Capítulo 1.

Seguridad Informática: Conceptos básicos.

1.1. ¿Qué es “network security” o la seguridad en la red (servicios digitales en Internet)?

Definimos la seguridad de información como la protección de ventajas de información de la revelación no autorizada, de la modificación, o de la destrucción, o accidental o intencional, o la incapacidad para procesar esa información. La seguridad de la red, se compone de esas medidas tomadas para proteger una red del acceso no autorizado, interferencia accidental o intencionada con operaciones normales, o con la destrucción, inclusive la protección de facilidades físicas, del software, y de la seguridad del personal.

La seguridad en el Web es un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios del Web y las organizaciones que los rodean. La Seguridad es una protección contra el comportamiento inesperado **[Garfinkel, 1999].**

1.1.1. ¿Por qué requiere atención especial la seguridad en el Web?

- Internet es una red de dos sentidos. Así como hace posible que los servidores Web divulguen información a millones de usuarios, permite a los hackers, crackers, criminales y otros “chicos malos” irrumpir en las mismas computadoras donde se ejecutan los servidores Web.
- Las empresas, instituciones y los gobiernos utilizan cada vez más el Word Wide Web para distribuir información importante y realizar transacciones comerciales. Al violar servidores Web se pueden dañar reputaciones y perder dinero.
- Aunque el Web es fácil de utilizar, los servidores son piezas de software extremadamente complicadas y tienen diversas fallas de seguridad potenciales.
- Es mucho más onerosa y tardada la recuperación de un incidente de seguridad que implementar medidas preventivas.

1.1.2. ¿Por qué preocuparse sobre la seguridad en el Web?

Los servidores son un blanco atractivo para los trangesores por varias razones **[Garfinkel, 1999]:**

Publicidad. Los servidores web son la cara que las organizaciones presentan al público y al mundo electrónico. Un ataque exitoso a alguno de ellos es acto público que puede ser visto en unas horas por cientos de miles de personas. Los ataques pueden lanzarse por razones ideológicas o financieras, o ser simples actos vandálicos cometidos al azar.

Comercio. Muchos servidores web estan ralacionados con el comercio y el dinero. De hecho los protocolos criptográficos integrados a Navigator de Netscape y otros navegadores fueron originalmete incluidos para permitir a los usuarios enviar números de tarjetas de crédito por Internet sin preocuparse de que fueran interceptados. De esta forma, los servidores web se han convertido en repositorios de información financiera confidencial, lo cual los convierte en un blanco atractivo para los atacantes.

Información confidencial. Para las organizaciones, la tecnología del Web se ha convertido en una forma de distribuir información con gran sencillez, tanto internamente, a sus propios miembros, como de manera externa, a sus socios en todo el mundo. Esta información confidencial es un blanco atractivo para sus competidores y enemigos.

Acceso a las redes. Al ser utilizados por personas tanto dentro como fuera de las organizaciones, los servidores web sirven efectivamente como puente entre la red interna de la organización y las redes externas. Su posición privilegiada en cuanto a las conexiones de red los convierte en un blanco ideal para ser atacados, ya que un servidor web violado puede emplearse como base para atacar desde ahí a las computadoras de una organización.

Extensibilidad de los servidores. Debido a su naturaleza, los servidores estan diseñados para ser extensibles, lo cual hace posible conectarlos con bases de datos, sistemas heredados y otros programas que se ejecutan en la red de una organización. Si no se implementan de modo adecuado, los módulos que se agregan a un servidor pueden comprometer la seguridad de todo el sistema.

Interrupción del servicio. Como la tecnología del Web se basa en la familia de protocolos TCP/IP, está sujeta a interrupciones del servicio: ya sea accidental o intencionamente por medio de ataques de negación del servicio. Las personas que utilizan dicha tecnologías den estar enteradas de sus fallas y prepararse para interrupciones importantes del servicio.

Soporte complicado. Los navegadores necesitan servicios internos, como DNS (Servicio de nombres de Dominio, Domain Name Service) y el enrutamiento del protocolo IP (Protocolo Interne, Internet Protocol) para funcionar bien. La robustez y confiabilidad de tales servicios pueden ser desconocidas y vulnerables a errores de programación, accidentes y subversión, la subversión de un servicio de mas bajo nivel puede causar problemas también a los navegadores.

