# CAPÍTULO 1



**"La seguridad absoluta tendría un costo infinito."**

**Anónimo**

# INTRODUCCIÓN


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

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

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

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

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

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



# 1.1 EVOLUCIÓN DEL TÉRMINO SEGURIDAD

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

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC) o el Hammurabi (2000 AC). También la Biblia, Homero, Cicerón, Cesar han sido autores de obras en donde aparecen ciertos rasgos de la seguridad en la guerra y el gobierno.

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

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

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

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

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

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

Seguridad Interna (aquella preocupada por las amenazas de nuestra organización con la organización misma). De estas dos se pueden desprender la Seguridad Privada y Pública al aparecer el estado y depositar su confianza en unidades armadas.

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

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

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

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

Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera. Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre Seguridad.

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

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

## 1.2 DE QUE ESTAMOS HABLANDO



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

"La Seguridad es hoy día una profesión compleja con funciones especializadas"[2].

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

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

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

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



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

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

Algunas aclaraciones:

1. El protector no siempre es el poseedor de valor.
2. El agresor no siempre es el aspirante a poseedor.
3. Ambas figuras pueden ser delegadas a terceros por el cambio de otro valor, generalmente dinero.
4. El valor puede no ser algo concreto. Por ejemplo se podría querer cuidar el honor, la intimidad, el conocimiento, etc.
5. La situación global indica que no será lo mismo el robo de un comercio en Argentina que en Andorra en donde sus habitantes se ven obligados a robar para subsistir.

Los competidores se pueden subdividir en:

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

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

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

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

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

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

En el presente, cada vez que se mencione Información se estará haciendo referencia a la Información que es procesada por un Sistema Informático; definiendo este último como el "conjunto formado por las personas, computadoras (hardware y software), papeles, medios de almacenamiento digital, el entorno donde actúan y sus interacciones."[4].

Luego:

**"El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora."[4]**

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

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

### 1.2.1 ANÁLISIS DEL OBJETIVO DE LA SEGURIDAD INFORMÁTICA

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

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

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



[3] TOFFLER, Alvin. La Tercera Ola. Editorial Sudamericana. España. 1998.
[4] ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. Argentina. 1997. Página 22.
[5] CALVO, Rafael Fernández. Glosario Básico Inglés–Español para usuarios de Internet. 1994–2000. *http://www.ati.es/novatica/2000/145*

Ejemplo: 1, 9, 8 y 7 son datos; su agregación 1987 es Información.

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

Existe Información que **debe o puede ser pública**: puede ser visualizada por cualquier persona (por ejemplo índice de analfabetismo en un país); y aquella que **debe ser privada**: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la Información:

1. Es Crítica: es indispensable para garantizar la continuidad operativa.
2. Es Valiosa: es un activo con valor en sí misma.
3. Es Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

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

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

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

El **Control** sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

La **Autenticidad** permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- **Protección a la Réplica:** mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- **No Repudio:** mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

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

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


**Gráfico 1.1 – Amenazas para la Seguridad**

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

a. **La Prevención (antes):** mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
b. **La Detección (durante):** mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.
c. **La Recuperación (después):** mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

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

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

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

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

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

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

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

La Seguridad indicara el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas imposible) en un 100% por lo que sólo se habla de **Fiabilidad** y se la define como "la probabilidad de que un sistema se comporte tal y como se espera de él"[6], y se habla de Sistema Fiable en vez de sistema seguro.

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

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

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



## 1.2.2 SISTEMA DE SEGURIDAD

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

1. **Reconocimiento**: cada usuario deberá identificarse al usar el sistema y cada operación del mismo será registrada con esta identificación. En este proceso se

[6] HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital – Open Publication License v.10. 2 de Octubre de 2000. *http://www.kriptopolis.com*

quiere conseguir que no se produzca un acceso y/o manipulación indebida de los datos o que en su defecto, esta quede registrada.

