.

Sin embargo, será lícita y estará exenta del pago de derechos de autor y de los intérpretes que establece el art. 56, la representación, la ejecución y la recitación de obras literarias o artísticas ya publicadas, en actos públicos organizados por establecimientos de enseñanza, vinculados en el cumplimiento de sus fines educativos, planes programas de estudio, siempre que el espectáculo no sea difundido fuera del lugar donde se realice y la concurrencia y la actuación de los intérpretes sea gratuita. También gozarán de la exención del pago del derecho de autor a que se refiere el párrafo anterior, la ejecución o interpretación de piezas musicales en los conciertos, audiciones y actuaciones públicas a cargo de las orquestas, bandas, fanfarrias, coros y demás organismos musicales pertenecientes a instituciones del Estado Nacional, de las provincias o de las municipalidades, siempre que la concurrencia de público a los mismos sea gratuita.

EXCEPCIÓN DE COPIA PRIVADA REMUNERADA PARA USO PERSONAL DE LA EDICIÓN

Art. 37: Habrá contrato de edición cuando el titular del derecho de propiedad sobre una obra intelectual, se obliga a entregarla a un editor y éste a reproducirla, difundirla y venderla.

Este contrato se aplica cualquiera sea la forma o sistema de reproducción o publicación.

Art. 38: El titular conserva su derecho de propiedad intelectual, salvo que lo renunciare por el contrato de edición. Puede traducir, transformar, refundir, etc., su obra y defenderla contra los defraudadores de su propiedad, aun contra el mismo editor.

Art. 39: El editor solo tiene los derechos vinculados a la impresión, difusión y venta, sin poder alterar el texto y sólo podrá efectuar las correcciones de imprenta si el autor se negare o no pudiese hacerlo.

Art. 40: En el contrato deberá constar el número de ediciones y el de ejemplares de cada una de ellas, como también la retribución pecuniaria del autor o de sus derechohabientes;

considerándose siempre oneroso el contrato, salvo prueba en contrario. Si las anteriores condiciones no constaran se estará a los usos y costumbres del lugar del contrato.

Art. 41: Si la obra pereciera en poder del editor antes de ser editada, éste deberá al autor o a sus derechohabientes como indemnización la regalía o participación que les hubiera correspondido en caso de edición. Si la obra pereciera en poder del autor o sus derechohabientes, éstos deberán la suma que hubieran percibido a cuenta de regalía y la indemnización de los daños y perjuicios causados.

Art. 42: No habiendo plazo fijado para la entrega de la obra por el autor o sus derechohabiente o para su publicación por el editor, el tribunal lo fijará equitativamente en juicio sumario y bajo apercibimiento de la indemnización correspondiente.

Art. 43: Si el contrato de edición tuviere plazo, y al expirar éste el editor conservase ejemplares de la obra no vendidos, el titular podrá comprarlos a precio de costo, más un 10% de bonificación. Si no hace el titular uso de este derecho, el editor podrá continuar la venta de dichos ejemplares en las condiciones del contrato fenecido.

Art. 44: El contrato terminará cualquiera sea el plazo estipulado si las ediciones convenidas se agotaran.

DE LA REPRESENTACIÓN

Art. 45: Hay contrato de representación cuando el autor o sus derechohabientes entregan a un tercero o empresario y éste acepta, una obra teatral para su representación pública.

Art. 46: Tratándose de obras inéditas que el tercero o el empresario debe hacer representar por primera vez, deberá dar recibo de ella al autor o sus derechohabientes y les manifestará dentro de los treinta días de su presentación si es o no aceptada. Toda obra aceptada debe ser representada dentro del año correspondiente a su representación. No siéndolo, el autor tiene derecho a exigir como indemnización una suma igual a la regalía de autor correspondiente a veinte representaciones de una obra análoga.

Art. 47: La aceptación de una obra no da derecho al aceptante a su reproducción o representación por otra empresa, o en otra forma que la estipulada no pudiendo hacer copias fuera de las indispensables, ni venderlas, ni localarlas sin permiso del autor.

Art. 48: El empresario es responsable, de la destrucción total o parcial del original de la obra y si por su negligencia ésta se perdiere se reproducere o representare, sin autorización del autor o sus derechohabientes, deberá indemnizar los daños y perjuicios causados.

Art. 49: El autor de una obra inédita aceptada por un tercero no puede mientras éste no la haya representado hacerla representar por otro, salvo convención en contrario.

Art. 50: A los efectos de esta ley se considerarán como representación o ejecución pública, la transmisión radiotelefónica, exhibición audiovisual, televisión o cualquier otro procedimiento de reproducción mecánica de toda obra literaria o artística.

DE LA VENTA

Art. 51: El autor y sus derechohabientes pueden enajenar o ceder total o parcialmente su obra. Esta enajenación es válida sólo durante el término establecido por la ley y confiere a

su adquirente el derecho a su aprovechamiento económico sin poder alterar su título, forma y contenido.

Art. 52 : Aunque el autor enajenare la propiedad de su obra, conserva sobre ella el derecho de exigir la fidelidad de su texto, en las impresiones, copias o reproducciones, como asimismo la mención de su nombre o seudónimo como autor.

Art. 53: La enajenación o cesión de una obra literaria, científica o musical, sea total o parcial, debe inscribirse en el Registro Nacional de Propiedad Intelectual, sin cuyo requisito no tendrá validez.

Art. 54: La enajenación o cesión de una obra pictórica, escultórica, fotográfica o de artes análogas, salvo pacto contrario, no lleva implícito el derecho de reproducción que permanece reservado al autor o sus derechohabientes.

Art. 55: La enajenación de planos, croquis y trabajos semejantes no da derecho al adquirente sino para la ejecución de la obra tenida en vista, no pudiendo enajenarlos, reproducirlos o servirse de ellos para otras obras. Estos derechos quedan reservados a su autor, salvo pacto en contrario.

DE LOS INTÉRPRETES

Art. 56: El intérprete de una obra literaria o musical, tiene el derecho de exigir una retribución por su interpretación difundida o retransmitida mediante la radiotelefonía, la televisión, o bien grabada o impresa sobre disco, película, cinta, hilo o cualquier otra sustancia o cuerpo apto para la reproducción sonora o visual. No llegándose a un acuerdo, el monto de la retribución quedará establecido en juicio sumario por la autoridad judicial competente.

El intérprete de una obra literaria o musical está facultado para oponerse a la divulgación de su interpretación, cuando la reproducción de la misma sea hecha en forma tal que pueda producir grave e injusto perjuicio a sus intereses artísticos.

Si la ejecución ha sido hecha por un coro o una orquesta, este derecho de oposición corresponde al director del coro o de la orquesta. Sin perjuicio del derecho de propiedad perteneciente al autor, una obra representada o ejecutada en un teatro o en una sala pública, puede ser difundida o retransmitida mediante la radiotelefonía o la televisión, con el solo consentimiento del empresario organizador del espectáculo.

DEL REGISTRO DE OBRAS

Art. 57: En el Registro Nacional de Propiedad Intelectual deberá depositar el editor de las obras comprendidas en el art. 1º., tres ejemplares completos de toda obra publicada, dentro de los tres meses siguientes a su aparición. Si la edición fuera de lujo o no excediera de cien ejemplares, bastará con depositar un ejemplar.

El mismo término y condiciones regirán para las obras impresas en país extranjero, que tuvieron editor en la República y se contará desde el primer día de ponerse en venta en territorio argentino.

Para las pinturas, arquitecturas, esculturas, etc., consistirá el depósito en un croquis o fotografía del original, con las indicaciones suplementarias que permitan identificarlas.

Para las obras audiovisuales, el depósito consistirá en una relación del argumento, diálogo, fotografías y escenarios de sus principales escenas.

Art. 58: El que se presente a inscribir una obra con los ejemplares o copias respectivas, será munido de un recibo provisorio, con los datos, fecha y circunstancias que sirven para identificar la obra, haciendo constar inscripción.

Art. 59: El Registro Nacional de la Propiedad Intelectual hará publicar diariamente en el Boletín Oficial, la nómina de las obras presentadas a inscripción, además de las actuaciones que la Dirección estime necesarias, con indicación de su título, autor, editor, clase a la que pertenece y demás datos que las individualicen. Pasado un mes desde la publicación, sin haberse deducido oposición, el Registro las inscribirá y otorgará a los autores el título de propiedad definitivo se éstos lo solicitaren.

Art. 60 : Si hubiese algún reclamo dentro del plazo del mes indicado, se levantará un acta de exposición, de la que se dará traslado por cinco días al interesado, debiendo el director del Registro Nacional de Propiedad Intelectual resolver el caso dentro de los diez días subsiguientes. De la resolución podrá apelarse al ministerio respectivo, dentro de los diez días y la resolución ministerial no será objeto de recurso alguno, salvo el derecho de quien se crea lesionado para iniciar el juicio correspondiente.

Art. 61 : El depósito de toda obra publicada es obligatorio para el editor. Si éste no lo hiciere será reprimido con una multa de diez veces el valor venal del ejemplar no depositado.

Art. 62: El depósito de las obras hecho por el editor, garantiza totalmente los derechos del autor sobre su obra y los del editor sobre su edición. Tratándose de obras no publicadas, el autor o sus derechohabientes pueden depositar una copia del manuscrito con la firma certificada del depositante.

Art. 63: La falta de inscripción trae como consecuencia la suspensión del derecho del autor hasta el momento en que la efectúa, recuperándose dichos derechos en el acto mismo de la inscripción, por el término y condiciones que corresponda, sin perjuicio de la validez de las reproducciones, ediciones, ejecuciones y toda otra publicación hecha durante el tiempo en que la obra no estuvo inscripta.

No se admitirá el registro de una obra sin la mención de su “pie de imprenta”. Se entiende por tal la fecha, lugar, edición y la mención del editor.

Art. 64: Todas las reparticiones oficiales y las instituciones, asociadas o personas que por cualquier concepto reciban subsidios del tesoro de la Nación, están obligadas a entregar a la Biblioteca del Congreso Nacional, sin perjuicio de lo dispuesto en el art. 57, el ejemplar correspondiente de las publicaciones que efectúen, en la forma y dentro de los plazos determinados en dicho artículo. Las reparticiones públicas están autorizadas a rechazar toda obra fraudulenta que se presente para su venta.

DE LA DIRECCIÓN NACIONAL DEL DERECHO DE AUTOR

Art. 65: El registro llevará los libros necesarios para que toda obra inscrita tenga su folio correspondiente, donde constarán su descripción, título, nombre del autor, fecha de la presentación, y demás circunstancias que a ella se refieran, como ser los contratos de que fuera objeto y las decisiones de los tribunales sobre la misma.

Art. 66: El registro inscribirá todo contrato de edición, traducción, comparaventa, cesión, participación y cualquier otro vinculado con el derecho de propiedad intelectual,

siempre que se hayan publicado las obras a las que se refieren y no sea contrario a las disposiciones de esta ley.

Art. 67: El registro percibirá por la inscripción de toda obra los derechos o aranceles que fijará el Poder Ejecutivo mientras ellos no sean establecidos en la ley respectiva.

Art. 68: El registro estará bajo la dirección de un abogado que deberá reunir las condiciones requeridas por el art. 70 de la Ley de Organización de los Tribunales y bajo la superintendencia del Ministerio de Justicia e Instrucción Pública.

Art. 69: Derogado por Dec. Ley 1224/58

Art. 70: Derogado por Dec. Ley 1224/58

DE LAS PENAS

Art. 71: Será reprimido con la pena establecida por el art. 172 del Código Penal, el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta ley.

Art. 72: Sin perjuicio de la disposición general del artículo precedente, se consideran casos especiales de defraudación y sufrirán la pena que él establece, además de secuestro de la edición ilícita:

- a) El que edite o reproduzca por cualquier medio o instrumento una obra inédita o publicada sin autorización de su autor o derechohabientes;
- b) El que falsifique obras intelectuales, entendiéndose como tal la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto;
- c) El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el título de la misma o alterando dolosamente su texto;
- d) El que edite o reproduzca mayor número de los ejemplares debidamente autorizados.

Art. 72 bis: Será reprimido con prisión de un mes a seis años:

- a) El que con fin de lucro reproduzca un fonograma sin autorización por escrito de su productor o del licenciado del productor;
- b) El que con el mismo fin facilite la reproducción ilícita mediante el alquiler de discos fonográficos u otros soportes materiales;
- c) El que reproduzca copias no autorizadas por encargo de terceros mediante un precio;
- d) El que almacene o exhiba copias ilícitas y no pueda acreditar su origen mediante la factura que lo vincule comercialmente con un productor legítimo;
- e) El que importe las copias ilegales con miras a su distribución al público.

El damnificado podrá solicitar en jurisdicción comercial o penal el secuestro de las copias de fonogramas reproducidas ilícitamente y de los elementos de reproducción.

El juez podrá ordenar esta medida de oficio, así como requerir caución suficiente al peticionario cuando estime que éste carezca de responsabilidad patrimonial. Cuando la medida precautoria haya sido solicitada por una sociedad autoral o de productores, cuya representatividad haya sido reconocida legalmente, no se requerirá caución.

Si no se dedujera acción, denuncia o querella, dentro de los 15 días de haberse practicado el secuestro, la medida podrá dejarse sin efecto a petición del titular de las copias secuestradas, sin perjuicio de la responsabilidad que recaiga sobre el peticionante. A pedido de damnificado, el Juez ordenará el comiso de las copias que materialicen el ilícito, así como los elementos de reproducción. Las copias ilícitas serán destruidas y los equipos de reproducción subastados. A fin de acreditar que no utilizará los aparatos de reproducción para fines ilícitos, el comprador deberá acreditar su carácter de productor fonográfico o de licenciado de un productor. El producto de la subasta se destinará a acrecentar el “fondo de fomento a las artes” del Fondo Nacional de Derechos de Autor a que se refiere el art. 6 del decreto-ley 1224/58.

Art. 73: Será reprimido con prisión de un mes a un año o con multa de \$ 100 a 1.000 m/n destinada al fondo de fomento creado por esta ley:

- a) El que representare o hiciere representar públicamente obras teatrales o literarias sin autorización de sus autores o derechohabientes;
- b) el que ejecutare o hiciere ejecutar públicamente obras musicales sin autorización de sus autores o derechohabientes.

Art. 74: Será reprimido con prisión de un mes a un año o con multa de treinta a un mil australes destinada al fondo de fomento creado por esta ley, el que atribuyéndose indebidamente la calidad de autor, derechohabiente o la representación de quien tuviere derechos hiciere suspender una representación o ejecución pública lícita.

Art. 75: En la aplicación de las penas establecidas por la presente ley, la acción se iniciará de oficio, por denuncia o querella.

Art. 76: El procedimiento y jurisdicción será el establecido por el respectivo Código de Procedimientos en lo Criminal vigente en el lugar donde se cometa el delito.

Art. 77: Tanto el juicio civil, como el criminal, son independientes y sus resoluciones definitivas no se afectan. Las partes sólo podrán usar en defensa de sus derechos las pruebas instrumentales de otro juicio, las confesiones y los peritajes, comprendido el fallo del jurado, más nunca las sentencias de los jueces respectivos.

Art. 78: La Comisión Nacional de Cultura representada por su presidente podrá acumular su acción a las de los damnificados para recibir el importe de las multas establecidas a su favor y ejercitar las acciones correspondientes a las atribuciones y funciones que se le asignan por esta ley.

DE LAS MEDIDAS PREVENTIVAS

Art. 79: Los jueces podrán, previa fianza de los interesados, decretar preventivamente la suspensión de un espectáculo teatral, cinematográfico, filarmónico u otro análogo; el embargo de las obras denunciadas, así como el embargo del producto que se haya percibido por todo lo anteriormente indicado y toda medida que sirva para proteger eficazmente los derechos que ampare esta ley.

Ninguna formalidad se ordena para aclarar los derechos del autor o de sus causahabientes. En caso de contestación, los derechos estarán sujetos a los medios de prueba establecidos por las leyes vigentes.

PROCEDIMIENTO CIVIL

Art. 80: En todo juicio motivado por esta ley, ya sea por aplicación de sus disposiciones, ya como consecuencia de los contratos y actos jurídicos que tenga relación con la propiedad intelectual, regirá el procedimiento que se determina en los artículos siguientes.

Art. 81: El procedimiento y términos serán, fuera de las medidas preventivas, el que se establece para las excepciones dilatorias en los respectivos Códigos de Procedimientos, en lo Civil y Comercial, con las siguientes modificaciones:

a) Siempre habrá lugar a prueba de pedido de las partes o de oficio pudiendo ampliarse su término a treinta días, si el juzgado lo creyere conveniente, quedando firme esta resolución;

b) Durante la prueba y a pedido de los interesados se podrá decretar una audiencia pública, en la sala del tribunal donde las partes, sus letrados y peritos expondrán sus alegatos u opiniones. Esta audiencia podrá continuar otros días si uno solo fuera insuficiente;

c) En las mismas condiciones del inciso anterior y cuando la importancia del asunto y la naturaleza técnica de las cuestiones lo requiera, se podrá designar un jurado de idóneos en la especialidad de que se trate, debiendo estar presidido para las cuestiones científicas por el decano de la Facultad de Ciencias Exactas o la persona que éste designare, bajo su responsabilidad, para reemplazarlo; para las cuestiones literarias, el decano de la Facultad de Filosofía y Letras; para las artísticas, el director del Museo Nacional de Bellas Artes, y para las musicales, el director del Conservatorio Nacional de Música. Complementarán el jurado dos personas designadas de oficio. El jurado se reunirá y deliberará en último término en la audiencia que establece el inciso anterior. Si no hubiere ella designado, en una especial y pública en la forma establecida en dicho inciso. Su resolución se limitará a declarar si existe o no la lesión a la propiedad intelectual, ya sea legal o convencional.

Esta solución valdrá como los informes de los peritos nombrados por partes contrarias, cuando se expiden de común acuerdo.

Art. 82: El cargo de jurado será gratuito y se le aplicarán las disposiciones procesales referentes a los testigos.

DE LAS DENUNCIAS ANTE EL REGISTRO NACIONAL DE LA PROPIEDAD INTELECTUAL

Art. 83: Después de vencidos los términos del art. 5º., podrá denunciarse al Registro Nacional de la Propiedad Intelectual la mutilación de una obra literaria, científica o artística, los agregados, las transposiciones, la infidelidad de una traducción, los errores de conceptos y las deficiencias en el conocimiento del idioma original o de la versión.

Estas denuncias podrá formularlas cualquier habitante de la Nación, o procederse de oficio, y para el conocimiento de ellas la dirección del Registro Nacional constituirá un jurado que integrarán:

a) Para las obras literarias, el Decano de la Facultad de Filosofía y Letras, dos representantes de la sociedad gremial de escritores, designados por la misma, y las personas que nombren el denunciante y el editor o traductor, una por cada uno;

b) Para las obras científicas, el Decano de la Facultad de Ciencias que corresponda por su especialidad, dos representantes de la sociedad científica de la respectiva especialidad,

designados por la misma, y las personas que nombren el denunciante y el editor o traductor, una por cada parte.

En ambos casos, cuando se haya objetado la traducción, el respectivo jurado se integrará también con dos traductores públicos nacionales, nombrados uno por cada parte, y otro designado por la mayoría del jurado.

c) Para las obras artísticas, el Director del Museo Nacional de Bellas Artes, dos personas idóneas designadas por la Dirección del Registro Nacional de la Propiedad Intelectual y las personas que nombren el denunciante y el denunciado, uno por cada parte;

d) Para las musicales, el Director del Conservatorio Nacional de Música, dos representantes de la sociedad gremial de Compositores de Música, popular o de cámara en su caso, y las personas que designen el denunciante y el denunciado, una por cada parte.

Cuando las partes no designen representantes, dentro del término que les fije la dirección del Registro, serán designados por esta.

El jurado resolverá declarando si existe o no la falta denunciada y en caso afirmativo, podrá ordenar la corrección de la obra e impedir su exposición o la circulación de ediciones no corregidas, que serán inutilizadas. Los que infrinjan esta prohibición pagarán una multa de cien mil pesos moneda nacional, que fijará el jurado y se hará efectiva en la forma establecida en los respectivos códigos de Procedimientos en lo Civil y Comercial para la ejecución de las sentencias. El importe de las multas ingresará en el fondo de fomento creado por esta ley. Tendrá personería para ejecutarlas la dirección del Registro.

