# C A P Í T U L O  I

## SEGURIDAD EN LA RED

## 1.1 INTRODUCCIÓN

En sus inicios, la red de Internet fue ideada como un medio de intercambio de información entre un grupo de científicos e investigadores que fue acogida con gran éxito. En esos momentos, nadie se preocupaba por la seguridad de la red ya que todas las personas eran de confianza. En la actualidad cuando millones de ciudadanos usan las redes para efectuar sus transacciones bancarias, compras, declaraciones de impuestos, envío de correo electrónico, intercambio de mensajes, etc., la seguridad de las mismas aparece en el horizonte como un problema potencial de grandes proporciones [LIB 001].

Internet es el medio de comunicación más usado y que beneficia a toda la sociedad, pero también esconde acciones delictivas como cualquier otro medio de comunicación. El intercambio seguro de información a través de una red abierta e insegura como Internet ha obligado a desarrollar numerosos sistemas de encriptación y autentificación de las transacciones, destinados a cubrir tres problemas fundamentales:

1. Conocer la identidad real de los clientes y servidores que se comunican, de forma que ambos dispongan de algún sistema para verificar la identidad del otro.
2. Garantizar que la transferencia de datos sólo pueda ser entendida por las aplicaciones que se comunican, utilizando métodos criptográficos para codificar todos los datos intercambiados, y evitar las 'escuchas' en la red.
3. Garantizar la integridad de los datos enviados, teniendo capacidad de detectar cualquier cambio, intencionado o no, en los mismos.

La información es uno de los activos más importantes de las entidades, y de modo especial en algunos sectores de actividad. Es indudable que cada día las entidades dependen en mayor medida de la información y de la tecnología. Por tal razón, se debe disponer de mecanismos sofisticados de seguridad que proporcionen confiabilidad y privacidad en el intercambio de mensajes, a la vez que eviten el repudio del contenido del mensaje por parte de los emisores y la alteración de los mensajes por parte de los receptores o cualquier otra persona maliciosa.

## 1.2 PROBLEMAS DE SEGURIDAD

La explotación comercial de Internet exige disponer de sistemas de comunicación seguros, capaces de adaptarse a las necesidades de los nuevos servicios, como la compra electrónica o la banca a distancia.

Con los sistemas de comunicación actualmente en uso, es técnicamente posible 'pinchar' un enlace de comunicaciones e interceptar el contenido de las comunicaciones TCP/IP que por él se transmiten. Cuando se envía información privada, por ejemplo, un número de tarjeta de crédito en un formulario de compra, es vital garantizar que la información sea recibida exclusivamente por su destinatario, y que la identidad es la esperada.

Es un hecho de todos conocido que Internet constituye un canal de comunicaciones inseguro, debido a que la información que circula a través de esta amplia red es fácilmente accesible en cualquier punto intermedio por un

posible atacante. Los datos transmitidos entre dos nodos de Internet[1], se segmentan en pequeños paquetes que son encaminados a través de un número variable de nodos intermedios hasta que alcanzan su destino. En cualquiera de ellos es posible leer el contenido de los paquetes, destruirlo e incluso modificarlo, posibilitando todo tipo de ataques contra la confidencialidad, disponibilidad, autenticidad y la integridad de sus datos. La *figura 1.1* muestra las cuatro categorías generales de agresión a la seguridad de las redes.

