Unidad 5: Seguridad en los Sistemas de Información

Contenidos:

Seguridad en los Sistemas de Información: Seguridad, Privacidad e Integralidad: Objetivos de la seguridad en la información Análisis de Riesgos de los sistemas de información. **Tecnologías y herramientas para proteger los recursos de información.** Medidas de controles generales, de aplicación, y en comunicaciones. **Firma Digital**. **Plan de Contingencia de los sistemas de información.** Plan de reanudación de negocios Medidas de recuperación. **Aspecto económico de las medidas de seguridad.** Estructura de control: Costos Beneficios.

Objetivos específicos:

- Entender las vulnerabilidades de los Sistemas de Información
- Conocer los componentes de un marco de trabajo organizacional para definir la seguridad y el control adecuados
- Conocer las herramientas y tecnologías para salvaguardar los recursos de información y áreas de TI para el aseguramiento de la disponibilidad la información sistemas
- Analizar y avaluar las políticas y procedimientos relativos a la planificación para la atención de contingencias y devolver a la gestión capacidad de respuesta y retorno a la normalidad

Bibliografía Básica:

- Sistemas de información gerencial / Laudon, Kenneth C. (2012) Sistemas de información gerencial [texto impreso] / Laudon, Kenneth C.; Laudon, Jane P.. - 12a. ed.. - México: Pearson Educación, 2012. ISBN 978-607-32-0949-6. Nota de contenido: Cap. 8. Seguridad en los sistemas de información
- Sistemas de información para la gestión empresaria / Lardent, Alberto R. (2001) Sistemas de información para la gestión empresaria: procedimientos, seguridad y auditoría [texto impreso] / Lardent, Alberto R.. - Buenos Aires : Pearson Educación, 2001. . ISBN 987-9460-51-0. Nota de contenido: II: Seguridad y auditoría informática: 19. Seguridad informática 22. Controles de accesos lógicos y físicos - 23. Seguridad en los sistemas de base de datos - 24. Seguridad de redes y sistemas distribuidos 29. Recuperación de desastres. Continuidad de operaciones.

Índice de Contenido

1. ¿Qué es firma digital?

Introducción

En el mundo de las cosas físicas hemos aprendido que por ejemplo los negocios normalmente tienen que realizarse entre partes presentes, por ello el marco normativo de códigos, leyes y normas en general regulaba entre otras cosas lo referente a la firma manuscrita. Al respecto el artículo 1012 del código civil establece que *"La firma de las partes es una condición esencial para la existencia de todo acto bajo forma privada. Ella no puede ser reemplazada por signos ni por iniciales de los nombres o apellidos". El articulo 1014 dice "Ninguna persona puede ser obligada a reconocer un instrumento que esté sólo firmado por iniciales o signos…"*.

Pero el avance de la tecnología informática acompañada a su vez de avances en cuestiones sociales, de negocios, etc., a permitido acortar las distancias físicas, el surgimiento de nuevas formas de contratación, el surgimiento de las transacciones electrónicas. Como ser el comercio electrónico, una realidad que involucra transferencias bancarias, operaciones de bolsa, contrataciones entre empresas, etcétera.

Esta nueva realidad virtual plantea la necesidad de que los instrumentos electrónicos cumplan los siguientes requerimientos:

- Certeza de quién es el emisor y quién es el receptor
- Demostración de la existencia de la voluntad jurídica
- Prueba fehaciente de la misma

De modo que aseguren puntos críticos en cuanto a la aceptabilidad y validez de los documentos electrónicos tales como:

1. credibilidad
2. no fugacidad
3. identificación y autenticación de las partes
4. identificación del documento
5. adecuación del orden jurídico

Definición

Según el Diccionario Abeledo Perrot, firma es “El trazo peculiar mediante el cual el sujeto consigna habitualmente su nombre y apellido, a fin de hacer constar las manifestaciones de voluntad”
Según la Revista Jurisprudencia Argentina “la firma es el nombre escrito de una manera particular, conforme el modo habitual seguido por una persona en actos sometidos al cumplimento de formalidades”

Desde un enfoque jurídico, el artículo 2 de la ley 25506 establece que la firma digital es el *resultado de aplicar a un documento digital un procedimiento matemático de exclusivo conocimiento del firmante.*

Para que una firma digital sea válida el artículo 9 de la ley de firma digital exige cumplir los siguientes requisitos:

a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;

b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;

c) Que dicho certificado haya sido emitido o reconocido por un certificador licenciado.

