

# Seguridad Informática

Giovanni Zuccardi  
Juan David Gutiérrez

Octubre de 2006

## CONTENIDO

Qué es *seguridad*?

Qué queremos proteger?

De qué nos queremos proteger?

Cómo nos podemos proteger?

Servicios

Gestión de Seguridad

ISO-27001:2005

## Seguridad Informática

### Qué es *seguridad*?

Podemos entender como **seguridad** una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de *seguridad* y se pasa a hablar de **fiabilidad** (probabilidad de que un sistema se comporte tal y como se espera de él) más que de *seguridad*; por tanto, se habla de *sistemas fiables* en lugar de hacerlo de *sistemas seguros*[SegUn02].

A grandes rasgos se entiende que mantener un sistema *seguro* (o fiable) consiste básicamente en garantizar tres aspectos [Pfl97]: confidencialidad, integridad y disponibilidad. Algunos estudios ([Lap91],[Olo92]) integran la seguridad dentro de una propiedad más general de los sistemas, la **confiabilidad**, entendida como el nivel de calidad del servicio ofrecido. Consideran la disponibilidad como un aspecto al mismo nivel que la seguridad y no como parte de ella, por lo que dividen esta última en sólo las dos facetas restantes, confidencialidad e integridad. En este trabajo no seguiremos esa corriente por considerarla minoritaria.

La **confidencialidad** nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades; la **integridad** significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada, y la **disponibilidad** indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la **negación de servicio**. Generalmente tienen que existir los tres aspectos descritos para que haya seguridad: un sistema puede conseguir confidencialidad para un determinado fichero haciendo que ningún usuario (ni siquiera el *root*) pueda leerlo, pero este mecanismo no proporciona disponibilidad alguna.

Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepone la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad: seguramente, es preferible que alguien borre información confidencial (que se podría recuperar después desde una cinta de *backup*) a que ese mismo atacante pueda leerla, o a que esa información esté disponible en un instante dado para los usuarios autorizados. En un entorno bancario, la faceta que más ha

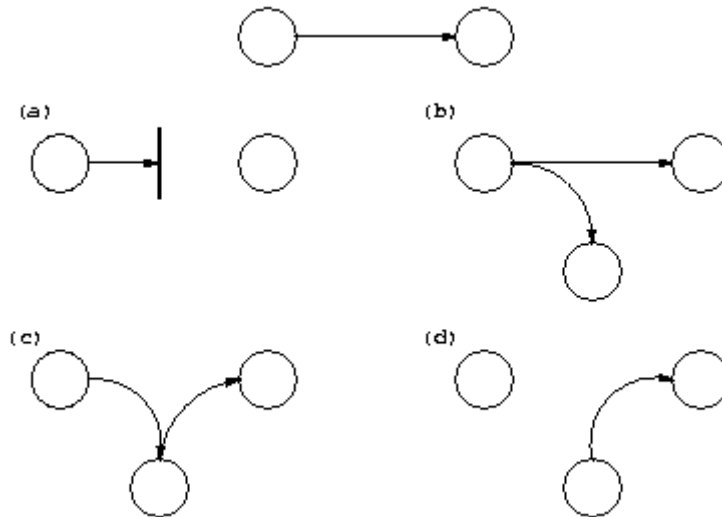
de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

### Qué queremos proteger?

Los tres elementos principales a proteger en cualquier sistema informático son el *software*, el *hardware* y los datos. Por **hardware** entendemos el conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, diskettes...) o tarjetas de red. Por **software** entendemos el conjunto de programas lógicos que hacen funcional al *hardware*, tanto sistemas operativos como aplicaciones, y por **datos** el conjunto de información lógica que manejan el *software* y el *hardware*, como por ejemplo paquetes que circulan por un cable de red o entradas de una base de datos. Aunque generalmente en las auditorías de seguridad se habla de un cuarto elemento a proteger, los **fungibles** (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, *tóners*, cintas magnéticas, *diskettes*...), aquí no consideraremos la seguridad de estos elementos por ser externos al sistema.

Habitualmente los datos constituyen el principal elemento de los tres a proteger, ya que es el más amenazado y seguramente el más difícil de recuperar: con toda seguridad una máquina está ubicada en un lugar de acceso físico restringido, o al menos controlado, y además en caso de pérdida de una aplicación este *software* se puede restaurar sin problemas desde su medio original (por ejemplo, el CD-ROM con el sistema operativo que se utilizó para su instalación). Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio 'original' desde el que restaurar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la política de copias sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

Contra cualquiera de los tres elementos descritos 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 ([Olo92]) 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 1.1 se muestran estos tipos de ataque de una forma gráfica.



