Tema 1. Fundamentos teóricos

1.1 Introducción

Desde el comienzo mismo del desarrollo de la humanidad, la comunicación, en cualquier forma que esta se presentase, ha resultado indispensable para el crecimiento y avance de cada aspecto de la civilización humana, pasando en su evolución por diferentes niveles de desarrollo de acuerdo con cada etapa en particular.

El desarrollo de las comunicaciones, auspiciado por los avances en electrónica de la mitad del siglo XX, ha propiciado desde entonces la evolución de la comunicación a distancia, así como diversas técnicas para garantizar su confidencialidad e integridad, entre otras.

A raíz del impetuoso avance de tecnologías tales como las telecomunicaciones, la información ha sufrido una radical transformación que permite observarla no sólo en cuestión de una comunidad o nación en particular, sino como un fenómeno de alcance mundial que precisa de normas reguladoras que protejan información sensible e importante.

Dentro de este indetenible desarrollo de la tecnología de la información, el uso de "Internet" juega un papel preponderante. Concebida originalmente como un proyecto de aplicaciones militares, su desarrollo fue rápidamente conglomerando computadoras enlazadas entre sí mediante protocolos de comunicación; perdiendo así su carácter militar para convertirse en una red global de comunicación, información, educación y ocio, entre muchas otras, a distancia.

La utilización masiva de computadoras y redes como dispositivos de almacenamiento, transferencia y procesamiento de información se ha incrementado exponencialmente en los últimos años, llegando a convertirse en un elemento indispensable en la sociedad actual; consecuentemente, la información en cualquiera de sus formas se ha convertido en un activo de gran valor e importancia que debe ser protegido y resguardado de influencias dañinas provenientes tanto del exterior como del interior y en cualquier forma que ésta se presente. Es por ello, que a continuación presentamos una serie de definiciones, normas y ejemplos que nos ayudarán a comprender mejor el mundo de la seguridad informática.

1.2 Concepto de seguridad informática

La seguridad informática es aquella disciplina que se relaciona a técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios. [1]

Técnicamente es imposible lograr un sistema informático cien por ciento seguro, pero buenas medidas de seguridad evitan daños y problemas que puedan ocasionar intrusos.

[1] "Introducción a la seguridad informática" en http://es.kioskea.net/contents/secu/secuintro.php3, 12/09/2009.

1.2.1 Seguridad con respecto a la naturaleza de la amenaza

Existen dos tipos de seguridad con respecto a la naturaleza de la amenaza:

- Seguridad lógica. Es la aplicación de procedimientos adecuados para evitar el acceso a los recursos del sistema por parte de personas no autorizadas, ya sea a nivel local o vía red. Ejemplos de lo anterior son las aplicaciones para seguridad, herramientas informáticas, por citar algunos. [2] (Véase figura 1.)

Figura 1. Logos de algunos de los más importantes antivirus del mercado, los antivirus son esenciales en cuanto a la seguridad lógica de un equipo se refiere. [3]

- Seguridad física. Se refiere a los controles y mecanismos de seguridad implementados para proteger el hardware y medios de almacenamiento de datos. Por ejemplo, el mantenimiento de las instalaciones eléctricas y anti-incendio, prevención de la humedad, entre muchos otros. [4] (Véase figura 2.)

Figura 2. Componentes básicos de un sistema anti-incendio, detectores de humo, extintor de polvo, manta ignífuga. [5]

[2] "Definición de Seguridad informática" en http://www.alegsa.com.ar/Dic/seguridad%20informatica.php, 12/09/2009.
[3] Tomada de http://www.blog.agenciabanana.com/programas/122-antivirus-.html
[4] "Definición de Seguridad informática" en http://www.alegsa.com.ar/Dic/seguridad%20informatica.php, 12/09/2009.
[5] Tomada de http://www.inforsecuritel.com/default.php?cPath=1_101

1.2.2 Amenazas a la seguridad de un sistema informático

- Programas malignos. Virus, gusanos, *phising*, *spamming*, sólo por mencionar algunos.

- Siniestros. Robos, incendios, humedad, entre otros, pueden provocar pérdida de información.

- Intrusos o piratas informáticos pueden acceder remotamente (en el caso de que se esté conectado a una red) o físicamente a un sistema para provocar daños.