DISPOSICIONES TRANSITORIAS

Art. 84: Las obras que se consideren del dominio público de acuerdo a la ley 11.723 sin que haya transcurrido el término de cincuenta años, volverán automáticamente al dominio privado hasta completar ese término, sin perjuicio de los derechos que hayan adquirido terceros, sobre las reproducciones de esas obras hechas durante el intervalo transcurrido entre el vencimiento del plazo de treinta años y la prolongación a cincuenta años dispuesta por el presente decreto–ley (texto ordenado por el Dec. Ley 12.063/57)

Art. 85: Las obras que en la fecha de promulgación de la presente ley se hallen en el dominio privado continuarán hasta cumplirse el término establecido en el art. 5°.

Art. 86: Créase el Registro Nacional de la Propiedad Intelectual del que pasará a depender la actual Oficina de Depósito Legal. Mientras no se incluya en la ley general de presupuesto el Registro Nacional de Propiedad Intelectual, las funciones que le están encomendadas por esta ley serán desempeñadas por la Biblioteca Nacional.

Art. 87: Dentro de los sesenta días subsiguientes a la sanción de esta ley, el Poder Ejecutivo procederá a su reglamentación.

Art. 88: Queda derogada la ley 9.141 y todas las disposiciones que se opongan a la presente

Art. 89: Comuníquese al poder ejecutivo.

R. Patrón Costas–Juan F. Caferata

LEY 25.036 – PROPIEDAD INTELECTUAL

Sancionada el 14 de Octubre de 1998 y promulgada en Noviembre de 1998.

Modifícanse los Art.s 1º, 4º, 9º y 57º e incorpórase el Art. 55º bis a la Ley N° 11.723

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ART. 1: Modifícase el Art. 1º de la ley 11.723, el que quedará redactado de la siguiente manera:

Art. 1: A los efectos de la presente ley, las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales; las obras dramáticas, composiciones musicales, dramático–musicales; las cinematográficas, coreográficas y pantomímicas, las obras de dibujo, pintura, escultura, arquitectura; modelos, y obras de arte o ciencias aplicadas al comercio o a la industria; los impresos, planos y mapas; los plásticos, fotografías, grabados y fonogramas; en fin, toda producción científica, literaria, artística o didáctica, sea cual fuere el procedimiento de reproducción. La protección del derecho de autor abarcará la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí.

ART. 2: Incorpórase como inciso d) del Art. 4º de la ley 11.723 el siguiente texto:

Art. 4: ...

d) Las personas físicas jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario.

ART. 3: Incorpórase como segundo párrafo del Art. 9º de la Ley 11.723 el siguiente texto:

Art. 9: ...

Quien haya recibido de los autores o de sus derecho–habientes de un programa de computación una licencia para usarlo, podrá reproducir una única copia de salvaguardia de los ejemplares originales del mismo. Dicha copia deberá estar debidamente identificada, con indicación del licenciado que realizó la copia y fecha de la misma. La copia de salvaguardia no podrá ser utilizada para otra finalidad que la de reemplazar el ejemplar original del programa de computación licenciado si ese original se pierde o deviene inútil para su utilización.

ART. 4: Incorpórase como Art. 55 bis de la Ley 11.723 el siguiente texto:

Art. 55 bis: La explotación de la propiedad intelectual sobre los programas de computación incluirá entre otras formas los contratos de licencia para su uso o reproducción.

ART. 5: Incorpórase como Art. 57, in fine, de la ley 11.723 el siguiente texto:

Art. 57, in fine: Para los programas de computación, consistirá el depósito de los elementos y documentos que determine la reglamentación.

ART. 6: Comuníquese al Poder Ejecutivo.

Dada en la sala de sesiones del Congreso Argentino, en Buenos Aires, a los catorce días del mes de octubre del año mil novecientos noventa y ocho.

Registrado bajo el N° 25.036.

Alberto Pierri – Carlos F. Ruckauf – Esther H. Pereyra Arandia de Pérez Pardo – Mario L. Pontaquarto

Decreto Nro. 1307/98

Bs. As. 6/11/98

Por Tanto: Téngase por Ley de la Nación N° 25.036 cúmplase, comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese.

Jorge A. Rodriguez–Raúl E. Granillo Ocampo

DECRETO 165/94

Sancionada el 3 de febrero de 1994 y Publicada el 8 de febrero de 1994.

Propiedad Intelectual – Software de Base de Datos – Protección – Normas

Art. 1: A los efectos del decreto y de la demás normativa vigente en la materia

a) Se entenderá por obras de software, incluidas entre las obras del art. 1° de la ley 11.723, a las producciones constituidas por una o varias de las siguientes expresiones:

- I. Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación;
- II. Los programas de computación, tanto en su versión “fuente”, principalmente destinada al lector humano, como su versión “objeto”, principalmente destinada a ser ejecutada por el computador;
- III. La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento del software.

b) Se entenderá por obras de bases de datos, incluidas en la categoría de obras literarias, a las producciones constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos.

c) Se considerarán procedimientos idóneos para reproducir obras de software de base de datos a los escritos o diagramas directa o indirectamente perceptibles por los sentidos humanos, así como a los registros realizados mediante cualquier técnica, directa o indirectamente procesables por equipos de procesamiento de información.

d) Se considerará que una obra de software o de base de datos tiene el carácter de publicada cuando ha sido puesta a disposición del público en general, ya sea mediante su reproducción sobre múltiples ejemplares distribuidos comercialmente o mediante la oferta generalizada de su transmisión a distancia con fines de explotación.

e) Se considerará que una obra de software o de base de datos tiene el carácter de inédita, cuando su autor titular o derechohabiente la mantiene en reserva o negocia la cesión de sus derechos de propiedad intelectual contratando particularmente con los interesados.

Art. 2: Para proceder al registro de obras de base de datos publicadas, cuya explotación se realice mediante su transmisión a distancia, se depositarán amplios extractos de su contenido y relación escrita de su estructura y organización así como de sus principales características, que permitan a criterio y riesgo del solicitante individualizar suficientemente la obra y dar la noción más fiel posible de su contenido.

Art. 3: Para proceder al registro de obras de software o de base de datos que tengan el carácter de inéditas, el solicitante incluirá bajo sobre lacrado y firmado todas las expresiones de la obra que juzgue convenientes y suficientes para identificar su creación y garantizar la reserva de su información secreta.

Art. 4: Comuníquese, etc. – Menem –Maiorano

LEY 24.766

Sancionada el 8 de febrero de 1997 y Publicada el 8 de febrero de 1994.

Ley de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos.

Sanción: 18 de diciembre de 1996

Promulgación: 20 de diciembre de 1996

Publicación: B.O. 30/12/96

Citas legales: Ley 24.481: LV-C, 2948

Art. 1: Las personas físicas o jurídicas podrán impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honestos, mientras información reúna las siguientes condiciones:

- a. Sea secreta en el sentido de que no sea, como cuerpo o en la configuración y reunión precisa de sus componentes, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y
- b. Tenga un valor comercial por ser secreta; y
- c. Haya sido objeto de medidas razonables, en las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la controla.

Art. 2: La presente ley se aplicará a la información que conste en documentos, medios electrónicos o magnéticos, discos, ópticos, microfilmes, películas u otros elementos similares.

LEY FIRMA DIGITAL (SENADORES PEDRO DEL PIERO Y LUIS MOLINARI ROMERO)

Presentación Proyecto: 20 de junio de 2000. Exp. 1155/00

Media Sanción en H. C. Diputados: 15 de agosto de 2001. Orden del Día N° 2651/01

Proyecto de ley

El Senado y la Cámara, etc.

LEY FIRMA DIGITAL

CAPITULO I

CONSIDERACIONES GENERALES

ARTICULO 1º: Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

ARTICULO 2º: Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose esta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

ARTICULO 3º: Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

ARTICULO 4º: Exclusiones. Las disposiciones de esta ley no son aplicables:

- a) a las disposiciones por causa de muerte;
- b) a los actos jurídicos del derecho de familia;
- c) a los actos personalísimos en general;
- d) a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

ARTICULO 5º: Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

ARTICULO 6º: Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTICULO 7º: Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

ARTICULO 8º: Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

ARTICULO 9º: Validez. Una firma digital es válida si cumple con los siguientes requisitos:

- a) haber sido creada durante el periodo de vigencia del certificado digital válido del firmante;
- b) ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;
- c) que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

ARTICULO 10º: Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

ARTICULO 11: Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTICULO 12: Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permita determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/ o recepción.

CAPITULO II

DE LOS CERTIFICADOS DIGITALES

ARTICULO 13: Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

ARTICULO 14: Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:

- a) Ser emitidos por un certificador licenciado por el Ente Licenciante;
- b) Responder a formatos estándares reconocidos internacionalmente fijados por la Autoridad de Aplicación y contener, como mínimo, los datos que permitan:
 - 1. identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;
 - 2. ser susceptible de verificación respecto de su estado de revocación;
 - 3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;
 - 4. contemplar la información necesaria para la verificación de la firma;
 - 5. identificar la política de certificación bajo la cual fue emitido.

ARTICULO 15: Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o con su revocación si fuere revocado.

La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

ARTICULO 16: Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

- a) reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República argentina y el país de origen del certificador extranjero, o;
- b) tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la Autoridad de Aplicación.

CAPITULO III

DEL CERTIFICADOR LICENCIADO

ARTICULO 17: Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados y presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el Ente Licenciante.

La actividad de los certificadores licenciados no pertenecientes al Sector Público se prestará en régimen de competencia. El arancel de los servicios prestados por los Certificadores Licenciados será establecido libremente por éstos.

ARTÍCULO 18: Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

ARTICULO 19: Funciones. El certificador licenciado tiene las siguientes funciones:

- a) recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;
- b) emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la Autoridad de Aplicación indique en la reglamentación de la presente ley;
- c) identificar inequívocamente los certificados digitales emitidos;
- d) mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;
- e) revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:
 - 1. a solicitud del titular del certificado digital
 - 2. si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación;
 - 3. si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguro;
 - 4. por condiciones especiales definidas en su política de certificación.
 - 5. por resolución judicial o de la Autoridad de Aplicación.
- f) informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

ARTICULO 20: Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el Ente Licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

ARTICULO 21: Obligaciones. Son obligaciones del certificador licenciado:

- a) informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el Ente Licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
- b) abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;
- c) mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;
- d) operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la Autoridad de Aplicación;
- e) notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable y de las obligaciones que asume por el solo hecho de ser titular de un certificado digital;
- f) recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;
- g) mantener la confidencialidad de toda información que no figure en el certificado digital;
- h) poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;
- i) mantener la documentación respaldatoria de los certificados digitales emitidos, por DIEZ (10) años a partir de su fecha de vencimiento o revocación;
- j) incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la Autoridad de Aplicación;
- k) publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoria de que hubiera sido objeto, su manual de procedimientos y toda información que determine la Autoridad de Aplicación;
- l) publicar en el Boletín Oficial aquellos datos que la Autoridad de Aplicación determine;
- m) registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;
- n) informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;

- o) verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;
- p) solicitar inmediatamente al Ente Licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenida haya dejado de ser seguro;
- q) informar inmediatamente al Ente Licenciante sobre cualquier cambio en los datos relativos a su licencia;
- r) permitir el ingreso de los funcionarios autorizados de la Autoridad de Aplicación, del Ente Licenciante o de los auditores, a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
- s) emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;
- t) someter a aprobación del Ente Licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;
- u) constituir domicilio legal en la República Argentina;
- v) disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;
- w) cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el Ente Licenciante.

ARTICULO 22: Cese del certificador. El certificador licenciado cesa en tal calidad:

- a) por decisión unilateral comunicada al Ente Licenciante;
- b) por cancelación de su personería jurídica;
- c) por cancelación de su licencia dispuesta por el Ente Licenciante.

La Autoridad de Aplicación determinará los procedimientos de revocación aplicables en estos casos.

ARTICULO 23: Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:

- a) para alguna finalidad diferente a los fines para los cuales fue extendido;
- b) para operaciones que superen el valor máximo autorizado cuando corresponda;
- c) una vez revocado.

CAPITULO IV

DEL TITULAR DE UN CERTIFICADO DIGITAL

ARTICULO 24: Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:

- a) a ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
- b) a que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;
- c) a ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;
- d) a que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;
- e) a que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.

ARTICULO 25: Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:

- a) mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;
- b) utilizar un dispositivo de creación de firma digital técnicamente confiable;
- c) solicitar la revocación de su certificado al Certificador Licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;
- d) informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.

CAPITULO V

DE LA ORGANIZACIÓN INSTITUCIONAL

ARTICULO 26: Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocido, según lo establecido por el artículo 16, por un certificador licenciado.

ARTICULO 27: Sistema de Auditoria. La Autoridad de Aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoria para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el Ente Licenciente.

ARTICULO 28: Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

CAPÍTULO VI

DE LA AUTORIDAD DE APLICACIÓN

ARTICULO 29: Autoridad de Aplicación. La Autoridad de Aplicación de la presente ley será la JEFATURA DE GABINETE DE MINISTROS

ARTICULO 30: Funciones. La Autoridad de Aplicación tiene las siguientes funciones:

- a) dictar las normas reglamentarias y de aplicación de la presente;
- b) establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;
- c) determinar los efectos de la revocación de los certificados de los certificadores licenciados o del Ente Licenciante;
- d) instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;
- e) determinar las pautas de auditoria, incluyendo los dictámenes tipo que deba emitirse como conclusión de las revisiones;
- f) actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;
- g) determinar los niveles de licenciamiento.
- h) otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;
- i) fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;
- j) homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;
- k) aplicar las sanciones previstas en la presente ley;

ARTICULO 31: Obligaciones. En su calidad de titular de certificado digital, la Autoridad de Aplicación tiene las mismas obligaciones que los titulares de certificados y que los Certificadores Licenciados. En especial y en particular debe:

- a) abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los Certificadores Licenciados;
- b) mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;
- c) revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;

- d) publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;
- e) supervisar la ejecución del plan de cese de actividades de los Certificadores Licenciados que discontinúan sus funciones;

ARTICULO 32: Arancelamiento. La Autoridad de Aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y de las auditorias realizadas por sí o por terceros contratados a tal efecto.

CAPÍTULO VII

DEL SISTEMA DE AUDITORÍA

ARTICULO 33: Sujetos a auditar. El Ente Licenciante y los Certificadores Licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoria que diseñe y apruebe la Autoridad de Aplicación.

La Autoridad de Aplicación podrá implementar el sistema de auditoria por sí o por terceros habilitados a tal efecto. Las auditorias deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, como así también el cumplimiento con las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el Ente Licenciante.

ARTICULO 34: Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorias las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales, que acrediten experiencia profesional acorde en la materia.

CAPÍTULO VIII

DE LA COMISIÓN ASESORA PARA LA INFRAESTRUCTURA DE FIRMA DIGITAL

ARTICULO 35: Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia, provenientes de Organismos del Estado Nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de Profesionales.

Los integrantes serán designados por el Poder Ejecutivo Nacional por un período de cinco (5) años renovables por única vez.

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la Autoridad de Aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la Autoridad de Aplicación regularmente informada de los resultados de dichas consultas.

ARTICULO 36: Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la Autoridad de Aplicación, sobre los siguientes aspectos:

- a) estándares tecnológicos;
- b) sistema de registro de toda la información relativa a la emisión de certificados digitales;
- c) requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;
- d) metodología y requerimiento del resguardo físico de la información;
- e) otros que le sean requeridos por la Autoridad de Aplicación.

CAPITULO IX

RESPONSABILIDAD

ARTICULO 37: Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley y demás legislación vigente.

ARTICULO 38: Responsabilidad de los certificadores licenciados ante terceros.

El Certificador que emita un Certificado Digital, o lo reconozca en los términos del art. 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de la ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio, demostrar que actuó con la debida diligencia.

ARTICULO 39: Limitaciones de responsabilidad. Los Certificadores Licenciados no son responsables en los siguientes casos:

- a) por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;
- b) por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;
- c) por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.

CAPITULO X

SANCIONES

ARTICULO 40: Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley será realizada por el Ente Licenciante. Es aplicable la Ley de Procedimientos Administrativos N° 19.549 y sus normas reglamentarias.

ARTICULO 41: Sanciones. El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:

- a) apercibimiento;
- b) multa de pesos diez mil (\$ 10.000) a pesos quinientos mil (\$ 500.000);
- c) caducidad de la licencia.

Su gradación según reincidencia y/u oportunidad será establecida por la reglamentación.

El pago de la sanción que aplique el Ente Licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

ARTICULO 42: Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos:

- a) emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;
- b) no facilitar los datos requeridos por el Ente Licenciante en ejercicio de sus funciones;
- c) cualquier otra infracción a la presente ley que no tenga una sanción mayor.

ARTICULO 43: Multa. Podrá aplicarse sanción de multa en los siguientes casos:

- a) incumplimiento de las obligaciones previstas en el artículo 21;
- b) si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causaren perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;
- c) omisión de llevar el registro de los certificados expedidos;
- d) omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;
- e) cualquier impedimento u obstrucción a la realización de inspecciones o auditorias por parte de la Autoridad de Aplicación y del Ente Licenciante;
- f) incumplimiento a las normas dictadas por la Autoridad de Aplicación;
- g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento;

ARTICULO 44: Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de:

- a) no tomar los debidos recaudos de seguridad en los servicios de certificación;
- b) expedición de certificados falsos;
- c) transferencia no autorizada o fraude en la titularidad de la licencia;
- d) reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;
- e) quiebra del titular.

La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

ARTICULO 45: Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los tribunales federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.

La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

ARTICULO 46: Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso Administrativo Federal.

CAPITULO XI

DISPOSICIONES COMPLEMENTARIAS

ARTICULO 47: Utilización por el Estado Nacional. El Estado Nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus Poderes.

ARTICULO 48: Implementación. El Estado Nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8 de la Ley N° 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley N° 24.156.

ARTICULO 49: Reglamentación. El Poder Ejecutivo Nacional deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

ARTICULO 50: Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

ARTICULO 51: Equiparación a los efectos del derecho penal. Incorpórase el siguiente texto como art. 78 (bis) del Código Penal: “Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los

términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.”

ARTICULO 52: Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo Nacional para que por la vía del artículo 99 inciso 2 de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

ARTICULO 53: Comuníquese al PODER EJECUTIVO NACIONAL.

ANEXO

INFORMACIÓN: conocimiento adquirido acerca de algo o alguien.

PROCEDIMIENTO DE VERIFICACIÓN: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

- a) que dicha firma digital ha sido creada durante el periodo de validez del certificado digital del firmante;
- b) que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante;
- c) la verificación de la autenticidad y la validez de los certificados involucrados.

DATOS DE CREACION DE FIRMA DIGITAL: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

DATOS DE VERIFICACION DE FIRMA DIGITAL: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

DISPOSITIVO DE CREACION DE FIRMA DIGITAL: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

DISPOSITIVO DE VERIFICACIÓN DE FIRMA DIGITAL: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

POLITICAS DE CERTIFICACIÓN: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

TECNICAMENTE CONFIABLE: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad, y procedimientos administrativos relacionados, que cumpla los siguientes requisitos:

1. resguardar contra la posibilidad de intrusión y/o de uso no autorizado;
2. asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;
3. ser apto para el desempeño de sus funciones específicas;
4. cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;
5. cumplir con los estándares técnicos y de auditoria que establezca la Autoridad de Aplicación.

CLAVE CRIPTOGRÁFICA PRIVADA: En un criptosistema asimétrico, es aquella que se utiliza para firmar digitalmente.

CLAVE CRIPTOGRÁFICA PÚBLICA: En un criptosistema asimétrico, es aquella que se utiliza para verificar una firma digital.

INTEGRIDAD: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

CRIPTOSISTEMA ASIMÉTRICO: Algoritmo que utiliza un “par de claves”, una “clave privada” para firmar digitalmente y su correspondiente “clave pública” para verificar dicha “firma digital”.

Sala de las Comisiones,

Expte. 3534-D-00

INFORME

Honorable Cámara:

Las Comisiones de Comunicaciones e Informática y de Legislación General han considerado el proyecto de ley del señor diputado Fontdevila y otros señores diputados, y han tenido a la vista el proyecto de ley del señor diputado Corchuelo Blasco y otros señores diputados, el proyecto de ley de la señora diputada Puiggrós, el proyecto de ley del señor diputado Cardesa y otros señores diputados y el proyecto de ley del señor diputado Atanasof y de la señora diputada Camaño, G., por el que se establece el régimen de habilitación y regulación del empleo de la firma digital. Luego de su análisis, han considerado conveniente dictaminarlo favorablemente, con modificaciones.

Por los motivos expuesto y otros que el miembro informante desarrollará es que solicitamos la aprobación del presente proyecto.

