UNIVERSIDAD NACIONAL DE CÓRDOBA
SECRETARÍA DE CIENCIA Y TECNOLOGÍA
CENTRO DE ESTUDIOS AVANZADOS

Proyecto

ASPECTOS DE LA EVALUACIÓN DE DOCUMENTOS EN AMÉRICA. TERMINOLOGÍA. PARTICULARIDADES DE LOS DOCUMENTOS DIGITALES. ESTUDIO DE CASOS EN CORDOBA

DOCUMENTO FINAL DEL ÁREA: PARTICULARIDADES DE LOS DOCUMENTOS DIGITALES

Integrantes:

Daniel L. DI MARI

Norma C. FENOGLIO

Aída Luz MENZOZA NAVARRO

Andrea R. TIBALDO

Córdoba, diciembre 2013

INDICE

	Pág.
ASPECTOS DE LA EVALUACIÓN DE DOCUMENTOS EN AMÉRICA. PARTICULARIDADESDE LOS DOCUMENTOS DIGITALES	3
CONSIDERACIONES GENERALES ACERCA DE LA LEGISLACIÓN RELEVADA	5
ANÁLISIS COMPARATIVO DE LA TERMINOLOGÍA UTILIZADA EN LA LEGISLACIÓN ESTUDIADA	11
Cuadro comparativo N° 1, Legislación: Argentina, Colombia y Perú	14
Comentarios y comparaciones	27
ACCESO A LA INFORMACIÓN, TRANSPARENCIA, PROTECCIÓN DE DATOS Y SU INCIDENCIA EN LA EVALUACIÓN DE DOCUMENTOS	32
Cuadro comparativo N° 2 : Principales disposiciones normativas: acceso a la información, transparencia y protección de datos	33
Análisis comparado: Argentina, Colombia y Perú	34
Cuadro comparativo N° 3: Resumen comparativo (área constitucional)	38
Cuadro comparativo N° 4: Resumen comparativo (Área de transparencia)	43
Cuadro comparativo N° 5: Resumen comparativo (Área protección de datos)	52
Apoyo legal para la toma de decisiones en evaluación documental	53
COMPARACION DE CONCEPTOS Y APLICACIONES SOBRE FIRMA DIGITAL	54
Cuadro comparativo N° 6: Análisis comparativo temático	55
Comentarios y consideraciones	63
Reflexiones finales	64
DIGITALIZACIÓN PARA SUSTITUCIÓN	65
Análisis	66
Apreciaciones	72
EVALUACIÓN DE DOCUMENTOS DIGITALES	73
CONCLUSIONES	74

ASPECTOS DE LA EVALUACIÓN DE DOCUMENTOS EN AMÉRICA. PARTICULARIDADES DE LOS DOCUMENTOS DIGITALES.

Introducción

El interés en estudiar algunos aspectos de la evaluación de los documentos reside en que, como se ha dicho ya en varias oportunidades, se trata de uno de los procesos más complejos y exigentes que debe encarar el archivero, por los múltiples conocimientos teóricos y prácticos que requiere, porque cada situación exige un estudio específico y porque de la decisión que se toma depende la conservación o eliminación de cada documento y, en consecuencia, la constitución del patrimonio documental. Y cuando se trata de evaluar documentos digitales, el tema es más complicado aún, porque se debe sumar la problemática de lo digital, que reside, fundamentalmente, en que todas las acciones producidas durante el período de retención y también en el momento de la disposición deben cumplir con los requisitos previstos para mantener la exactitud, la fiabilidad y la autenticidad, atributos que conforman la **confianza** de un documento de archivo digital.

En esta oportunidad, se optó por tratar el aspecto legal específico para documentos digitales y, para ello, se realizó un estudio comparado de la legislación relacionada con este tema en tres países de América Latina: Argentina, Colombia y Perú, a los fines de encontrar similitudes y diferencias.