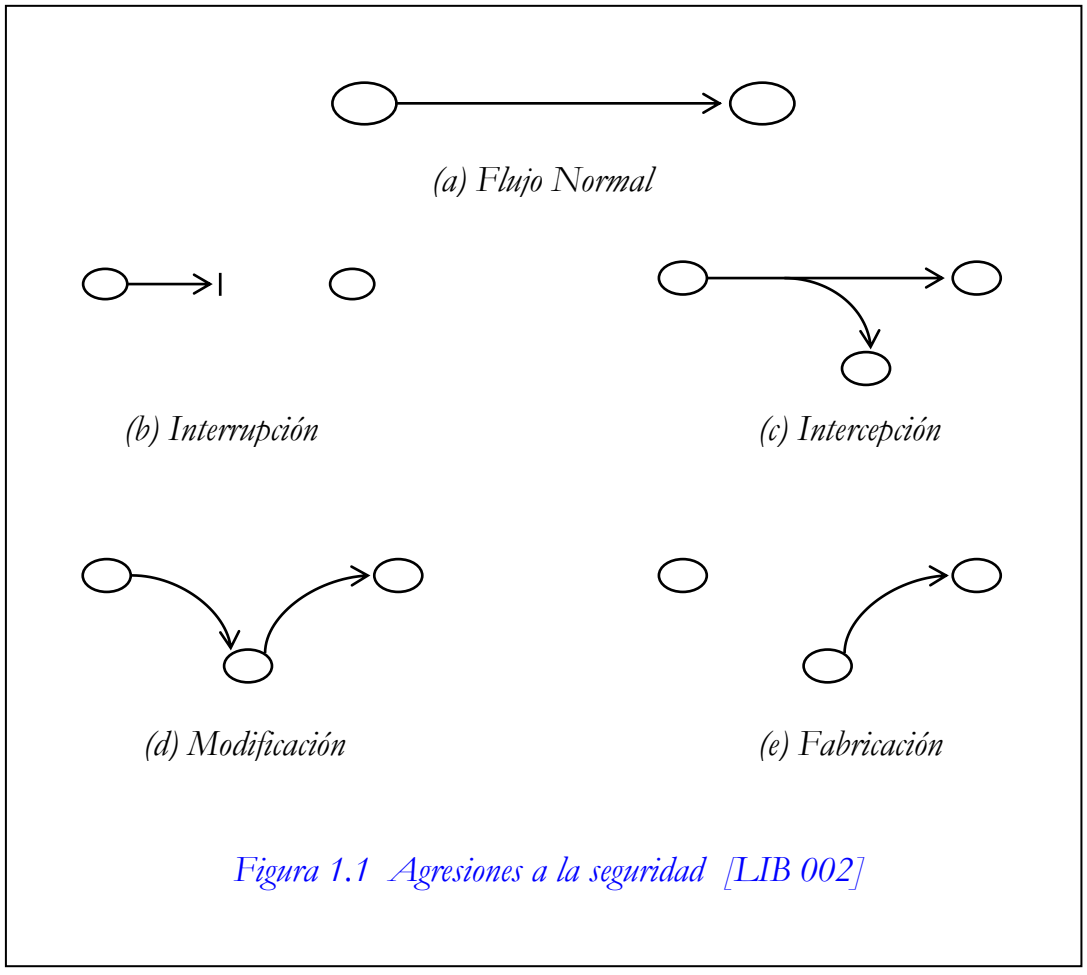


*Figura 1.1 Agresiones a la seguridad [LIB 002]*

- *Interrupción.-* Un recurso del sistema se destruye o no llega a estar disponible. Esta es una agresión activa a la disponibilidad.

[1] Por ejemplo su máquina y el servidor Web desde el que quiere descargar una página.

- *Intercepción.*- Un ente no autorizado consigue acceder a un recurso. Esta es una agresión pasiva a la confidencialidad.
- *Modificación.*- Un ente no autorizado no solamente gana acceso si no que deteriora el recurso. Esta es una agresión activa a la integridad.
- *Fabricación.*- Una parte no autorizada inserta objetos falsos en el sistema. Esta es una agresión activa a la autenticidad.

Además, es de sobra conocido que la mayor traba a la expansión del comercio electrónico a través de redes abiertas es la sensación de inseguridad que experimentan los consumidores y usuarios a la hora de transmitir datos confidenciales, en especial los números de sus cuentas bancarias o tarjetas de crédito.

## 1.3 NIVELES DE SEGURIDAD

La necesidad de evaluar la seguridad o de tener una medición confiable en el uso de las computadoras es uno de los objetivos principales del Departamento de Seguridad de los Estados Unidos y de las Industrias, por lo que crean y establecen los Criterios Estándares de Evaluación de Computadoras Confiables, conocido como el "Libro Naranja". Éste documento define cuatro niveles de seguridad para proteger de ataques de hardware, software y la información almacenada. Cada nivel se define con un grupo específico de criterios que un sistema debe cubrir, para ser certificado con la evaluación en alguna clase. Este criterio cae en 4 categorías generales: Políticas de seguridad, Responsabilidad, Confianza y Documentación.