- Usuarios. Los mismos usuarios de un sistema pueden debilitar y ser una amenaza a la seguridad de un sistema, no sólo por boicot, sino también por falta de capacitación o desidia. [6] (Véase figura 3.)

Figura 3. Muchas veces son los mismos usuarios autorizados la mayor amenaza de un sistema de información. [7]

1.3 Objetivos de la seguridad informática

Generalmente, la seguridad informática consiste en garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto.

Los objetivos de la seguridad informática se pueden resumir en la garantía de los seis servicios de seguridad:

- Integridad. Garantizar que los datos sean los que se supone que son.

- Confidencialidad. Asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.

- Disponibilidad. Garantizar el correcto funcionamiento de los sistemas de información.

- No repudio. Certificar que una operación realizada no pueda ser negada.

[6] "Introducción a la seguridad informática" en http://es.kioskea.net/contents/secu/secuintro.php3, 12/09/2009.
[7] Tomada de http://www.tomandang.com/blog/images/smashedComputer.jpg

- Control de acceso. Avalar que sólo los individuos autorizados tengan acceso a los recursos. (Véase Figura 4.)

- Autenticación. Verificar que los individuos sean quienes dicen ser. [8]

Figura 4. La lectura de la huella digital es un medio para autenticar la identidad de una persona. [9]

Como ya se mencionó, los puntos anteriores tienen el objetivo de proteger los activos de las organizaciones. Son tres los elementos que los conforman:

- Información. Es el objeto de mayor valor para una organización, el objetivo es el reguardo de la misma, independientemente del lugar en donde se encuentre registrada, en algún medio electrónico o físico.

- Equipos. Software, hardware y organización.

- Usuario. Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información. [10]

1.4 Amenazas y vulnerabilidades

1.4.1 Conceptos

Por vulnerabilidad entendemos la exposición latente a un riesgo u amenaza. En el área de la informática existen varias amenazas tales como: ataque de virus, códigos maliciosos, gusanos, caballos de Troya y *hackers*. Con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y ahora las empresas deben enfrentar ataques de denegación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de *hackeo*, accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos. De lo anterior, podemos definir amenaza como un factor externo de riesgo, representado por la posibilidad de que ocurra

[8] "Introducción a la seguridad informática" en http://es.kioskea.net/contents/secu/secuintro.php3, 12/09/2009.
[9] Tomada de http://www.masternewmedia.org/es/2005/05/15/la_red_de_autoidentificacion_para.htm
[10] "Introducción a la seguridad informática" en http://es.kioskea.net/contents/secu/secuintro.php3, 12/09/2009.

un fenómeno o evento adverso que podría generar daño parcial o total en bienes o en los servicios. [11]

1.4.2 Clasificación de amenazas y vulnerabilidades

Las amenazas y vulnerabilidad se clasifican como sigue:

A. Fuentes de amenazas

Las amenazas provienen de cinco fuentes principales:

- Desastres naturales. Popularmente conocidos como actos de Dios debido a que el hombre no puede controlar su ocurrencia ni predecirlos; son desastres naturales los huracanes, terremotos, maremotos, por ejemplo.

- Errores de hardware. Se refieren a las fallas físicas en cualquiera de los dispositivos involucrados; la falla puede ser parcial o total.

- Errores de software. Se refieren a las posibles fallas debido a incorrectas implementaciones en el sistema o a vulnerabilidades en el código fuente del software, aquí intervienen los códigos maliciosos (virus, gusanos, caballos de Troya, entre otros) que explotan dichas vulnerabilidades.

- Errores de red. Se presentan debido a un mal diseño, uso o implementación de la vía de comunicación informática.

- Humana. Se presenta por la ignorancia, diversión, descuido, malicia o indiferencia del usuario. [12]

B. Tipos de vulnerabilidades

Los tipos de vulnerabilidades, de manera muy similar a las amenazas, se clasifican como sigue:

- Desastres naturales. Se refiere al grado en que cierto sistema pudiera verse afectado por algún incidente natural. Se podría contar como una vulnerabilidad de este tipo cuando no se contara con un sistema adecuado de ventilación y nuestros equipos trabajen en condiciones climáticas adversas como podría ser un clima caluroso y húmedo.

- De Hardware. Se trata de la utilización de equipo en mal estado, inadecuado para el trabajo o bajo condiciones que no son las propicias. Como ejemplo, podemos considerar el uso de equipo de cómputo sin el uso de regulador en una zona con altas variaciones de voltaje.