1.2. Objetivos de la Seguridad.

Seguridad informática es el conjunto de procedimientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información de una entidad.

Integridad. Es necesario asegurar que los datos no sufran cambios no autorizados, la pérdidad de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques. El sistema contiene información que debe se protegida de modificaciones imprevistas, no autorizas o accidentales, como información de censo o sistemas de transacciones financieras.

Disponibilidad. Se refiere a la continuidad operativa de la entidad, la pérdidad de disponibilidad puede implicar, la pérdida de productividad o de cridibilidad de la entidad. El sistema contiene información o proporciona servicios que deben estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes, como sistemas esenciales de seguridad y protección de la vida.

Confidencialidad. Se refiere a la protección de datos frente a la difusión no autorizada, la pérdida de confidencialidad puede rsultar en problemas legales, pérdida del negocio o de credibilidad. El sistema contiene información que necesita protección contra la divulgación no autorizada, como información parcial de informes, información personal o información comercial patentada

Estos aspectos además de lidiar con el riesgo que representan los atacantes remotos, se ven amenazados también por los riesgos por desastres naturales, empleados desleales, virus y sabotaje, entre otros.

1.3. Estrategias de Seguridad.

La metodología de seguridad está diseñada para ayudar a los profesionales de la seguridad a desarrollar una estrategia para proteger la *disponibilidad, integridad y confidencialidad* de los datos de los sistemas informáticos (IT) de las organizaciones. Es de interés para los administradores de recursos de información, los directores de seguridad informática y los administradores, y tiene un valor especial para todos aquellos que intentan establecer directivas de seguridad.

La metodología ofrece un acercamiento sistemático a esta importante tarea y, como precaución final, también implica el establecimiento de planes de contingencia en caso de desastre.

Los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados.

Cada organización debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación. Cada sistema informático, entorno y directiva organizativa es distinta, lo que hace que cada servicio y cada estrategia de seguridad sean únicos. Sin embargo, los fundamentos de una buena seguridad siguen siendo los mismos y este proyecto se centra en dichos principios **[Benson, 2001].**

a) Identificar métodos, herramientas y técnicas de ataques probables.

Las listas de amenazas, de las que disponen la mayor de las organizaciones, ayudan a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar en los ataques. Los métodos pueden abarcar desde virus y gusanos a la adivinación de contraseñas y la interceptación del correo electrónico. 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.

b) Establecer estrategias proactivas y reactivas.

En cada método, el plan de seguridad debe incluir una estrategia *proactiva* y otra *reactiva*. La estrategia *proactiva* o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar la estrategia proactiva.

La estrategia *reactiva* o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

c) Pruebas.

El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y proactiva. La realización de ataques simulados en sistemas de pruebas o en laboratorios permite 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.

d) Equipos de respuestas a incidentes.

Es aconsejable formar un equipo de respuesta a incidentes. Este equipo debe estar implicado en los trabajos proactivos del profesional de la seguridad. Entre éstos se incluyen:

- El desarrollo de instrucciones para controlar incidentes.
- La identificación de las herramientas de software para responder a incidentes y eventos.
- La investigación y desarrollo de otras herramientas de seguridad informática.
- La realización de actividades formativas y de motivación.
- La realización de investigaciones acerca de virus.
- La ejecución de estudios relativos a ataques al sistema.

Estos trabajos proporcionarán los conocimientos que la organización puede utilizar y la información que hay que distribuir antes y durante los incidentes. Una vez que el administrador de seguridad y el equipo de respuesta a incidentes han realizado estas funciones proactivas, el administrador debe delegar la responsabilidad del control de incidentes al equipo de respuesta a incidentes.

Esto no significa que el administrador no deba seguir implicado o formar parte del equipo, sino que no tenga que estar siempre disponible, necesariamente, y que el equipo debe ser capaz de controlar los incidentes por sí mismo. El equipo será el responsable de responder a incidentes como virus, gusanos o cualquier otro código dañino, invasión, engaños, desastres naturales y ataques del personal interno. El equipo también debe participar en el análisis de cualquier evento inusual que pueda estar implicado en la seguridad de los equipos o de la red.