Estos niveles de seguridad se refieren a diferentes tipos de seguridad física, autentificación de usuario, confiabilidad del software del sistema operativo y aplicaciones de usuario, y se muestran en la *figura 1.2*:

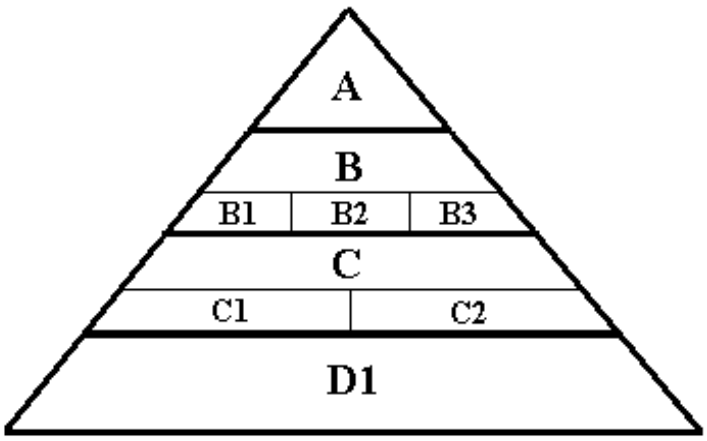


*Figura 1.2 Niveles de Seguridad*

**NIVEL D1.-**

El nivel D1 es la forma más baja de seguridad. Esta norma establece que el sistema operativo no es confiable. No se dispone de protección para el hardware; el sistema operativo se compromete fácilmente y no existe autentificación respecto a los usuarios y los derechos a tener acceso a la información almacenada en la computadora. Este nivel de seguridad por lo general se refiere a los sistemas operativos de escritorio tales como MS-DOS, MS Windows 95/98.

Estos sistemas operativos no distinguen entre los usuarios y no tienen definido ningún método para determinar quien está en el teclado. Así mismo, no tienen ningún control con respecto a la información a la que se pueda tener acceso a las unidades de disco de la computadora.

**NIVEL C.-**

El nivel ***C*** tiene dos subdivisiones de seguridad: el ***C1*** y el ***C2***.

**El Subnivel C1**.- El sistema de Protección de Seguridad Discrecional, se refiere a la seguridad disponible en el sistema Unix típico. Existe cierto nivel de protección para el hardware, ya que este no puede comprometerse fácilmente, aunque es posible. Los usuarios deben de identificarse ante el sistema mediante su login y contraseña. Se emplea esta combinación para determinar los derechos de acceso a programas e información que tiene cada usuario. Estos derechos de acceso son los permisos de archivos y directorios.

Los controles de acceso discrecional permiten al dueño del archivo o directorio, así como al administrador del sistema, evitar que ciertas personas o grupos tengan acceso a dichos programas o información. Sin embargo, no se impide que la cuenta del administrador del sistema realice ninguna actividad. En consecuencia, un administrador poco escrupuloso puede comprometer fácilmente la seguridad del sistema sin que nadie lo sepa.

**El Subnivel C2.-** Está diseñado para ayudar a resolver los problemas anteriores. Además de las funciones del subnivel ***C1***, el subnivel ***C2*** cuenta con características adicionales que crean un ambiente de acceso controlado. Este ambiente tiene la capacidad de restringir aun más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, con base no solo en los permisos[2], sino también en los niveles de autorización. Además este nivel de seguridad requiere que se audite al sistema, lo cual implica registrar los eventos que ocurran en el sistema.

[2] Son reglas que regulan que usuarios pueden utilizar los recursos (archivos, carpetas, impresoras, etc.).

La auditoría se utiliza para llevar registros de todas las acciones relacionadas con la seguridad, como pueden ser las actividades efectuadas por el administrador del sistema. Microsoft Windows NT Server 4.0 ha conseguido la Certificación C2.

