SEGURIDAD INFORMATICA

Dra. Esc. María José Viega

1. Introducción

Quiero iniciar este tema con una frase de Reynaldo de la Fuente, quien en un trabajo sobre Aportes a la Seguridad y Privacidad en Informática y Comunicación de datos manifiesta que: "El mito de los computadores ha enmascarado al verdadero héroe de estos tiempos que es la información"[1].

Esta es una apreciación de relevancia en la medida que el análisis de la vulnerabilidades tecnológicas y las diferentes medidas que apuntan a lograr su seguridad, nos interesa desde el punto de vista de la protección de la información, de la integridad de la misma, ya sea a la hora de trasmitir documentos electrónicos, de celebrar contratos o de ejecutar los mismos.

La seguridad informática tiene como objetivo la protección del dato, lo que implica que el mismo mantenga la siguientes cualidades:

a) La integridad: implica que el contenido, ya sea que se encuentre en un computador o que circule a través de una red, permanezca inalterado. En caso de sufrir modificaciones que sea por persona autorizada y que exista en el sistema la constancia de esta modificación, que hará viable su control al realizarse auditorías.

[1] DE LA FUENTE Reynaldo. "Aportes a la Seguridad y Privacidad en Informática y Comunicación de Datos". Polo Ltda. 2da. Edición Actualizada. Montevideo, 1995.

b) La disponibilidad: u operatividad de la información es su capacidad de estar disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware o el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria[2].

c) La confidencialidad o privacidad: implica el conocimiento de la misma exclusivamente por las personas autorizadas. Esto se logra a través de control de acceso, sistemas criptográficos y métodos apropiados de conducción de las personas, los documentos y los medios de almacenamiento de datos.

Reynaldo de la Fuente clasifica las vulnerabilidades en:

1. Físicas: ingreso a los edificios y/o salas de computación sin autorización , formando puertas y cerraduras.

2. Naturales: las computadoras son vulnerables a desastres naturales como incendio, inundación, terremotos, un rayo o pérdida de la energía eléctrica, así como la suciedad, la humedad y las temperaturas extremas pueden causar daños a los datos.

3. Del hardware y el software: las fallas del hardware pueden comprometer la seguridad del sistema. Las fallas del software pueden abrir el sistema a ingresos no autorizados.

4. De dispositivos de almacenamiento de información: los disquetes, discos, cintas y listados pueden ser robados o dañados por distintas razones, perdiendo el contenido de la información.

5. De emanaciones electromagnéticas: emitidas por los equipos pueden ser interceptados por actividades de espionaje electrónicos.

[2] A.S.S. BORGHELLO, Cristian Fabián. Director de Tesis: Ing. GOTTLIEB Bernardo. Asesor científico: MINGO Graciela. “Tesis Licenciatura en Sistemas: Seguridad Informática sus implicancias e implementación”. Universidad Tecnológica Nacional. Setiembre, 2001. www.cfbsoft.com.ar

6. De comunicación de datos: los computadores conectados en red o que puedan ser accedidos por comunicaciones telefónicas incrementan el riesgo de ingresos no debidos. Respecto al envío de mensajes hay que tener en cuenta que los mismos pueden ser interceptados, mal ruteados y/o alterados.

7. Del factor humano: debemos distinguir aquí las conductas erróneas de las maliciosas. El error en el manejo del sistema puede alterar o borrar en forma perjudicial la información. Pero también hay que tener presente los delitos informáticos, sean realizados por personas externas o internas de la empresa.

La seguridad informática puede analizarse en tres instancias, antes del ataque, durante el mismo o después de la realización.

La prevención implica la utilización de mecanismos que aumentan la seguridad del sistema durante el funcionamiento normal. El cifrado de la información antes de trasmitirla es un mecanismo preventivo.

La detección son los mecanismos orientados a revelar violaciones a la seguridad que operan durante el ataque, normalmente mediante programas de auditoría.

La recuperación, que se opera después del ataque, son los mecanismos que permiten retornar el sistema al funcionamiento normal, como la recuperación de backup.

¿De quien nos protegemos?