Características

1. Equivalente a la firma manuscrita.
2. No es la imagen escaneada de la firma manuscrita.
3. Es la encripción (criptografía) de un documento con la llave privada del hash (huella).
4. Existe una diferente para cada documento.

Desde un enfoque tecnológico, la firma digital es una nueva herramienta tecnológica que intenta cumplir con la finalidad que tradicionalmente cumplía la firma ológrafa (manuscrita), pero adaptada ahora al marco del ciberespacio. Esto es, la operatoria en redes. Debe constar de por lo menos de dos partes:

1. Método que haga imposible la alteración de la firma.
2. Verificación que la firma pertenece al firmante.

Objetivos

La firma digital debe cubrir los siguientes objetivos:

Asegurar:

- la identidad del firmante
- la integridad respecto a la no modificación del documento luego de ser firmado
- el no repudio es decir que el firmante no pueda negar haber firmado

Resumiendo, la firma digital es un conjunto de datos asociados a un mensaje que permite asegurar la **identidad** del firmante y la **integridad** del mensaje.

La firma digital no implica que el mensaje esté encriptado, es decir, que este no pueda ser leído por otras personas; al igual que cuando se firma un documento holográficamente este sí puede ser visualizado por otras personas.

Es un instrumento idóneo para agilizar el sistema de transacciones electrónicas y para dar confianza.

Se puede aplicar tanto a un correo electrónico como a un documento (texto, multimedia, etc.).

¿Qué valor legal tiene la firma digital?

En la firma digital existe una presunción "iuris tantum" a su favor.

Por ejemplo:

Si un documento firmado digitalmente es verificado correctamente, se presume *salvo prueba en contrario* que proviene del suscriptor del certificado asociado y que no fue modificado

2. ¿Cómo funciona?

La firma digital funciona de acuerdo al siguiente esquema:
El firmante genera mediante una función matemática una huella digital del mensaje. Esta huella digital se encripta con la clave privada del firmante, y el resultado es lo que se denomina firma digital la cual se enviará adjunta al mensaje original.
De esta manera el firmante va a estar adjuntando al documento una marca que es única para ese documento y que sólo él es capaz de producir.
El receptor del mensaje generará la huella digital del mensaje recibido, luego desencriptará la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice ser.

Este complejo procedimiento comprende a los efectos del cifrado funciones matemáticas que a continuación se detallan:

La función matemática: $D_k (E_k (P)) = P$

Donde: E y D son funciones matemáticas parametrizadas con la clave k. Estas funciones E y D son conocidas pero no la clave k. Las funciones son conocidas fundamentalmente por dos motivos:

1. Es un gran esfuerzo inventar, probar e instalar un método nuevo (función).
2. El cifrado con claves permite fácilmente cambiar la clave y mantener la función.