CÓDIGO CIVIL ARGENTINO

Art. 1072: el acto ilícito ejecutado a sabiendas y con intención de dañar la persona o los derechos del otro se llama, en este Código, delito, obligando a reparar los daños causados por tales delitos.

Art. 1083: En todos los casos, el resarcimiento de daños consistirá en la reposición de las cosas a su estado anterior, excepto si fuera imposible, en cuyo caso la indemnización se fijará en dinero”.

Art. 1094: En caso de probarse la existencia de delito de daño por destrucción de la cosa ajena, “la indemnización consistirá en el pago de la cosa destruida; si la destrucción de la cosa fuera parcial, la indemnización consistirá en el pago de la diferencia de su valor y el valor primitivo”.

Art. 1109: Existe la posibilidad de reclamar indemnización cuando el hecho no pudiera ser considerado delictivo, en los casos en que “alguien por su culpa o negligencia ocasiona un daño a otro”.

Art. 1111: Pero “el hecho que no cause daño a la persona que lo sufre, sino por una falta imputable a ella, no impone responsabilidad alguna” .

PROYECTOS DE LEY

PROYECTO DE LEY PENAL Y DE PROTECCIÓN DE LA INFORMÁTICA (SENADOR EDUARDO BAUZA)

Número de Proyecto: 815/00

Publicado DAE. N° 43/00

REGIMEN DE PROPIEDAD INTELECTUAL DE LAS OBRAS DE INFORMATICA Y REGIMEN PENAL

TITULO PRIMERO

De la Protección Intelectual a las Obras de Informática

CAPITULO UNICO

Art. 1: DE LA PROTECCIÓN INTELECTUAL.

Los propietarios de las obras de informática tendrán derecho a la protección de esa propiedad intelectual, conforme al derecho vigente y, en particular, a las disposiciones de la presente ley.

Art. 2: EL DERECHO DE PROPIEDAD. FACULTADES.

La propiedad intelectual de una obra de informática, a partir de su registración, comprende para su autor o las demás personas mencionadas en el Art. 5° de esta ley, las facultades y derechos de:

- 1) Publicarla.
- 2) Ejecutarla.
- 3) Representarla y exponerla en público
- 4) Enajenarla, total o parcialmente
- 5) Traducirla y reproducirla en cualquier forma, inclusive mediante el uso de redes.
- 6) De distribuirla
- 7) Autorizar a terceros a ejercer en su nombre o por si todos y cada uno de los derechos aquí establecidos.

Art. 3: RESPONSABILIDAD DEL PROPIETARIO DE LA OBRA

El autor de una obra de informática no será responsable civil ni penalmente por los daños que la obra pudiera ocasionar a terceros en razón de su uso indebido, incorrecto o contrario a las reglas del arte, y cuando se hubiera consignado en la misma obra una advertencia sobre los efectos perniciosos de tal uso.

Las partes podrán formular pactos destinados a extender la responsabilidad civil del autor de una obra de informática, atendiendo a las circunstancias del caso.

Art. 4: DERECHOS DE AUTOR SOBRE OBRAS ILÍCITAS

No podrán ser objeto de los derechos de propiedad intelectual consagrados por esta Ley las obras de informática contrarias a la legislación vigente, ni los que pretendan registrarse sobre una obra de informática que se encontrare registrada en el extranjero, estuviera en el dominio público o hubiera sido elaborada sobre la base de otra obra de informática, sin la debida autorización del propietario de esta última.

El autor material de los programas consignados en el párrafo precedente será civilmente responsable por el daño que ocasionare su uso por parte de terceros, aún cuando éstos tuvieran conocimiento de su ilegalidad o del daño que pudieran provocar, salvo que demostrare que aún obrando con cuidado y previsión no hubiera podido impedir el daño.

Art. 5: TITULARES DEL DERECHO DE PROPIEDAD.

Son titulares del derecho de propiedad intelectual sobre las obras de informática:

- I. el autor de la obra,
- II. los herederos o derechohabientes del autor, y
- III. los que con permiso del autor la traducen, reforman, adaptan, modifican o transportan sobre la nueva obra intelectual resultante.

Salvo pacto en contrario, cuando una obra de software o de base de datos hubiese sido elaborada por un trabajador dependiente de una empresa dedicada a la creación de obras de informática en ejecución de su misión o directivas impartidas por la empresa, los derechos de propiedad sobre la obra corresponderán a la empresa. Salvo pacto en contrario, cuando una obra de informática hubiese sido elaborada por un trabajador dependiente de una empresa cuyo objeto comercial exclusivo no fuese la creación, distribución y venta de obras de informática, los derechos de propiedad corresponderán al trabajador

Art. 6: DEL PLAZO DE LOS DERECHOS.

Los derechos consagrados en la presente ley tendrán un plazo de vigencia de veinte (20) años, durante el cual las obras debidamente registradas pertenecerán a sus respectivos titulares. Vencido dicho plazo las obras de informática pasarán a pertenecer al dominio público.

Las obras de informáticas creadas en el extranjero e inscriptas en los respectivos registros de otros países otorgarán a sus titulares los derechos de propiedad intelectual reconocidos por esta ley durante el plazo de vigencia de su reconocimiento en el lugar de creación de la obra informática, entendiéndose por tal el de su primera registración, pero ese plazo nunca podrá exceder el de 20 años contados desde esa primera registración, cualquiera fuera la fecha de la registración en nuestro país.

Art. 7: DE LA DISTRIBUCIÓN.

Toda persona que distribuya una obra de informática en la República Argentina, a través de cualquier medio, deberá consignar su domicilio y los datos de identidad del titular de la obra, a fin de permitir a las Autoridades Competentes verificar si la propiedad de tales obras se encuentra ajustada a las disposiciones de la presente Ley.

Art. 8: DE LAS OBRAS INFORMÁTICAS EXTRANJERAS.

Sin perjuicio de lo expuesto en el artículo anterior, las disposiciones de esta ley son aplicables a las obras informáticas publicadas en países extranjeros, sea cual fuere la nacionalidad de sus autores, siempre que pertenezcan a naciones que reconozcan el derecho de propiedad intelectual y su registración en el país no contravenga el orden público nacional.

Para asegurar la protección de la legislación argentina, en los términos y condiciones previstos por esta ley y con el alcance temporal fijado en el artículo anterior, el autor de una obra extranjera debe acreditar el cumplimiento de las formalidades establecidas para su protección por las leyes del país en que se haya hecho su publicación y efectuado el registro pertinente de la obra conforme las disposiciones de los artículos 57 a 68 de la Ley 11.723.

En el caso de mediar diversas inscripciones de una misma obra informática, en registros de diversos países, se otorgará preferencia a aquella registración que coincida con la primera divulgación de la obra o de quien pueda acreditar fehacientemente la anterioridad de su invención.

Art. 9: PROCEDIMIENTOS IDÓNEOS PARA REPRODUCIR OBRAS DE SOFTWARE O DE BASE DE DATOS.

Se considerarán procedimientos idóneos para reproducir obras de software o de base de datos a los escritos o diagramas directa o indirectamente perceptibles por los sentidos humanos, así como a los registros realizados mediante cualquier técnica, directa o indirectamente procesables por equipos de procesamiento de información

Art. 10: OBRA PUBLICADA.

Se considerará que una obra de informática tiene carácter de publicada cuando ha sido puesta a disposición del público en general, ya sea mediante su reproducción sobre múltiples ejemplares distribuidos comercialmente o por la oferta generalizada de su transmisión a distancia con fines de explotación comercial.

Art. 11: REGISTRO DE OBRA PUBLICADA.

Para proceder al registro de una obra de informática publicada, cuya explotación comercial se realice mediante su transmisión a distancia, o mediante su reproducción sobre múltiples ejemplares distribuidos comercialmente, se depositarán amplios extractos de su contenido y relación escrita de su estructura y organización, así como de sus principales características, que permitan, a criterio y riesgo del solicitante, individualizar suficientemente la obra y dar la noción mas fiel posible de su contenido.

Este registro se deberá efectuar ante la Dirección Nacional del Derecho de Autor, dependiente del Ministerio de Justicia y Derechos Humanos de la Nación.

Art. 12: OBRA INÉDITA.

Se considerará que una obra de informática tiene carácter de inédita, cuando su autor, titular o derechohabiente la mantiene en reserva o negocia la cesión de sus derechos de propiedad intelectual contratando particularmente con los interesados, siempre y cuando haya registrado la obra en los términos de la Ley 11.723.

Art. 13: REGISTRO DE OBRA INÉDITA.

Para proceder al registro de obras de informática que tengan carácter de inéditas, el solicitante incluirá, bajo sobre lacrado y firmado, todas las expresiones de la obra que juzgue convenientes para identificar su creación y garantizar la reserva de su información secreta.

Este registro se deberá efectuar ante la Dirección Nacional del Derecho de Autor, dependiente del Ministerio de Justicia y Derechos Humanos de la Nación.

TITULO SEGUNDO

Régimen Penal

CAPITULO PRIMERO

De la Piratería Informática

Art. 14: DE LA COPIA ILEGAL.

Será reprimido con dos meses a tres años de prisión y con una multa accesoria equivalente a cinco veces el valor de venta al tiempo de la sentencia de la obra copiada ilegalmente, el que defraudare al titular de alguno de los derechos de propiedad intelectual sobre una obra de informática que reconoce esta ley mediante cualquier ardid o engaño.

Art. 15: DE LA PIRATERÍA.

Será reprimido con prisión de tres a seis años:

- a) El que edite, venda, reproduzca, alquile o distribuya por cualquier medio o instrumento, una obra de informática inédita o publicada, sin autorización por escrito del titular de los derechos respectivos, conforme los términos del artículo 5° de la presente Ley.
- b) El que edite una obra de informática atribuyéndose falsamente la condición de editor autorizado, invocando sin autorización el nombre del editor autorizado, o desbaratando de cualquier forma los derechos del editor autorizado.
- c) El que edite, venda, reproduzca, alquile o distribuya una obra de informática suprimiendo o cambiando el nombre del autor, el título de la misma o alterando, dolosamente su texto.
- d) El que edite, venda, reproduzca, alquile o distribuya mayor número de ejemplares que los que estuviese autorizado a realizar por el titular de los derechos respectivos.
- e) El que de cualquier modo facilite la edición, venta, reproducción, alquiler o distribución de obras de informática en forma ilícita.
- f) El que reproduzca copias no autorizadas de una obra de informática, por encargo de terceros.
- g) El que almacene o exhiba copias ilícitas y no pueda acreditar su origen mediante la factura o el recibo que lo vincule comercialmente con el titular de los derechos respectivos.
- h) El que importe al país las copias ilegales con miras a su distribución al público o utilización personal.

- i) El que atribuyere falsamente a otra persona la autoría de una obra de informática, de modo que pudiera resultar perjuicio.
- j) El titular de los derechos sobre una obra de informática que, de cualquier modo desbaratare o perjudicare los derechos atribuidos por si o por personas autorizadas a terceros, en virtud de un contrato.
- k) El que cometiere defraudación sustituyendo, ocultando o mutilando algún proceso u otro documento importante, o los medios informáticos utilizados para poner las resoluciones judiciales que se dictaran en conocimiento de las partes o terceros, mediante el uso de sistemas o cualquier otra maquinación o medio informáticos.

Art. 16: DEL SECUESTRO U OTRAS MEDIDAS CAUTELARES.

Los jueces que recibieren denuncias por la comisión de los delitos previstos en este capítulo dispondrán el secuestro de las obras o las demás medidas cautelares que estimen necesarias para evitar la afectación de los bienes jurídicos protegidos.

CAPITULO SEGUNDO

De los Abusos Fraudulentos en la venta de Obras de Informática.

Art. 17: DE LOS ABUSOS FRAUDULENTOS.

Se impondrá una multa equivalente a diez (10) veces el valor de la obra al vendedor o distribuidor que no advirtiera al comprador de una obra de informática sobre la limitación de su validez y operatividad por un plazo al cabo del cual el usuario deberá adquirir necesariamente su actualización para continuar utilizándola.

En la misma pena incurrirá quien al momento de efectuar una operación comercial no advirtiera a su contraparte que el objeto de la operación es una obra informática de demostración o “shareware”.

Art. 18: DE LA VENTA DE ORAS DE INFORMATICA CON HARDLOCKS O LLAVES DE SOFTWARE .

Se impondrá una multa de veinte veces el valor de la Obra de Informática al vendedor o, distribuidor que no advierta al comprador o adquirente, antes del perfeccionamiento de la compraventa, u otra operación comercial que implique la transferencia del uso y goce de la obra de modo equivalente a la compraventa, que la obra vendida contiene Hardlocks u otros dispositivos o programas de seguridad tendientes a evitar su copiado, o que necesiten una periódica actualización o cuya pérdida, robo, extravío o rotura provoquen un reemplazo necesario, todo lo cual será cobrado al comprador de modo separado al precio inicial de compra.

En la misma pena incurrirá quien antes del perfeccionamiento u otra operación comercial que implique la transferencia del uso y goce de la obra de modo equivalente a la compraventa no advirtiera al comprador de una obra de informática que ésta contiene una función tal que podría causar que algún programa deje de funcionar o daño al mismo programa o a otros programas.

Art. 19: DE LA DISTRIBUCIÓN ILEGAL.

Será sancionado con multa de pesos mil a diez mil aquél que no habiendo suscrito un contrato en legal forma con el autor de una obra de informática o con su distribuidor autorizado, distribuya en forma comercial obras de informática, aún habiendo adquirido copias legales en forma legítima. La presente penalidad se aplicará también en el supuesto en que la distribución de una Obra de Informática se efectúe sin advertir al comprador que la misma es de simple demostración, o bien la distribución de programas, sin la advertencia de que los mismos carecen de soporte en el país.

CAPITULO TERCERO

Del Uso Ilegítimo de Passwords y Accesos no Autorizados e Intercepción ilegal.

Art. 20: DE LOS ACCESOS NO AUTORIZADOS.

Será reprimido con prisión de seis a dieciocho meses el que mediante alguna manipulación informática o artificio semejante ingresara a un sistema o computadora al que no tuviera derecho de acceso.

Art. 21: DEL USO ILEGITIMO DE UN PASSWORD.

Será reprimido con prisión de uno a tres años el que dolosamente, mediante ardid, engaño o abuso de confianza:

- a) Ingresare a un sistema o computadora utilizando un password ajeno.
- b) Obtenga datos utilizados para transacciones financieras, tales como números de tarjetas de crédito, códigos de autorización, códigos de verificación, números "pin" o cualquier otro material codificado, sin la debida autorización del titular de los derechos o datos respectivos.

Art. 22: INTERCEPCION ILEGAL DE PAQUETES DE DATOS.

Será reprimido con prisión de dos a cuatro años aquél que intercepte, interfiera o acceda a los datos o información existente en una red, sin una debida y legal autorización de acceso

CAPITULO CUARTO

De la Destrucción de Datos y Sistemas. Los Virus Informáticos y el Software Nocivo.

Art. 23: DE LA DESTRUCCIÓN DE DATOS Y SISTEMAS.

Será reprimido con prisión de una a tres años el que maliciosamente destruya o inutilice una computadora o sistema de redes, o sus partes o sus componentes, o impida, obstaculice o modifique su funcionamiento, mediante la transmisión de cualquier elemento de software o hardware que pueda causar daño a un sistema, o cualquier otro daño.

Se impondrá la pena de dos a cuatro años de prisión si como consecuencia de las conductas descritas en el párrafo anterior se alteraren o destruyeren los datos o la información contenidos en una computadora o un sistema de redes.

Art. 24: DE LOS VIRUS INFORMÁTICOS Y SOFTWARE NOCIVO.

Será reprimido con prisión de tres a seis años el que de cualquier forma incorpore o introduzca virus u otros programas o mecanismos de energía electromagnética u otro tipo, que

alteraren, dañaran o destruyeran los datos o la información contenidos en una computadora, en una base de datos o en un sistema de redes, con o sin salida externa, mediante el envío de mensajes por e-mail o mediante el uso de cualquier otro ardid o engaño.

Si la conducta descripta en el apartado precedente se efectuare mediante la venta o distribución de programas al público, la pena se aumentará de cuatro a ocho años de prisión

CAPITULO QUINTO

De la Violación del Correo Electrónico.

Art. 25: VIOLACIÓN DE SECRETOS.

Será reprimido con prisión de quince días a seis meses, el que abriera indebidamente un mensaje enviado a través de correo electrónico o mediante sistema de “chat-room” que no le esté dirigido o se impusiera de su contenido o copiare indebidamente dicho mensaje, aunque no esté protegido por encriptado, o suprimiere o desviare de su destino un mensaje electrónico que no le esté dirigido.

La pena se aumentará de un mes a un año, si se comunicare a otro o publicare el contenido de un mensaje electrónico al que se accediera en los términos del párrafo anterior.

Art. 26: FALSIFICACIÓN DE DATOS PARA ATRIBUIRSE IDENTIDAD.

Será reprimido con prisión de quince días a seis meses, el que falsificare datos informáticos para atribuirse falsamente una identidad o transmitiere indebidamente mensajes a nombre de un tercero sin contar con la debida autorización del titular si no resultare un delito mayor.

Art. 27: DIVULGACIÓN INDEBIDA.

Será reprimido con multa de mil a diez mil pesos, si no resultare un delito mayor, el que accediere un mensaje electrónico no destinado a publicidad y lo divulgare o hiciere publicar indebidamente aunque dicho mensaje le hubiera sido dirigirlo, si el hecho causare o pudiera causar perjuicios a terceros.

Art. 28: DIVULGACIÓN DE SECRETOS.

Será reprimido con multa de treinta mil a cincuenta mil pesos, el que en razón de sus conocimientos de informática, su situación laboral o profesional, o por cualquier otra causa tuviere mayores posibilidades de acceso a la lectura de correos electrónicos, si revelare hechos, actuaciones o documentos contenidos en el Correo Electrónico, que debiera mantener en secreto por disposición de la ley u obligación de su profesión o cargo.

Art. 29: USO ILEGITIMO DEL CORREO ELECTRÓNICO.

Será sancionado con multa de mil a diez mil pesos el que de cualquier modo emitiera propaganda u otros mensajes, a ser transmitidos por una red informática u otros sistemas interconectados a destinatarios que no lo hubieran solicitado, si con ello saturase o cargase indebidamente de mensajes el Mail Box o sitio informático del receptor en la red.

CAPITULO SEXTO

De las Estafas Electrónicas

Art. 30: ESTAFAS EN EL USO DE SISTEMAS O COMPUTADORAS.

Será reprimido con prisión de uno a seis años aquél que al efectuar una compra telemática, o una transferencia electrónica de fondos, causare daño a otro a través de cualquier ardid o engaño en el uso de una computadora y/o cualquier equipamiento informático de propiedad, uso o explotación del damnificado.

Art. 31: ESTAFA A TERCEROS POR MEDIOS INFORMATICOS.

Será reprimido con prisión de un mes a seis años el que, con el fin de conseguir una ventaja patrimonial ilícita para si o para otro, cause un perjuicio a un tercero distinto del propietario, usuario o explotador de una computadora y/o cualquier equipamiento, mediante el uso indebido de cualquier recurso informático.

CAPITULO SEPTIMO

De los delitos contra la seguridad, la salud, el orden y los poderes públicos cometidos por medios informáticos.

Art. 32: INCENDIO, EXPLOSION, INUNDACION Y OTROS ESTRAGOS POR MEDIOS INFORMATICOS.

Será reprimido con prisión de tres a diez años, si hubiere peligro común, el que causare incendio, explosión, inundación u otros estragos, valiéndose de medios informáticos o de la alteración de sistemas interconectados, de redes o de otro tipo.

En la misma pena incurrirá quien mediante el acceso a sistemas interconectados, redes o con la utilización de cualquier elemento o facilidad informática impidiera o dificultare las tareas para impedir la concreción o extensión de los daños causados por incendios, inundaciones, explosiones u otros estragos, o las actividades de rescate de cualquier naturaleza.

Será reprimido con prisión de un mes a un año el que por imprudencia o negligencia, por impericia en su arte o profesión o por inobservancia de los reglamentos u ordenanzas, cometiere alguna de las conductas comprendidas en cualquiera de los párrafos del artículo anterior.

Art. 33: DELITOS CONTRA LA SEGURIDAD DE LOS MEDIOS DE TRANSPORTE Y DE COMUNICACIÓN Y LA PRESTACIÓN O USO DE LOS SERVICIOS PUBUCOS POR MEDIOS INFORMATICOS.