**Figura 1.1:** Flujo normal de información entre emisor y receptor y posibles amenazas: (a) interrupción, (b) interceptación, (c) modificación y (d) fabricación.

### De qué nos queremos proteger?

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 ([ISV95], [Mey89]), 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, como por ejemplo programas, catástrofes naturales o, por qué no, fuerzas extraterrestres; si un usuario pierde un trabajo importante a causa de un ataque, poco le importará que haya sido un intruso, un gusano, un simple error del administrador [SegUn02]. En resumen podemos observar las amenazas la figura 1.2



## Figura 1.2: Amenazas para la seguridad

A continuación se presenta una relación de los elementos que potencialmente pueden amenazar a nuestro sistema. A lo largo de este proyecto se profundizará en aspectos de algunos de los elementos presentados aquí.

### Personas

No podemos engañarnos: la mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas que intentan conseguir el máximo nivel de privilegio posible aprovechando alguno (o algunos) de los riesgos lógicos de los que hablaremos a continuación, especialmente agujeros del *software*. Pero con demasiada frecuencia se suele olvidar que los piratas `clásicos' no son los únicos que amenazan nuestros equipos: es especialmente preocupante que mientras que hoy en día cualquier administrador preocupado por la seguridad va a conseguir un sistema relativamente fiable de una forma lógica (permaneciendo atento a vulnerabilidades de su *software*, restringiendo servicios, utilizando cifrado de datos...), pocos administradores tienen en cuenta factores como la ingeniería social o el basureo a la hora de diseñar una política de seguridad.

Aquí se describen brevemente 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

Las amenazas a la seguridad de un sistema provenientes del personal de la propia organización rara vez son tomadas en cuenta; se presupone un entorno de confianza donde a veces no existe, por lo que se pasa por alto el hecho de que casi cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática (secretariado, personal de seguridad, personal de limpieza y mantenimiento...) puede comprometer la seguridad de los equipos.

Aunque los ataques pueden ser intencionados (en cuyo caso sus efectos son extremadamente dañinos, recordemos que nadie mejor que el propio personal de la organización conoce mejor los sistemas...y sus debilidades), lo normal es que más que de ataques se trate de **accidentes** causados por un error o por desconocimiento

de las normas básicas de seguridad: un empleado de mantenimiento que corta el suministro eléctrico para hacer una reparación puede llegar a ser tan peligroso como el más experto de los administradores que se equivoca al teclear una orden y borra todos los sistemas de ficheros; y en el primer caso, el `atacante' ni siquiera ha de tener acceso lógico (ni físico) a los equipos, ni conocer nada sobre seguridad.

- **Ex-empleados**  
Otro gran grupo de personas potencialmente interesadas en atacar nuestro sistema son los antiguos empleados del mismo, especialmente los que no abandonaron el entorno por voluntad propia (y en el caso de redes de empresas, los que pasaron a la competencia). Generalmente, se trata de personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo: amparados en excusas como `No me han pagado lo que me deben' o `Es una gran universidad, se lo pueden permitir' pueden insertar troyanos, bombas lógicas, virus...o simplemente conectarse al sistema como si aún trabajaran para la organización (muchas veces se mantienen las cuentas abiertas incluso meses después de abandonar la universidad o empresa), conseguir el privilegio necesario, y dañarlo de la forma que deseen, incluso chantajeando a sus ex-compañeros o ex-jefes.
- **Curiosos**  
Junto con los *crackers*, los curiosos son los atacantes más habituales de sistemas en redes de I+D. Recordemos que los equipos están trabajando en entornos donde se forma a futuros profesionales de la informática y las telecomunicaciones (gente que *a priori* tiene interés por las nuevas tecnologías), y recordemos también que las personas suelen ser curiosas por naturaleza; esta combinación produce una avalancha de estudiantes o personal intentando conseguir mayor privilegio del que tienen o intentando acceder a sistemas a los que oficialmente no tienen acceso. Y en la mayoría de ocasiones esto se hace simplemente para leer el correo de un amigo, enterarse de cuánto cobra un compañero, copiar un trabajo o comprobar que es posible romper la seguridad de un sistema concreto. Aunque en la mayoría de situaciones se trata de ataques no destructivos (a excepción del borrado de huellas para evitar la detección), parece claro que no benefician en absoluto al entorno de fiabilidad que podamos generar en un determinado sistema.
- **Crackers**  
Los entornos de seguridad media son un objetivo típico de los intrusos, ya sea para fisgonear, para utilizarlas como enlace hacia otras redes o simplemente por diversión. Por un lado, son redes generalmente abiertas, y la seguridad no es un factor tenido muy en cuenta en ellas; por otro, el gran número y variedad de sistemas conectados a estas redes provoca, casi por simple probabilidad, que al menos algunos de sus equipos (cuando no la mayoría) sean vulnerables a problemas conocidos de antemano. De esta forma un atacante sólo ha de utilizar un escáner de seguridad contra el dominio completo y luego atacar mediante un simple *exploit* los