En general nos protegemos de los intrusos, de aquellas personas que acceden sin autorización al sistema, a los que normalmente conocemos con el nombre de hackers.

Estos intrusos pueden ser de diferentes tipos[3]:

a) Clase A: 80 % son aquellos que bajan programas y realizan pruebas en Internet, no son peligrosos.

b) Clase B: 10 % son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, detectan el sistema operativo testean vulnerabilidades e ingresan por ellas.

C) Clase C: 7 % saben lo que hacen, tienen objetivos claros.

D) Clase D: 3 % ingresan buscando información que necesitan.

Los niveles de protección son cuatro[4]:

1º. Legal o ético: consiste en la protección provista por la legislación y la obligación moral que nuestra condición humana nos impone.

2º. Auditoria y controles del sistema informático: es la protección provista por las políticas, la organización y la metodología de contralor de las personas, los procedimientos operativos y los programas de aplicación.

3º. Seguridad física y ambiental: medios de protección contra incendios, robos, estado de las instalaciones.

4º. Seguridad lógica: protección prevista por dispositivos de hardware y software.

[3] ARDITA Julio Cesar. "Evitemos el Fraude electrónico". http://www.cybsec.com
[4] DE LA FUENTE Reynaldo. "Aportes a la Seguridad y Privacidad en Informática y Comunicación de Datos". Ob. Cit.

Es esta última clase de seguridad la que nos interesa abordar a los efectos del análisis del documento electrónico.

2. Principios de seguridad documental

Elementos de relevancia para la contratación electrónica:

Cuando realizamos un contrato en forma electrónica es de fundamental importancia que la transferencia de información sea un sistema seguro, para lo cual es importante tener en cuenta los siguientes elementos:

a) Confidencialidad: la comunicación no debe estar expuesta a terceras personas, ni permitir que estas comprendan el mensaje que se está trasmitiendo.

b) Integridad de la transacción: es importante tener la certeza que el mensaje trasmitido y recibido por la otra parte esté completo y no halla sufrido modificación alguna.

c) Identificación de las partes: debemos tener seguridad de quien es la persona con la cual nos estamos comunicando.

d) Seguridad de la transacción: Toda comunicación debe estar firmada, de forma tal que el negocio tenga expresado el consentimiento de forma inequívoca.

3. Diferentes tipos de firma

Firma ológrafa o tradicional: cuando una persona "firma" un documento en papel está manifestando su voluntad y lo que hace es dibujar sobre él una serie de símbolos que lo identifican.

Pablo Palazzi[5] define la firma como "*el trazo particular por el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad*".

[5] Palazzi, Pablo Andrés. "*Firma digital y comercio electrónico en Internet*". VI Congreso Iberoamericano de Derecho e Informática. Libro de Ponencias. Montevideo – Uruguay, l998.

La firma en este caso cumple diversas funciones, lo cual dependerá de la naturaleza del documento:

- Establecer la autoría del propio texto.
- Aceptar las obligaciones que surgen de un texto.
- Adherir a lo expresado por otro.
- Determinar la presencia del mismo

Cuando un Escribano certifica una firma lo que está asegurando es que la persona que firma es quien dice ser, que lo hizo libre y conscientemente, que firmó dicho documento en un lugar y día determinado.

Dice Palazzi[6] que: "*Si se encuentra un medio que reemplace a la firma ológrafa en ambientes digitales, éste nuevo medio deberá cumplir con las funciones tradicionales de la firma. Estas son: (i) indicativa: informa acerca de la identidad de un autor; (ii) declarativa: se refiere al acuerdo respecto al contenido del acto; (iii) probatoria: permite vincular al autor con el signatario*".