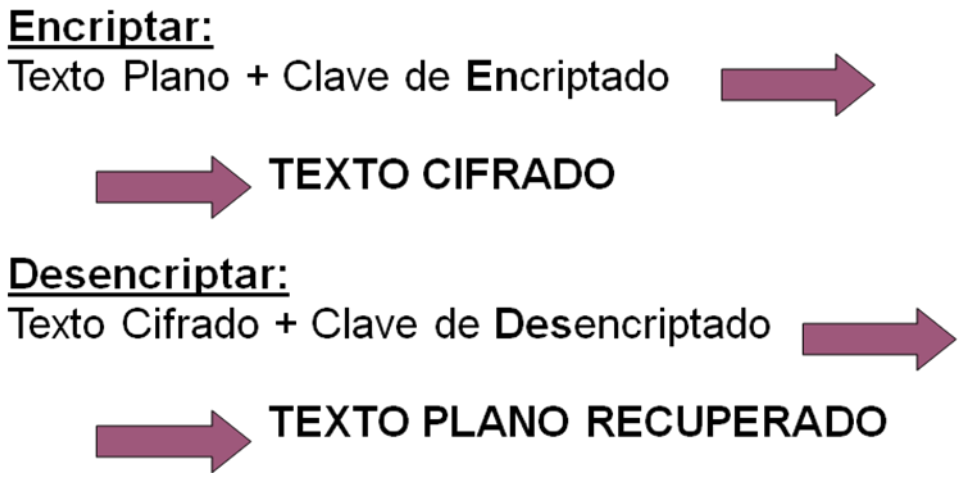
Ejemplos de cifrado

1. Relleno de una sola vez (función XOR – bit a bit)
2. Criptografía clásica: sustitución y transposición (Julio César desplazamiento a derecha e izquierda del alfabeto)
3. Criptografía moderna: algoritmos de clave privada y clave pública.

Dentro de la criptografía moderna tenemos el criptosistema asimétrico, algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital. A su vez comprende dos etapas:

a) Encriptación: transformación un documento legible (texto plano) en uno ilegible (texto cifrado) de acuerdo a una fórmula matemática (algoritmo) y de la utilización de una palabra clave o simplemente la "clave"
b) Desencriptación: transformación de un texto cifrado en un texto plano utilizando el algoritmo y la clave de desencriptación. Es el proceso inverso a la encriptación.

Gráficamente el esquema es el siguiente:



3. Claves Privadas y Claves Públicas

Las claves privadas y publicas son los dos elementos que integran el sistema criptografico asimétrico.

Se caracterizan por estar fuertemente relacionadas entre sí, siendo imposible calcular la primera a partir de los datos de la segunda, ni tampoco a partir de los documentos cifrados con la clave privada.

La clave criptográfica privada es aquella que se utiliza para firmar digitalmente. Es uno de los datos únicos que permite crear una firma digital.

El cifrado de clave privada, es más rápido que el de clave pública (de 100 a 1000 veces), y por tanto se utiliza generalmente en el *intercambio de información dentro de una sesión*. Estas claves también son conocidas como claves de sesión o de cifrado simétricas, ya que en ambos extremos de una comunicación basada en red, se posee la misma clave.

Los medios de resguardo de la clave privada pueden ser:

Llaves por puerto USB – Existen dos tipos :

- *Almacenan clave Privada generada en PC.*
- *Generan la Clave Privada directamente y la almacenan.*

Lectores de Tarjetas

- *Almacenan clave Privada generada en PC.*
- *Generan la Clave Privada directamente y la almacenan.*
- *Grabación en Mini CD*

La clave criptográfica pública es aquella que se utiliza para verificar una firma digital. Es uno de los datos únicos que se utiliza para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

El cifrado de clave pública es más lento y por tanto *se utiliza para intercambiar las claves de sesión*. Como este algoritmo utiliza dos claves diferentes, una privada y otra pública el cifrado se conoce como cifrado asimétrico.

4. Certificado Digital

¿Qué son los certificados digitales?

Un certificado digital es un documento electrónico firmado digitalmente que relaciona una entidad o individuo con una clave pública (DNI digital).

Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

¿Qué contiene un certificado digital?

Básicamente, el certificado contiene una clave pública y un nombre. También contiene periodo de validez, el nombre de la Autoridad de Certificación que la emitió, un número de serie, versión, identificador del algoritmo, firma y alguna otra información. Pero lo más importante es que el certificado esté firmado digitalmente por el emisor del mismo.