**NIVEL B.-**

El nivel de seguridad ***B*** consta de tres subniveles, el ***B1***, ***B2*** y el ***B3***.

**El Subnivel B1**, llamado Protección de Seguridad Etiquetada, requiere todas las características solicitadas para el nivel C2. Además de la seguridad obligatoria y acceso por Etiquetas[3] a todos los objetos (archivos, procesos, dispositivos, etc.), Verificación de la Integridad de las etiquetas, Auditoría de objetos Etiquetados.

**El Subnivel B2**, conocido como Protección Estructurada, los sistemas deben estar basados en una documentación formal y contar con un modelo de política de seguridad bien definido que requiera un control de acceso discrecional y obligatorio. Las imposiciones a los sistemas encontradas en la clase B1, se deben extender a todos los eventos y objetos en el sistema. Además posee Etiquetas de dispositivos jerárquicas y Comprobación de la seguridad. Un ejemplo de estos sistemas operativos es el Honeywell Multics.

**El Subnivel B3**, llamado de Dominios de Seguridad, debe satisfacer los requisitos de herramientas de monitoreo que interviene en todos los accesos de usuarios a los objetos, a fin de ser comprobada, y que sea lo bastante minuciosa para ser sujeta al análisis y pruebas. Debe de contar también con un Administrador de Seguridad, los mecanismos de auditoría se amplían para

[3] Son identificadores que se les asignan a los usuarios o a los objetos dentro del sistema, se utilizan para verificar los permisos que tiene el usuario o el objeto para permitir o denegar las acciones.

señalar acontecimientos relevantes de la seguridad, y se necesitan procedimientos de recuperación del sistema. El sistema es altamente resistente a la penetración no autorizada.

**NIVEL A.-**

El nivel ***A***, conocido como Diseño Verificado, constituye actualmente el nivel de seguridad válido más alto en todo el Libro Naranja. Cuenta con un proceso estricto de diseño, control y verificación. Para alcanzar el nivel de seguridad, deben incluirse todos los componentes de los niveles inferiores; el diseño debe verificarse matemáticamente, debe realizarse un análisis de los canales cubiertos y de distribución confiable. La distribución confiable significa que el hardware y el software hayan estado protegidos durante su traslado para evitar violaciones de los sistemas de seguridad.

## 1.4 POLÍTICAS DE SEGURIDAD

Una vez identificados los problemas generales de seguridad, llega la pregunta que supone el principal escollo para desarrollar un plan que corrija la situación: ¿cómo se debe abordar la seguridad en la organización?
El Plan de Seguridad debe ser un proyecto que desarrolle los objetivos de seguridad a largo plazo de la organización, siguiendo el ciclo de vida completo desde la definición hasta la implementación y revisión.

La forma adecuada para plantear la planificación de la seguridad en una organización debe partir siempre de la definición de una política de seguridad que defina el QUÉ se quiere hacer en materia de seguridad en la organización

para a partir de ella, decidir mediante un adecuado plan de implementación el CÓMO se alcanzarán en la práctica los objetivos fijados.

La Política de Seguridad englobará pues los objetivos, conductas, normas y métodos de actuación y distribución de responsabilidades y actuará como documento de requisitos para la implementación de los mecanismos de seguridad. La política debe contemplar al menos la definición de funciones de seguridad, la realización de un análisis de riesgos, la definición de normativas y procedimientos, la definición de planes de contingencia ante desastres y la definición del plan de auditoría. A partir de la Política de Seguridad se podrá definir el Plan de Implementación, que es muy dependiente de las decisiones tomadas en ella, en el que se contemplará: el estudio de soluciones, la selección de herramientas, la asignación de recursos y el estudio de viabilidad.

Hay dos cuestiones fundamentales que deberán tenerse en cuenta para implantar con éxito una política de seguridad: Es necesario que la política sea aprobada para que esté respaldada por la autoridad necesaria que asegure su cumplimiento y la asignación de recursos; y es necesario que se realicen revisiones periódicas que la mantengan siempre actualizada y acorde con la situación real del entorno. Un enfoque como el propuesto asegurará la adecuación del nivel de seguridad implantado con las necesidades de la organización y el correcto seguimiento y control de los riesgos.