equipos que presentan vulnerabilidades; esto convierte a las redes de I+D, a las de empresas, o a las de ISPs en un objetivo fácil y apetecible para piratas con cualquier nivel de conocimientos, desde los más novatos (y a veces más peligrosos) hasta los expertos, que pueden utilizar toda la red para probar nuevos ataques o como nodo intermedio en un ataque a otros organismos, con el consiguiente deterioro de imagen (y a veces de presupuesto) que supone para una universidad ser, sin desearlo, un apoyo a los piratas que atacan sistemas teóricamente más protegidos, como los militares.

- Terroristas  
Por 'terroristas' no debemos entender simplemente a los que se dedican a poner bombas o quemar autobuses; bajo esta definición se engloba a cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él. Por ejemplo, alguien puede intentar borrar las bases de datos de un partido político enemigo o destruir los sistemas de ficheros de un servidor que alberga páginas *web* de algún grupo religioso; en el caso de redes de I+D, típicos ataques son la destrucción de sistemas de prácticas o la modificación de páginas *web* de algún departamento o de ciertos profesores, generalmente por parte de alumnos descontentos.
- Intrusos remunerados

Este es el grupo de atacantes de un sistema más peligroso, aunque por fortuna el menos habitual en redes normales; suele afectar más a las grandes - muy grandes - empresas o a organismos de defensa. Se trata de piratas con gran experiencia en problemas de seguridad y un amplio conocimiento del sistema, que son pagados por una tercera parte generalmente para robar secretos (el nuevo diseño de un procesador, una base de datos de clientes, información confidencial sobre las posiciones de satélites espía...) o simplemente para dañar la imagen de la entidad afectada. Esta tercera parte suele ser una empresa de la competencia o un organismo de inteligencia, es decir, una organización que puede permitirse un gran gasto en el ataque; de ahí su peligrosidad: se suele pagar bien a los mejores piratas, y por si esto fuera poco los atacantes van a tener todos los medios necesarios a su alcance.

### 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 en los sistemas se presenta en un nivel más general, cabe aclarar que estas se engloban en una definición de *malware* proviene de una agrupación de las palabras (**malicious software**); este programa o archivo, que es dañino para el ordenador, está diseñado para insertar virus, gusanos, troyanos, spyware o incluso los bots, intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí[CurSeg03].

- Puertas traseras

Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar 'atajos' en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando. A estos atajos se les denomina puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos: por ejemplo, los diseñadores de un *software* de gestión de bases de datos en el que para acceder a una tabla se necesiten cuatro claves diferentes de diez caracteres cada una pueden insertar una rutina para conseguir ese acceso mediante una única clave 'especial', con el objetivo de perder menos tiempo al depurar el sistema. Algunos programadores pueden dejar estos atajos en las versiones definitivas de su *software* para facilitar un mantenimiento posterior, para garantizar su propio acceso, o simplemente por descuido; 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, lo que obviamente supone un grave peligro para la integridad de nuestro sistema.

- Bombas lógicas

Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.

Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la ejecución bajo un determinado UID o la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona que ejecuta el programa: si las activa el *root*, o el programa que contiene la bomba está setuidado a su nombre, los efectos obviamente 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. Al ser difíciles de programar su número no es muy elevado, pero el daño que pueden causar es muy grande: el mayor incidente de seguridad en Internet fué precisamente el *Internet Worm*, un gusano que en 1988 causó pérdidas millonarias al infectar y detener más de 6000 máquinas conectadas a la red.

Hemos de pensar que un gusano puede automatizar y ejecutar en unos segundos todos los pasos que seguiría un atacante humano para acceder a nuestro sistema: mientras que una persona, por muchos conocimientos y medios que posea, tardaría como mínimo horas en controlar nuestra red completa (un tiempo más que razonable para detectarlo), un gusano puede hacer eso mismo en pocos minutos: de ahí su enorme peligro y sus devastadores efectos.