[11] María Jaquelina López Barrientos, Cintia Quezada Reyes, *Fundamentos de seguridad informática*, México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2006. p. 90.
[12] *Idem*, p. 91.

- De Software. Entendemos que existe vulnerabilidad de software cuando se emplean aplicaciones con carencias a nivel de programación que las hacen más susceptibles a ser atacadas exitosamente, este tipo de vulnerabilidades también engloban a los sistemas operativos. Un ejemplo son las páginas Web que requieren autenticación por parte de sus usuarios y que no cuentan con protección contra ataques de tipo *sql injection:* un usuario maligno podría ver, modificar o aun borrar su base de datos.

- De Red. Al conectar cualquier equipo a una red, se incrementa de forma exponencial el riesgo al que estará expuesto, y es que aumenta el número de personas que podrían tener acceso a él ya sea de forma legítima o no. Además, una pobre implementación en la estructura y diseño del cableado estructurado de la misma podría llevar a su colapso con todas sus implicaciones.

- Humana. Se refiere al papel que juegan los usuarios o personal, cuando por desidia, malestar, diversión, ignorancia o simple ocio, comprometen la seguridad del sistema. No contar con un departamento de recursos humanos eficiente, reglamento claro y a la vista de todos, no capacitar a nuestros usuarios o empleados para que eviten ciertas prácticas riesgosas, así como el no contar con un sistema de control de acceso a las instalaciones, son fuentes de vulnerabilidad humana.

- Física. Esta se refiere al emplazamiento en el cual se encuentra el equipo informático, un ejemplo de vulnerabilidad física podría ser, por ejemplo, el no considerar que el edificio en el que se instalará nuestro sistema tenga cimientos firmes, si cuenta con un sistema contra incendios adecuado, entre otros. [13]

1.5 Políticas de seguridad

Actualmente la importancia que la información tiene dentro de una organización es sumamente grande. Las necesidades y retos que las empresas deben satisfacer en este rubro cambian constantemente a la par de la evolución de los medios de transmisión existentes, de las peticiones de sus clientes o de sus socios.

Una de las tareas clave dentro de las organizaciones debe ser proteger su información de riesgos que comprometan su integridad, confidencialidad o disponibilidad, esto a través de normas o políticas dirigidas tanto a los sistemas que manipulan los datos como a cada uno de los miembros de la empresa.

Una política de seguridad es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma. [14]

[13] *Idem*, pp. 100-103.
[14] *Idem*, pp. 127-131.

Al redactarse debe considerarse la visión de la empresa involucrada, las potenciales amenazas a las que la información de ésta estará expuesta y, sobre todo, debe ser escrita en un lenguaje que todos y cada uno de los miembros de la organización entiendan. Además, debe atender a cada uno de los principios siguientes:

- Responsabilidad individual. Los miembros de la organización deben estar conscientes de todas sus actividades, ya que éstas serán registradas y examinadas.

- Autorización. Son las reglas que especifican quién, cuándo y cómo puede acceder a la información.

- Mínimo privilegio. Los miembros de la organización deben tener los permisos mínimos necesarios para realizar sus funciones.

- Separación de obligaciones. Las funciones deben estar divididas entre todo el personal relacionado con la misma actividad o función.

- Auditoría. Las actividades del personal deben ser monitoreadas desde el inicio y hasta su término.

- Redundancia. Deben guardarse varias copias de información importante en varios lugares.

- Reducción de riesgo. Se debe reducir, dentro de lo posible, todos los riesgos a un nivel aceptable. [15]

1.6 Normas de seguridad a través de la historia

1.6.1 ITIL

Desarrollado inicialmente en 1980 por el gobierno británico, ITIL (Information Technology Infrastructure Library) es un set de 8 libros (en su versión 2, liberada entre los años 2000 y 2001) que describe conceptos y buenas prácticas concernientes a la administración, desarrollo y operación de las tecnologías de la información. [16]

Cada volumen cubre un área específica de la gestión de servicios:

- Soporte al servicio.

- Provisión del servicio.

- Administración de la infraestructura de las tecnologías de la información y comunicaciones.

[15] *Idem*.
[16] "What is ITIL?" en http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx, 01/05/2011.

- Administración de la seguridad.
- La perspectiva de negocio.
- Administración de las aplicaciones. Señala buenas prácticas
- Administración de los activos de software.
- Planificación para implementar la administración de los servicios.