Firma electrónica: con relación a las diferentes técnicas utilizadas para firmar electrónicamente un documento, Guillermo Balay[7] describe las siguientes: "*Una técnica disponible es el uso de una tableta sensible y un lápiz magnético conectados a un PC donde se registra la presión, velocidad y coordenadas donde el operador apoya el lápiz. Esos datos se combinan matemáticamente para formar la "firma electrónica" de la persona. Posteriormente, se puede comparar esa firma almacenada con otra para verificar si pertenecen a la misma persona.*

Otra técnica de firma electrónica disponible en el mercado podría ser el registro de la huella digital y de ciertos factores biológicos de la piel que identifican unívocamente a la persona. El dispositivo consiste en un tablero donde la persona coloca su dedo. Allí se digitalizan la huella y los parámetros biológicos del dedo de la persona, de tal forma que es imposible reproducirlos salvo que se obligue a la persona a colocar su dedo en el dispositivo".

c) Firma digital: en sí misma es un dato (secuencia de bits) y el peligro radica en que una vez divulgado, cualquiera puede utilizarlo y hacerse pasar

[6] Idem cita anterior.
[7] Balay, Guillermo. "*Enfoque informático del Decreto N° 65/998*". Procedimiento administrativo electrónico. Presidencia de la República. Oficina Nacional del Servicio Civil. 1998.

por su titular. Para que esto no suceda, en la firma digital se utiliza lo que se denomina “criptografía de clave pública”.

4. Sistema de seguridad del documento informático

Los primeros esfuerzos realizados convergieron en torno a dotar al documento electrónico de una codificación que permitiese que su usuario se estimase protegido de los riesgos especialmente criminales, que pudiesen ejecutarse a su respecto; así desde un punto de vista jurídico, se recurrió a su protección penal y civil, desde el punto de vista técnico, se establecieron códigos secretos, conocidos sólo por el usuario, a objeto de impedir la violación documental[8].

Los códigos secretos o de ciframientos numéricos funcionan en base a un número de identificación (PIN personal identification number). El ejemplo más común es el de las tarjetas bancarias que funcionan en base a estas claves.

4.1 Biometría

La Biometría es la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivios utilizando métodos estadísticos. La biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de las personas. La forma de identificación consiste en la comparación de características físicas d cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz)[9].

[8] GAETE GONZALEZ Eugenio Alberto. “Instrumento público electrónico”. Editorial Bosch. España 2000.

[9] BORGHELLO Cristian Fabian. “Seguridad Informática. Sus implicancias e implementación”. Tesis Licenciatura en Sistemas. Universidad Tecnológica Nacional. Setiembre de 2001. Capítulo 2, página 11. www.cfbsoft.com.ar

Con relación a las diferentes técnicas utilizadas para firmar electrónicamente un documento, podemos distinguir[10]:

a) Una técnica disponible es el uso de una tableta sensible y un lápiz magnético conectados a un PC donde se registra la presión, velocidad y coordenadas donde el operador apoya el lápiz. Esos datos se combinan matemáticamente para formar la "firma electrónica" de la persona. Posteriormente, se puede comparar esa firma almacenada con otra para verificar si pertenecen a la misma persona[11].

b) Emisión de calor: se mide la emisión de calor de un cuerpo (termograma) realizando un mapa de valores sobre la forma de cada persona.

c) Otra técnica de firma electrónica disponible en el mercado podría ser el registro de la huella digital y de ciertos factores biológicos de la piel que identifican unívocamente a la persona. El dispositivo consiste en un tablero donde la persona coloca su dedo. Allí se digitalizan la huella y los parámetros biológicos del dedo de la persona, de tal forma que es imposible reproducirlos salvo que se obligue a la persona a colocar su dedo en el dispositivo[12].

d) Verificación de la voz: la dicción de una (o más) frase es grabada y en el acceso se compara la voz (entonación, agudeza, etc.). Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, envejecimiento, etc[13].

e) Verificación de patrones oculares: Estos modelos pueden ser basados en patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0). Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en los mismos enfermedades que en ocasiones se prefiere mantener en secreto.