- 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 (generalmente en detrimento de la seguridad) sin el conocimiento del usuario; como el Caballo de Troya de la mitología griega, al que deben su nombre, ocultan su función real bajo la apariencia de un programa inofensivo que a primera vista funciona correctamente. En la práctica la totalidad de los ataques, cuando un intruso consigue el privilegio necesario en el sistema instala troyanos para ocultar su presencia o para asegurarse la entrada en caso de ser descubierto: por ejemplo, es típico utilizar lo que se denomina un *rootkit*, que no es más que un conjunto de versiones troyanas de ciertas utilidades (*netstat*, *ps*, *who...*), para conseguir que cuando el administrador las ejecute no vea la información relativa al atacante, como sus procesos o su conexión al sistema; otro programa que se suele suplantar es *login*.

- Spyware

Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. Recolectan información proveniente del teclado de la víctima, descubriendo contraseñas e información valiosa para cualquier atacante.

- Adware

El adware es software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla. Esta práctica se utiliza para subvencionar económicamente la aplicación, permitiendo que el usuario la obtenga por un precio más bajo e incluso gratis y, por supuesto, puede proporcionar al programador un

beneficio, que ayuda a motivarlo para escribir, mantener y actualizar un programa valioso. Se carga generalmente con nuestro permiso.

- Spoofing

Uo de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Existen diferentes tipos de spoofing dependiendo de la tecnología a la que nos refiramos, los cuales se describirán más adelante, como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

- Phishing

Un de un tipo de ingeniería social y spoofing, caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido como *phisher* se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico o algún sistema de mensajería instantánea.

- Spam

Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de spam incluyen grupos de noticias usenet, motores de búsqueda, wikis y blogs. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.

- Exploits

Es un programa o técnica (del inglés *to exploit*, explotar, aprovechar) que aprovecha una vulnerabilidad. Los exploits dependen de los S.O y sus configuraciones, del as configuraciones de los programas que se están ejecutando y de la LAN donde están.

Los *exploits* se pueden caracterizar según las categorías de vulnerabilidades utilizadas:

- ✓ Vulnerabilidades de desbordamiento de buffer.
- ✓ Vulnerabilidades de condición de carrera (race condition).
- ✓ Vulnerabilidades de error de formato de cadena (format string bugs).
- ✓ Vulnerabilidades de Cross Site Scripting (XSS).

- ✓ Vulnerabilidades de Inyección SQL.
- ✓ Vulnerabilidades de Inyección de Caracteres (CRLF).
- ✓ Vulnerabilidades de denegación del servicio
- ✓ Vulnerabilidades de Inyección múltiple HTML (Multiple HTML Injection).
- ✓ Vulnerabilidades de ventanas enganosas o mistificación de ventanas (Window Spoofing).

Las anteriores estaban enmarcadas en malware, a continuación presentamos mas amenazas lógicas

- 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. Herramientas como NESSUS, SAINT o SATAN pasan de ser útiles a ser peligrosas cuando las utilizan *crackers* que buscan información sobre las vulnerabilidades de un *host* o de una red completa. La conveniencia de diseñar y distribuir libremente herramientas que puedan facilitar un ataque es un tema peliagudo; incluso expertos reconocidos como Alec Muffet (autor del adivinador de contraseñas Crack) han recibido enormes críticas por diseñar determinadas herramientas de seguridad. Tras numerosos debates sobre el tema, ha quedado bastante claro que no se puede basar la seguridad de un sistema en el supuesto desconocimiento de sus problemas por parte de los atacantes: esta política, denominada *Security through obscurity*, se ha demostrado inservible en múltiples ocasiones. Si como administradores no utilizamos herramientas de seguridad que muestren las debilidades de nuestros sistemas (para corregirlas), tenemos que estar seguro que un atacante no va a dudar en utilizar tales herramientas (para explotar las debilidades encontradas); por tanto, hemos de agradecer a los diseñadores de tales programas el esfuerzo que han realizado (y nos han ahorrado) en pro de sistemas más seguros.

- Técnicas salami

Por técnica salami se conoce al robo automatizado de pequeñas cantidades de bienes (generalmente dinero) de una gran cantidad origen. El hecho de que la cantidad inicial sea grande y la robada pequeña hace extremadamente difícil su detección: si de una cuenta con varios millones de pesetas se roban unos céntimos, nadie va a darse cuenta de ello; si esto se automatiza para, por ejemplo, descontar una peseta de cada nómina pagada en la universidad o de cada beca concedida, tras un mes de actividad seguramente se habrá robado una enorme cantidad de dinero sin que nadie se haya percatado de este hecho, ya que de cada origen se ha tomado una

cantidad ínfima.  
Las técnicas salami no se suelen utilizar para atacar sistemas normales, sino que su uso más habitual es en sistemas bancarios; sin embargo, como en una red con requerimientos de seguridad medios es posible que haya ordenadores dedicados a contabilidad, facturación de un departamento o gestión de nóminas del personal, comentamos esta potencial amenaza contra el *software* encargado de estas tareas.