A. Administración de la seguridad en ITIL

La conforman los siguientes 6 procesos.

- Control. Define los procesos subsiguientes, la asignación de responsabilidades, las políticas y el marco de la administración en general.
- Planeación. Detallas las medidas a tomar para elaborar los planes de seguridad correspondientes a cada unidad de las organizaciones.
- Implementación. Tiene el fin de asegurar que todas las medidas especificadas en el subproceso anterior sean implementadas correctamente.
- Evaluación. Mide el éxito en la implementación de los planes de seguridad.
- Mantenimiento. Evalúa la posible actualización de los riesgos de seguridad debida a cambios en la infraestructura de las tecnologías de la información o en la misma organización.
- Modelo completo procesos-datos. Documenta la integración de todos los subprocesos y, por lo tanto, de la infraestructura de seguridad implementada. [17]

1.6.2 TCSEC

TCSEC (Trusted Computer System Evaluation Criteria), también conocido como "Libro Naranja", es un estándar desarrollado en 1983 por el Departamento de Defensa de los Estados Unidos que tiene como objetivo establecer los requerimientos mínimos necesarios para evaluar la seguridad de un sistema computacional dedicado a almacenar y procesar información clasificada. [18] (Véase figura 5.)

Define siete criterios de evaluación y en cada uno de ellos se considera la política de seguridad, la rendición de cuentas, el aseguramiento y la documentación:

[17] *Ídem.*
[18] "TCSEC" en https://www.ccn-cert.cni.es/publico/2008/401/es/t/tcsec.htm, 17/09/2011.

- Clase D: protección mínima.
- Clase C: protección discrecional.
  i. C1: protección de seguridad discrecional.
  ii. C2: protección de acceso controlado.
- Clase B: protección obligatoria.
  i. B1: protección de seguridad etiquetada.
  ii. B2: protección estructurada.
  iii. B3: dominios de seguridad.
- Clase A: protección verificada.
  i. A1: diseño verificado. [19]

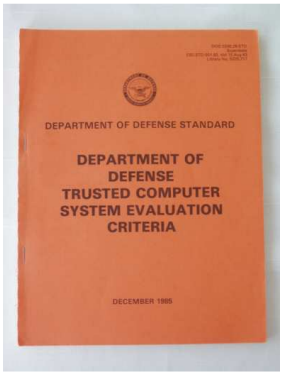


Figura 5. Portada de la norma TCSEC o "libro naranja". [20]

1.6.3 ITSEC

ITSEC (Information Technology Security Evaluation Criteria) es otro de los estándares existentes para la evaluación de la seguridad dentro de productos y sistemas. Fue publicado en conjunto por Francia, Alemania, Holanda y el Reino Unido en 1990 y la validez de criterios de su versión 1.2 fue reconocida por la Unión Europea en 1991. [21]

Las características de seguridad del producto a ser evaluado (llamado objetivo de evaluación) son sometidas a un gran número de pruebas funcionales y de penetración, cuyo nivel de exigencia irá creciendo de acuerdo con el nivel de

[19] "Trusted Computer System Evaluation Criteria, Orange Book" en http://nsi.org/Library/Compsec/orangebo.txt, 17/09/2011.
[20] Tomada de http://upload.wikimedia.org/wikipedia/en/4/4f/Orange-book-small.PNG
[21] "Information Technology Security Evaluation Criteria (ITSEC)" en http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf, 18/09/2009.

confianza certificada que el objetivo desee. Estos niveles de exigencia están definidos en 7 criterios de evaluación denotados desde E0 hasta E6 y en cada uno de ellos se consideran los puntos siguientes:

- Construcción. El proceso de desarrollo.
  i. Fase 1. Requerimientos.
  ii. Fase 2. Diseño de arquitectura.
  iii. Fase 3. Diseño Detallado.
  iv. Fase 4. Implementación.
- Construcción. El entorno de desarrollo.
  i. Aspecto 1. Control de configuración.
  ii. Aspecto 2. Lenguajes de programación y compiladores.
  iii. Aspecto 3. Seguridad de los desarrolladores.
- Operación. La documentación operacional.
  i. Aspecto 1. Documentación de usuario.
  ii. Aspecto 2. Documentación de administrador.
- Operación. El entorno operacional.
  i. Aspecto 1. Envío y configuración.
  ii. Aspecto 2. Puesta en marcha y operación. [22]

1.6.4 COBIT

COBIT (Control Objectives for Information and related Technology), liberada originalmente en 1996 por la Asociación de Auditoría y Control de los Sistemas de Información, es un conjunto de buenas prácticas para la administración de las tecnologías de la información. [23]

Clasifica sus procesos en 4 dominios:

[22] *Ídem*.
[23] "COBIT Framework for IT Governance and Control" en http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx, 01/05/2011.