Respecto del estudio del Derecho comparado, Juan Carlos Galindo Vácha señala:

> Estos análisis permitirán examinar la evolución social y la conveniencia de las diversas formas jurídicas expedidas y utilizadas en un momento dado. Resulta de capital importancia el estudio de la historia del derecho, en cuanto, que a pesar de la evolución tecnológica alcanzada, la vida humana es un incesante movimiento pendular que muchas veces repite las conductas o los problemas sociales; por lo tanto, conociendo el pasado se conocerá no sólo el origen de las instituciones, sino

> la respuesta a muchos de los obstáculos repetitivos de la vida social.[1]

De modo coincidente, Julio Ayasta comenta:

> Es indudable que el Derecho Comparado ocupa un lugar relevante en el campo del Derecho en general. Su importancia es considerable. Es un elemento indispensable de la cultura jurídica, porque da a los estudiosos un sentido de humanismo y de universalidad. El Derecho Comparado permite conocer y desarrollar los diversos estilos de realización jurídica del fenómeno humano. Es una ciencia humanista, porque representa en sus aplicaciones un elemento de comprensión mutua entre los hombres y los pueblos y, por lo mismo, un factor que contribuye a la paz internacional.[2]

La Archivística y en especial la evaluación documental tienen una preocupación constante respecto de los documentos como testimonios del pasado porque, no obstante el cambio tecnológico, la vida humana muchas veces repite conductas del pasado, y allí estarán siempre los documentos para recordárnoslo y testimoniar los hechos que sucedieron históricamente, por lo que los documentos, cualquiera sea el soporte en el que se encuentren, en todas las épocas, son y serán fuente valiosa de información que debemos proteger, de donde se desprende la gran responsabilidad en la toma de decisiones acertadas y técnicas que debemos tomar toda vez que se evalúa documentos de archivo.

Se trató entonces, de estudiar y analizar las fórmulas legales de los países en estudio, en los que encontramos diversos estilos de realización jurídica en torno a los temas específicos abordados en que se desenvuelve la sociedad de cada uno de los países objeto de nuestro estudio y que sirven de base legal para la toma de decisiones respecto de los plazos de retención y conservación de los documentos de valor permanente en medio electrónico

Además del tema específico de la evaluación de los documentos digitales, los asuntos

---

[1] GALINDO VÁCHA, Juan Carlos, (2002) *Derecho europeo de sociedades: con referencias a la legislación colombiana*, Pontificia Universidad Javeriana, Colección Profesores 34, Bogotá DC. Colombia, p. 53.

[2] AYASTA GONZALEZ, Julio, (1991) *El Derecho Comparado y los Sistemas Jurídicos Contemporáneos*, Ediciones RJP, Lima, p. 16.

puntuales hallados y que fueron estudiados particularmente son: “Terminología utilizada”, “Acceso a la información, transparencia, protección de datos y su incidencia en la evaluación de documentos”, “Firma digital” y “Digitalización para sustitución”, los que, después de una serie de consideraciones generales, se analizan a continuación.

CONSIDERACIONES GENERALES ACERCA DE LA LEGISLACIÓN RELEVADA

En los tres países objeto de estudio se relevaron instrumentos legales de distinto nivel jerárquico -leyes, decretos, resoluciones, acuerdos, etc.- vinculados de alguna manera a la evaluación de documentos o que, aunque sea parcialmente, tratan el tema de los documentos digitales, la firma digital, la evaluación de los documentos y temas complementarios a éstos, como la digitalización, el acceso a la información, la transparencia, a los fines de comprobar la existencia de similitudes y diferencias en el tratamiento de los temas, los procedimientos adoptados y la terminología utilizada.