### Amenazas Físicas

Los errores o daños de Hardware son una amenaza que esta presente en la mayoría de los sistemas, y se puede presentar en cualquier momento; como ejemplo tenemos daños en discos duros, procesadores y cualquier otra parte del computador que comprometa la información.

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 como Madrid, Valencia o Barcelona, 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 si se produjeran generarían los mayores daños.

Un subgrupo de las catástrofes es el denominado de **riesgos poco probables**. Obviamente se denomina así al conjunto de riesgos que, aunque existen, la posibilidad de que se produzcan es tan baja (menor incluso que la del resto de catástrofes) que nadie toma, o nadie puede tomar, medidas contra ellos. Ejemplos habituales de riesgos poco probables son un ataque nuclear contra el sistema, el impacto de un satélite contra la sala de operaciones, o la abducción de un operador por una nave extraterrestre. Nada nos asegura que este tipo de catástrofes no vaya a ocurrir, pero la probabilidad es tan baja y los sistemas de prevención tan costosos que no vale la pena tomar medidas contra ellas.

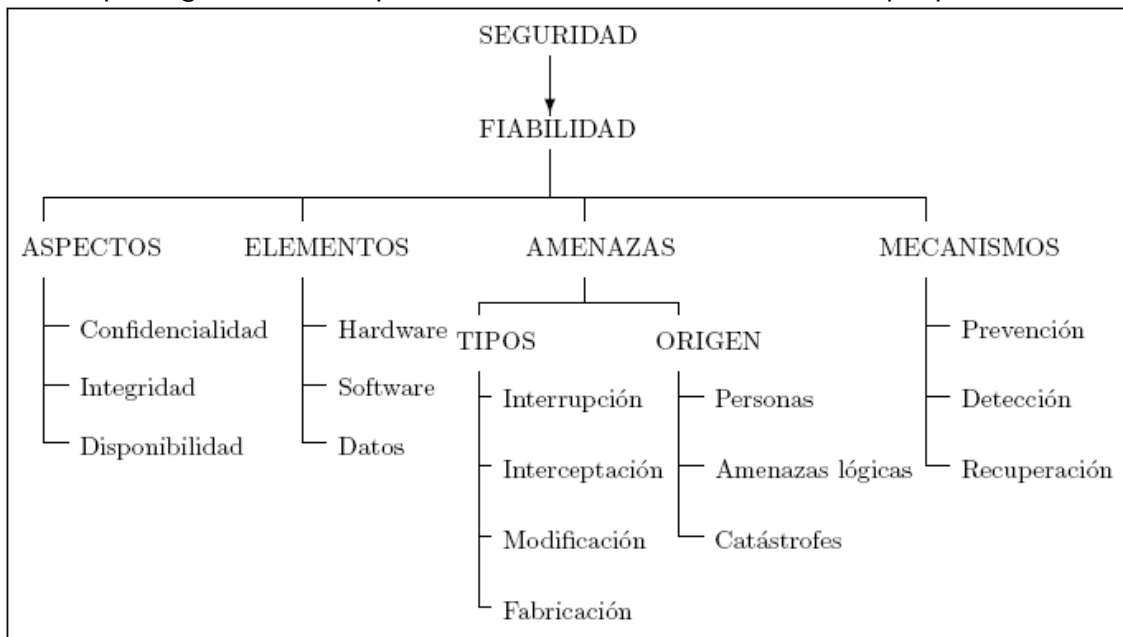
Como ejemplos de catástrofes hablaremos de terremotos, inundaciones, incendios, humo o atentados de baja magnitud (más comunes de lo que podamos pensar); obviamente los riesgos poco probables los trataremos como algo anecdótico. De cualquier forma, vamos a hablar de estas amenazas sin extendernos mucho, ya que el objetivo de este proyecto no puede ser el proporcionar las directrices para una construcción de edificios a prueba de terremotos, o un plan formal de evacuación en caso de incendio.

### Cómo nos podemos proteger?

Hasta ahora hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; parece claro que, para completar nuestra visión de la seguridad, hemos de hablar de las

formas de protección de nuestros sistemas. Cuando hayamos completado este punto, habremos presentado a grandes rasgos los diferentes puntos a tratar en este proyecto, tal y como se sintetiza en la figura 1.3.

Para proteger nuestro sistema hemos de realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generar, y la probabilidad de su ocurrencia; a partir de este análisis hemos de diseñar una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implementar esta política de seguridad se les denomina **mecanismos de seguridad**; son la parte más visible de nuestro sistema de seguridad, y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.