- Planificación y organización. Define la estrategia a seguir en el área de los sistemas de información, con la finalidad de proveer eficientemente los servicios que las diferentes áreas de negocio de las organizaciones requieran.

- Adquisición e implementación. Busca garantizar que la compra de aplicaciones comerciales, desarrollo de herramientas, la implementación y el mantenimiento de ambas se encuentre alineado con las necesidades del negocio.

- Entrega y soporte. Busca asegurar la eficiencia y la eficacia en la entrega de los servicios que las organizaciones requieren.

- Supervisión y evaluación. Se centra en validar la alineación de los sistemas de acuerdo a la estrategia del negocio y paralelamente, incluye la verificación de los controles por parte de auditores internos o externos. [24]

1.6.5 CTCPEC

CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) es un estándar de seguridad canadiense que combina las aproximaciones y conceptos de TCSEC e ITSEC. Aborda tanto la funcionalidad como la confiabilidad de los productos a desarrollar o evaluar. [25]

- Funcionalidad. Proporciona las bases para desarrollar un método de especificación para productos de cómputo confiables y funcionales. Evalúa la efectividad de los servicios siguientes:

  i. Confidencialidad.

  ii. Integridad.

  iii. Disponibilidad.

  iv. Auditoría.

- Confiabilidad. Verifica la correcta implementación del producto basándose en las políticas de seguridad. Evalúa los siguientes requerimientos:

  i. Arquitectura.

  ii. Desarrollo ambiental.

  iii. Desarrollo de evidencias.

[24] *Ídem.*
[25] "Estándares de evaluación para sistemas de cómputo seguros" en http://mixtli.utm.mx/Estandares_de_Evaluacion_para_Sistemas_de_Computo_Seguros.ppt, 19/09/2009.

iv. Ambiente operacional.

v. Documentación.

vi. Seguridad.

vii. Seguridad en las pruebas. [26]

1.6.6 Criterios comunes

Los criterios comunes para la evaluación de seguridad de las tecnologías de la información, son una norma internacional basada en los criterios europeos, norteamericanos y canadienses existentes en el tema. Los resultados obtenidos al realizar una evaluación de este tipo son reconocidos internacionalmente. [27] (Véase figura 6.)

Especifican una evaluación de niveles de confianza para los productos y cada uno de éstos provee a consumidores, desarrolladores y evaluadores la información necesaria para determinar las necesidades de seguridad de los productos a adquirir, cubrir los requerimientos de los consumidores en el proceso de desarrollo de una aplicación o determinar el nivel de seguridad que ha alcanzado un producto.

Los niveles de aseguramiento dentro de los criterios comunes son los siguientes:

- EAL1. Es el nivel más bajo tanto para el desarrollador como para el usuario. Se basa en el análisis de las funciones de seguridad del producto, tal como son presentadas por el mismo.

- EAL2. Es el nivel de aseguramiento más alto que se le puede otorgar al desarrollador sin imponerle tareas adicionales. Un software de excelente calidad recibe esta certificación.

- EAL3. Es el nivel moderado de seguridad independiente y lo realiza una fuente externa. La seguridad se toma en cuenta desde la fase de diseño, no solamente cuando el producto está terminado.

- EAL4. Es el nivel de aseguramiento más alto, en el que es factible reparar una línea de productos ya existentes. En este nivel, un producto es diseñado, probado y revisado metódicamente. Dispone también de una búsqueda de puntos vulnerables.

- EAL5. No es común que los productos ya existentes alcancen esta clasificación, ya que deben ser diseñados con tal fin. El desarrollador debe de dar un enfoque riguroso de seguridad, teniendo en cuenta las especificaciones de diseño y su modo funcional en el producto.

[26] Ídem.
[27] María Jaquelina López Barrientos, Cintia Quezada Reyes, Fundamentos de seguridad informática, México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2006. pp. 27-30.