Será reprimido con prisión de tres a seis años el que mediante el uso de elementos o sistemas informáticos de cualquier naturaleza destruya, obstruya, inhabilite, afecte o debilite cualquier estructura informática de modo que ponga en peligro la seguridad de una nave, construcción flotante o aeronave; la prestación o el uso de los medios de transporte público o cualquier otro servicio público, los sistema bancarios y financieros, los sistemas de transmisión vía satélite o los sistema de televisión.

La pena será de seis meses a dos años de prisión cuando la conducta descrita en el párrafo anterior resultare de imprudencia o negligencia o por impericia en el arte o profesión o inobservancia de los reglamentos u ordenanzas a cargo del autor.

Art. 34: DELITOS INFORMATICOS CONTRA LA SALUD.

Será reprimido con prisión de tres a diez años el que alterando de cualquier modo un sistema interconectado, una red, o cualquier otra facilidad informática intentará o consiguiera

directa o indirectamente envenenar o adulterar, de un modo peligroso para la salud, aguas potables o sustancias alimenticias o medicinales, destinadas al uso público o al consumo de una colectividad de personas.

La misma pena se aplicará a quien con iguales medios facilitare indebidamente de cualquier modo la entrega indebida de medicamentos o mercaderías peligrosas para la salud, disimulando su carácter nocivo, u obtuviere, hiciere extender o adulterare recetas médicas a los mismos fines.

Si el hecho fuere seguido de la muerte de alguna persona, la pena será de diez a veinticinco años de reclusión o prisión

Art. 35: INSTIGACIÓN.

Será reprimido con prisión de un dos a seis años el que mediante el uso de cualquier medio o sistema informático de acceso al público, instigare a la comisión de un delito determinado contra una persona o institución.

Art. 36: INTIMIDACIÓN PUBLICA POR VÍA INFORMÁTICA.

Será reprimido con prisión de dos a seis años el que para infundir un temor público o suscitar tumultos o desórdenes propalare o transmitiera por cualquier medio o sistema informático, señales o voces de alarma, amenazare con la comisión de un delito de peligro común.

En la misma pena incurrirá el que, por idénticos medios, incitare a la violencia colectiva contra grupos de personas o instituciones, por la sola incitación

Art. 37: APOLOGÍA INFORMÁTICA DEL DELITO.

Será reprimido con prisión de seis meses a dos años el que a través de la utilización de Internet, redes interconectadas o por cualquier medio informático de acceso público hiciere la apología de un delito o de un condenado por delito.

CAPITULO OCTAVO

De la Violación al Derecho de Intimidad por el uso indebido de Bases de Datos

Art. 38: DEL USO INDEBIDO DE BASES DE DATOS

Será reprimido con prisión de dos a cuatro años el que mediante la utilización de recursos o cualquier manipulación, el uso de sistemas, redes u otros artificios informáticos semejantes ingrese, utilice, comercialice, divulgue o reproduzca datos relativos a la vida íntima de una persona, cuando no mediare consentimiento previo expreso del titular de los datos otorgado a los fines específicos para los que han sido o serán utilizados.

La pena será de tres a seis años de prisión cuando los datos revelados sean de carácter bancario, financiero o se relacionen con la solvencia patrimonial de la persona, o estuvieren dirigidos a provocar discriminación de una persona o grupos de personas por cualquier causa

CAPITULO NOVENO

Agravantes.

Art. 39: AGRAVANTE EN RAZÓN DE LA PROFESIÓN O ACTIVIDAD.

El profesional o experto dedicado a tareas de informática, o la persona que tuvieran a su cargo la administración de una red u otros sistemas interconectados, y valiéndose de sus conocimientos, profesión, actividad o situación laboral o comercial promoviera, instigara, ejecutara o encubriera alguno de los delitos previstos en este título, sufrirá además inhabilitación especial por el doble del tiempo de la condena privativa de libertad que correspondiera Si la pena que correspondiera a la conducta fuera de multa la inhabilitación será de seis meses.

Art. 40: AGRAVANTE POR EL EJERCICIO DE FUNCIÓN PÚBLICA.

El funcionario público que, valiéndose de cualquier modo de su condición de tal, promoviera, instigara, ejecutara o encubriera cualquiera de los delitos previstos en este Título, sufrirá además inhabilitación especial por el doble del tiempo de la pena privativa de libertad que correspondiere Si la pena fuera de multa, la inhabilitación será de seis meses.

Art. 41: AGRAVANTE POR CAUSAS DE SEGURIDAD DE LA NACIÓN.

Las penas previstas para los delitos descriptos en este título se elevarán de un tercio a la , mitad, cuando la promoción, instigación, ejecución o encubrimiento de tales delitos pusiera en peligro la seguridad de la Nación.

Eduardo Bauzá

PROYECTO DE LEY MODIFICACIÓN RÉGIMEN PENAL (SENADOR ANTONIO CAFIERO)

Numero de Proyecto:117/00

Publicado DAE N° 007/00

Art. 1: Incorpórase al Art. 153 del Código Penal el siguiente como segundo párrafo:

“Será reprimido con la misma pena a quien con el objeto de descubrir secretos de un tercero o vulnerar su intimidad y sin consentimiento de este:

se apoderare mensajes de correo electrónico o cualquier otro documento o efecto producido en soporte digital.

Interceptare comunicaciones cuando por las mismas circularen mensajes de correo electrónico o cualquier otro documento en soporte digital.

Utilizare artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen de una persona o cualquier otra comunicación cuando fueran obtenidas invadiendo su vida privada”.

Art. 2: Incorpórase al Art. 153 del Código Penal el siguiente como tercer párrafo:

“La pena aumentará en un tercio a quien ilegítimamente se apoderare, utilizare, modificare, revelare, difundiera o cediera datos reservados de carácter personal que se hallen registrado en ficheros o soportes informáticos, electrónicos o telemáticos; y en la mitad cuando dichos actos afecten datos de carácter sensible que revelen la ideología, creencia, religión, salud, vida sexual u origen de su titular”.

Art. 3: El actual segundo párrafo del Art. quedará incorporado como cuarto párrafo.

Art. 4: Incorpórase al Art. 172 del Código Penal el siguiente como segundo párrafo:

“La misma pena se aplicará a quien mediante manipulación informática o artificios tecnológicos provoquen la transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero”.

Art. 5: Incorpórase al Art. 183 del Código Penal el siguiente como segundo párrafo:

“La pena aumentará en un tercio cuando el daño consistiera en la destrucción, alteración, inutilización o cualquier otra modalidad por la que se dañaren datos, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos”.

Art. 6: Incorpórase el siguiente como segundo párrafo del Art. 164 del Código Penal:

“Se aplicará la misma pena cuando el hecho se perpetrare mediante el uso de tarjetas magnéticas falsas o robadas, o de mandos o instrumentos de apertura a distancia, de utilización de claves de acceso ajenas sin autorización o la inutilización de sistemas específicos de alarma o custodia”.

Art. 7: Incorpórase el siguiente como Art. 185 bis del Código Penal:

“Será reprimido con la misma pena que el autor del hecho en el que fuera utilizado, al que fabricare, almacenare, comercializare o por cualquier título distribuyere útiles, materiales, instrumentos, programas de computación o aparatos de tecnología destinados a la comisión de delitos”.

Art. 8: Comuníquese al Poder Ejecutivo.

Antonio F. Cafiero

PROYECTO DE LEY MODIFICACIÓN CÓDIGO CIVIL (SENADOR ALBERTO ROMERO FERIS)

Numero de Proyecto: 168/00

Publicado DAE N° 014/00–Maglietti (Reproducción)

Art. 1: Sustitúyese el texto del Art. 1.112 del Código Civil por el siguiente:

“Art. 1.112: Todo funcionario o empleado público que faltare a los deberes a su cargo, ya sea por acción u omisión, es responsable directamente por los daños materiales y morales causados a un tercero, aun cuando el perjuicio que ellos irroguen no sea susceptible de apreciación pecuniaria.

Quedan comprendidos dentro de los deberes a cargo de los funcionarios y empleados públicos el cumplimiento de las obligaciones impuestas por leyes, reglamentos, ordenanzas, circulares, y las que resulten de las disposiciones constitucionales contenidas en el capítulo de “Declaraciones, derechos y garantías”.

La obligación de reparar el daño se extiende al órgano al cual pertenece el funcionario o empleado y se rige por las disposiciones de este código relativas a las obligaciones divisibles y simplemente mancomunadas, con la siguiente excepción. La insolvencia del funcionario o empleado será soportada por el órgano estatal, pero para hacer efectiva la responsabilidad de este último por la parte de la deuda que corresponde al primero, el accionante deberá acreditar la previa excusión de los bienes del funcionario o empleado.

Art. 2: Comuníquese al Poder Ejecutivo.

Alberto R. Maglietti

PROYECTO DE LEY RÉGIMEN PENAL DEL USO INDEBIDO DE LA COMPUTACIÓN (SENADOR ANTONIO BERTHONGARAY)

Numero de Proyecto: 2381/98

Publicado DAE N° 137/98–Caducó: 29/02/2000

LEY DE SEGURIDAD Y DEFENSA EN MATERIA INFORMATICA

TITULO I

Principios Fundamentales

Capítulo único

Art 1: La presente ley establece las bases orgánicas y funcionales para preservar la defensa nacional y la seguridad interior del país ante eventuales ataques por parte de naciones extranjeras, terroristas informáticos u otras personas, que empleando la informática o atacando instalaciones o sistemas informáticos, pretendan vulnerar la seguridad de tales sistemas o provocarles alteraciones o daños, o bien provocar otros perjuicios empleando la informática; y para asegurar una adecuada capacidad de defensa, frente al posible empleo de la informática como arma.

Art. 2: Constituyen objetivos a ser alcanzados a través de la aplicación de la presente ley:

- 1) Proteger las instalaciones y sistemas informáticos del país cuya preservación afecte significativamente el interés público, contra ataques provenientes de naciones extranjeras, terroristas o informáticos u otras personas que pretendan vulnerarlos;
- 2) Mantener una adecuada capacidad de defensa y actualización tecnológica, en lo relativo al empleo de la informática como arma en hipotéticos conflictos armados de carácter internacional.

TÍTULO II

Del Centro Nacional de Protección Informática (CENAPRI)

Capítulo Único

Art. 3: Créase en jurisdicción del Ministerio del Interior, el Centro Nacional de Protección Informática (CENAPRI).

Constituirá un ente descentralizado.

Será su misión la de prevenir, detectar, enfrentar y analizar amenazas informáticas contra todo tipo de sistemas informáticos públicos o de interés público civiles, de propiedad estatal, o privada afectados a la prestación de servicios públicos o actividades reglamentadas de interés nacional.

Formulará y gestionará el Programa de Seguridad Informática Civil.

Podrá asimismo cumplir las antedichas funciones respecto de otros sistemas informáticos privados que así lo soliciten, pagando la tasa correspondiente.

Art. 4: El CENAPRI estará presidido por un directorio integrado por un presidente y cinco vocales, designados por el Poder Ejecutivo nacional de la siguiente forma:

El presidente, a propuesta del Ministro del Interior;

Un vocal, a propuesta de la Secretaría de Seguridad Interior;

Un vocal, a propuesta de la Secretaría de Inteligencia de Estado;

Un vocal, a propuesta del Consejo de Rectores de Universidades Nacionales;

Un vocal, a propuesta del Ministerio de Educación;

Un vocal, a propuesta de las entidades privadas que posean sistemas informáticos bajo la protección del Centro, elegido en la forma que determine la reglamentación.

Deberán en todos los casos ser personas con conocimiento y experiencia en aspectos vinculados con informática o seguridad pública.

El directorio dictará su reglamento interno, que deberá reconocer al presidente doble voto en caso de empate.

El directorio tendrá a su cargo la dirección y administración del Ente, siendo facultades exclusivas del presidente las de designación y remoción del personal.

Art. 5: Integrarán el patrimonio del CENAPRI:

1. Los recursos presupuestarios que se le asignen;
2. Las tarifas que perciba por sus servicios de las entidades privadas;
3. Las donaciones y legados que reciba;
4. El producto de las multas que aplique.

Art. 6: El CENAPRI además de establecer y perfeccionar medidas de seguridad tendientes a la protección de los sistemas informáticos antedichos, procederá a efectuar y mantener copias del “software” y registros de los sistemas informáticos correspondientes para reemplazo de los originales en caso de destrucción o alteración, debiendo tales copias ser guardadas bajo especiales medidas de seguridad.

Art. 7: El Centro contará con la activa cooperación de las instituciones policiales y fuerzas de seguridad del Estado Nacional y de la Secretaría de Inteligencia de Estado u organismos que la sustituyeran. Cada una de las instituciones, fuerzas y organismo u organismos de inteligencia contará con un delegado permanente ante el Centro.

Integrarán el personal del Centro los funcionarios y empleados civiles, así como el personal de las instituciones policiales y fuerzas de seguridad en actividad y retiro especializados en materia informática que se consideren necesarios.

Art. 8: El Centro estará facultado para proponer normas de seguridad informática a ser adoptadas por los organismos públicos y empresas privadas comprendidos dentro de sus funciones, las que deberán ser adoptadas por el Presidente de la Nación por medio de decreto.

También podrá aplicar multas por montos de pesos cien mil (\$ 100.000) a cinco millones (\$5.000.000) de pesos, por violación a tales normas, a las entidades privadas que infrinjan las mismas.

Tratándose de organismos públicos, corresponderá la aplicación de las sanciones previstas en el Régimen Jurídico Básico de la Función Pública, a cuyo efecto el Centro deberá elaborar el informe pertinente, que constituirá cabeza del correspondiente sumario administrativo.

La aplicación de multas por parte del Ente requerirá la formación del pertinente sumario administrativo, preservándose el derecho de defensa del imputado.

Se aplicarán al respecto las normas que establezca la reglamentación y en subsidio, el Reglamento de Investigaciones de la Administración Pública Nacional.

Podrá interponerse contra tales sanciones recurso judicial directo, para ante la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal.

El recurso deberá interponerse y fundarse dentro de los treinta días hábiles judiciales de notificada la sanción, ante el órgano que impuso la misma, quien deberá elevar las actuaciones sin otro trámite.

Regirán subsidiariamente las normas correspondientes al recurso de apelación concedido libremente, y en ambos efectos.

TÍTULO III

De las medidas a adoptar en el ámbito de la defensa

Capítulo I: De la Dirección de Seguridad Informática de Defensa

Art. 9: Créase, en jurisdicción del Ministerio de Defensa, la Dirección de Seguridad Informática de Defensa (DISID).

Constituirá un organismo desconcentrado.

Su titular será designado por el Ministerio de Defensa, debiendo ser un civil o militar retirado con relevantes conocimientos en materia informática.

Tendrá por misión la de prevenir, detectar, enfrentar y analizar amenazas informáticas contra todo tipo de sistemas informáticos correspondientes a la jurisdicción del Ministerio de Defensa, incluyendo los pertenecientes a las Fuerzas Armadas.

Para el cumplimiento de su misión dependerán funcionalmente de la Dirección todos los sistemas informáticos existentes en el Ministerio de Defensa y en las Fuerzas Armadas, pudiendo emitir directivas tendientes a proveer a la seguridad de tales sistemas.

Tendrá también a su cargo analizar los requerimientos de adquisición de equipo informático por parte de las Fuerzas Armadas, pronunciándose respecto de su idoneidad para la finalidad propuesta, compatibilidad con los sistemas existentes y seguridad informática.

Gestionará además el Programa de Seguridad Informática Militar.

Capítulo II: Del Comando Estratégico Operacional Conjunto Informático

Art. 10: El Presidente de la Nación dispondrá la creación de un Comando Estratégico Operacional Conjunto Informático, cuya misión comprenderá todos los aspectos relativos al empleo de la informática en materia de defensa, incluyendo el planeamiento y adiestramiento a ese fin.

TÍTULO IV

Disposiciones finales

Art. 11: Los gastos que demande el cumplimiento de la presente ley serán tomados de “Rentas generales” con imputación a la presente ley, hasta su inclusión en el Presupuesto de la administración nacional correspondiente al ejercicio subsiguiente al de su entrada en vigencia.

Art. 12: Queda derogada toda norma que se oponga a la presente ley.

Art. 13: Comuníquese al Poder Ejecutivo.

Antonio T. Berhongaray

PROYECTO DE LEY DELITOS INFORMÁTICOS (SENADOR CARLOS H. ALMIRÓN)

Numero de Proyecto: 1471/98

Publicado DAE. N° 76/98–Caducó: 29/02/2000

DELITOS INFORMÁTICOS:

Art. 1: Será reprimido con prisión de un mes a dos años, el que se apoderare ilegítimamente, a través del uso de una computadora, de datos personales, que deben ser mantenido en reserva, en virtud del derecho a la intimidad.

Art. 2: Será reprimido con prisión de un mes a seis años, el que difundiere aquellos datos, maliciosamente, con el objeto de obtener un provecho económico.

Art. 3: Será reprimido con prisión de dos meses a cuatro años, el que, a sabiendas, alterar o destruyere, un sistema informático, un programa o un equipo de computación.

Art. 4: Será reprimido con prisión de dos meses a seis años, el que defraudare a otro, a través de una computadora o un sistema informático.

Art. 5: Cuando los hechos precedentes fueran realizados por un funcionario público, se la aplicará la accesoria de inhabilitación especial perpetua.

Art. 6: Incluyese en los Art. 71, 72 y 72 bis de la ley 11.723, las obras de software y de base de datos.

Art. 7: Comuníquese al Poder Ejecutivo.

Carlos H. Almirón.

ANEXO II



HACKERS Y CRACKERS FAMOSOS

CRACKERS

DRAPER JOHN, “CAPTAIN CRUNCH”

En septiembre de 1970 John Draper, también conocido como Captain Crunch, descubre que el obsequio ofrecido en las cajas de cereal Captain Crunch duplica perfectamente la frecuencia de tono de 2600 hz. de una línea de WATS, permitiéndole hacer llamadas telefónicas gratis y la gran víctima era AT&T.

HOLLAND WAU Y WENERY STEFFEN

"Lo logramos, por fin... Sólo hay algo seguro, la infinita inseguridad de la seguridad". Fue lo que escribió Wau Holland, en su cuaderno de notas, el 2 de mayo de 1987. Los dos hackers alemanes, de 23 y 20 años respectivamente, habían ingresado sin autorización al sistema de la central de investigaciones aerospaciales más grande del mundo (NASA).

¿Por qué lo hicieron?, "Porque es fascinante, la única aventura posible está en la pantalla de un ordenador", respondieron.

Cuando Wau y Steffen advirtieron que los técnicos los habían detectado, le enviaron un telex, avisando de su intrusión.

ING-HOU CHEN

Taipei, Taiwan, Abril 30 de 1999. El autor del virus "Chernobyl", dijo a los investigadores que él creó el bug con la esperanza de humillar y vengarse de los que llamo "proveedores incompetentes de antivirus para software". Pero él admitió que no esperaba que CIH (iniciales de su autor) causara daño alrededor del mundo. Este virus devastó cientos de miles de computadoras alrededor del mundo.

Chen creó el virus en Abril, cuando todavía era estudiante de ingeniería computacional en el Instituto Tecnológico.

Este inusual virus destructivo, programado para funcionar el 26 de Abril, (13° aniversario del desastre nuclear de Chernobyl), trata de borrar el disco rígido y escribir "basura" en algunos otros componentes, evitando de este modo el futuro encendido de la computadora.

KEVIN Y RONALD

Ronald y Kevin, con los nombres de guerra Makaveli y TooShort en el ciberespacio, asaltaron los ordenadores del Pentágono en Marzo del año 1998, a la tierna edad de 17 años. Estos dos forajidos virtuales, con sus conocimientos y con un equipo básico informático, se introdujeron en cuatro sistemas de la Marina y siete de las fuerzas aéreas, relacionados con centros digitales en Estados Unidos y Okinawa.

LA MACCHIA DAVID

En 1994 David La Macchia, estudiante de 20 años del prestigioso y serio MIT, reconoce que ha distribuido en Internet multitud de programas informáticos obtenidos sin licencia y por valor de un millón de dólares. Para ofrecerlos a los cibernautas montó su propia BBS.

LEVIN VLADIMIR

Un matemático ruso de 24 años, penetró vía Internet desde San Petersburgo en los sistemas informáticos centrales del banco Citybank en Wall Street, Este pirata logró transferir a diferentes cuentas de EE.UU., Rusia, Finlandia, Alemania, Israel, Holanda y Suiza fondos por valor de 10 millones de dólares, según el FBI. Detenido en el Reino Unido a principios de 1995, Levin espera que los tribunales británicos se pronuncien sobre una demanda de extradición solicitada por EE.UU.

