Unidad 1

SEGURIDAD EN LOS SISTEMAS

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 computadoras, 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.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

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.

Valor y Protección de la Información

La información es hoy en día considerada como un bien activo en la organización; de un importante valor económico no tangible, por lo que se hace necesaria la instalación de controles destinados a su protección.

La información está sujeta a determinadas contingencias que pueden afectar las propiedades que la caracterizan. Estas propiedades se refieren a su *INTEGRIDAD, OPERATIVIDAD, CONFIDENCIALIDAD , Y AUTENTICIDAD.*

Por INTEGRIDAD entendemos la característica que asegura que su contenido permanezca invariable a menos que sea modificado por una personas y/o procesos debidamente autorizados. Podríamos decir que la integridad existe cuando la información no difiere de la contenida en sus documentos originales y no ha sido accidentalmente o maliciosamente alterada o destruida.

Por OPERATIVIDAD O DISPONIBILIDAD entenderemos la capacidad de tenerla accesible para ser procesada y/o consultada. Esto requiere que esté correctamente almacenada en los formatos preestablecidos y que el hardware que lo contiene funcione adecuadamente.

Por CONFIDENCIALIDAD O PRIVACIDAD la necesidad de que la información sea sólo conocida por personas y/o procesos debidamente autorizados.

Y Por AUTENTICIDAD debemos entender la propiedad de poder reconocer y certificar el origen y destino de la información, como así la documentación que la sustenta. Podemos corroborar que una entidad, ya sea de origen o destino de la información, es la deseada.

Las contingencias pueden ser de carácter intencional o accidental y pueden ser categorizadas en actos de naturaleza, errores u omisiones, actos fraudulentos y daño intencional ocasionado por los individuos. En base a ello podemos ensayar una clasificación por el origen de la contingencia en:

Contingencias de Origen Natural (CONTINGENCIAS NATURALES) producidas por fenómenos naturales, climatológicos o tectónicos. Incendios forestales, inundaciones, tormentas eléctricas, terremotos, maremotos, etc.

Contingencias de Origen Técnico (CONTINGENCIAS TECNICAS) las que podremos subdividir en *Contingencias de Origen Técnico vinculadas directamente con el sistema informático* (Fallas de Hardware -disco rígido, fuente de alimentación, fallas en las impresoras, en los modems, en el monitor; Fallas de Software - incompatibilidades de librerías, conflictos en el uso de recursos, errores de programación); y *Contingencias de Origen Técnico no vinculadas directamente con el sistema informático* (Fallas en la red de Energía Eléctrica, fallas en los sistemas de climatización, proximidad a sistemas generadores de campos electromagnéticos - motores, ascensores-, fallas en sistemas de distribución de fluidos -gases o líquidos - por explosiones, humedad)

Contingencias de Origen Humano (CONTINGENCIAS HUMANAS) ocasionadas por la interacción entre el hombre y el sistema informático, puede tratarse de hechos fortuitos o no; que actúan contra el recurso físico o lógico (datos erróneos, alteración de programas, destrucción de periféricos, virus informáticos, negación de servicios).

La protección de un sistema informático nunca podrá alcanzar una cobertura del 100 x 100.

Ejemplo de factores de riesgo

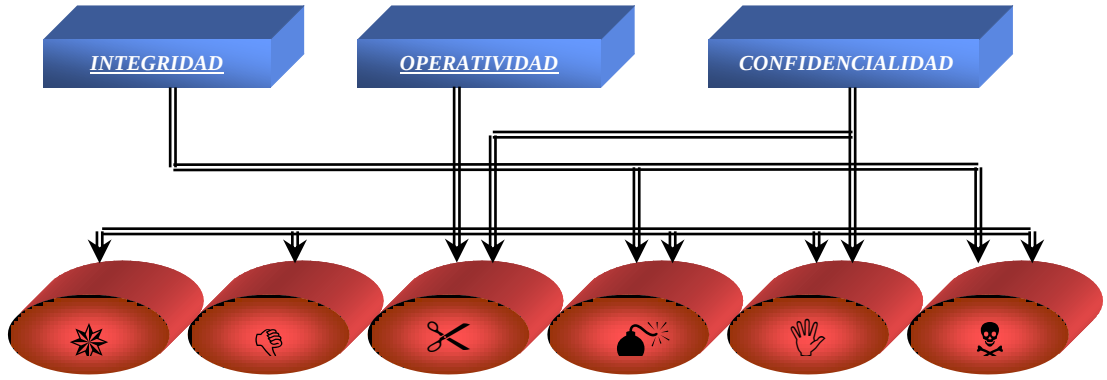
Se debe analizar en forma concienzuda todos y cada uno de los Factores de riesgo que puedan afectar un sistema informático. Estos factores pueden ser de distintos tipos. A continuación se da una descripción de estos factores clasificados en tres categorías:

- **INTEGRIDAD**
  - **Sabotaje**
  - **Virus Informáticos**
- **OPERATIVIDAD**
  - **Catástrofe climática**
  - **Incendio**
  - **Hurto**

- **Sabotaje**
- **Intrusión**
- **Virus Informáticos**

➢ **CONFIDENCIALIDAD**

- **Hurto**
- **Intrusión**



La Protección de la Información disminuye la operatividad

La seguridad informática es siempre, en alguna medida, restrictiva de la Operatividad.

Ejm Si se requiere que determinada información de una empresa sea sólo conocida por los gerentes, es lógico generar un mecanismo que impida el acceso del resto de los empleados y que los gerentes deban hacer algún tipo de operación adicional para acceder a ella (como por ejemplo identificarse).

Ejm Cuando se instala un programa antivirus, éste ocupa lugar en el disco rígido, e la memoria y consume tiempo de procesamiento, inclusive su operación periódica y su mantenimiento llevará tiempo.

Los anteriores son sólo dos ejemplos que aclaran la idea de que cualquier tipo de elemento de protección que se utilice restringirá la Operatividad de alguna manera.

Por lo tanto, es una ley fundamental de la seguridad informática que "si se aumenta la seguridad de un sistema informático, forzosamente se disminuye la operatividad".

Seguridad informática y Operatividad

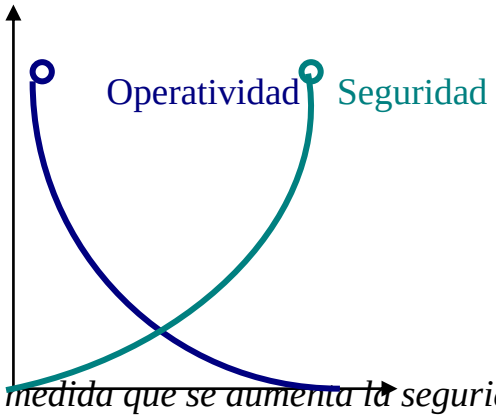


FIGURA *A medida que se aumenta la seguridad de un sistema*

informático se disminuye su Operatividad, por lo que son inversamente proporcionales. Esta es una de las leyes fundamentales de la seguridad informática.

CONCEPTO DE SEGURIDAD ACTIVA Y PASIVASEGURIDAD ACTIVA:

Es el conjunto de todos aquellos elementos que contribuyen a proporcionar una mayor eficacia y estabilidad al SISTEMA, en la medida de lo posible, para evitar CONTINGENCIAS O INCONVENIENTES.

Así tenemos como ejemplos: EN UN AUTO, SEGURIDAD ACTIVA es el Sistema de Frenos, Sistema de Dirección, Sistema de Suspensión entre otros. SEGURIDAD PASIVA: son los elementos que reducen al mínimo los daños que se pueden producir cuando el accidente es inevitable. Así tenemos como ejemplo: cinturón de seguridad y airbags.

Repercusión de las infracciones de seguridad

Las infracciones de seguridad afectan a las organizaciones de diversas formas. Con