2. **Integridad**: un sistema integro es aquel en el que todas las partes que lo constituyen funcionan en forma correcta y en su totalidad.
3. **Aislamiento**: Los datos utilizados por un usuario deben ser independientes de los de otro física y lógicamente (usando técnicas de ocultación y/o compartimiento). También se debe lograr independencia entre los datos accesibles y los considerados críticos.
4. **Auditabilidad**: procedimiento utilizado en la elaboración de exámenes, demostraciones, verificaciones o comprobaciones del sistema. Estas comprobaciones deben ser periódicas y tales que brinden datos precisos y aporten confianza a la dirección. Deben apuntar a contestar preguntas como:
   - ¿El uso del sistema es adecuado?
   - ¿El sistema se ajusta a las normas internas y externas vigentes?
   - ¿Los datos arrojados por el sistema se ajustan a las expectativas creadas?
   - ¿Todas las transacciones realizadas por el sistema pueden ser registradas adecuadamente?
   - ¿Contienen información referentes al entorno: tiempo, lugar, autoridad, recurso, empleado, etc.?
5. **Controlabilidad**: todos los sistemas y subsistemas deben estar bajo control permanente.
6. **Recuperabilidad**: en caso de emergencia, debe existir la posibilidad de recuperar los recursos perdidos o dañados.
7. **Administración y Custodia:** la vigilancia nos permitirá conocer, en todo momento, cualquier suceso, para luego realizar un seguimiento de los hechos y permitir una realimentación del sistema de seguridad, de forma tal de mantenerlo actualizado contra nuevas amenazas.



## 1.2.3 DE QUIEN DEBEMOS PROTEGERNOS

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

Ante la pregunta de los tipos de intrusos existentes actualmente, Julio C. Ardita[7] contesta lo siguiente:

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

1. **Clase A:** el 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, están jugando (...) son pequeños grupitos que se juntan y dicen vamos a probar.

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

2. **Clase B:** es el 12% son más peligroso, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo que está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.
3. **Clase C:** es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.
4. **Clase D:** el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

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

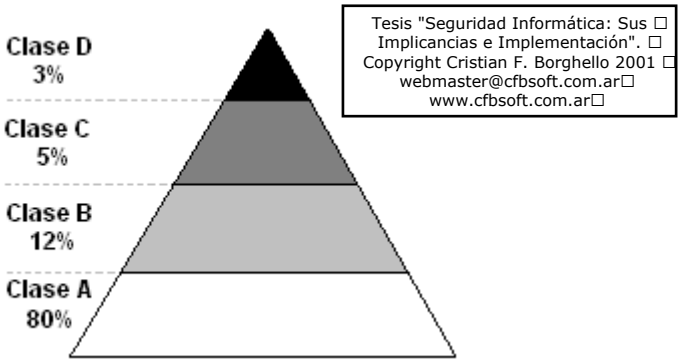


**Gráfico 1.2 – Tipos de Intrusos. Fuente:** CybSec S.A. *http://www.cybsec.com*

## 1.2.4 QUÉ DEBEMOS PROTEGER

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

Por **hardware** entendemos el conjunto de todos los sistemas físicos del sistema informático: CPU, cableado, impresoras, CD–ROM, cintas, componentes de comunicación.

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

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

Además, generalmente se habla de un cuarto elemento llamado **fungibles**; que son los aquellos que se gastan o desgastan con el uso continuo: papel, tonner, tinta, cintas magnéticas, disquetes.

De los cuatro, los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar: hemos de pasar obligatoriamente por un sistema de copias de seguridad, y aún así es difícil de devolver los datos a su forma anterior al daño.