MITNICK KEVIN, “EL CÓNDOR”, “EL CHACAL DE LA RED”

Como hacker, la carrera de Mitnick tiene sus inicios en 1980 cuando apenas contaba 16 años y, obsesionado por las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, lo hizo “solo para mirar”.

La primera vez que lo detuvieron fue en 1981 por robar manuales de la Pacific Telephone. La información robada tenía un valor equivalente a los 200 mil dólares y tuvo que cumplir una condena tres meses de cárcel y a un año bajo libertad condicional.

En 1983 intentó ingresar en las computadoras de la universidad de California del Sur y poco después penetró el sistema de la agencia de créditos TRW.

En 1987 lo condenaron a treinta y seis meses de libertad condicional por robo de soft, tras hackear los sistemas del Departamento de Defensa de EE.UU. y la NASA.

Un año más tarde fue arrestado de nuevo cuando era estudiante de la Universidad del Sur de California. En esta ocasión entró ilegalmente a ARPAnet (la predecesora de Internet) y trató de acceder a la computadora del Pentágono. Lo sentenciaron a seis meses de cárcel en una prisión juvenil en California.

Durante ese tiempo le negaron el acceso a los teléfonos y a lo largo de los doce meses de rehabilitación no pudo acercarse a una computadora.

Más tarde, y ya en libertad, se apoderó de 16 códigos de seguridad de MCI y junto a un amigo, Lenny DiCicco, entraron a la red del laboratorio de investigaciones de Digital Corporation, conocida como Easynet.

Ambos hackers querían obtener una copia del prototipo del nuevo sistema operativo de seguridad de Digital llamado VMS. El personal de seguridad de Digital se dio cuenta inmediatamente del ataque y dieron aviso al FBI, y comenzaron a rastrear a los hackers.

Mitnick fue arrestado en 1988 por invadir el sistema de Digital Equipment. La empresa acusó a Mitnick y a DiCicco ante un juez federal de causarles daños por 4 millones de dólares en el robo de su sistema operativo. Fue declarado culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia.

Adicional a la sentencia el fiscal obtuvo una orden de la corte que prohibía a Mitnick el uso del teléfono en la prisión alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono. A petición de Mitnick el juez lo autorizó a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela y sólo bajo supervisión de un oficial de la prisión.

Este caso produjo revuelo en los Estados Unidos, no sólo por el hecho delictivo sino por la táctica que utilizó la defensa. Su abogado convenció al juez que Mitnick sufría de una adicción por las computadoras equivalente a la de un drogadicto, un alcohólico o un apostador. Gracias a esta maniobra de la defensa Mitnick fue sentenciado a sólo un año de prisión y al salir de allí debía seguir un programa de seis meses para tratar su “adicción a las computadoras”. Durante su tratamiento le fue prohibido tocar una computadora o un módem y llegó a perder más de 45 kilos.

Para 1991 ya era el hacker que había ocupado la primera plana del New York Times y uno de sus reporteros, John Markoff, decidió escribir un libro de estilo Cyberpunk narrando las aventuras de Mitnick. Al parecer a Mitnick no le gustó el libro ya que luego de salir a la venta, la cuenta en Internet de Markoff fue invadida, cambiando su nivel de acceso, de manera de que cualquier persona en el mundo conectada a Internet podía ver su correo electrónico.

En 1992, y luego de concluir su programa, Mitnick comenzó a trabajar en una agencia de detectives. Pronto se descubrió un manejo ilegal en el uso de la base de datos y fue objeto de una investigación por parte del FBI quien determinó que había violado los términos de su libertad condicional. Se ofreció una recompensa de 1 millón de dólares a quien arrestara a Mitnick.

Luego de convertirse en prófugo de la justicia cambió de táctica y concluyó que la mejor manera de no ser rastreado era utilizando teléfonos celulares.

Luego de varios intentos infructuosos, en cuanto a calidad de información, se encontró con la computadora de Tsutomu Shimomura la cual invadió en la Navidad de 1994. Shimomura, físico computista y experto en sistemas de seguridad del San Diego Supercomputer Center, era además un muy buen hacker, pero era de los “chicos buenos”, ya que cuando hallaba una falla de seguridad en algún sistema lo reportaba a las autoridades, no a otros hackers.

Shimomura notó que alguien había invadido su computadora en su ausencia, utilizando un método de intrusión muy sofisticado y que él nunca antes había visto. El intruso le había robado su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet. Allí comenzó la cuenta regresiva para Mitnick. Shimomura se propuso como orgullo personal atrapar al hacker que había invadido su privacidad.

Más tarde, El 16 de febrero de 1995, Mitnick fue capturado, juzado y condenado a 25 años de prisión, lejos de computadoras y teléfonos.

Pero, el 22 de marzo de 1999, se consigue un acuerdo con jueces y fiscales. Los términos concretos se desconocen, pero se sabe que en marzo de 2000 Mitnick quedaría en libertad con la condición irrevocable de no poder acercarse a una computadora.

Kevin Mitnick, este sencillo nombre, oculta la verdadera identidad de uno de los mayores crackers de la historia. Fue una de las mayores pesadillas del Departamento de justicia de los Estados Unidos. Entró virtualmente en una base de misiles, llegó a falsificar 20.000 números de tarjetas de crédito y a causar pérdidas millonarias a varias empresas.

MORRIS ROBERT

En noviembre de 1988, Morris lanzó un programa “gusano”, diseñado por él mismo, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de y más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causó a las víctimas muchos días de productividad perdidos, y millones de dólares.

Como consecuencia, se creó el CERT (Equipo de Respuesta de Emergencias Computacionales) para combatir problemas similares en el futuro. Morris fue condenado y sentenciado a tres años de libertad condicional, 400 horas de servicio comunitario y US \$10000 de fianza, bajo el cargo de Fraude computacional y abuso. La sentencia fue fuertemente criticada debido a que fue muy ligera, pero reflejaba lo inocuo de las intenciones de Morris más que el daño causado.

MURPHY IAN, “CAPTAIN ZAP”

En julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba “Captain Zap”, gana notoriedad cuando entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

En 1981, no había leyes muy claras para prevenir el acceso no autorizado a las computadoras militares o gubernamentales. “Captain Zap” mostró la necesidad de hacer más clara la legislación. Con cargos de robo de propiedad, finalmente, Murphy fue multado por US\$ 1000 y sentenciado a 2½ años de prueba.

“PAINT” Y “HAGIS”

Estos son los seudónimos de los dos hackers que el 10 de Diciembre de 1997 accedieron a uno de los buscadores más utilizados en Internet. Los terroristas informáticos autodenominados "Paints & Hagis", accedieron al servidor del popular navegador Yahoo! y dejaron un mensaje amenazante a los casuales visitantes.

Este ataque no resultó ser más de una modificación de una página web, y un ejemplo temprano de las muchas que se modifican hoy día a día.

PETERSON JUSTIN TANNER, “AGENT STEAL”

Peterson crackeaba las agencias de crédito. Esta falta de personalidad le llevó a su caída y a la de otros. Tiempo después, se dice, obtuvo un trato con el FBI. Esto le facilitó su salida de la cárcel y “no” pudo ser demostrado un fraude mediante una transferencia de dinero.

POULSEN KEVIN, “DARK DANTE”

En diciembre de 1992 Kevin Poulsen fue acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusó Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y fue condenando a 10 años en la cárcel (salió bajo palabra a los 5 años).

Como Cracker, siguió el mismo camino que Kevin Mitnick, pero fue más conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llegó a “ganar” un Porsche en un concurso radiofónico, si su llamada fuera la 102, y así fue. Poulsen también crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional. Esto fue lo que lo llevó a su estancia en la cárcel, 5 años, fue liberado en 1996, supuestamente “reformado”.

SMITH DAVID

Programador de 30 años, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, “Melissa”. Entre los cargos presentados contra él, figuran el de “bloquear las comunicaciones publicas” y de “dañar los sistemas informáticos”. Acusaciones que en caso de demostrarse en el tribunal podrían acarrearle una pena de hasta 10 años de cárcel.

Por el momento y a la espera de la decisión que hubiese tomado el juez, David Smith esta en libertad bajo fianza de U\$S 10000. Melissa en su “corta vida” había conseguido contaminar a más de 100.000 computadoras de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del Gobierno del Estado de Dakota del Norte y el Departamento del Tesoro.

Sin embargo, la detención de Smith no significa que el virus haya dejado de actuar. Compañías informáticas siguen alertando que aún pueden quedar miles de usuarios expuestos a sus efectos, por desconocimiento o por no haber instalado en sus equipos sistemas antivíricos que frenen la actividad de Melissa u otros virus, que han venido apareciendo últimamente como Happy99 o Papa.

THE MENTOR Y GRUPO H4G13

El autodenominado grupo H4G13, con Mentor a su cabeza quería demostrar hasta donde eran capaces de llegar, y lo dejaron plasmado de una manera efectiva, colocando en la pagina principal de la NASA, durante media hora, el “manifiesto” hacker más conocido hasta el momento. Ver Capítulo 5.

ZINN HERBERT, “SHADOWHACK”

Herbert Zinn, (expulsado de la educación media superior), y que operaba bajo el seudónimo de “Shadowhawk”, fue el primer sentenciado bajo el cargo de Fraude

Computacional y Abuso. Zinn tenía 16 cuando violó el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US\$ 174000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publicó contraseñas y instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US\$ 10000.

HACKERS

ARDITA JULIO CESAR, “EL GRITÓN”

Es considerado el hacker más famoso de Argentina. Nació en Río Gallegos, el 28 de marzo del 1974. Utilizó su primera computadora mientras realizaba su secundaria. En quinto año, junto con dos compañeros ayudaron a informatizar el sistema de notas y facturación del colegio en el cual estudiaba.

Este muchacho, saltó a la fama el 28 de diciembre de 1995, día de los Santos Inocentes, cuando su domicilio fue allanado por la Justicia Argentina luego de que los Estados Unidos alertaran sobre reiteradas intrusiones a varias de sus redes informáticas de Defensa, entre ellas la del Pentágono.

Las intrusiones provenían de una computadora conectada a una línea telefónica desde un departamento de Barrio Norte, en la Capital Federal. “El Gritón” ingresaba en la red de computadoras de la empresa Telecom a través de líneas gratuitas 0800, para luego realizar intromisiones en sistemas informáticos ajenos.

En la causa argentina número 45048/95, con carátula "Ardita Julio C., sobre defraudación", el juzgado de Instrucción número 38 a cargo de la jueza Wilma López, dispuso que Ardita compareciera ante un tribunal oral pero por fraude telefónico (estimado por la empresa Telecom en \$50), ya que las intrusiones informáticas no están contempladas en el Código Penal.

Sin embargo, por el mismo episodio, Ardita ya tuvo que recorrer una espinosa demanda penal en los Estados Unidos, donde las intrusiones informáticas, las violaciones de códigos secretos y la posesión de claves ajenas sí son delitos graves. El proceso terminó el 19 de mayo 1999, cuando un tribunal de la ciudad de Boston, lo condenó a 3 años de libertad condicional y a pagar una multa de US\$5000 por haber vulnerado, entre otros varios, el sistema informático de la Marina.

Hoy en día, con 27 años, Julio Cesar Ardita paga religiosamente sus facturas telefónicas; se levanta temprano por las mañanas y camina hasta la zona de Tribunales. Allí está Cybsec S.A., la exitosa empresa de seguridad informática que el ex-Gritón administra junto a su socio.

BARAM PAUL

Posiblemente el mayor hacker de la historia. Ya hackeaba Internet antes de que existiera. El fué quien introdujo el concepto de hacker.

FARMER DAN

Trabajó con Spafford en la creación de COPS (1991) y al mismo tiempo con el famoso Computer Emergency Response Team (CERT). Tiempo más tarde Farmer ganó gran notoriedad al crear el System Administrator Tool for Analyzing Networks (SATAN). Una gran herramienta para analizar vulnerabilidades en redes.

GATES BILL Y ALLEN PAUL

En sus tiempos de aprendices, estos dos hombres de Washington se dedicaban a hackear software. Empezaron en los 80 y han creado los mayores imperios de software de todo el mundo.

RITCHIE DENNIS, THOMSON KEN Y KERRIGHAN BRIAN

Programadores de los Laboratorios Bell. Son los desarrolladores de UNIX y C. Se los considera los padres de la informática masiva al desarrollar el sistema operativo y el lenguaje más poderosos de la actualidad.

SPAFFORD EUGENE

Profesor de informática. Colaboró para crear el Computer Oracle Password Security System (COPS) un sistema de seguridad semiautomático. Es un hombre muy respetado en el campo de la seguridad.

STALLMAN RICHARD

Se unió al Laboratorio de inteligencia artificial de la MIT en 1971. Fue ganador del premio McArthur por sus desarrollos de software. Fue fundador de Free Software Foundation, creando aplicaciones y programas gratis.

TORVALDS LINUS

Torvalds empezó a conocer el UNIX y a tomar clases de programación en C sobre los 90. Un año después empezó a escribir un SO parecido al UNIX. Después de otro año, lo subió a Internet pidiendo colaboración; hoy es llamado LINUX.

VEHEMA WIETSE

Vehema viene de la Universidad de Tecnología de Eindhoven, en los Países Bajos. Un gran programador, con un don para ello, además de tener un amplio historial en programas sobre seguridad. Es el coautor del SATAN con Farmer. Vehema escribió el TCP Wrapper, uno de los programas de seguridad más usado en el mundo.

ANEXO III



HERRAMIENTAS

HERRAMIENTAS DE SEGURIDAD

Estas son algunas herramientas que permiten verificar y violar la seguridad de su sistema. Es su responsabilidad evaluarlas antes de su uso, y de complementarlas con algunas otras para garantizar la seguridad de su sistema.

Actividad en Internet

Air SmartGate
Cyber Snoop
Ianalyst
Internet Cleanup
Internet Manager
Internet Resource Manager
Internet Risk Management
NetFocus
System Activity Manager
Web Spy
WebTrends Firewall Suite
WinGuardian

Análisis de Red

Abend-AID Fault Manager
Actiview Trouble Manager
AimIT
BindView
Centennial Discovery
Enterprise Security Manager
Event Log Monitor
Expert Observer
Kane Security Analyst
Link Analyst
NT Manage
NTRama
Sentinel Software Security
SPQuery
TripWire
WebTrends Netware Management

Anti-Espionaje

Ad-Search
Anticotillas Plus
FlashLock
Guideon
Hook Protect
Iprotect
PC Security Guard
Rainbow Diamond Intrusion Detector
Top Secret Office

Anti-Spam

Spam Buster
Spamkiller
SpammerSlammer

Anti-Virus y Troyanos

AntiViral Toolkit Pro
AVTrojan
AVX
BootProtect
Compucilina
eSafe Protect
Fobiasoft Guardian
F-Secure
Inoculate
InVircible Antivirus
iRis Antivirus

Kaspersky Anti-Virus
MAMSoft
Mcfee VirusScan
Norman Thunderbyte Virus Control
Norton Antivirus
Panda Antivirus Platinum
PC-cillin
Protector Plus
Quick HealRAV AntiVirus
Sophos
The Cleaner
Trojan Defense Suite
VirIT
VirusSafe Web

Arranque

Access Denied
Boot Sentry
BootLocker
MindSoft Custody
ScreenLock
SCUA Security
Sentry
ThunderGuard
Xlock

Auditoria

FileAudit
Log Monitor
SecurityCharge

Backup

@Backup
Adsm
ArcServe
AutoSave
Backup ATM Network
Backup Exec
Connected Online Backup
Data Recovery for NetWare
DataKeeper
Discview
Drive Image
ImageCast
NetBackup
Norton Ghost
Novabackup
Open File Manager
Replica
Retrospect
SurviveIT
Ultrabac

Bloqueo y Restricción

Absolute Security
AceControl
Anfibia Soft Deskman
CDLock
ChildProof

Clasp2000
Deskman
Desktop Locker 1.0
DesktopShield
DeviceLock Me
GS98 Access Control
ISS Complock
Lock n Safe
MausTrap
MicroManager
MindSoft GuardianShip
Mindsoft Restrictor
PC Lock
PC Restrictor
RedHand Pro
SecureIt Pro
SecurityWizard
Smart98
StormWindow
System Security
TrueFace
Windows Security Officer
WinFile Vault
WinLock

Contraseñas

007 Password Recovery
Aadun
Absolute Security
Advanced Password Generator
Asterisco
Claves
ePassword Keeper
EXE Protector
Guardian
Info Keep
LockDown
Locker
MasterPass
Office Password
Open Pass
PassGo
PassGuard
Password Corral
Password Generator
Password Guardian
Password Keeper
Password Power
Password Tracker
Passwords
Planet.Keeper
Private Bookmarks
PwITool
Qwallet
Random Password Generator
Secret Surfer
Software Safe
v-GO Universal Password
WMVault

Control Remoto

AMI Server Manager
ControlIT
CoSession

Kane Security Monitor
LapLink
NetOp
NetSupport Manager
PcAnywhere
Proxy
ReachOut Enterprise
Remote Administrator
ServerTrak
Timbuktu Pro
TrendTrak

Cookies

Cache & Cookie Washer
Cookie Crusher
Cookie Pal
CyberClean
The Watchman
Window Washer

Detectores de Agujeros de Seguridad

Check Point RealSecure
Hackershield
Intruder Alert
LanGuard Network Scanner
Lucent RealSecure
NetProwler
NetRecon
PassMan Plus
SecureNet Pro Software
WebTrends Security Analyzer

Encriptación de Comunicaciones

Bbcom VPN
F-Secure VPN
Go Secure
GuardianPRO VPN
Intel VPN
KryptoGuard LAN and VPN
PGP
Power VPN
SafeGuard VPN
Sidewinder
SmartGate
SonicWall Pro
VPN 1 Internet Gateway
VPNWare System

Encriptación de Software

ABI- CODER
Absolute Security
AutoEncrypt
BestCrypt
CodedDrag
Combo
CrypText
Cryptit
CryptoIdentify
Cryptoman
Data Safe
DataCloak
Easy Code

Easycrypto
 Emerald Encryption
 Encrypt IT!
 Encrypted Magic Folders
 Enigma
 Enigma 98
 File Protector
 FileCrypto
 FileDisk Protector
 FlyCrypt
 Folder Guard
 Hideit! Pro
 HotCrypt
 InfoSafe
 Interscope BlackBox
 Invisible Secrets
 Jumblezilla
 Kremlin
 Krypton Encoding System
 MindSoft Shelter
 Neocrypt
 Norton Secret Stuff
 NovaLock
 Passworx
 PCSafe
 PGP
 Quick:CRYPT
 RSA Bsafe
 SafeGuard LanCrypt
 SafeSuite Realsecure
 SECRETsweeper
 SECURE
 Secure Shuttle Transport
 Security BOX
 SecurityManager
 ShyFile
 SpartaCom Cryptogram
 TEACrypt
 Text Watchdog
 The DESX Utility
 ThunderCrypt
 Unbreakable Encryption
 WINZAP
 Xcrypto

Espionaje

2Spy!
 Activity Monitor
 Alot Monica
 AppsTraka
 ASCII Spy
 AY Spy
 Boss Everyware
 Canary
 Date Edit
 Desktop Surveillance
 El Espía
 EventControl
 IntraSpy
 Key Logger
 Keyboard Monitor
 KeyKey
 MyGuardian
 Omniquad Detective
 Password Revealers

PC Spy
 RemoteView
 Snooper
 Spector
 SpyAnywhere
 Stealth Activity
 Stealth Keyboard Interceptor
 Stealth Logger
 SupervisionCam
 System Spy
 Watcher
 WinGuardian

Filtros de Internet

CommandView
 Cyber Attack Defense System
 Cyber Sentinel
 Digital ID
 e-Sweeper
 Go Secure!
 Mail-Gear
 MailSweeper
 MailVault
 Message Inspector
 Predator Guard
 Private-I
 Real Secure
 Shields UP!
 SigabaSecure
 SmartFilter
 WEBSweeper
 World Secure Mail

Firewalls

Altavista Firewall
 BlackIce
 CheckPoint
 CyberArmor
 Elron Firewall
 FireProof Firewall KIT System
 GuardianPRO Firewall
 GuardIT
 HackTracer
 MindSoft Firewall
 NeoWatch
 Netmax Firewall
 Norton Personal Firewall
 Raptor Firewall
 Secure Connect Firewall
 SmartWall
 Sygate Personal Firewall
 Tiny Personal Firewall
 Watchguard Livesecurity SYS
 WinRoute Pro
 ZoneAlarm Pro

Gestión de Accesos

Absolute Protect
 Access Manager Secondary Radius
 Azza Air Bus
 Border Protector
 c2000
 Cnet/2

Defender
E-Z Lock
GuardianPro Authentication
Hands Off Personal
Identity Protector
IKey
Lock Protector
Navis Access
Navis Radius Access Control
Palladium Secure Remote Access
Panda Security
Personal Protector
PrivateEXE
RSA SecurID
SafeGuard Easy
SafeWord Plus
SmartGuard
SmartLock
Steel-Belted RADIUS
UserLock
VicinID
WinFuel

Mantenimiento

Diskeeper
More Space
Partition Commander
Partition Magic
Security Setup
System Commander
Windows Commander

Ocultación

BlackBoard FileWipe
Boss
Camouflage
Don't Panic!
Hidden 7
Invisible Files
Sentry98
WebPassword
WinShred
WipeClean

Recuperación de Datos

ConfigSafe Desktop
CoreSave
Easy Recovery
Easy Restore
Esupport
GoBack
Instant Recovery
Lost & Found
PictureTaker Personal Edition
SecondChance
Shredder
System Snapshot
Undelete

Seguridad en Comercio Electrónico

Commerce Protector
CryptoSwift
ETrust
NetSecure
RSA Keon
SAFEsuite Decisions
Safety Net

Suites de Seguridad Informática

eSafe Desktop
F-Secure Workstation Suite
Mcafee Office 2000 Pro
NetMax Professional Suite
Norton Internet Security 2000
Observer Suite
Ontrack SystemSuite 2000
Secur-All

GLOSARIO

a

ACK (Confirmación): Notificación enviada desde un dispositivo de red a otro para confirmar que ocurrió cierto evento (por ejemplo, la recepción de un mensaje).