1.3.1. Metodología para la definición de una estrategia de seguridad [Benson, 2001].

La figura 1.1 explica una metodología para definir una estrategia de seguridad informática que se puede utilizar para implementar directivas y controles de seguridad con el objeto de aminorar los posibles ataques y amenazas. Los métodos se pueden utilizar en todos los tipos de ataques a sistemas, independientemente de que sean intencionados, no intencionados o desastres naturales, y, por consiguiente, se puedan volver a utilizar en distintos casos de ataque.

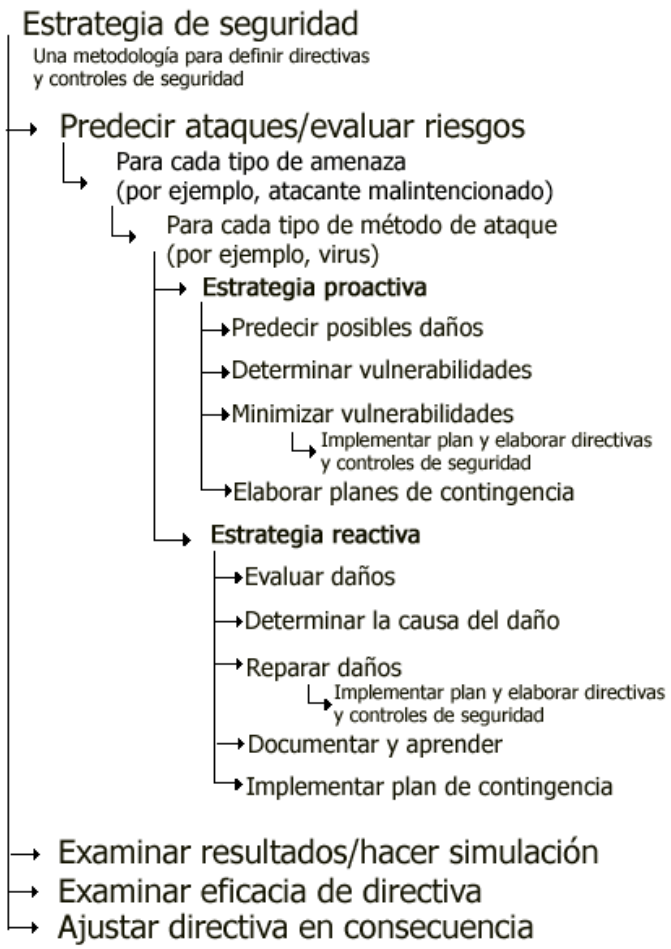

Figura 1.1 Metodología de estrategias de seguridad **[Miguel, 1998].**

a) Predecir posibles ataques y analizar riesgos.

La primera fase de la metodología esquematizada en la figura 1.1, es determinar los ataques que se pueden esperar y las formas de defenderse contra ellos. Es imposible estar preparado contra todos los ataques; por lo tanto, hay que prepararse para los que tiene más probabilidad de sufrir la organización. Siempre es mejor prevenir o aminorar los ataques que reparar el daño que han causado.

Para mitigar los ataques es necesario conocer las distintas amenazas que ponen en peligro los sistemas, las técnicas correspondientes que se pueden utilizar para comprometer los controles de seguridad y los puntos vulnerables que existen en las

directivas de seguridad. El conocimiento de estos tres elementos de los ataques ayuda a predecir su aparición e, incluso, su duración o ubicación. La predicción de los ataques trata de pronosticar su probabilidad, lo que depende del conocimiento de sus distintos aspectos. Los diferentes aspectos de un ataque se pueden mostrar en la siguiente ecuación:

Amenazas + Motivos + Herramientas y técnicas + Puntos vulnerables = Ataque

b) Para cada tipo de amenaza,

Considere todas las amenazas posibles que causan ataques en los sistemas. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales. La siguiente figura clasifica las distintas amenazas a los sistemas:

Figura 1.2. Amenazas para la Seguridad **[Martín, 2004].**

Amenazas como empleados ignorantes o descuidados, y los desastres naturales no implican motivos u objetivos; por lo tanto, no se utilizan métodos, herramientas o técnicas predeterminadas para iniciar los ataques. Casi todos estos ataques o infiltraciones en la seguridad se generan internamente; raras veces los va a iniciar alguien ajeno a la organización.

Para estos tipos de amenazas, el personal de seguridad necesita implementar estrategias proactivas o reactivas siguiendo las instrucciones de la figura 1.1.

c) Para cada tipo de método de ataque.