**Figura 1.3:** Visión global de la seguridad informática

Los mecanismos de seguridad se dividen en tres grandes grupos: de prevención, de detección y de recuperación. Los mecanismos **de prevención** son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema en la red. Por mecanismos **de detección** se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoría como *Tripwire*. Finalmente, los mecanismos **de recuperación** son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el *hardware* adicional. Dentro de este último grupo de mecanismos de seguridad encontramos un subgrupo denominado **mecanismos de análisis forense**, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta

utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red [SegUn02].

Parece claro que, aunque los tres tipos de mecanismos son importantes para la seguridad de nuestro sistema, hemos de enfatizar en el uso de mecanismos de prevención y de detección; la máxima popular *'más vale prevenir que curar'* se puede aplicar a la seguridad informática: para nosotros, evitar un ataque, detectar un intento de violación, o detectar una violación exitosa inmediatamente después de que ocurra es mucho más productivo y menos comprometedor para el sistema que restaurar el estado tras una penetración de la máquina. Es más, si consiguiéramos un sistema sin vulnerabilidades y cuya política de seguridad se implementara mediante mecanismos de prevención de una forma completa, no necesitaríamos mecanismos de detección o recuperación.

Los mecanismos de prevención más habituales en redes son los siguientes:

- Mecanismos de autenticación e identificación

Estos mecanismos hacen posible identificar entidades del sistema de una forma única, y posteriormente, una vez identificadas, autenticarlas (comprobar que la entidad es quién dice ser). Son los mecanismos más importantes en cualquier sistema, ya que forman la base de otros mecanismos que basan su funcionamiento en la identidad de las entidades que acceden a un objeto.

Un grupo especialmente importante de estos mecanismos son los denominados Sistemas de Autenticación de Usuarios, a los que prestaremos una especial atención por ser los más utilizados en la práctica [SegUn02].

- Mecanismos de control de acceso

Cualquier objeto del sistema ha de estar protegido mediante mecanismos de control de acceso, que controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema.

- Mecanismos de separación

Cualquier sistema con diferentes niveles de seguridad ha de implementar mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso. Los mecanismos de separación se dividen en cinco grandes grupos, en función de como separan a los objetos: separación física, temporal, lógica, criptográfica y fragmentación.

- Mecanismos de seguridad en las comunicaciones

Es especialmente importante para la seguridad de nuestro sistema el proteger la integridad y la privacidad de los datos cuando se transmiten a través de la red. Para garantizar esta seguridad en las comunicaciones, hemos de utilizar ciertos mecanismos, la mayoría de los cuales se basan en la Criptografía: cifrado de clave pública, de clave privada, firmas digitales... Aunque cada vez se utilizan más los protocolos seguros (como SSH o Kerberos), aún es frecuente encontrar conexiones en texto claro ya no sólo entre máquinas de una misma subred, sino entre redes diferentes. Una de las mayores amenazas a la integridad de las redes es este tráfico sin cifrar, que hace extremadamente fáciles ataques encaminados a robar contraseñas o suplantar la identidad de máquinas de la red.

## **Servicios**

Para lograr hacer cumplir la preservación y el cumplimiento de los tres principios básicos de la seguridad informática, discutidos anteriormente, se han planeado ciertos servicios principales, que sirven como base para la implementación de una infraestructura de seguridad en una organización ([NIST95], [STON01], [GASS88], [ALSI05], [BRIN95b], [HARR03]).

**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 que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

**Auditoria:** se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este grupo el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

**No repudio:** La administración de un sistema de información debe estar en capacidad de asegurar quién o quiénes son los remitentes y destinatarios de cualquier información. Es por esto que este servicio provee los medios y mecanismos para poder identificar quien ha llevado a cabo una o varias acciones en un sistema, para que los usuarios no puedan negar las responsabilidades de las acciones que han llevado a cabo.

## **Gestión de la seguridad**

Diariamente se escucha en varios medios (periódicos, televisión, Internet, foros de discusión, reportes de fabricantes de productos y proveedores de servicios, etc.) acerca de incidentes de seguridad informática, como ataques de virus que causan pérdidas y daños que pueden llegar a representar grandes sumas de dinero para una organización, ataques remotos de hackers a instituciones financieras, ataques a los sitios Web de grandes y prestigiosas empresas y corporaciones, etc. Este tipo de incidentes son los que hacen cada vez más interesante la seguridad informática, pero así mismo significa tareas y responsabilidades diarias de esta área para prevenir ataques como los antes mencionados. Es por esto que la administración de la seguridad informática es uno de los temas más importantes en la estructura de seguridad informática de una organización [HARR03].