ActiveX: Lenguaje desarrollado por Microsoft® para la elaboración de aplicaciones exportables a la red y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores.

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones al mismo. Véase También Root y SysOp.

AH (Authentication Header): Protocolo IP 51. Protocolo de la familia IPSec utilizado para garantizar la integridad de los datos y la autenticación del Host. Ver Capítulo 8.

ANSI (American National Standard Institute): Asociación sin fines de lucros, formada por fabricantes, usuarios, compañías que ofrecen servicios públicos de comunicaciones y otras organizaciones interesadas en temas de comunicación. Es el representante estadounidense en **ISO**. Que adopta con frecuencia los estándares ANSI como estándares internacionales.

Antivirus: Programa que encargado de evitar que cualquier tipo de virus ingrese al sistema, se ejecute y se reproduzca.. Para realizar esta labor existen muchos programas, que comprueban los archivos para encontrar el código de virus en su interior. Ver Capítulo 6.

Applet: Pequeña aplicación escrita en Java y que se difunde a través de la red para ejecutarse en el navegador cliente.

Archie: Aplicación que permite localizar los archivos accesibles vía **FTP** anónimo. Si se conoce el nombre de un archivo, pero no se sabe dónde se encuentra, Archie le permite localizarlo.

Archivo: Conjunto bytes relacionados y tratados como una unidad. Un archivo puede contener programas, datos o ambas cosas.

ARP (Address Resolution Protocol): Este Protocolo de Resolución de Direcciones permite mantener asignaciones de pares formados por las direcciones **IP** y las direcciones físicas (**MAC**) de los distintos dispositivos de comunicación. Véase también **RARP**.

ASCII (American Standard Code for Information Interchange): Código estándar americano para intercambio de información. Sistema de codificación de 7 bits que asigna un número del 0 al 127 a cada letra, número, caracteres especiales y de control recogidos. El uso del octavo bit no está tan estandarizado aunque se suele utilizar como código de paridad calculado (normalmente par).

ASV (Automatic Sign Verification): Sistema de verificación automática de firmas. Ver Capítulo 2.

Ataque: Intento de traspasar un control de seguridad de un sistema. Ver Capítulo 6.

b

Backdoor: Puerta trasera de entrada a una computadora, programa o sistema en general. Es utilizado para acceder sin usar un procedimiento normal. Ver Capítulo 6.

Backup: Copia de seguridad que se realiza con el fin de mantener los datos en forma segura. Ver Capítulo 9.

Boxing: Uso de aparatos electrónicos o eléctricos (**Boxes**) para hacer **Phreaking**.

Bouncer: Técnica que consiste en usar un sistema de puente para conseguir **redireccionar** la salida a un puerto determinado de otro sistema. Ver Capítulo 6.

Bastión Host: Sistema configurado para resistir los ataques y que se encuentran instalado en una red en la que se prevé que habrá ataques. Son componentes de los Firewalls ejecutando alguna aplicación o sistema operativo de propósito general. Ver Capítulo 8.

BBS (Bulletin Board System): Boletín Electrónico. Es un sistema mediante el cual se pone a disposición de los demás una serie de recursos.

Bit: En informática, unidad mínima de información.

Black Box: Aparato que engaña a la central telefónica haciéndole creer que no se levantó el tubo del teléfono cuando en realidad se está produciendo una comunicación. Ver Capítulo 5.

Bomba Lógica: Programa ilegítimo contenido dentro de un sistema y que ante un hecho o una fecha prevista “explota” causando daño al sistema que lo contiene u a otro. Raramente tienen la capacidad de reproducción. Ver Capítulo 6.

BPS (Bits por Segundo): Medida de velocidad de transmisión.

BroadCast: Difusión. Tipo de comunicación en que todo posible receptor es alcanzado por una sola transmisión. Véase también **Multicast**.

Buffer Overflow: Error generado cuando un programa (generalmente un servidor o “demonio”) recibe una entrada mayor a la que espera, sobrescribiendo áreas críticas de memoria.

Bug: Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otro motivo.

Byte: Combinación de **Bits**. En la representación más común 8 bits forman un byte.

C

Caballo de Troya: Programa aparentemente útil el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar algún daño. Ver Capítulo 6. Véase también **Troyano**.

CCITT (Comité Consultatif International de Télégraphique et Téléphonique): Organización de la Naciones Unidas constituida, en principio, por las autoridades de Correos, Telégrafos y Teléfonos (PTT) de los países miembros. Se encarga de realizar recomendaciones técnicas sobre teléfonos, telégrafos e interfaces de comunicación de datos, que a menudo se reconocen como estándares. Trabaja en colaboración con **ISO** (que en la actualidad es miembro de CCITT). Véase también **ITU-T**.

CERT/CC (Computer Emergency Response Team/Coordination Center): Grupo establecido en diciembre de 1988 por Defense Advanced Research Projects Agency (DARPA) para manejar los problemas concernientes a la Seguridad Informática. El CERT es dirigido por expertos en diagnósticos y resolución de problemas de seguridad. Para la resolución de estos problemas están en permanente contacto con usuarios de todo el mundo y las autoridades gubernamentales apropiadas. Por más información consultar <http://www.cert.org> - <http://www.arcert.gov.ar>.

Ciberspacio: “(...) alucinación consensual experimentada diariamente por millones de legítimos operadores en todas las naciones...una representación gráfica de información proveniente de todas las computadoras del sistema humano. Una complejidad inimaginable (...)”. GIBSON, William. Neuromante.

Cifrar: Ver **Criptografía**.

Clave, Contraseña (Password): palabra o frase que permite acceder a un sistema, encriptar un dato, determinar privilegios de usuarios, etc.

Clave Pública: En un **Sistema Asimétrico de Cifrado** es la clave que todos conocen para **Cifrar** o descifrar un mensaje.

Clave Privada: : En un **Sistema Asimétrico de Cifrado** es la clave que solo el emisor del mensaje conocen para **cifrar** o descifrar un mensaje.

Cliente: Sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una computadora que solicita el contenido de un archivo a otra (**Servidor**) es un cliente de la misma.

Código Fuente: Un programa escrito en un formato entendible por el hombre pero no por la computadora. Necesita ser "traducido" (**Compilar**) a código máquina para ser interpretado por esta última.

Colgar: Hacer que un sistema deje de funcionar. Desconectar una comunicación telefónica.

Compilador: Programa que toma el **Código Fuente** de un programa y lo convierte a un ejecutable.

Cookie: Es un pequeño trozo de información enviado por un servidor de Web al sistema de un usuario.

Correo electrónico: aplicación que permite enviar mensajes a otros usuarios de la red sobre la que esté instalado. También denominado **E-Mail**.

Cortafuegos: Ver **Firewall**.

Cracker: Persona que quita la protección a programas con sistemas anticopia. Hacker maligno, que se dedica a destruir información.

Criptografía: Ciencia que consiste en transformar un mensaje inteligible en otro que no lo es, mediante la utilización de **claves**, que solo el emisor y receptor conocen. Ver Capítulo 8.

d

Datagrama: Conjunto de datos que se envían como mensajes independientes. Unidad utilizada por el protocolo **UDP**.

Denial of Service (DoS): Negación de Servicio. Acciones que impiden a cualquier sistema funcionar de acuerdo con su propósito. Ver Capítulo 6.

Detección de Intrusos: Sistemas que agrupa un conjunto de técnicas cuyo propósito es detectar las intrusiones en una computadora o un sistema. Ver Capítulo 6-8.

Decoy (Señuelo): Programa diseñado para que vigilar el comportamiento de un usuario.

Diccionarios: Conjunto de palabras almacenadas en un archivo. Su fin es utilizar cada palabra para se probada como posible **Password** de un sistema que se quiere violar. Véase también **Fuerza Bruta**. Ver capítulo 6.

DNS (Domain Name Server): Servicio que proporciona una dirección IP a partir de un nombre de dominio proporcionado. Este protocolo evita tener que recordar las complicadas combinaciones de números que forman una dirección IP. Ver Capítulo 6.

DoS (Denial of Service): Negación de Servicio. **Ataque** masivo para **Colgar** un ordenador.

e

E-Mail: Ver **Correo Electrónico**.

EIA (Electronic Industries Association): Asociación vinculada al ámbito de la electrónica. Es miembro de **ANSI**. Sus estándares se encuadran dentro del nivel 1 del modelo de referencia **OSI**.

Encriptar: Ver **Criptografía**.

ESP (Encapsulating Security Payload): Protocolo IP 50. Protocolo de la familia IPSec que incluye las características de AH y agrega, opcionalmente, la confidencialidad de los datos. Ver Capítulo 8.

Ethernet: Protocolo de comunicación. Especificación de LAN de banda base, inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel, y Digital Equipment Corporation.

Exploit: Programa que aprovecha un **Bug** de un sistema. Programa que abusa de algún error de un sistema operativo para conseguir aumentar los privilegios de un usuario o la caída del sistema.

f

Fake Mail: Enviar correo falseando el remitente.

FAQ (Frequently Asked Questions): Documento donde se vuelcan las preguntas más frecuentes sobre un tema y sus respuestas.

Finger: Define los estándares para buscar información de un usuario.

Firewall: Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los límites entre dos o más redes y restringe la entrada y salida de la información. Ver Capítulo 6.

FTP (File Transfer Protocol): Protocolo del nivel de usuario (protocolos de aplicación) para la transferencia de archivos entre computadoras. También pueden hacer referencia a la aplicación que permite transferir archivos de una computadora a otra usando el mismo protocolo. Ver Capítulo 6.

Fuerza Bruta: Se basan en aprovechar **Diccionarios** para comparar las palabras almacenadas en él con las **Passwords** del sistema y obtenerlos.

g

Gateway: Dispositivo de enrutamiento. En la actualidad, se utiliza el término **Router** para describir los nodos que realizan esta función, mientras que **Gateway** se refiere a un dispositivo para fines especiales que convierte información de la capa de aplicación de un stack de protocolo a otro. Ver capítulo 6.

Gopher: Aplicación de Internet que permite utilizar recursos remotos mediante el uso de un sistema de simples menús. Se tiene a su alcance la mayoría de los recursos de Internet desplegados en diferentes opciones de los distintos menú.

Guest (Invitado): Cuenta pública en un sistema. Su objetivo es ser utilizada por alguien que no tiene una cuenta propia.

Gusano: Programa ilegítimo que es capaz de reproducirse a si mismo infinitas veces hasta colapsar el sistema, en el que se está ejecutando, por falta de recursos. Ver Capítulo 6.

h

Hacker: Una persona que disfruta explorando los detalles de las computadoras y de cómo extender sus capacidades. Ver Capítulo 5.

Handshake (Saludo): Secuencia de mensajes intercambiados entre dos o más dispositivos de red para garantizar la sincronización de la transmisión.

Hardware: Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación.

Hexadecimal: Base 16. Una representación numérica que utiliza los dígitos 0 a 9, con su significado usual, más las letras A a F para representación de los dígitos hexadecimales con valores de 10 a 15.

Host: Sistema Central. Computadora que permite a los usuarios comunicarse con otros sistemas de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el **Correo Electrónico**, **Telnet** y **FTP**.

HTML (HyperText Markup Language): Formato especial de archivos sobre el que está basada la estructura de la aplicación **WWW (World Wide Web)**.

HTTP (HyperText Transfer Protocol): Es un protocolo de la capa de aplicaciones con la velocidad necesaria para sistemas de información hipermediales en un ambiente distribuido y colaborativo. Ver Capítulo 6.

Hub (Concentrador): Dispositivo que sirve como centro de una red de topología en estrella.

i

ICMP (Internet Control Message Protocol): Protocolo utilizado para gestionar la comunicación de mensajes de error entre distintos puntos de la red. Ver Capítulo 6.

ID: Identificación.

IDEA (International Data Encryption Algorithm): Algoritmo de encriptación simétrico. Ver Capítulo 8.

IEEE (Institute of Electrical and Electronics Engineers): Instituto de ingeniería eléctrica y electrónica. Organización profesional entre cuyas actividades se incluye el desarrollo de estándares para comunicaciones y **Redes**.

IETF (Internet Engineering Task Force): Grupo Encargado de definir Solicitudes de comentarios (**RFC**).

Ingeniería Social: Arte de convencer a la gente para que realice actos que pueden comprometer un sistema. Obtención de información por medios ajenos a la informática.

Internet: Sistema de redes de computación ligadas entre sí, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias.

Intruso: Aquella persona que con una variedad de acciones intenta comprometer un recurso de hardware o software. Ver Capítulo 5.

Invitado: Ver **Guest**.

IP (Internet Protocol): Protocolo de comunicación sin conexión, que por sí mismo proporciona un servicio de datagramas. Es el Protocolo que proporciona el servicio de envío de paquetes para los protocolos soportados **TCP**, **UDP** e **ICMP**. Protocolo de capa de red de la pila **TCP/IP** que ofrece un servicio de internetwork sin conexión. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y rearmado, y seguridad. Ver Capítulo 6.

IP Spoofing Método para falsear la **IP** en una conexión remota. Ver Capítulo 7.

IPX/SPX: Es el conjunto de protocolos de bajo nivel utilizados por el sistema operativo de red Netware de Novell. **SPX** actúa sobre **IPX** para asegurar la entrega de los datos.

IPSec: Protocolo creado por el IETF para brindar seguridad a nivel de red. Capítulo 8.

IRC (Internet Relay Chat): Charla Interactiva en Internet. **Protocolo** para conversaciones simultáneas; que permite a varias personas comunicarse entre sí por escrito y en tiempo real.

ISO (International Organization for Standardization): Organización voluntaria, no gubernamental, cuyos miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información. Han desarrollado el modelo de referencia **OSI** y protocolos estándares para varios niveles de este modelo. Ver Capítulo 6.

ISP (Internet Service Provider): Compañía o individuo dedicado a vender acceso (servicio) a Internet.

ITU-T (International Telecommunication Union Telecommunication Standardization Sector): Unión Internacional de las Telecomunicaciones (ex Comité de Consultoría Internacional para Telefonía y Telegrafía –**CCITT**–). Organización internacional que desarrolla estándares de comunicación. Véase también **CCITT**.

j

Jargon (Jerga, Jerigonza): Lenguaje peculiar de un determinado grupo, profesión u oficio, difícil (e incluso imposible) de entender por los no iniciados.

Java: Lenguaje de programación desarrollado por **SUN** para la elaboración de pequeñas aplicaciones exportables a la red (**Applets**) y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores.

k

Kerberos: Sistema de seguridad en el que los login y los passwords viajan encriptados a través de la red. Ver Capítulo 7.

Key Logger: Grabador de teclas pulsadas. Es utilizado cuando se desea conocer las contraseñas, nombres de usuarios o cualquier otra información en donde se utilice el teclado como vía de entrada al sistema.

l

L2TP (Layer To Tunneling Protocol): protocolo estándar del **IETF** que encapsula las tramas del Protocolo Punto a Punto (**PPP**) que van a enviarse a través de redes. Ver Capítulo 8.

Lamer: Término aplicado por los **Hackers** a las personas con pocos conocimientos. Ver Capítulo 5.

LAN (Local Area Network): Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. Véase también **MAN** y **WAN**.

Linux: Sistema Operativo de la familia **UNIX**. El proyecto original pertenece a Linus Torvalds.

Login: Nombre de acceso de un usuario a una red o sistema multiusuario. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de ingresar a un sistema de este tipo. El usuario debe usar el nombre, así como su contraseña (password), para tener acceso al sistema.

Log: Archivo de registro de actividades.

m

MAC (Media Access Control): Control de acceso al medio. La inferior de las dos subcapas de la capa de enlace de datos definida por **IEEE**. La subcapa **MAC** administra el acceso a medios compartidos.

Mail Bomber: Consiste en el envío masivo de mails a una dirección de la víctima.

MainFrame: Gran computadora central.

MAN (Metropolitan Area Network): Red de área metropolitana. En general, una MAN abarca un área geográfica más vasta que una **LAN**, pero cubre un área geográfica más pequeña que una **WAN**.

MIME (Multipurpose Internet Mail Extensions): Extensiones de Internet Mail Multipropósito. Ver Capítulo 6.

MultiCast (MultiDifusión): Modo de difusión de información, que permite que ésta pueda ser recibida por múltiples nodos de la red y por lo tanto por múltiples usuarios. Véase también **BroadCast**.

n

Negación de Servicio: Ver **DoS**.

Newbie: Término aplicado por los **Hackers** a los novatos en el hacking. Ver Capítulo 5.

Newsgroup: Grupo de noticias. Es un servicio **Internet** que permite el envío y compartición de mensajes entre usuarios que tienen un interés común. Forma habitual de denominar el sistema de listas de correo. También se lo denomina **News**.

Nodo: Cualquier computadora o periférico conectado directamente a una red.

NetBeui (NetBIOS Extended User Interface): Protocolo de los niveles de transporte y red del modelo **ISO/OSI**, se integra con **NetBIOS** para ofrecer un sistema de comunicaciones eficiente en el entorno LAN de grupos de trabajo.

NetBIOS (Network BIOS): Protocolo del nivel de sesión, que establece y mantiene las sesiones de comunicación entre computadores.

Network (Red): Red de computadoras es un sistema de comunicación de datos. Conecta entre sí sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

Número IP: Número que identifica de manera única una máquina dentro de la red que utiliza el **Protocolo TCP**.

O

OSI: Open System Interconnection): Interconexión de sistemas abiertos. Programa de estandarización internacional creado por **ISO** e **ITU-T** para desarrollar normas para networking de datos que faciliten la interoperabilidad entre equipos de diversos fabricantes. Ver Capítulo 6.

p

Password (Clave): Ver **Clave**, **Contraseña**.

Patch (Parche): Modificación de un programa ejecutable para solucionar un problema, corregir un **Bug** o para cambiar su comportamiento.

Payload: Efecto visible de un software maligno.

PC (Personal Computer): Computadora Personal.

Perfil de Usuario: Información a la que el usuario necesita acceder para el desarrollo de sus tareas, criticidad de la información, funciones del puesto, etc.

PGP (Pretty Good Privacy): Privacidad Bastante Buena. Programa de encriptación de correo electrónico para Internet, que utiliza una combinación de claves públicas y privadas. Ver Capítulo 8.

Phreaker: Persona que usa los medios de comunicaciones sin pagarlos o pagando menos de lo que corresponde. Ver Capítulo 5.

Pirata Informático: Persona que copia software, con derecho de autor, ilegalmente sin que medie el permiso expreso del desarrollador. No confundir con el término **Hacker** o **Cracker**. Ver Capítulo 5.

PIN: Personal Identification Number. Número de Identificación Personal.