Para iniciar un ataque, se necesita un método, una herramienta o una técnica para explotar los distintos puntos vulnerables de los sistemas, de las directivas de seguridad y de los controles. Los agresores pueden utilizar varios métodos para iniciar el mismo ataque. Por lo tanto, la estrategia defensiva debe personalizarse para cada tipo de método utilizado en cada tipo de amenaza.

De nuevo, es importante que los profesionales de la seguridad estén al día en los diferentes métodos, herramientas y técnicas que utilizan los agresores. La siguiente es una lista breve de esta técnica:

- Ataques de denegación de servicio.
- Ataques de invasión.
- Ingeniería social.
- Virus.
- Gusanos.
- Caballos de Troya.
- Modificación de paquetes.
- Adivinación de contraseñas.
- Interceptación de correo electrónico.

d) Estrategia proactiva.

La estrategia proactiva es un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran. Entre estos pasos se incluye observar cómo podría afectar o dañar el sistema, y los puntos vulnerables. Los conocimientos adquiridos en estas evaluaciones pueden ayudar a implementar las directivas de seguridad que controlarán o aminorarán los ataques.

Éstos son los tres pasos de la estrategia proactiva:

- Determinar el daño que causará el ataque.
- Establecer los puntos vulnerables y las debilidades que explotará el ataque.
- Reducir los puntos vulnerables y las debilidades que se ha determinado en el sistema para ese tipo de ataque específico.

El seguimiento de estos pasos para analizar los distintos tipos de ataques tiene una ventaja adicional: comenzará a emerger un modelo, ya que en los diferentes factores se superponen para diferentes ataques. Este modelo puede ser útil al determinar las áreas de vulnerabilidad que plantean el mayor riesgo para la empresa. También es necesario tomar nota del costo que supone la pérdida de los datos frente al de la implementación de controles de seguridad. La ponderación de los riesgos y los costos forma parte de un análisis de riesgos del sistema que se explica en el documento técnico acerca del diseño de la seguridad.

Las directivas y controles de seguridad no serán, en ningún caso, totalmente eficaces al eliminar los ataques. Éste es el motivo por el que es necesario desarrollar planes de recuperación y de contingencia en caso de que se quebranten los controles de seguridad.

e) Determinar el daño posible que puede causar un ataque.

Los daños posibles pueden oscilar entre pequeños fallos del equipo y la pérdida, catastrófica, de los datos. El daño causado al sistema dependerá del tipo de ataque. Si es posible, utilice un entorno de prueba o de laboratorio para clarificar los daños que provocan los diferentes tipos de ataques. Ello permitirá al personal de seguridad ver el daño físico que causan los ataques experimentales. No todos los ataques causan el mismo daño.

f) Determinar los puntos vulnerables o las debilidades que pueden explotar los ataques

Si se pueden descubrir los puntos vulnerables que explota un ataque específico, se pueden modificar las directivas y los controles de seguridad actuales o implementar otras nuevas para reducir estos puntos vulnerables. La determinación del tipo de ataque, amenaza y método facilita el descubrimiento de los puntos vulnerables existentes. Esto se puede reconocer por medio de una prueba real. Se deben determinar los puntos vulnerables o debilidades en las áreas de seguridad física, de datos y de red.

g) Reducir los puntos vulnerables y debilidades que puede explotar un posible ataque.

La reducción de los puntos vulnerables y las debilidades del sistema de seguridad que se determinaron en la evaluación anterior es el primer paso para desarrollar directivas y controles de seguridad eficaces. Ésta es la compensación de la estrategia proactiva. Mediante la reducción de los puntos vulnerables, el personal de seguridad puede hacer disminuir tanto la probabilidad de un ataque como su eficacia, si se produce alguno. Tenga cuidado de no implementar controles demasiado estrictos, ya que la disponibilidad de la información se convertiría en un problema. Debe haber un cuidado equilibrio entre los controles de seguridad y el acceso a la información. Los usuarios deben tener la mayor libertad posible para tener acceso a la información.

h) Elaborar planes de contingencia.

Un plan de contingencia es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. El plan se sigue si el sistema no se puede restaurar a tiempo. Su objetivo final es mantener la disponibilidad, integridad y confidencialidad de los datos (es el proverbial "Plan B").