- EAL6. Incluye todos los elementos del nivel EAL5, pero garantizando un alto grado de resistencia a ataques. Exige también:

  i. Proceso de desarrollo estructurado.

  ii. Controles de desarrollo.

  iii. Controles de manejo de comunicación.

- EAL7. Está destinado a aquellas aplicaciones de seguridad en las que el alto riesgo de violaciones y ataques justifiquen el alto costo de desarrollo. Es un proceso exhaustivo y la dependencia evaluadora debe participar desde la concepción de la idea hasta la finalización del proyecto. [28]

Figura 6. Logo de la norma "Criterios comunes". [29]

1.6.7 ISO 27002

Tiene sus orígenes en el estándar británico BS7799 publicado en 1995. En el año 2000 fue adoptado y publicado nuevamente por ISO/IEC como ISO 17799 y, tras ser objeto de una revisión en el año 2005, fue renombrado como ISO 27001. Con la finalidad de alinearlo al resto de los estándares de la serie 27000, en 2007 cambia su nombre a ISO 27002, que se mantiene en la actualidad. [30]

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No especifica los requisitos necesarios para el establecimiento de un sistema de certificación adecuado para este documento. Contiene 39 objetivos de control y 133 controles, agrupados en los siguientes 11 dominios:

- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad ligada al personal.
- Seguridad física y del entorno.

[28] *Ídem*, pp. 54-62.
[29] Tomada de http://www.cse.fau.edu/~maria/CommonCriteria_logo.gif
[30] "ISO 27000" en http://www.iso27000.es/iso27000.html, 21/09/2009.

- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de seguridad de la información.
- Gestión de continuidad de negocio.
- Conformidad. [31]

1.7 Servicios de seguridad

Un servicio de seguridad es "*aquel que mejora la seguridad de un sistema de información y el flujo de la información de una organización*" [32]. Tienen la finalidad de evitar ataques y utilizan uno o más mecanismos de seguridad para proveer el mismo.

Los servicios de seguridad se clasifican de la siguiente manera:

- Confidencialidad. Protegen la información y el almacenamiento de la misma para prevenir que nadie pueda leer, copiar o modificar la información sin los permisos necesarios para hacerlo.

  La forma más común de lograr los objetivos antes mencionados es mediante la utilización del cifrado basado en criptografía. (Véase figura 7.)

Figura 7. Ejemplo de funcionamiento de un método de cifrado. [33]

- Autenticación. Tiene la finalidad de asegurar que una comunicación es auténtica. Provee al sistema de una prueba de que realmente se es quien se pretende ser.

  Generalmente se realiza mediante:

[31] *Ídem.*
[32] María Jaquelina López Barrientos, Cintia Quezada Reyes, *Fundamentos de seguridad informática*, México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2006, p. 116.
[33] Tomada de http://www.itchetumal.edu.mx/paginasvar/Maestros/redes1/unidad9/unidad9.htm

i. Algo que se sabe: Por ejemplo, una contraseña o número de identificación personal que el sistema compara con una copia almacenada una vez que se ingresa.

ii. Algo que se tiene: Por ejemplo, una tarjeta que el sistema utilizará para verificar la identidad. (Véase figura 8.)

iii. Algo que se es: Cualquier parte biológica como, por ejemplo, la voz, la retina o una huella digital.

Figura 8. La credencial de elector es un ejemplo típico de una forma de autenticación. [34]

- Integridad. Permite asegurar que el contenido de los datos no haya sido modificado, si esta no se garantizara, entonces se corre el riesgo de que cualquier persona puede manipular los mismos según su conveniencia.

  Este servicio se relaciona más con la detección que con la prevención, ya que una vez que una violación de integridad es detectada, se necesita de la partición humana o de otro software para recuperarse de tal violación.

  Los mecanismos de seguridad de este tipo más utilizados son los siguientes:

  i. Código de detección de modificación. Es una suma de comprobación de los datos generada utilizando un algoritmo criptográfico.

  ii. Código de autenticación del mensaje. Es una suma de comprobación cifrada de los datos generada con base en la criptografía.

  iii. Firma digital. Es un tipo de información asociada con los datos que solamente puede ser creada por el firmante y puede ser verificada por cualquier persona. [35] (Véase figura 9.)

[34] Tomada de http://estafadoresdeinternet.blogspot.com/2009_04_02_archive.html
[35] María Jaquelina López Barrientos, Cintia Quezada Reyes, *Fundamentos de seguridad informática*, México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2006, pp. 120-122.