Administrar la Seguridad Informática de una organización, es un trabajo fundamental para conservar confiables, los sistemas de la misma. La tarea de administración, comprende la administración de riesgos, definición, creación e implementación de políticas de seguridad, procedimientos, estándares, guías, clasificación de información, organización de la estructura de seguridad de la compañía, y la educación de los individuos de la organización, entre otras. [HARR03] [ALSI05]

Como se mencionó en la sección anterior, la clave de un programa de seguridad informática, es la protección de los activos más importantes de la compañía. Estos activos pueden ser identificados mediante los análisis de riesgos, además de la identificación de las vulnerabilidades y amenazas que materialización de una o más de dichas amenazas. Como resultado de los análisis de riesgos se puede lograr tener un presupuesto de las inversiones necesarias para la protección de dichos activos, contra los riesgos anteriormente identificados, no solo en cosas materiales, sino también en implementación de políticas, educación del personal, desarrollo de guías o estándares, etc. [ALSI05]

El administrador no es un simple observador de un sistema y de sus operaciones posteriores a su instalación. Esta labor también incluye tareas previas de la instalación del sistema, tales como validar y estructurar las políticas de seguridad para el mismo, aunque esto no quiere decir que esta administración pertenece solo al área técnica, también tiene tareas administrativas como son la creación de políticas, hacer que se cumplan y actualizarlas cuando sea necesario. La administración de seguridad debe tener en cuenta que el desarrollo y crecimiento de un sistema, las redes, etc., producen cambios constantes en las políticas de seguridad, en la protección de bienes y las amenazas establecidas, lo cual requiere también de una debida gestión y administración. [HARR03]

Una de las formas más utilizadas para hacer administración de la seguridad informática, se basa en la utilización de estándares. El crecimiento de las necesidades de gestión de la seguridad informática en las organizaciones, ha motivado la creación de estándares locales e internacionales para la administración de tecnología de información, y en particular la seguridad de dicha información, y todo lo que a ésta concierne [OUD05].

La historia de los estándares se remonta a los inicios del siglo XX, con los primeros usos que se dieron a la electricidad; se comenzaron a desarrollar entonces aplicaciones eléctricas bajo los primero estándares establecidos por la International Electronic Committee (IEC). Más adelante con el paso del tiempo, fue surgiendo la necesidad de nuevos y mejores estándares en

más y más áreas del conocimiento, y así nació la International Organisation of Standardisation (ISO) [OUD05].

Pero no sólo existen estándares reconocidos internacionalmente, sino también han surgido estándares locales o nacionales, referentes a la administración de seguridad informática. La razón principal de la creación de estos estándares locales, radica en la casuística y especificidad que pueden llegar a tener las mejores prácticas en el área, en un país o región determinada [OUD05].

Uno de los factores positivos de la existencia actual de los estándares, es la cantidad que hay de los mismos, ya que esto permite a una organización particular, acoplarse o acomodarse a uno de estos estándares, según sus características y necesidades, o en una situación determinada. Adicionalmente, otro punto a favor de las organizaciones gracias a los estándares, no sólo es el ahorro de recursos, tanto de dinero, como de personas y tiempo, en desarrollar estándares propios, sino que pueden utilizar estándares que han sido demostrados a partir de las mejores prácticas en el área, que para el caso de esta investigación, son las mejores prácticas en administración de la seguridad informática [OUD05].

En dicha área, la administración de seguridad informática, existen varios estándares, nacionales e internacionales, que están orientados a ser una guía para las organizaciones en la formación y mantenimiento de la infraestructura de seguridad informática de las empresas. A continuación se listan algunos de los estándares más importantes que existen en el área:

- ISO/IEC 13335-1:2004: Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management
- ISO/IEC TR 13335-3:1998: Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
- ISO/IEC TR 13335-4:2000: Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards
  
- ISO/IEC TR 13335-5:2001: Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security
- ISO/IEC 17799:2005: Information technology -- Security techniques -- Code of practice for information security management
- British Standard 7799 – BS7799
- Estándares publicados por NIST (National Institute of Standards and Technology)
- ISO/IEC 27001:2005
- COBIT Security Baseline
- ISF Standard of Good Practice

Para lograr los objetivos de la administración de la seguridad informática, ésta se vale de controles que se utilizan para hacer cumplir las directivas que esta área ha fijado para la organización. Dichos controles se clasifican en: controles administrativos, controles técnicos y controles físicos. [HARR03]

Los controles administrativos, hacen referencia al desarrollo y publicación de políticas, estándares, procedimientos, investigación del personal, entrenamiento y el cambio de los procedimientos de control.