Debe haber un plan para cada tipo de ataque y tipo de amenaza. Cada plan consta de un conjunto de pasos que se han de emprender en el caso de que un ataque logre pasar las directivas de seguridad.

i) Estrategia reactiva.

La estrategia reactiva se implementa cuando ha fallado la estrategia proactiva y define los pasos que deben adoptarse después o durante un ataque. Ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar por qué tuvo lugar, a reparar el daño que causó y a implementar un plan de contingencia, si existe. Tanto la estrategia reactiva como la proactiva funcionan conjuntamente para desarrollar directivas y controles de seguridad con el fin de reducir los ataques y el daño que causan. El equipo de respuesta a incidentes debe incluirse en los pasos adoptados durante o después del ataque para ayudar a evaluarlo, a documentar el evento y a aprender de él.

j) Evaluar el daño.

Determine el daño causado durante el ataque. Esto debe hacerse lo antes posible para que puedan comenzar las operaciones de restauración. Si no se puede evaluar el daño a tiempo, debe implementarse un plan de contingencia para que puedan proseguir las operaciones comerciales y la productividad normales.

k) Determinar la causa del daño.

Para determinar la causa del daño, es necesario saber a qué recursos iba dirigido el ataque y qué puntos vulnerables se explotaron para obtener acceso o perturbar los servicios. Revise los registros del sistema, los registros de auditoría y las pistas de auditoría. Estas revisiones suelen ayudar a descubrir el lugar del sistema en el que se originó el ataque y qué otros recursos resultaron afectados.

m) Reparar el daño.

Es muy importante que el daño se repare lo antes posible para restaurar las operaciones comerciales normales y todos los datos perdidos durante el ataque. Los planes y procedimientos para la recuperación de desastres de la organización (que se tratan en el documento acerca del diseño de la seguridad) deben cubrir la estrategia de

restauración. El equipo de respuesta a incidentes también debe poder controlar el proceso de restauración y recuperación, y ayudar en este último.

n) Documentar y aprender.

Es importante documentar el ataque una vez que se ha producido. La documentación debe abarcar todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado (en hardware y software, pérdida de datos o pérdida de productividad), los puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos tomados para reparar el daño. La documentación ayudará a modificar las estrategias proactivas para evitar ataques futuros o mermar los daños.

ñ) Implementar un plan de contingencia.

Si ya existe algún plan de contingencia, se puede implementar para ahorrar tiempo y mantener el buen funcionamiento de las operaciones comerciales. Si no hay ningún plan de contingencia, desarrolle un plan apropiado basado de la documentación del paso anterior.

l) Revisar el resultado y hacer simulaciones.

Tras el ataque o tras defenderse de él, revise su resultado con respecto al sistema. La revisión debe incluir la pérdida de productividad, la pérdida de datos o de hardware, y el tiempo que se tarda en recuperarlos.

Documente también el ataque y, si es posible, haga un seguimiento del lugar en el que se originó, qué métodos se utilizaron para iniciarlo y qué puntos vulnerables se explotaron. Para obtener los mejores resultados posibles, realice simulaciones en un entorno de prueba.

o) Revisar la eficacia de las directivas.

Si hay directivas para defenderse de un ataque que se ha producido, hay que revisar y comprobar su eficacia. Si no hay directivas, se deben redactar para aminorar o impedir ataques futuros.

p) Adjustar las directivas en consecuencia.

Si la eficacia de la directiva no llega al estándar, hay que ajustarla en consecuencia. Las actualizaciones de las directivas debe realizarlas el personal directivo relevante, los responsables de seguridad, los administradores y el equipo de respuesta a incidentes. Todas las directivas deben seguir las reglas e instrucciones generales de la organización.

1.4. Amenazas a la seguridad de la información.

Los tres elementos principales a proteger en cualquier sistema informático son el *software*, el *hardware* y los datos. Contra cualquiera de los tres elementos dichos anteriormente (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación. Un ataque se clasifica como **interrupción** si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una **interceptación** si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una **modificación** si además de conseguir el acceso consigue modificar el objeto; algunos autores **[Olovsson, 1992]** consideran un caso especial de la modificación: la **destrucción**, entendiéndola como una modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una **fabricación** si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el “fabricado”. En la figura 1.3 se muestran estos tipos de ataque de una forma gráfica.