Figura 9. La firma digital puede vincularse a un documento para identificar al autor, para señalar conformidad o disconformidad, que no se ha modificado su contenido, etc. [36]

- No repudio. Previene a los emisores o a los receptores de negar un mensaje transmitido, se aplica al problema de la denegación falsa de la información que se recibe de otros o de la que alguien envía a otro. Se clasifican en los siguientes:

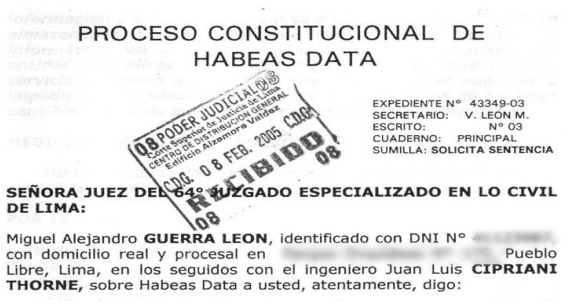
  i. De origen. Provee pruebas del origen de los datos para prevenir denegación falsa en el suministro.

  ii. De envío. Provee pruebas del envío de los datos para prevenir denegación falsa en la recepción.

  iii. De presentación. Provee pruebas de presentación de los datos para prevenir denegación de que la información fue presentada para el envío.

  iv. De transporte. Provee pruebas del transporte de los datos para prevenir que se niegue que los mismos fueron trasladados.

  v. De recepción. Provee pruebas de la recepción de los datos para prevenir que se niegue que la información ha sido recibida. [37] (Véase figura 10.)



PROCESO CONSTITUCIONAL DE HABEAS DATA

PODER JUDICIAL 08 FEB. 2005 RECIBIDO

EXPEDIENTE N° 43349-03
SECRETARIO: V. LEON M.
ESCRITO: N° 03
CUADERNO: PRINCIPAL
SUMILLA: **SOLICITA SENTENCIA**

SEÑORA JUEZ DEL 64° JUZGADO ESPECIALIZADO EN LO CIVIL DE LIMA:

Miguel Alejandro **GUERRA LEON**, identificado con DNI N° [redacted], con domicilio real y procesal en [redacted] Pueblo Libre, Lima, en los seguidos con el ingeniero Juan Luis **CIPRIANI THORNE,** sobre Habeas Data a usted, atentamente, digo:

Figura 10. El documento sellado impide se niegue haber recibido el documento, esto es una forma de no repudio de recepción. [38]

[36] Tomada de http://www.kimaldi.com/area_de_conocimiento/firma_digital/que_es_la_firma_digital.
[37] María Jaquelina López Barrientos, Cintia Quezada Reyes, *Fundamentos de seguridad informática*, México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2006, p. 122.

- Control de acceso. Es la habilidad para limitar y controlar el acceso a los sistemas y las aplicaciones mediante los puentes de comunicación. Para lograrlo, cada entidad que busca ingresar, debe autenticarse y así ganar los derechos de acceso que le correspondan. [39] (Véase figura 11.)

Figura 11. Una forma de control de acceso, mediante llave y cerradura. [40]

- Disponibilidad. Para prevenir que la información no esté disponible cuando se requiere, deben existir soluciones alternas con copias actualizadas de la información crítica y de los programas en un lugar diferente, además de un plan de continuidad que permita restablecer las operaciones a la brevedad. [41] (Véase figura 12.)

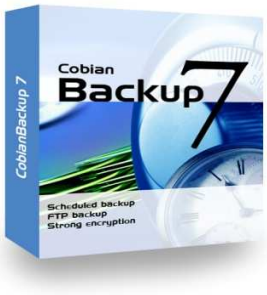


Figura 12. Realizar copias de seguridad de la información crítica garantiza su disponibilidad. [42]

[38] Tomada de http://www.gratisweb.com/miguelguerra/excomunion/habeasdata_3.htm
[39] "Definición de Seguridad informática" en http://www.alegsa.com.ar/Dic/seguridad%20informatica.php, 12/09/2009.
[40] Tomada de http://www.vidanuevalourdes.com/category/el-blog-de-alex/
[41] María Jaquelina López Barrientos, Cintia Quezada Reyes, *Fundamentos de seguridad informática*, México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2006, p. 125.
[42] Tomada de http://grupogeek.com/wp-content/uploads/2008/12/26-12-cobian-backup.jpg