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

1. **Ataques Pasivos**: el atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Generalmente se emplean para:
   - Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados.
   - Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
   - Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

   Es posible evitar el éxito, si bien no el ataque, mediante el cifrado de la información y otros mecanismos que se verán posteriormente.
2. **Ataques Activos**: estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:
   - **Interrupción:** si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
   - **Intercepción:** si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
   - **Modificación:** si además de conseguir el acceso consigue modificar el objeto.
   - **Fabricación:** se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.
   - **Destrucción:** es una modificación que inutiliza el objeto.

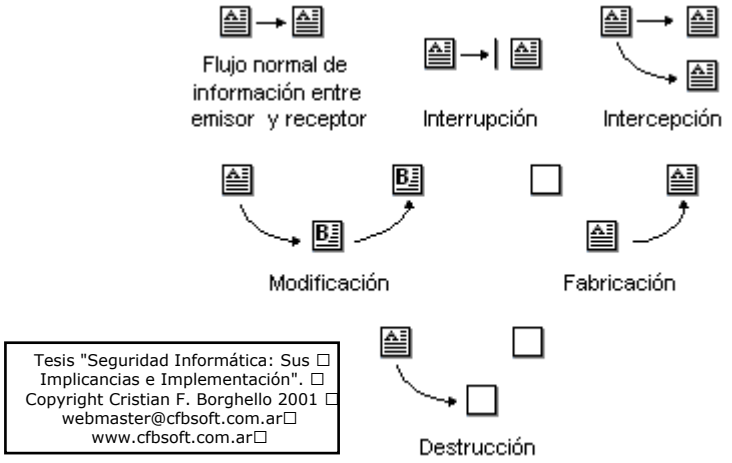


**Gráfico 1.3 – Tipos de Ataques Activos. Fuente:** HOWARD, John D. Thesis: An Analysis of security on the Internet 1989–1995. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. *http://www.cert.org*. Capítulo 6–Página 59.

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

## 1.2.5 RELACIÓN OPERATIVIDAD–SEGURIDAD

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

Para ilustrar lo antes dicho imaginemos una computadora “extremadamente” segura:

- Instalada a 20 metros bajo tierra en un recinto de hormigón.
- Aislada informáticamente de otras computadoras.
- Aislada eléctricamente y alimentada por un sistema autónomo de triple reemplazo.

Ahora imaginemos la utilidad de está “súper segura” computadora: tendiente a nula.

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

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

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

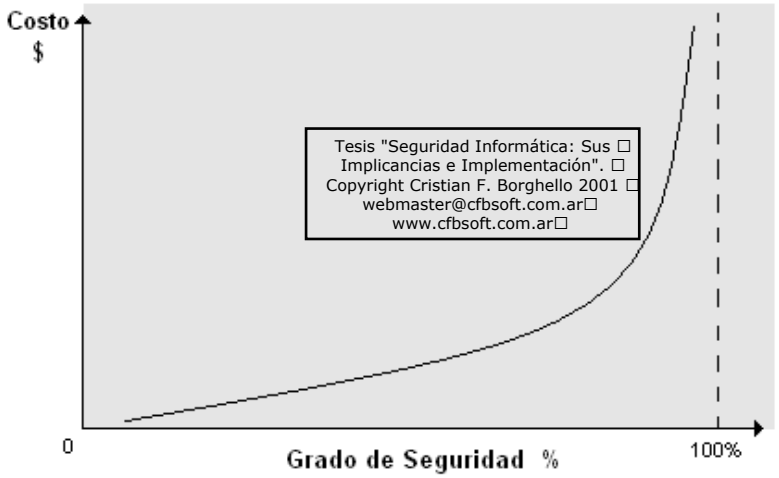


**Gráfico 1.4 – Relación Operatividad–Seguridad. Fuente:** ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1° Edición. Argentina. 1997. Página 26

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

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

Para ubicarnos en la vida real, veamos los datos obtenidos en marzo de 2001 por la consultora Ernst & Young[8] sobre 273 empresas de distintos sectores de actividad y países.

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



[8] "Encuesta de Seguridad Informática 2001". Marzo 2001. *http://www.ey.com*