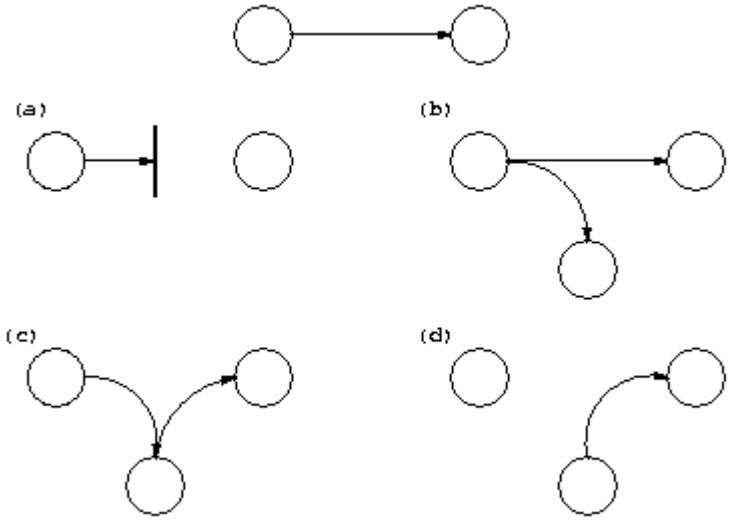

Figura 1.3: Flujo normal de información entre emisor y receptor y posibles amenazas: (a) interrupción, (b) interceptación, (c) modificación y (d) fabricación **[Gallo, 2001].**

En la gran mayoría de publicaciones relativas a la seguridad informática en general, tarde o temprano se intenta clasificar en grupos a los posibles elementos que pueden atacar nuestro sistema. Con frecuencia, especialmente en las obras menos técnicas y más orientadas a otros aspectos de la seguridad **[Icove, 1995] [Meyer, 1989]**, se suele identificar a los atacantes únicamente como personas; esto tiene sentido si hablamos por ejemplo de responsabilidades por un delito informático. Pero en este trabajo es preferible hablar de "elementos" y no de personas: aunque a veces lo olvidemos, nuestro sistema puede verse perjudicado por múltiples entidades aparte de humanos. A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a nuestro sistema. No pretende ser exhaustiva, ni por supuesto una taxonomía formal (para este tipo de estudios, se recomienda consultar **[Landwher, 1994][Aslam, 1996]**); simplemente trata de proporcionar una idea acerca de qué o quién amenaza un sistema.

a) Personas.

No podernos engañarnos, la mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas.

Aquí se listan los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los atacantes **pasivos**, aquellos que fisgonean por el sistema pero no lo modifican o destruyen, y los **activos**, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los *crackers* realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y activos en caso contrario, y el personal realiza ambos tipos indistintamente, dependiendo de la situación concreta.

- Personal.
- Ex-empleados.
- Curiosos.
- Crackers.
- Terroristas.
- Intrusos (remunerados).

b) Amenazas lógicas.

Bajo la etiqueta de "amenazas lógicas" encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (*software* malicioso, también conocido como *malware*) o simplemente por error (*bugs* o agujeros). Una excelente lectura que estudia las definiciones de algunas de estas amenazas y su implicación se presenta en **[Garfinkel, 1996]**; otra buena descripción, pero a un nivel más general, se puede encontrar en **[Parker, 1981].**

- **Software incorrecto.** Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones.
- **Herramientas de Seguridad.** Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para

detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

- **Puertas traseras.** Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar “atajos”. A estos atajos se les denomina puertas traseras. Algunos programadores pueden dejar estos atajos en las versiones definitivas de su *software*; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer.
- **Bombas lógicas.** Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona, los efectos pueden ser fatales.
- **Virus.** Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado *huésped*), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.
- **Gusanos.** Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando *bugs* de los sistemas a los que conecta para dañarlos.
- **Caballos de Troya.** Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas sin el conocimiento del usuario.

c) Catástrofes.

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas informáticos en una gran ciudad, es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que sí se produjeran generarían los mayores daños.

En este capítulo he tocado a profundidad los temas más importantes de acuerdo a la seguridad informática. Desde los conceptos más básicos hasta las estrategias y métodos que se deben seguir para hacer que un sistema o una aplicación sean seguros, confiables y ofrezca calidad.