La normativa relevada fue la siguiente:

Para **ARGENTINA**:

Legislación nacional:

- Ley 24.624 de 28/12/1995
- Ley 25.506 de 14/11/2001
- Ley 25.831 de 26/11/2003
- Ley 25.326, de 04/10/2000 y sus modificatorias, Leyes 26.343 y 26.388
- Decreto Nº 1558/2001, de29/11/2001, reglamentario de la Ley 25.326
- Decreto Nº 658/2002
- Decreto Nº 2628/2002: reglamentario de la Ley Nº 25.506/2002
- Decreto 1172/2003

- Decreto 409/2005
- Resolución Nº 555/97 Ministerio De Trabajo y Seguridad Social
- Decisión Administrativa 43/96 del Jefe de Gabinete de Ministros
- Disposición 7/2005 Dir. Nac. de Protección de datos Personales
- Disposición 11/2006 Dir. Nac. de Protección de datos Personales

Legislación provincial:

- Constitución de la Ciudad autónoma de Buenos Aires – 01/10/1996
- Ley n° 3 – Ciudad Autónoma de Buenos Aires – 03/02/1998
- Ley 104 - Ciudad Autónoma de Buenos Aires – 19/11/98
- Ley 1845 - Ciudad Autónoma de Buenos Aires – 24/11/2005
- Ley 2.602 - Ciudad Autónoma de Buenos Aires -06/12/2007
- Ley 2.817 - Ciudad Autónoma de Buenos Aires -14/08/2008
- Ley 12.475 - Provincia de Buenos Aires (B.O. nº 24.120, de 29/08/2000)
- Ley 8.803 - Provincia de Córdoba. 06/10/1999 - (B.O. de 15/11/1999)
- Ley 9.380 - Provincia de Córdoba; 18/04/2007
- Decreto nº 58 HCD de 21/12/2006 - Provincia de Entre Ríos (B.O. de 26/11/2007)

Para **COLOMBIA:**

- Ley nº 227 de 21/04/1998
- Ley 527 de 18/08/1999
- Ley 594 del 14/07/2000
- Ley Estatutaria 1581 de 17/10/2012

- Decreto 1747 del 11/09/2000
- Decreto 2578 de 2012 13/12/2012
- Decreto 2609 de 14/12/2012
- Decreto 2639 21/12/2012
- Decreto 2364 de 22/11/2012
- Decreto 805/2013
- Acuerdo Nº 027-2006
- Acuerdo AGN No 004 15/03/2013
- Circular Externa Nº 002 AGN – 06/03/2012
- Circular Externa Nº 005 AGN – 11/09/2012

Para **PERÚ**:

- Constitución Política 1993
- Ley 26.612 del 10/05/1996
- Ley nº 27.038 del 30/12/1998
- Ley 27269 del 8/05/2000
- Ley 27.291, de 2/06/2000
- Ley nº 27310/2000
- Ley 27.444 del 21/03/2001
- Ley 27.806 del 13/07/2002
- Ley 27.927 del 13/01/2003, que modifica la Ley 27.806
- Ley 28186 del 04/03/2004
- Ley 28.493 del 18/03/2005

- Ley 29.733 del 2/07/2011
- Decreto Supremo nº 009-92-JUS del 26/06/1992
- Decreto Supremo nº 018-2001-PCM
- Decreto Supremo nº 019-2002/JUS del 15/05/2002
- Decreto Supremo nº 072-2003-PCM del 7/08/2003
- Decreto Supremo nº 052-2008-PCM del 18/07/2008
- Decreto Supremo nº 015-2010-TR del 17/12/2010
- Decreto Supremo nº 003-2013-JUS -
- Decreto Legislativo nº 681 del 11/10/1991
- Decreto Legislativo nº 822, del 23/04/1996
- Decreto Legislativo nº 827, del 31/05/1996
- Resolución Superintendencia nº 0188-2010-SUNAT del 16/06/2010
- Carta Patrimonio Digital del 6/03/2009, de la Oficina Nacional de Gobierno Electrónico e Informática
- Norma Técnica Peruana NTP 392.030-2 del 22/09/2005

En general, se comprueba que el tema comienza a ser tratado en la última década del siglo XX y, entre los países en estudio, Perú es el primero en legislar al respecto. En efecto, la norma más antigua que se ha relevado es el **Decreto Legislativo nº 681 del 11 de octubre de 1991**, que establece las disposiciones que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos (digitalización-microformas), así como sobre los efectos legales de los documentos digitalizados obtenidos producto de la conversión o del microfilmado.