4.2 Sistemas de Cifrado

[10] VIEGA María José. "Firma Digital". XIII Ciclo de Encuentros Técnicos Regionales". Rivera, 26 de julio de 2003. Edita Asociación de Escribanos del Uruguay.
[11] BALAY, Guillermo. "Enfoque informático del Decreto N° 65/998". Procedimiento administrativo electrónico. Presidencia de la República. Oficina Nacional del Servicio Civil. 1998.
[12] BALAY, Guillermo. "Enfoque informático del Decreto N° 65/998". Ob. Cit.
[13] BORGHELLO Cristian Fabian. "Seguridad Informática. Sus implicancias e implementación". Ob. Cit., Capítulo 2, página 12. www.cfbsoft.com.ar

Históricamente, podemos destacar los cifrados por sustitución y por transposición.

a) Cifrado por sustitución

Cada letra o grupo de letras se reemplaza por otra letra o grupo de letras.

Ejemplo: cifrado de César se basa en la rotación del alfabeto N caracteres, que originariamente eran tres.

Texto en claro a b c d e f g ..... z

Texto cifrado d e f g h i j k c

En el caso de sustitución monoalfabética cada letra se corresponde con otra arbitraria del alfabeto, existiendo entonces 26 claves diferentes. Se descifra fácilmente usando la frecuencia relativa de las letras.

c) Cifrado por transposición

Reordena las letras pero sin cambiarlas. Por ejemplo la transposición columnar, en la cual la clave es la palabra o frase que no contiene letras repetidas, enumerándose las columnas en el orden alfabético de las letras de la clave.

Es fácil descifrarlo conociendo la clave y ordenando las columnas.

Un ejemplo de cifrado por transposición es el siguiente[14]:

H I P O T E C A

4 5 7 6 8 3 2 1

p o r f a v o r

t r a n s f i e

r a d e m i c u

e n t a d o s m

i l l o n e s d

e d o l a r e s

Texto cifrado: reumdsoicssevfioerptreieoranldfneaolradloasmdna

4.3 Criptografía simétrica y asimétrica. Firma digital

La criptografía es la ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Es una rama de las matemáticas que procura hacer incomprensibles los mensajes, para que no puedan ser leídos por terceros, y luego tornarlos a su estado natural.

La criptografía es una rama de las Matemáticas -y en la actualidad de la Informática y la Telemática- que hace uso de métodos y técnicas matemáticas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a los criptosistemas que permiten asegurar cuatro aspectos fundamentales de la seguridad informática: confidencialidad, integridad, disponibilidad y no repudio de emisor y receptor[15].

[14] DI PASCUA Diego. "Introducción a la Criptografía". Presentación a cargo del Ing en el Servicio Central de Informática de la Universidad de la República.

[15] RAMIÓ AGUIRRE Jorge. "Curso de Seguridad Informática". Universidad Politécnica de Madrid.

Clasificación de los criptosistemas

Los criptosistemas pueden ser:

Según el tratamiento del mensaje se dividen en:

Cifrado en bloque (DES, IDEA, RSA: 64 - 128 bits)

Cifrado en flujo (A5) cifrado bit a bit

Según el tipo de claves se dividen en:

Cifrado con clave secreta

Cifrado con clave pública

Existen dos tipos de encriptamiento documental:

a) La criptografía simétrica o de clave secreta o llave única

Se caracteriza porque la persona que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave. Es una forma conocida también como simétrica.

Quien envía el mensaje codifica el texto utilizando la clave y al llegar al destinatario lo decodifica con la misma clave.

El sistema de criptografía simétrica, se denomina técnicamente, Data Encryption Standard, DES, y fue desarrollado en 1977 por la Agencia Nacional de Seguridad de los Estados Unidos de Norteamérica – National Security Agency, NSA- como un sistema de seguridad único, estandarizado, para la

administración pública norteamericana, y es hasta la actualidad el sistema más aplicado[16].

Para mejorar este sistema, se han utilizado hasta tres claves diferentes para encriptar partes del mensaje con diferentes claves, tornándose en un sistema de llave múltiple.

El peligro que acarrea es que normalmente las personas no se conocen personalmente, por lo tanto el canal para el envío de la clave debe ser un canal seguro.

Otra desventaja del sistema es que no puede asegurarse que el receptor del mensaje no lo modifique luego de desencriptarlo.

b) La criptografía asimétrica o de clave pública o doble llave

El sistema asimétrico fue desarrollado en Estados Unidos, en la Universidad de Stanford a partir del año 1975, por dos ingenieros electrónicos Whilfield Diffie y Martín Hellman.