Requisitos

El articulo 14 de la ley de firma digital establece que los certificados digitales para ser validos deben:

a) Ser emitidos por un certificador licenciado por el ente licenciante;

b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:

1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;

2. Ser susceptible de verificación respecto de su estado de revocación;

3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;

4. Contemplar la información necesaria para la verificación de la firma;

5. Identificar la política de certificación bajo la cual fue emitido.

5. Marco Normativo

En materia de firma digital el marco normativo en Argentina esta constituido por:

Ley 25.506 de Firma Digital que contempla aspectos como: Definición – Requerimientos – Exclusiones – Presunciones - Validez - Originales - Conservación – de los certificados digitales – Del certificador licenciado – Del titular de un certificado digital – De la autoridad de aplicación - Otros

Los decretos 2628/02 - 283/03 -624/03 – 1028/03 – 409/05 – 724/06 que contemplan aspectos como: Autoridades de Aplicación/registros – Infraestructura – estándares - certificadores

Acordada 8.893/02 de la Corte de justicia

Código Civil y Comercial de la Nación

Con fecha Agosto 2015, mediante ley N° 26.694, entró en vigencia el nuevo Código Civil y Comercial de la Nación, en el cual se reconoce la firma digital como firma válida en instrumentos generados por medios electrónicos. Esto es en el artículo 288 de la sección 3ª, Forma y prueba acto jurídico. Dicho artículo establece:

ARTÍCULO 288. Firma. La firma prueba autoría declaración de voluntad expresada en el texto[…]. Debe consistir en el nombre del firmante o en un signo.

En instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho **si se utiliza una firma digital**, que asegure indubitablemente autoría e integridad del instrumento.

El formulario F780 – para fines fiscales – Presentación electrónica

Decisión Administrativa 6/2007 que establece el marco normativo de firma digital aplicable al otorgamiento y revocación de las licencias a los certificadores que así lo soliciten.

Y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

6. Infraestructura de Firma Digital

La infraestructura de la firma digital también denominado PKI que significa Public Key Infraestructure o Infraestructura de Clave Pública es un sistema de hardware, software, personal, normas y procedimientos que proveen garantías de seguridad para los documentos, transacciones y comunicaciones electrónicas por internet.

Los actores participes de esta infraestructura son:

Autoridades Certificantes: terceras partes confiables que dan fe de la veracidad de la información incluida en los certificados digitales que emiten

Autoridades de registración: atestiguan el vínculo entre las claves públicas y las entidades propietarias de los certificados.

Titulares de certificados digitales: los que pueden firmar documentos digitales

7. Aplicaciones

Las aplicaciones que aprovechan la nueva tecnología son principalmente en el campo de las finanzas, comercial, gubernamental, legal y fiscal. Entre las que podemos mencionar:

- ✓ Mensajes con autenticidad asegurada
- ✓ Mensajes sin posibilidad de repudio
- ✓ Contratos comerciales electrónicos
- ✓ Factura electrónica
- ✓ Desmaterialización de documentos
- ✓ Transacciones comerciales electrónicas
- ✓ Invitación electrónica
- ✓ Dinero electrónico
- ✓ Notificaciones judiciales electrónicas
- ✓ Voto electrónico
- ✓ Decretos ejecutivos (gobierno)

Situación en Argentina

En Argentina el tema firma digital si bien se realizaron avances aún queda bastante por hacer. A pesar que desde febrero 2007 se reglamentó el otorgamiento y revocación de licencias a los certificadores que así lo soliciten, el mayor desarrollo se presenta en los sectores gubernamentales, bursátil y financiero.

Desde marzo de 2009 se incorporación al sistema de Firma Digital de la Administración Federal de Ingresos Públicos (AFIP) y la Administración Nacional de Seguridad Social (ANSES). Convirtiéndolas en las primeras entidades certificadoras de firma digital, lo que permite que ambas entreguen a los ciudadanos que lo requieran certificados que le garanticen el uso de este instrumento legal.