Entre los temas puntuales localizados y tratados en los tres o en alguno de los tres países, se pueden citar: acceso a la información pública, protección de datos personales, firma y

certificado digital, conservación y eliminación de documentos y/o de información con cambio de soporte (microfilmación y/o digitalización para sustitución), plazos de conservación, conservación del patrimonio digital, derecho de autor para software, gestión del documento digital, comunicación electrónica oficial.

En cuanto a las características de la legislación, por país, se constata que:

A nivel nacional, en **Argentina** no existe legislación específica sobre evaluación de documentos digitales de archivo, ni que establezca la gestión informática de los documentos.

A los fines de permitir la utilización de las nuevas tecnologías en los procedimientos administrativos, se han dictado algunas disposiciones que adecuan o modifican otras más antiguas. Así, por ejemplo, a la ley 24.240 de defensa del consumidor se le incorporaron artículos relacionados con las ventas “por medio electrónico o similar”.

Más recientemente, la Ley 26.685 del 1 de junio de 2011 autoriza la utilización de expedientes, documentos, firmas, comunicaciones, domicilios electrónicos y firmas digitales en todos los procesos judiciales y administrativos que se tramiten ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales.

La legislación sobre acceso a la información tampoco es específica sobre documentos digitales: la Ley 25.831 trata sobre el acceso a la información pública relacionada específicamente con el ambiente y el Decreto 1172/2003 de fecha 3/12/2003, que aprueba el "Reglamento General del Acceso a la Información Pública para el Poder Ejecutivo Nacional”, establece que se debe “garantizar el respeto de los principios de igualdad, publicidad, celeridad, informalidad y gratuidad” y se refiere a todo tipo de información.

Es interesante la Ley 24.624 del 28/12/1995 que autoriza la “reproducción en soporte electrónico u óptico indeleble” de los documentos financieros, de personal y de control de la Administración Pública Nacional, como también la administrativa y comercial, para su archivo, y autoriza la eliminación de los documentos originales, cualquiera sea su soporte.

La Decisión Administrativa 43/96 del Jefe de Gabinete de Ministros fija el procedimiento para estas eliminaciones.

En cuanto a firma digital, Ley 25.506, del 14/11/2001, establece el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en determinadas condiciones. Con anterioridad, el Ministerio de Trabajo y Seguridad Social de la Nación, dictó la Resolución 555/97, en la que se establecen una serie de normas y procedimientos para la incorporación de documentos y firma digital en ese Ministerio.

A nivel de las provincias, tampoco existe abundante legislación. La Ciudad Autónoma de Buenos Aires es la que más ha legislado al respecto, en especial con relación a acceso a la información y a plazos de conservación.

Colombia dispone de algunas medidas concretas específicas en materia de tecnología informática en las que se tienen en cuenta los archivos. Así, la Ley 594 del 14/07/2000 autoriza a las entidades del Estado a "incorporar tecnologías de avanzada en la administración y conservación de su archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático", exigiendo como requisitos la "organización archivística de los documentos".