POP (Postal Office Protocol): Protocolo que brinda la posibilidad de que el correo electrónico sea depositado en “buzones” ubicados en algún tipo de sistema servidor de correo, y no directamente en una estación de trabajo. Ver Capítulo 6.

Port Scanner: Programa que indica los **Puertos** abiertos de un sistema.

PPP (Point to Point Protocol): Protocolo de comunicación serie que opera sobre líneas de enlace telefónico alquiladas (dedicadas) para proporcionar conexiones dentro de redes IP. Ver Capítulo 6.

PPTP (Point to Point Tunneling Protocol): Protocolo antecesor de **L2TP** fue diseñado para proporcionar comunicaciones autenticadas y cifradas entre un cliente y un **Gateway** o entre dos Gateways. Ver Capítulo 8.

Promiscuo (Modo): Normalmente interfaz **Ethernet** que permite leer toda la información sin importar su destino, aplicable a un segmento de **Red**. Ver Capítulo 5.

Protocolo: Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información). Ver Capítulo 6.

Proxy: Entidad que, a fin de lograr mayor eficiencia, esencialmente suple otra entidad.

Puerto: Proceso de capa superior que está recibiendo información de capas más bajas. Ver Capítulo 6.

r

RARP (Reverse Address Resolution Protocol): La función de este **Protocolo** complementa la función de **ARP**, pues permite mantener asignaciones de direcciones físicas a direcciones **Internet**.

Red: Conjunto de computadoras, impresoras, **Routers**, **Switches**, y otros dispositivos, que pueden comunicarse entre sí por algún medio de transmisión.

Redirigir: Cambiar el destino de algo. Por ejemplo, redirigir una llamada es hacer que suene en un teléfono distinto del que se intentaba llamar.

RFC (Request For Comment): Documentos especiales escritos y publicados por individuos comprometidos en el desarrollo y mantenimiento de Internet. Tienen el importante propósito de servir de documentación para nuevos desarrollos tecnológicos y ofrecer los estándares sobre los cuales se edificará la nueva tecnología.

Root: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo. Véase también **Administrador** y **SysOp**.

Rootkit: Software que permite a los intrusos depositar **Puertas Traseras**, **Caballos de Troya** y diversos mecanismos para asegurar su regreso al sistema atacado, y al mismo tiempo esconderse del resto de los usuarios del sistema, en particular del **Administrador**. Ver Capítulo 6.

Router: Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Los routers envían paquetes de una red a otra en base a la información de capa de red. Ocasionalmente llamado Gateway (aunque esta definición de gateway está cayendo en desuso). Ver capítulo 6.

S

SATAN (Security Administrator Tool for Analyzing Networks): Herramienta para el Análisis de Administradores de Seguridad de Redes. Aplicación realizada por el informático norteamericano Dan Farmer y el gurú americano-holandés Wietse Venema. Es capaz de establecer el nivel de vulnerabilidad de un **Host** y de todas las máquinas conectadas a él vía Internet (su dominio).

Server (Servidor): Máquina que ofrece servicios a otras dentro de una red. También llamado **Host**.

SET (Secure Electronic Transaction): Transacción Electrónica Segura. **Protocolo** creado y publicado por Visa y MasterCard con el fin de permitir la realización de transacciones electrónicas (compraventas fundamentalmente) a través de la red. Ver Capítulo 6.

Shell: Intérprete de comandos de un sistema operativo. Es el que se encarga de tomar las órdenes del usuario y hacer que el resto del **Sistema Operativo** las ejecute.

Shoulder Surfing: Espiar por detrás de un hombro para tratar de ver información interesante. Es un método comúnmente usado para acceder cuentas de otras personas.

Sistema Asimétrico de Cifrado: Sistema mediante el cual se emplea una doble **Clave** **kp (privada)** y **KP (Pública)**. Una de ellas es utilizada para **Cifrar** y la otra para descifrar. El emisor conoce una y el receptor la otra. Cada clave no puede obtenerse a partir de la otra.

Sistema Simétrico de Cifrado: Sistema mediante el cual se emplea la misma **Clave** para **Cifrar** y descifrar. El emisor y receptor deben conocerlas.

SLIP (Serial Line Internet Protocol): Es usado para transmitir paquetes IP a través de líneas de comunicación seriales. Ver Capítulo 6.

SMTP (Simple Mail Transfer Protocol): Protocolo que proporciona la capacidad de almacenamiento y reenvío del correo entre los host de los sistemas de correo de la red. Ver Capítulo 6.

Sniffer: Es un programa que permite “escuchar furtivamente” en redes de medios de comunicación compartidos (tales como **Ethernet**). Se ejecuta en una máquina que está conectada a la red, en modo **Promiscuo** y captura el tráfico de todo el segmento de red. Ver Capítulo 6.

SNMP (Simple Network Management Protocol): Protocolo que permite obtener información de gestión de los dispositivos conectados a la red. Ver Capítulo 6.

Socks: Protocolo que permite la conexión a equipos situados detrás un **Firewall**. Ver Capítulo 8.

Software: Programas de sistema, utilerías o aplicaciones expresadas en un lenguaje de maquina.

SOLARIS: Sistema Operativo de la empresa Sun. Es una implementación de **Unix**.

Spam: Correo electrónico que se recibe sin haberlo solicitado (llamados "e-mail basura"). Un envío masivo de Spam puede provocar un colapso en el sistema que los recibe, en este caso se les denomina MailBombing.

SSL (Secure Sockets Layers): Protocolo que provee una conexión segura entre dos hosts. Ver Capítulo 8.

SUN OS: Sistema Operativo de la empresa Sun. Es una implementación de **Unix**.

SysOp: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo. Véase también **Administrador** y **Root**.

Switch: Dispositivo que opera en la capa de enlace de datos del modelo **OSI**. Dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

TCP (Transmission Control Protocol): Este Protocolo de Control de Transmisión es un protocolo orientado a conexión. Su función principal es proporcionar mecanismos que ofrezcan seguridad en el proceso de entrega de los paquetes a su destino, así como ordenar paquetes de información y evitar la repetición de éstos. Ver Capítulo 6.

TCP/IP (Transfer Control Protocol/Internet Protocol): Arquitectura de red con un conjunto de protocolos que permiten compartir recursos a través de una red. Esta familia de protocolos es la más importante difundida en la actualidad, por ser la base de **Internet**. Ver Capítulo 6.

TELNET: Protocolo estándar utilizado para realizar un servicio de conexión desde una terminal remota. Ver Capítulo 6.

Terminal: Acceso a una computadora o sistema. Puede tratarse de un monitor y teclado o de una computadora completa.

TLS (Transport Layer Security): Protocolo que dio origen a **SSL**. Ver Capítulo 8.

Tracear: Seguir la “pista”, a través de la red mediante direcciones IP, de una persona o información.

Trashing: Arte de revolver la basura para encontrar información útil.

Troyano: Programa legítimo que ha sido alterado de alguna forma y que contiene funciones desconocidas por (y generalmente dañinas). Generalmente no contienen código reproductor. Véase también **Caballo de Troya**. Ver Capítulo 6.

U

UDP (User Datagram Protocol): El Protocolo de Datagramas de Usuario es un protocolo no orientado a conexión. Su desventaja principal es que no garantiza que los datagramas sean entregados en destino. Ver Capítulo 6.

UNIX: Sistema operativo utilizado por la gran mayoría de máquinas de Internet.

UPS (Uninterrupted Power Supply): Sistema de energía ininterrumpido.

UseNet: Red que contiene cientos de foros electrónicos de discusión (**Newsgroups**), las computadoras que procesan los protocolos y, finalmente, las personas que leen y envían las noticias.

Username (Usuario): Nombre único que identifica a un usuario, y es utilizado como medio de identificación ante un sistema.

V

Virus: Programa de actuar subrepticio para el usuario; cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas, puedan reproducirse y ser susceptibles de mutar; resultando de dicho

proceso la modificación, alteración y/o daño de los programas, información y/o hardware afectados. Ver Capítulo 7.

Vulnerabilidad: **Hardware**, firmware o **Software** que contiene **Bugs** que permiten su explotación potencial. Ver Capítulo 6.

W

WAN (Wide Area Network): Red de area extensa. Red de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Véase también LAN y MAN.

Warez: Programas comerciales ofrecidos por **Internet** “gratuitamente”. Ver **Piratería Informática**.

Web Sites (Sitio Web): Sistema dedicado al intercambio de información **On-Line**.

Worm: Ver **Gusano**.

Windows: Sistema Operativo gráfico de la empresa Microsoft.

WWW (World Wide Web): Gran red de servidores de Internet que brinda servicios de hipertexto y otros a las terminales que corren aplicaciones cliente como por ejemplo un explorador WWW.

X

X.25: Protocolo utilizado principalmente en WAN y, sobre todo, en las redes públicas de transmisión de datos. Funciona por conmutación de paquetes, esto es, que los bloques de datos contienen información del origen y destino de los mismos para que la red los pueda entregar correctamente aunque cada uno circule por un camino diferente.

Xploit: Ver **Exploit**.

Z

Zapper: Programa que se encarga de borrar los **Logs** que graban las entradas, acciones y salidas de usuarios.

✦ Consultar el “Glosario Básico Inglés-Español Para Usuarios de Internet”. Rafael Fernández Calvo[®] 1994-2001. <http://www.ati.es/novatica/glointv2.html>. rfoalvo@ati.es

✦ Consultar “Hacking Lexicon”. <http://www.robertgraham.com/pubs/hacking-dict.html>

TABLAS

- ✦ **Tabla 6.1:** Fuente: <http://www.isi.edu/in-notes/iana/assignments/port-numbers> según RFC 768, RFC 793 y RFC 1060.
- ✦ **Tabla 6.2:** Jerarquías más comunes en UseNet.
- ✦ **Tabla 7.1:** Porcentaje de Vulnerabilidades por tipo de sitio. Fuente: <http://www.trouble.org/survey>
- ✦ **Tabla 7.2:** Detalle de Ataques. Fuente: HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6-Página 71.
- ✦ **Tabla 7.3:** Vulnerabilidades Reportadas al CERT 1988-2001. Fuente: CERT Internacional. <http://www.cert.org/statistics>.
- ✦ **Tabla 7.4:** Cantidad de claves generadas según el número de caracteres empleado.
- ✦ **Tabla 9.1:** Tipo de Riesgo-Factor.
- ✦ **Tabla 9.2:** Valuación de Riesgos.

GRÁFICOS

- ✦ **Gráfico 1.1:** Amenazas para la Seguridad
- ✦ **Gráfico 1.2:** Tipos de Intrusos. Fuente: CybSec S.A. <http://www.cybsec.com>
- ✦ **Gráfico 2.3:** Tipos de Ataques Activos. Fuente: HOWARD, John D. Thesis: An Analysis of security on the Internet 1989-1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. <http://www.cert.org>. Capítulo 6-Página 59
- ✦ **Gráfico 1.4:** Relación Operatividad-Seguridad. Fuente: ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1º Edición. Argentina. 1997. Página 26
- ✦ **Gráfico 5.1:** Intrusiones. Fuente: <http://www.cybsec.com>
- ✦ **Gráfico 6.1:** Modelo OSI. Fuente: CISCO Networking Academies. Curriculum Online Versión 1.1
- ✦ **Gráfico 6.2:** Comparación Modelo OSI-TCP
- ✦ **Gráfico 6.3 – Constitución de un datagrama TCP**
- ✦ **Gráfico 6.4:** Conexión FTP
- ✦ **Gráfico 6.5:** Conexión HTTP
- ✦ **Gráfico 6.6:** Conexión SMTP
- ✦ **Gráfico 6.7:** Relación SMTP-POP
- ✦ **Gráfico 7.1:** Porcentaje de Ataques. Fuente: <http://www.disa.mil>
- ✦ **Gráfico 7.2:** Conexión en tres pasos.
- ✦ **Gráfico 7.3:** Ataque Spoofing
- ✦ **Gráfico 7.4:** Ataque Smurf
- ✦ **Gráfico 7.5:** Técnicas de Infección en Archivos Ejecutables
- ✦ **Gráfico 7.6:** Técnica de infección en Zona de Boot
- ✦ **Gráfico 7.7:** Infección de múltiples Documentos
- ✦ **Gráfico 7.8:** Módulos de los Virus Informáticos
- ✦ **Gráfico 7.9:** Modelo de un Antivirus
- ✦ **Gráfico 8.1:** Firewall
- ✦ **Gráfico 8.2:** Bastión Host
- ✦ **Gráfico 8.3:** Dual-Homed Host
- ✦ **Gráfico 8.4:** Screened Host
- ✦ **Gráfico 8.6:** Criptograma

- ✦ **Gráfico 8.7:** Proceso Encriptado-Firmado de SET
- ✦ **Gráfico 8.8:** Proceso de Kerberos
- ✦ **Gráfico 8.9:** Fuente: MONSERRAT COLL, Francisco Jesús. Seguridad en los protocolos TCP/IP. Página 30. <http://www.rediris.es/ftp>
- ✦ **Gráfico 9.1:** Punto de equilibrio Costo/Seguridad.
- ✦ **Gráfico 9.2:** Fuente: Manual de Seguridad en Redes. <http://www.arcert.gov.ar>

| | |
|---|-----------|
| CAPÍTULO 1 | 3 |
| INTRODUCCIÓN | 3 |
| 1.1 EVOLUCIÓN DEL TÉRMINO SEGURIDAD | 4 |
| 1.2 DE QUE ESTAMOS HABLANDO | 5 |
| 1.2.1 ANÁLISIS DEL OBJETIVO DE LA SEGURIDAD INFORMÁTICA | 7 |
| 1.2.2 SISTEMA DE SEGURIDAD | 10 |
| 1.2.3 DE QUIEN DEBEMOS PROTEGERNOS | 11 |
| 1.2.4 QUÉ DEBEMOS PROTEGER | 12 |
| 1.2.5 RELACIÓN OPERATIVIDAD–SEGURIDAD | 14 |
| CAPÍTULO 2 | 16 |
| SEGURIDAD FÍSICA..... | 16 |
| 2.1 TIPOS DE DESASTRES | 17 |
| 2.1.1 INCENDIOS | 17 |
| 2.1.1.1 Seguridad del Equipamiento..... | 18 |
| 2.1.1.2 Recomendaciones..... | 18 |
| 2.1.2 INUNDACIONES | 19 |
| 2.1.3 CONDICIONES CLIMATOLÓGICAS | 19 |
| 2.1.3.1 Terremotos..... | 19 |
| 2.1.4 SEÑALES DE RADAR | 20 |
| 2.1.5 INSTALACIÓN ELÉCTRICA | 20 |
| 2.1.5.1 Picos y Ruidos Electromagnéticos | 20 |
| 2.1.5.2 Cableado..... | 20 |
| 2.1.5.2.1 Cableado de Alto Nivel de Seguridad | 21 |
| 2.1.5.2.2 Pisos de Placas Extraíbles | 21 |
| 2.1.5.3 Sistema de Aire Acondicionado | 21 |
| 2.1.5.4 Emisiones Electromagnéticas | 21 |
| 2.1.6 ERGOMETRÍA | 22 |
| 2.1.6.1 Trastornos Óseos y/o Musculares..... | 22 |
| 2.1.6.2 Trastornos Visuales | 22 |
| 2.1.6.3 La Salud Mental | 23 |
| 2.1.6.4 Ambiente Luminoso | 23 |
| 2.1.6.5 Ambiente Climático | 24 |
| 2.2 ACCIONES HOSTILES | 24 |
| 2.2.1 ROBO..... | 24 |
| 2.2.2 FRAUDE | 24 |
| 2.2.3 SABOTAJE | 24 |
| 2.3 CONTROL DE ACCESOS..... | 25 |

| | |
|---|-----------|
| 2.3.1 UTILIZACIÓN DE GUARDIAS | 25 |
| 2.3.1.1 Control de Personas | 25 |
| 2.3.1.2 Control de Vehículos | 25 |
| 2.3.2 DESVENTAJAS DE LA UTILIZACIÓN DE GUARDIAS | 26 |
| 2.3.3 UTILIZACIÓN DE DETECTORES DE METALES | 26 |
| 2.3.4 UTILIZACIÓN DE SISTEMAS BIOMÉTRICOS | 26 |
| 2.3.4.1 Los Beneficios de una Tecnología Biométrica | 26 |
| 2.3.4.2 Emisión de Calor | 26 |
| 2.3.4.3 Huella Digital | 27 |
| 2.3.4.4 Verificación de Voz | 27 |
| 2.3.4.5 Verificación de Patrones Oculares | 27 |
| 2.3.5 VERIFICACIÓN AUTOMÁTICA DE FIRMAS (VAF) | 27 |
| 2.3.6 SEGURIDAD CON ANIMALES | 28 |
| 2.3.7 PROTECCIÓN ELECTRÓNICA | 28 |
| 2.3.7.1 Barreras Infrarrojas y de Micro-Ondas | 28 |
| 2.3.7.2 Detector Ultrasónico | 28 |
| 2.3.7.3 Detectores Pasivos Sin Alimentación | 29 |
| 2.3.7.4 Sonorización y Dispositivos Luminosos | 29 |
| 2.3.7.5 Circuitos Cerrados de Televisión | 29 |
| 2.3.7.6 Edificios Inteligentes | 29 |
| 2.4 CONCLUSIONES | 30 |
| CAPÍTULO 3 | 31 |
| SEGURIDAD LÓGICA | 31 |
| 3.1 CONTROLES DE ACCESO | 32 |
| 3.1.1 IDENTIFICACIÓN Y AUTENTIFICACIÓN | 32 |
| 3.1.2 ROLES | 34 |
| 3.1.3 TRANSACCIONES | 34 |
| 3.1.4 LIMITACIONES A LOS SERVICIOS | 34 |
| 3.1.5 MODALIDAD DE ACCESO | 35 |
| 3.1.5 UBICACIÓN Y HORARIO | 35 |
| 3.1.6 CONTROL DE ACCESO INTERNO | 35 |
| 3.1.6.1 Palabras Claves (Passwords) | 35 |
| 3.1.6.2 Encriptación | 36 |
| 3.1.6.3 Listas de Control de Accesos | 36 |
| 3.1.6.4 Límites sobre la Interfase de Usuario | 36 |
| 3.1.6.5 Etiquetas de Seguridad | 37 |
| 3.1.7 CONTROL DE ACCESO EXTERNO | 37 |
| 3.1.7.1 Dispositivos de Control de Puertos | 37 |

| | |
|---|-----------|
| 3.1.7.2 Firewalls o Puertas de Seguridad | 37 |
| 3.1.7.3 Acceso de Personal Contratado o Consultores | 37 |
| 3.1.7.4 Accesos Públicos | 37 |
| 3.1.8 ADMINISTRACIÓN | 37 |
| 3.1.8.1 Administración del Personal y Usuarios | 38 |
| 3.1.8.1.1 Organización del Personal | 38 |
| 3.2 NIVELES DE SEGURIDAD INFORMÁTICA | 39 |
| 3.2.1 NIVEL D | 39 |
| 3.2.2 NIVEL C1: PROTECCIÓN DISCRECIONAL | 39 |
| 3.2.3 NIVEL C2: PROTECCIÓN DE ACCESO CONTROLADO | 40 |
| 3.2.4 NIVEL B1: SEGURIDAD ETIQUETADA | 40 |
| 3.2.5 NIVEL B2: PROTECCIÓN ESTRUCTURADA | 41 |
| 3.2.6 NIVEL B3: DOMINIOS DE SEGURIDAD | 41 |
| 3.2.7 NIVEL A: PROTECCIÓN VERIFICADA | 41 |
| CAPÍTULO 4 | 42 |
| DELITOS INFORMATICOS | 43 |
| 4.1 LA INFORMACIÓN Y EL DELITO | 43 |
| 4.2 TIPOS DE DELITOS INFORMÁTICOS | 45 |
| 4.3 DELINCUENTE Y VICTIMA | 47 |
| 4.3.1 Sujeto Activo | 47 |
| 4.3.2 Sujeto Pasivo | 48 |
| 4.4 LEGISLACIÓN NACIONAL | 49 |
| 4.5 LEGISLACIÓN INTERNACIONAL | 53 |
| 4.5.1 Alemania | 53 |
| 4.5.2 Austria | 53 |
| 4.5.3 Chile | 54 |
| 4.5.4 China | 54 |
| 4.5.5 España | 54 |
| 4.5.6 Estado Unidos de América | 55 |
| 4.5.7 Francia | 56 |
| 4.5.8 Holanda | 56 |
| 4.5.9 Inglaterra | 57 |
| 4.6 CONCLUSIÓN | 57 |
| CAPÍTULO 5 | 59 |
| AMENAZAS HUMANAS | 59 |
| 5.1 PATAS DE PALO Y PARCHES | 60 |
| 5.1.1 CARTA DE PRESENTACIÓN | 60 |
| 5.1.2 LA ACTITUD DEL HACKER | 63 |