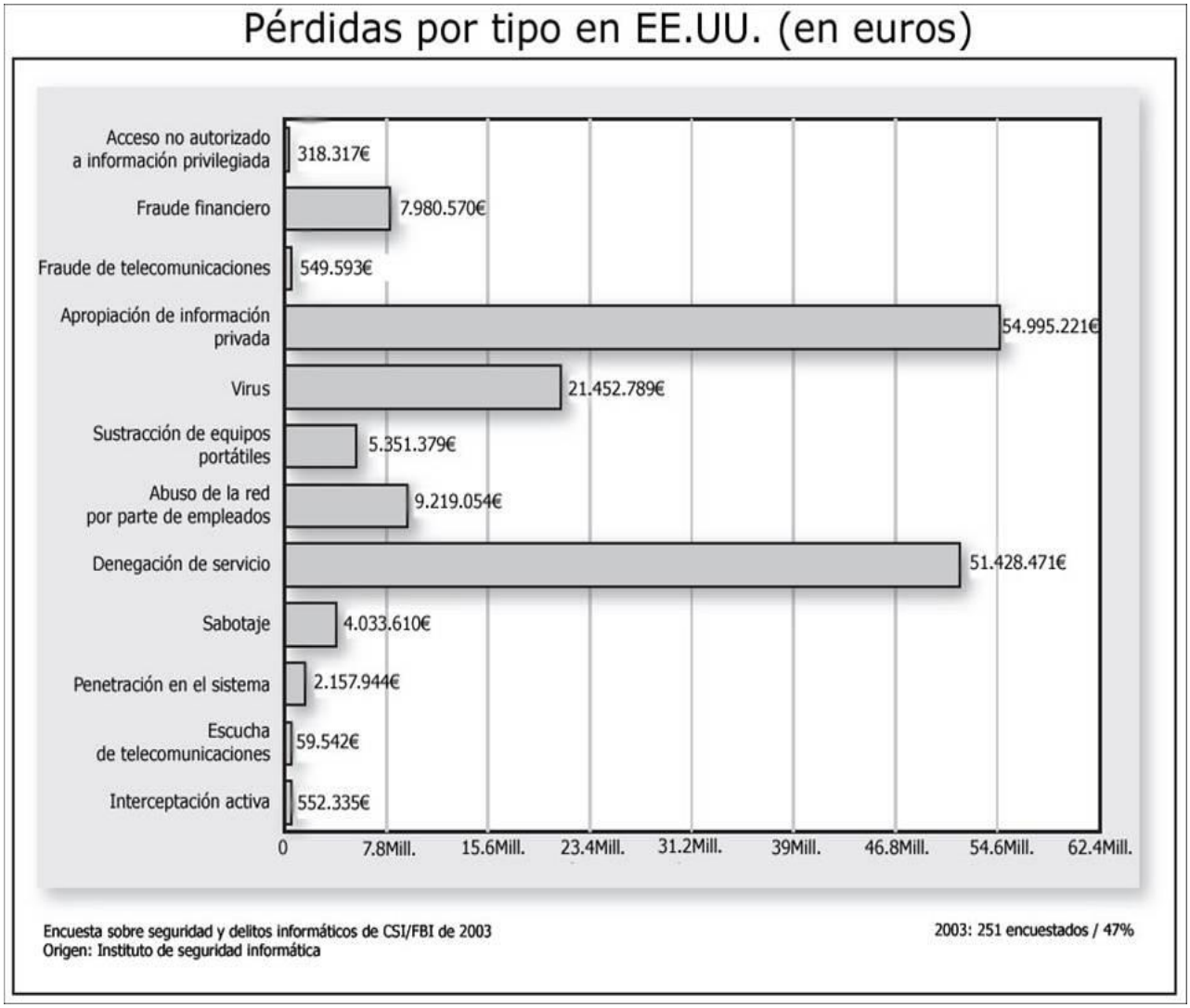
frecuencia, tienen los resultados siguientes:

- Pérdida de beneficios
- Perjuicio de la reputación de la organización
- Pérdida o compromiso de la seguridad de los datos
- Interrupción de los procesos empresariales
- Deterioro de la confianza del cliente
- Deterioro de la confianza del inversor
- Consecuencias legales: en muchos estados o países, la incapacidad de proteger un sistema tiene consecuencias legales;

Las infracciones de seguridad tienen efectos de gran repercusión. Cuando existe una debilidad en la seguridad, ya sea real o sólo una percepción, la organización debe emprender acciones inmediatas para garantizar su eliminación y que los daños queden restringidos.

- Muchas organizaciones tienen ahora servicios expuestos a los clientes, como los sitios Web. Los clientes pueden ser los primeros en observar el resultado de un ataque. Por lo tanto, es esencial que la parte de una compañía que se expone al cliente sea lo más segura posible.

Encuesta de CSI/FBI



- El costo de la implementación de medidas de seguridad no es trivial; sin embargo, sólo es una fracción del costo que supone mitigar un incidente de seguridad.
- La encuesta más reciente sobre seguridad y delitos informáticos del Instituto de seguridad de equipos y de la Oficina Federal de Investigación (CSI/FBI, Computer Security Institute/Federal Bureau of Investigation) de Estados Unidos, incluye cifras interesantes relativas a las pérdidas financieras que suponen los ataques a equipos para las organizaciones que los sufren.
- La encuesta demuestra que los ataques de denegación de servicio (DoS, Denial Of Service) y de robo de información son los responsables de las mayores pérdidas.
- En consecuencia, es importante saber que aunque el costo de la implementación de sistemas de protección de la seguridad no es trivial, supone una fracción del costo que conlleva mitigar los compromisos de la seguridad.
- La solución de seguridad más efectiva es la creación de un entorno en niveles de modo que se pueda aislar un posible ataque llevado a cabo en uno de ellos. Un ataque tendría que poner en peligro varios niveles para lograr su propósito. Esto se conoce como defensa en profundidad.