## 1.5 INTRUSOS EN LA RED

El tráfico de información que fluye en las redes de telecomunicaciones normalmente se envía sin protección[4] y dadas las características de redes como Internet o comunicación basada en redes públicas como la telefónica, es factible que la información sea interceptada por intrusos. El monitoreo ilegal o "Sniffing" es una de las formas de ataque pasivo más comunes. La verdad es que es difícil decir cada cuanto tiempo se comete un fraude en Internet, pero lo importante es que las operaciones fraudulentas son técnicamente posibles y existen.

Internet es el medio de comunicación más usado actualmente y beneficia a toda la sociedad, pero también esconde acciones delictivas como cualquier otro medio de comunicación. Dado que la información que va por la Red pasa realmente por muchas computadoras durante todo su transcurso, existe la posibilidad de que alguien robe la información confidencial. Este alguien puede ser un hacker[5], cracker[6], phreaker[7] ó un ex-empleado de una entidad, que buscan simplemente divertirse o causar serios daños, que incluso pueden llevar a la quiebra más grande a instituciones muy sólidas. Cabe mencionar que estas personas son verdaderos expertos en el tema y a veces están muy bien remunerados.

Según estudios realizados, aproximadamente el 70% de los ataques a los sistemas informáticos y telemáticos son efectuados por los propios usuarios internos de la organización.

[4] Información legible.
[5] Persona con sólidos conocimientos informáticos que rompe la seguridad de un sistema por interés, diversión, satisfacción personal o por incrementar sus conocimientos y habilidades.
[6] Persona con sólidos conocimientos informáticos que rompe la seguridad de un sistema con la finalidad de obtener algún beneficio.
[7] Pirata telefónico.

## 1.6 ASPECTOS SOCIALES

Desde mediados de los noventa, la Internet ha pasado de ser un medio de comunicación académico a ser el medio natural de intercambio de información para una gran parte de los sectores productivos. Este hecho ha provocado un crecimiento espectacular del comercio de bienes en soporte electrónico. Con el avance de estas nuevas tecnologías, la informática se ha convertido en un instrumento que nos proporciona infinitas posibilidades de desarrollo y progreso. Sin embargo, se ha dado lugar a una nueva forma de delincuencia, la delincuencia informática.

Las implicaciones de la seguridad de las redes para la confidencialidad individual y social en general son abrumadoras. Los delitos cometidos utilizando la computadora han crecido en tamaño, forma y variedad. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

Entre los hechos delictivos ocurridos más sobresalientes tenemos [WWW 013]:

- El caso de la NASA, donde dos alemanes ingresaron en sus archivos confidenciales.
- Un joven estudiante de 15 años que ingresando a los computadores de la Universidad de Berkeley en California destruyo gran cantidad de archivos.
- Muchos host de Internet han sido dados de baja por el "ping de la muerte", una versión trampa del comando ping[8]. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reseteo o el apagado instantáneo del equipo.

[8] Aplicación de la administración de redes, que permite comprobar si otra computadora está activa y funcionando. Envía un mensaje corto, al cual la otra computadora responde automáticamente. [LIB 003]

- Debemos también mencionar lo sucedido a mediados de febrero del 2000 cuando varios sitios importantes dentro de la Internet (Yahoo, Zdnet, Amazon.com, Buy.com, eBay, CNN.com, E-trade y Datek) fueron bloqueados por horas en los Estados Unidos, por medio de sabotajes informáticos, produciendo grandes perdidas a los proveedores de Internet.
- Estafas a entidades bancarias, que por motivos de Ranking no son denunciadas y publicadas.

En conclusión, el peligro que aqueja a la seguridad de las redes es un hecho y seguirá siéndolo por mucho tiempo mientras exista personas ingeniosas y escrupulosas capaces de inmiscuirse en los sistemas de información privados. Mientras tanto debemos tomar las medidas de seguridad necesarias y sencillamente aprender a sobrevivir con ellos.