| | |
|---|-----------|
| 5.1.3 DEFINICIÓN DE HACKER | 64 |
| 5.1.4 LA CONEXIÓN HACKER – NERD | 66 |
| 5.1.5 CRACKERS | 66 |
| 5.1.6 PHREAKERS | 66 |
| 5.1.7 CARDING – TRASHING | 67 |
| 5.1.8 DESAFÍOS DE UN HACKER | 68 |
| 5.1.9 HABILIDADES BÁSICAS EN UN HACKER. | 68 |
| 5.1.10 ¿CÓMO LO HACEN? | 69 |
| 5.1.11 LA ÉTICA DEL HACKER | 69 |
| 5.1.12 MANIFIESTO HACKER | 70 |
| 5.1.13 OTROS HABITANTES DEL CIBERESPACIO | 71 |
| 5.1.13.1 Gurús | 71 |
| 5.1.13.2 Lamers o Script-Kidders | 71 |
| 5.1.13.3 CopyHackers | 71 |
| 5.1.13.4 Bucaneros | 71 |
| 5.1.13.5 Newbie | 71 |
| 5.1.13.6 Wannaber | 71 |
| 5.1.13.7 Samurai | 71 |
| 5.1.13.8 Piratas Informáticos | 72 |
| 5.1.13.9 Creadores de virus | 72 |
| 5.2 PERSONAL (INSIDERS) | 72 |
| 5.2.1 PERSONAL INTERNO | 73 |
| 5.2.2 EX-EMPLEADO | 74 |
| 5.2.3 CURIOSOS | 74 |
| 5.2.4 TERRORISTAS | 74 |
| 5.2.5 INTRUSOS REMUNERADOS | 74 |
| 5.2.6 RECOMENDACIONES | 74 |
| CAPÍTULO 6 | 76 |
| COMUNICACIONES | 76 |
| 6.1 OBJETIVOS DE LAS REDES | 77 |
| 6.1.1 ESTRUCTURAS | 77 |
| 6.1.1.1 Tecnologías de Transmisión | 78 |
| 6.1.1.2 Modelo Cliente/Servidor | 78 |
| 6.1.1.3 Tecnología de Objetos | 78 |
| 6.1.1.4 Sistemas Abiertos | 79 |
| 6.1.1.5 El Modelo OSI | 79 |
| 6.1.1.5.1 Transmisión de Datos en el Modelo OSI | 81 |
| 6.2 PROTOCOLOS DE RED | 82 |

| | | |
|-------------------------|---|------------|
| 6.2.1 | NETBIOS–NETBEUI–NWLINK–WINS | 82 |
| 6.2.2 | TCP/IP | 82 |
| 6.2.2.1 | Las capas del modelo TCP/IP | 83 |
| 6.2.2.2 | Funcionamiento | 84 |
| 6.2.2.3 | Comparación con el Modelo OSI | 84 |
| 6.2.3 | NIVEL FÍSICO DEL MODELO TCP/IP | 85 |
| 6.2.3.1 | ARP | 85 |
| 6.2.3.2 | RARP | 85 |
| 6.2.4 | NIVEL DE DATOS DEL MODELO TCP/IP | 85 |
| 6.2.4.1 | SLIP | 85 |
| 6.2.4.2 | PPP | 86 |
| 6.2.5 | NIVEL DE RED DEL MODELO TCP/IP | 86 |
| 6.2.5.1 | IPX–SPX | 86 |
| 6.2.5.2 | IP | 86 |
| 6.2.5.2.1 | DNS – Nombres de Dominio | 88 |
| 6.2.5.2.2 | Puertos | 88 |
| 6.2.5.3 | AppleTalk | 89 |
| 6.2.6 | NIVEL DE TRANSPORTE DEL MODELO TCP/IP | 89 |
| 6.2.6.1 | TCP | 89 |
| 6.2.6.2 | UDP | 92 |
| 6.2.7 | NIVEL DE APLICACIÓN DEL MODELO TCP/IP | 92 |
| 6.2.7.1 | ICMP | 92 |
| 6.2.7.2 | FTP | 92 |
| 6.2.7.3 | HTTP | 93 |
| 6.2.7.4 | SMTP | 94 |
| 6.2.7.5 | POP | 95 |
| 6.2.7.6 | MIME | 95 |
| 6.2.7.7 | NNTP | 96 |
| 6.2.7.8 | SNMP | 96 |
| 6.3 | ESTRUCTURA BÁSICA DE LA WEB..... | 96 |
| 6.3.1 | SERVICIOS DE INTERNET | 97 |
| 6.3.1.1 | TELNET | 97 |
| 6.3.1.2 | IRC | 97 |
| 6.3.1.3 | UseNet | 98 |
| 6.3.1.4 | Finger | 99 |
| 6.3.1.5 | WhoIs | 99 |
| CAPÍTULO 7 | | 101 |
| AMENAZAS LÓGICAS | | 101 |

| | |
|---|------------|
| 7.1 ACCESO – USO – AUTORIZACIÓN | 102 |
| 7.2 DETECCIÓN DE INTRUSOS..... | 102 |
| 7.3 IDENTIFICACIÓN DE LAS AMENAZAS | 103 |
| 7.4 TIPOS DE ATAQUE..... | 106 |
| 7.4.1 INGENIERA SOCIAL | 107 |
| 7.4.2 INGENIERÍA SOCIAL INVERSA | 107 |
| 7.4.3 TRASHING (CARTONEO)..... | 108 |
| 7.4.4 ATAQUES DE MONITORIZACIÓN | 108 |
| 7.4.4.1 <i>Shoulder Surfing</i> | 108 |
| 7.4.4.2 <i>Decoy (Señuelos)</i> | 109 |
| 7.4.4.3 <i>Scanning (Búsqueda)</i> | 109 |
| 7.4.4.3.1 TCP Connect Scanning | 109 |
| 7.4.4.3.2 TCP SYN Scanning..... | 110 |
| 7.4.4.3.3 TCP FIN Scanning– Stealth Port Scanning | 111 |
| 7.4.4.3.4 Fragmentation Scanning | 111 |
| 7.4.4.4 <i>Eavesdropping–Packet Sniffing</i> | 111 |
| 7.4.4.5 <i>Snooping–Downloading</i> | 112 |
| 7.4.5 ATAQUES DE AUTENTIFICACIÓN | 112 |
| 7.4.5.1 <i>Spoofing–Looping</i> | 113 |
| 7.4.5.2 <i>Spoofing</i> | 113 |
| 7.4.5.2.1 IP Spoofing | 113 |
| 7.4.5.2.2 DNS Spoofing | 114 |
| 7.4.5.3 <i>Web Spoofing</i> | 114 |
| 7.4.5.4 <i>IP Splicing–Hijacking</i> | 114 |
| 7.4.5.5 <i>Utilización de BackDoors</i> | 115 |
| 7.4.5.6 <i>Utilización de Exploits</i> | 116 |
| 7.4.5.7 <i>Obtención de Passwords</i> | 116 |
| 7.4.5.7.1 Uso de Diccionarios..... | 116 |
| 7.4.6 DENIAL OF SERVICE (DoS) | 117 |
| 7.4.6.1 <i>Jamming o Flooding</i> | 118 |
| 7.4.6.2 <i>Syn Flood</i> | 118 |
| 7.4.6.3 <i>Connection Flood</i> | 119 |
| 7.4.6.4 <i>Net Flood</i> | 119 |
| 7.4.6.5 <i>Land Attack</i> | 120 |
| 7.4.6.6 <i>Smurf o Broadcast Storm</i> | 120 |
| 7.4.6.7 <i>OOB, Supernuke o Winnuke</i> | 121 |
| 7.4.6.8 <i>Teardrop I y II–Newtear–Bonk–Boink</i> | 121 |
| 7.4.6.9 <i>E–Mail Bombing–Spamming</i> | 121 |

| | |
|---|------------|
| 7.4.7 ATAQUES DE MODIFICACIÓN-DAÑO | 122 |
| 7.4.7.1 <i>Tampering o Data Diddling</i> | 122 |
| 7.4.7.2 <i>Borrado de Huellas</i> | 122 |
| 7.4.7.3 <i>Ataques Mediante Java Applets</i> | 123 |
| 7.4.7.4 <i>Ataques con JavaScript y VBScript</i> | 123 |
| 7.4.7.5 <i>Ataques Mediante ActiveX</i> | 123 |
| 7.4.7.6 <i>Vulnerabilidades en los Navegadores</i> | 124 |
| 7.4.8 ERRORES DE DISEÑO, IMPLEMENTACIÓN Y OPERACIÓN | 125 |
| 7.4.9 IMPLEMENTACIÓN DE ESTAS TÉCNICAS | 125 |
| 7.4.10 ¿CÓMO DEFENDERSE DE ESTOS ATAQUES? | 126 |
| 7.5 CREACIÓN Y DIFUSIÓN DE VIRUS | 128 |
| 7.5.1 VIRUS INFORMÁTICOS VS VIRUS BIOLÓGICOS | 128 |
| 7.5.2 ORIGEN | 129 |
| 7.5.3 LOS NÚMEROS HABLAN | 131 |
| 7.5.4 DESCRIPCIÓN DE UN VIRUS | 132 |
| 7.5.4.1 <i>Técnicas de Propagación</i> | 132 |
| 7.5.4.2 <i>Tipos de Virus</i> | 133 |
| 7.5.4.2.1 Archivos Ejecutable (virus ExeVir) | 133 |
| 7.5.4.2.2 Virus en el Sector de Arranque (Virus ACSO) | 134 |
| 7.5.4.2.3 Virus Residente | 134 |
| 7.5.4.2.4 Macrovirus | 135 |
| 7.5.4.2.5 Virus de Mail | 135 |
| 7.5.4.2.6 Virus de Sabotaje | 136 |
| 7.5.4.2.7 Hoax, los Virus Fantasmas | 136 |
| 7.5.4.2.8 Virus de Applets Java y Controles ActiveX | 136 |
| 7.5.4.2.9 Reproductores-Gusanos | 136 |
| 7.5.4.2.10 Caballos de Troya | 136 |
| 7.5.4.2.11 Bombas Lógicas | 137 |
| 7.5.4.3 <i>Modelo de Virus Informático</i> | 137 |
| 7.5.5 TIPOS DE DAÑOS OCASIONADOS POR LOS VIRUS | 137 |
| 7.5.6 LOS AUTORES | 138 |
| 7.5.7 PROGRAMA ANTIVIRUS | 139 |
| 7.5.7.1 <i>Modelo de un Antivirus</i> | 140 |
| 7.5.7.2 <i>Utilización de los Antivirus</i> | 140 |
| 7.5.8 ASPECTOS JURÍDICOS SOBRE VIRUS INFORMÁTICOS | 141 |
| 7.5.9 CONSEJOS | 142 |
| CAPÍTULO 8 | 144 |
| PROTECCIÓN | 144 |

| | |
|--|------------|
| 8.1 VULNERAR PARA PROTEGER | 145 |
| 8.1.1 ADMINISTRACIÓN DE LA SEGURIDAD | 145 |
| 8.1.2 PENETRATION TEST, ETHICAL HACKING O PRUEBA DE VULNERABILIDAD | 147 |
| 8.1.3 HONEYPOTS–HONEYNETS | 148 |
| 8.2 FIREWALLS | 149 |
| 8.2.1 ROUTERS Y BRIDGES | 149 |
| 8.2.2 TIPOS DE FIREWALL | 150 |
| 8.2.2.1 Filtrado de Paquetes | 150 |
| 8.2.2.2 Proxy–Gateways de Aplicaciones | 151 |
| 8.2.2.3 Dual–Homed Host | 151 |
| 8.2.2.4 Screened Host | 152 |
| 8.2.2.5 Screened Subnet | 152 |
| 8.2.2.6 Inspección de Paquetes | 153 |
| 8.2.2.7 Firewalls Personales | 154 |
| 8.2.3 POLÍTICAS DE DISEÑO DE FIREWALLS | 154 |
| 8.2.4 RESTRICCIONES EN EL FIREWALL | 155 |
| 8.2.5 BENEFICIOS DE UN FIREWALL | 155 |
| 8.2.6 LIMITACIONES DE UN FIREWALL | 156 |
| 8.3 ACCESS CONTROL LISTS (ACL)..... | 156 |
| 8.4 WRAPPERS | 156 |
| 8.5 DETECCIÓN DE INTRUSOS EN TIEMPO REAL | 157 |
| 8.5.1 INTRUSIÓN DETECTION SYSTEMS (IDS) | 158 |
| 8.5.1.1 Características de IDS | 159 |
| 8.5.1.2 Fortalezas de IDS | 159 |
| 8.5.1.3 Debilidades de IDS | 160 |
| 8.5.1.4 Inconvenientes de IDS | 160 |
| 8.6 CALL BACK | 160 |
| 8.7 SISTEMAS ANTI–SNIFFERS | 161 |
| 8.8 GESTION DE CLAVES “SEGURAS” | 161 |
| 8.8.1 NORMAS DE ELECCIÓN DE CLAVES | 162 |
| 8.8.2 NORMAS PARA PROTEGER UNA CLAVE | 162 |
| 8.8.3 CONTRASEÑAS DE UN SÓLO USO | 163 |
| 8.9 SEGURIDAD EN PROTOCOLOS Y SERVICIOS..... | 164 |
| 8.9.1 NETBIOS | 164 |
| 8.9.2 ICMP | 164 |
| 8.9.3 FINGER | 164 |
| 8.9.4 POP | 165 |
| 8.9.5 NNTP | 165 |

| | |
|---|------------|
| 8.9.6 NTP | 166 |
| 8.9.7 TFTP | 166 |
| 8.9.8 FTP | 166 |
| 8.9.8.1 FTP Anónimo | 167 |
| 8.9.8.2 FTP Invitado | 167 |
| 8.9.9 TELNET | 167 |
| 8.9.10 SMTP | 168 |
| 8.9.11 SERVIDORES WWW | 168 |
| 8.10 CRIPTOLOGÍA | 170 |
| 8.10.1 HISTORIA | 170 |
| 8.10.2 CRIPTOGRAFÍA | 170 |
| 8.10.3 CRIPTOANÁLISIS | 171 |
| 8.10.4 CRIPTOSISTEMA | 171 |
| 8.10.4.1 Transposición | 172 |
| 8.10.4.2 Cifrados Monoalfabéticos | 173 |
| 8.10.4.2.1 Algoritmo de César | 173 |
| 8.10.4.2.2 Sustitución General | 173 |
| 8.10.5 ALGORITMOS SIMÉTRICOS MODERNOS (LLAVE PRIVADA) | 173 |
| 8.10.5.1 Redes de Feistel | 174 |
| 8.10.5.2 DES | 174 |
| 8.10.5.2.1 DES Múltiple | 174 |
| 8.10.5.3 IDEA | 175 |
| 8.10.5.4 BlowFish | 175 |
| 8.10.5.5 RC5 | 175 |
| 8.10.5.6 CAST | 175 |
| 8.10.5.7 Rijndael (el nuevo estándar AES) | 176 |
| 8.10.5.8 Criptoanálisis de Algoritmos Simétricos | 176 |
| 8.10.6 ALGORITMOS ASIMÉTRICOS (LLAVE PRIVADA-PÚBLICA) | 176 |
| 8.10.6.1 RSA | 177 |
| 8.10.6.1.1 Ataques a RSA | 177 |
| 8.10.6.2 Curvas Elípticas (CEE) | 178 |
| 8.10.7 AUTENTIFICACIÓN | 178 |
| 8.10.7.1 Firma Digital | 179 |
| 8.10.7.1.1 MD5 | 179 |
| 8.10.7.1.2 SHA-1 | 179 |
| 8.10.8 PGP (PRETTY GOOD PRIVACY) | 180 |
| 8.10.8.1 Funcionamiento de PGP | 180 |
| 8.10.8.1.1 Anillos de Claves | 180 |

| | |
|---|------------|
| 8.10.8.1.2 Codificación de Mensajes | 180 |
| 8.10.8.1.3 Decodificación de Mensajes | 180 |
| 8.10.8.1.4 Compresión de Archivos | 181 |
| 8.10.8.1.5 Algoritmos Utilizados por PGP | 181 |
| 8.10.9 ESTEGANOGRAFÍA | 181 |
| 8.11 COMERCIO ELECTRÓNICO | 181 |
| 8.11.1 DINERO ELECTRÓNICO | 182 |
| 8.11.1.1 <i>Certificados X.509</i> | 182 |
| 8.11.1.2 <i>SSL</i> | 183 |
| 8.11.1.2.1 Limitaciones y Problemas de SSL | 184 |
| 8.11.1.2.2 Ventajas de SSL | 185 |
| 8.11.1.3 <i>TLS</i> | 185 |
| 8.11.1.4 <i>SET</i> | 185 |
| 8.12 OTROS PROTOCOLOS DE SEGURIDAD | 187 |
| 8.12.1 SSH | 187 |
| 8.12.2 S/MIME | 188 |
| 8.12.3 SOCKS | 188 |
| 8.12.4 KERBEROS | 189 |
| 8.12.4.1 <i>Resumen de Kerberos</i> | 190 |
| 8.12.4.2 <i>Problemas de Kerberos</i> | 191 |
| 8.13 VPN-REDES PRIVADAS VIRTUALES | 192 |
| 8.13.1 REQUERIMIENTOS DE UNA VPN | 192 |
| 8.13.2 L2TP | 193 |
| 8.13.3 PPTP | 193 |
| 8.13.4 IPSEC | 193 |
| 8.14 INVERSIÓN | 195 |
| CAPÍTULO 9 | 196 |
| POLÍTICAS DE SEGURIDAD | 196 |
| 9.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA | 197 |
| 9.2 EVALUACIÓN DE RIESGOS | 199 |
| 9.2.1 NIVELES DE RIESGO | 200 |
| 9.2.2 IDENTIFICACIÓN DE AMENAZA | 201 |
| 9.2.3 EVALUACIÓN DE COSTOS | 202 |
| 9.2.3.1 <i>Valor Intrínseco</i> | 203 |
| 9.2.3.2 <i>Costos Derivados de la Perdida</i> | 203 |
| 9.2.3.3 <i>Punto de Equilibrio</i> | 204 |
| 9.3 ESTRATEGIA DE SEGURIDAD | 204 |
| 9.3.1 IMPLEMENTACIÓN | 205 |

| | |
|--|------------|
| 9.3.2 AUDITORÍA Y CONTROL | 208 |
| 9.3.3 PLAN DE CONTINGENCIA | 208 |
| 9.3.4 EQUIPOS DE RESPUESTA A INCIDENTES | 209 |
| 9.3.5 BACKUPS | 210 |
| 9.3.6 PRUEBAS | 211 |
| 9.4 LA POLÍTICA | 211 |
| 9.4.1 NIVEL FÍSICO | 211 |
| 9.4.1.1 Amenaza no Intencionada (Desastre Natural) | 212 |
| 9.4.2 NIVEL HUMANO | 212 |
| 9.4.2.1 El Usuario | 212 |
| 9.4.2.1.1 Amenaza no Intencionada (Empleado) | 213 |
| 9.4.2.1.2 Amenaza Malintencionada (Insider) | 214 |
| 9.4.1.2 Personas Ajenas al Sistema | 214 |
| 9.4.1.2.1 Amenaza No Intencionada | 214 |
| 9.4.1.2.2 Amenaza Malintencionada (Out-Sider) | 215 |
| CONCLUSIONES | 216 |
| AISLAMIENTO VS GLOBALIZACIÓN | 216 |
| DISEÑO SEGURO REQUERIDO | 217 |
| LEGISLACIÓN VIGENTE | 217 |
| TECNOLOGÍA EXISTENTE | 217 |
| DAÑOS MINIMIZABLES | 217 |
| RIESGOS MANEJABLES | 218 |
| COSTOS | 218 |
| PERSONAS INVOLUCRADAS | 218 |
| ANEXO I | 219 |
| LEYES ARGENTINAS VIGENTES | 219 |
| CÓDIGO CIVIL ARGENTINO | 251 |
| PROYECTOS DE LEY | 252 |
| ANEXO II | 270 |
| CRACKERS | 270 |
| HACKERS | 276 |
| ANEXO III | 278 |
| HERRAMIENTAS DE SEGURIDAD | 278 |
| GLOSARIO | 283 |