Los controles técnicos, se refieren a los mecanismos de control de acceso, administración de recursos y contraseñas para su acceso, métodos de autenticación y autorización, dispositivos de seguridad, y la configuración de la infraestructura técnica de seguridad de la organización.

Los controles físicos corresponden a los controles físicos de acceso a diferentes locaciones de la organización, bloqueo de sistemas, monitoreo de los lugares críticos de almacenamiento y manejo de información, etc.

[HARR03]

Dentro de la administración de la seguridad de la información, se deberían tener en cuenta las inversiones requeridas para el desarrollo de los procedimientos, políticas, estándares, etc., anteriormente mencionados, y para que dichas inversiones lleguen a retornar los beneficios o ganancias esperadas, se debería también conocer la forma de estimar las ganancias o posibles pérdidas de dichas inversiones. En la sección que se presenta a continuación, se expondrán algunas ideas y acercamientos planteados por diferentes autores acerca del cálculo del retorno de las inversiones en seguridad informática.

## **Figuras**

**Figura 1.1:** Flujo normal de información entre emisor y receptor y posibles amenazas: (a) interrupción, (b) interceptación, (c) modificación y (d) fabricación.

**Figura 1.2:** Amenazas para la seguridad

**Figura 1.3:** Representación del modelo "Plan-Do-Check-Act".

**Figura 1.4:** Metodología de un SGSI según ISO 27001

## Bibliografía

[ALSI05] ACADEMIA LATINOAMERICANA DE SEGURIDAD INFORMÁTICA. Unidad 1: Introducción a la Seguridad de la Información. Microsoft Technet. 2005. Disponible en:

<http://www.mslatam.com/latam/technet/cso/Html-ES/home.asp>

[BRIN95b] BRINKLEY, Donald L. y SCHELL, Roger R. Information Security: An Integrated Collection of Essays: Essay 2 Concepts and Terminology for Computer Security. California, Estados Unidos de América. ACSAC. 1995. Disponible en:

<http://www.acsac.org/secshelf/book001/02.pdf>

[CurSeg03] Curso de seguridad Informática Version 3.1 Jorge Ramiro Aguirre Marzo 2003

[GASS88] GASSER, Morrie. Building a Secure Computer System. Nueva York, Estados Unidos de América. Library of Congreso. 1988. Disponible en:

<http://www.acsac.org/secshelf/book002.html>

[HARR03] HARRIS, Shon. CISSP Certification: All-in-one Exam Guide. Second Edition. Emerville, California, Estados Unidos de América. McGraw Hill. 2004

[ISV95] David Icové, Karl Seger, and William VonStorch. *Computer Crime. Crimefighter's handbook*. O'Reilly & Associates, 1995.

[Mey89] Gordon R. Meyer. *The Social Organization of the Computer Underground*. PhD thesis, Northern Illinois University, 1989.

[NIST95] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12 Washington, Estados Unidos de América. National Institute of Standards and Technology (NIST), 1995. Disponible en:

<http://www.csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

[Lap91] J.C. Laprie. *Dependability: Basic concepts and terminology*. Springer-Verlag, 1991.

[Olo92] Tomas Olovsson. A structured approach to computer security. Technical Report 122, Chalmers University of Technology, 1992.

[OUD05] OUD, Ernst Jan. The value to IT of using Internacional Standards. En: Information Systems Control Journal. Vol. 3. (2005); p. 35-39

[Pfi97] Charles P. Pfleeger. *Security in computing*. Prentice Hall, 1997.

[SegUn02] SEGURIDAD EN UNIX Y REDES Version 2.1 Antonio Villalon Huerta Julio, 2002 Disponible en:

[www.rediris.es/cert/doc/unixsec/unixsec.pdf](http://www.rediris.es/cert/doc/unixsec/unixsec.pdf)

[STON01] STONEBURNER, Gary. NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security. Gaithersburg, Estados Unidos de América. National Institute of Standards and Technology (NIST), 2001. Disponible en:  
<http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf>

[TesSeg01] Tesis Seguridad Informática: Sus Implicancias e implementaciones F. Borghello 2001  
<http://www.htmlweb.net/seguridad/tesis/Cap1.pdf>

[TesSROI06] Tesis UNA GUÍA METODOLÓGICA PARA EL CÁLCULO DEL RETORNO A LA INVERSIÓN (ROI) EN SEGURIDAD INFORMÁTICA: UN CASO DE ESTUDIO. Nicolas Sanchez, Juan Sebastián Segura. Junio 2006  
Disponible en:  
<http://www.criptored.upm.es/descarga/TesisRetornoInversionSI.zip>