Desde febrero de 2012 la AFIP emite la Disposición 20/12 del procedimiento para la gestión de firma digital y establece que a partir del 30 de marzo del año 2012, la obligatoriedad de utilización de la firma digital mediante Certificado Digital Clase 4,

por parte de los niveles de jefatura de Departamento inclusive y superiores, para las comunicaciones y trámites internos llevados a cabo mediante correo electrónico, relacionados con el ejercicio del cargo que se desempeña.

Estos hechos son medidas importantes para agilizar todo tipo de trámites del estado en sus distintas áreas y de los ciudadanos en general. Por ejemplo, un ciudadano del Mercosur, quien antes tardaba mucho tiempo para efectuar un trámite, ahora a través de la documentación digital tardará solo tres días.

Por otro lado, también se firmo un acuerdo con el poder judicial para tramitar sus expedientes por este sistema.

Situación en la profesión de ciencias económicas

Respecto a la profesión desde agosto 2008 la Federación Argentina de Consejos Profesionales en Ciencias Económicas aprobó la iniciativa que facilitará la emisión de estados contables con sus informes profesionales en formato digital y firmados electrónicamente.

8. Firma Digital Cloud y Firma Digital Token

Para obtener firma digital existen dos modalidades:

Firma Digital Token: requiere un dispositivo físico donde se almacena el certificado. Tales como: llaves por puerto USB, lectores de tarjeta, Mini CD, entre otros.

Firma Digital Cloud: Permite firmar a través de una plataforma online, sin la necesidad de un token.

9. Firma Digital Blockchain

Definición Blockchain

Tecnología símil contabilidad pública entre pares que se mantiene mediante una red distribuida de PC y que no requiere ninguna autoridad central ni terceras partes que actúen como intermediarios.

Componentes fundamentales:

1) **Transacción**

2) **Registro de transacciones**

3) **Sistema que verifica y almacena la transacción**

Los bloques se generan a través de software de código abierto y registran la información sobre cuándo y en qué secuencia ha tenido lugar la transacción.

Este "bloque" almacena cronológicamente información de todas las transacciones.

La tecnología Blockchain es la unión de:

- ✓ La tecnología peer to peer o P2P (una red de ordenadores conectados que facilita transacciones entre usuarios)
- ✓ La criptografía de clave pública que permite la creación de Internet del Valor

10. Glosario Firma Digital

Firma digital: Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma (Art. 2)

Firma electrónica: Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez (Art. 5)

Documento digital: se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura (Art. 6)

Digitalizar: convertir algo en números (dígitos)

Clave criptográfica privada: En un criptosistema asimétrico es aquella que se utiliza para firmar digitalmente.

Clave criptográfica pública: En un criptosistema asimétrico es aquella que se utiliza para verificar una firma digital.

Datos de verificación de firma digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

Datos de creación de firma digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

Dispositivo de creación de firma digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

Criptosistema asimétrico: Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital.

Integridad: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

Procedimiento de verificación: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos: a) que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante; b) que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado

del firmante; c) la verificación de la autenticidad y la validez de los certificados involucrados.

PKI: Public Key Infraestructure o Infraestructura de Clave Pública

Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, para el caso de certificados extranjeros, por un certificador licenciado (Art. 26)
Certificado digital: se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (Art. 13)

Certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante (Art. 17)

11. Conclusiones

Para un mayor éxito de la firma digital en cuanto a su aplicabilidad practica se deben cubrir aspectos de seguridad, beneficios ciertos para el usuario, aspectos funcionales adecuados para evitar costos innecesarios e incidencias.

Resumiendo, el gran desafío que se plantea es proyectar aspectos de la vida papel transformándose a partir del uso de la firma digital. Haciendo mas confiable el comercio y el intercambio de información.

12. Fuentes de consultas

Ley 25.506 de Firma Digital y sus complementarias.

Lardent Alberto, *"Sistemas de información para la gestión empresaria"*, Pearson Educacion, Argentina, 0000

www.pki.gob.ar

www.microsoft.com

www.wikipedia.com