Este tipo decodificación fue aplicado por el MIT (Massachussets Institute of Technology) a la firma electrónica y a la encriptación del documento electrónico.

No es necesario en esta caso un canal seguro para el envío de la clave, porque cada persona dispone de dos claves, una pública (conocida por todos) y otra privada (conocida únicamente por el titular).

Para encriptar el mensaje el remitente utiliza la clave pública del destinatario, de tal manera que solo el destinatario pueda descencriptarlo con su clave privada.

Con relación a la seguridad de este sistema el P/S Guillermo Balay[17] dice que: "*Ambas claves de un mismo usuario están relacionadas matemáticamente, pero es casi imposible calcular la clave privada a partir de la pública, aún conociendo el algoritmo empleado para construirlas*".

La desventaja del sistema radica en el factor tiempo, ya que el encriptado simétrico es muchísimo más rápido que el de criptografía asimétrica.

Por ello, en general, lo que se tiende a encriptar a través de este sistema son cortos mensajes, y principalmente la firma electrónica, para la cual como

[16] GAETE GONZALEZ Eugenio Alberto. "Instrumento público electrónico". Ob. Cit. Página 212.
[17] BALAY, Guillermo. "Enfoque informático del Decreto N° 65/998". Ob. Cit.

veremos, reporta grandes ventajas. No se presta, como el sistema DES para el ciframiento de documentos y menos, naturalmente, para el ciframiento de contratos, de suyo de gran extensión[18].

Este es el sistema utilizado en la firma digital, el emisor cifra el mensaje con la clave pública del receptor, y firma el mensaje aplicando su clave privada; el receptor del mensaje utiliza su clave privada para descifrar el mensaje y la clave pública del emisor para verificar la firma digital.

El sistema no permite que ni el remitente ni el destinatario realicen cambios en el documentos, porque el remitente, después de encriptarlo con la clave pública del destinatario no puede desencriptarlo.

c) Sistema asimétrico con utilización de código Hash

El sistema asimétrico requiere de un Tercero que provee el servicio , al que se le conoce con el nombre de Autoridad Certificadora. Este tercero es quien emite los certificados digitales, los cuales constituyen un resumen con los requisitos exigidos por las leyes de firma digital.

Este certificado, será normalmente el que estará cubierto con el código Hash, que utiliza una función matemática consistente en crear una representación numérica para todo el certificado, de tal forma que éste pasa a ser representado por un valor numérico o cadena de datos. Así por ejemplo la palabra documento estará representada por un valor por cada letra[19]:

D o c u m e n t o
3 7 2 9 5 4 6 8 7

El emisor codifica el mensaje con la clave pública del destinatario, quien lo decodificará con su clave privada.

Con la función Hash el resumen quedará representado numéricamente, generando un código que será encriptado con la clave privada de quien lo origina y desencriptado por el destinatario con la clave pública.

Este certificado con función Hash aplicada y luego codificado de manera inversa al documento constituye la firma digital.

[18] GAETE GONZALEZ Eugenio Alberto. “Instrumento público electrónico”. Ob. Cit. Página 215.
[19] GAETE GONZALEZ Eugenio Alberto. “Instrumento público electrónico”. Ob. Cit. Página 217.

5. Reflexión final

La tecnología nos ofrece no solamente nuevas formas para entablar relaciones jurídicas electrónicas y telemáticas, sino también las herramientas para operar con una seguridad óptima.

Acostumbrarnos a adoptar medidas de seguridad informática no nos parece sencillo y no confiamos en ellas. Pero este no es un hecho o creencia con un sustento real, sino que es necesario un cambio de mentalidad colectiva, un proceso de adaptación social.

Desde el punto de vista jurídico se ha consagrado a texto expreso en nuestro Derecho el pleno valor probatorio del documento electrónico y la utilización de las firmas electrónicas y digitales como equivalente funcional de la firma ológrafa.

Montevideo, mayo de 2004