Más recientemente, el Decreto 2609 del 14/12/2012 dicta una serie de disposiciones en materia de Gestión Documental para todas las Entidades del Estado, incluyendo a los expedientes mixtos (híbridos), digitales y electrónicos, entre las que se encuentran la obligatoriedad de las entidades de garantizar "la autenticidad, integridad, confidencialidad y la conservación a largo plazo de los documentos electrónicos de archivo que de acuerdo con las Tablas de Retención Documental o las Tablas de Valoración Documental lo ameriten, así como su disponibilidad, legibilidad (visualización) e interpretación, independientemente de las tecnologías utilizadas en la creación y almacenamiento de los documentos". Autoriza la migración, la emulación o el refreshing, o cualquier otro proceso de reconocida capacidad técnica que se genere en el futuro y establece que el Archivo General de la Nación es el organismo responsable de dictar "los requisitos de archivo y conservación en medios electrónicos de los documentos y expedientes de archivo, que se

hayan gestionado utilizando dichos medios". Al respecto, el Acuerdo AGN No 004, del 15/03/2013 fija el procedimiento para la elaboración, presentación, evaluación, aprobación e implementación de las Tablas de Retención Documental y Tablas de Valoración Documental, así como los criterios básicos para la clasificación, ordenación y descripción de los archivos, incluyendo los producidos en soporte electrónico.

Perú cuenta con un marco legal mucho más abundante en el tema que se está estudiando, el que está incluido en legislación de fondo. La Constitución Política, que data de 1993, incluye el derecho al acceso a la información y el Código Civil permite la utilización de medios electrónicos para la comunicación de la manifestación de voluntad así como el empleo de la firma electrónica, sobre todo en el área de contratos.

Es interesante señalar que, cuando se trata de normar sobre valor de los documentos y su eliminación eventual, la legislación remite a la autoridad del Archivo General de la Nación, organismo que debe autorizar cualquier destrucción documental, en cualquier soporte, aunque aún no se ha establecido normativa precisa al respecto.

ANÁLISIS COMPARATIVO DE LA TERMINOLOGÍA UTILIZADA EN LA LEGISLACIÓN ESTUDIADA

En la primera etapa de este proyecto se comprobó que en los distintos países de Iberoamérica no se utiliza el mismo término para denominar la misma acción, asunto u objeto y que, a la inversa, un vocablo puede utilizarse con distinto significado, siempre en la lengua castellana, según el país en el que uno se encuentre.

Comparar las definiciones de palabras específicas relacionadas con los documentos de archivo digitales, obrantes en los glosarios de la legislación de Argentina, Colombia y Perú, y confeccionar un glosario comparado específico, es de suma importancia para comprender el sentido dado a cada locución.

Se tomaron los vocablos existentes en los glosarios y, entre ellos, se seleccionaron los que

son específicos para la temática en estudio en general y no puntuales solo en y para el contexto de un texto legislativo determinado. En una segunda instancia, y como el objetivo es comparar los conceptos, se eliminaron los términos que no se repiten en por lo menos dos de los países analizados, dejando solo tres de ellos (copia de sustitución, dato y sistema de Información) por considerarlos básicos.

De ese modo, se ha confeccionado un glosario que incluye un total de 33 palabras relacionadas con los documentos digitales y su tratamiento.

Para realizar la comparación se tomaron las definiciones existentes en los glosarios incluidos en los siguientes instrumentos legales:

De **ARGENTINA**:

- Ley 25.506 de 14/11/2001, sobre Firma digital
- Ley 25.326, de 04/10/2000, de Protección de los datos personales
- Decreto 1172/2003 de 3/12/2003, sobre acceso a la información pública., Anexo VII: Reglamento general del acceso a la información pública para el Poder Ejecutivo Nacional
- Decisión Administrativa 43/96 del Jefe de Gabinete de Ministros, Anexo, Cap.II
- Anexo I Resolución Nº 555/97 Ministerio De Trabajo Y Seguridad Social
- Ley 1845 de protección de datos personales de la Ciudad Autónoma de Buenos Aires
- Ley 12.475, de la Provincia de Buenos Aires, por la que se reconoce a toda persona física o jurídica que tenga interés legítimo el derecho de acceso a todos los documentos administrativos (B.O.P. nº 24.120, de 29/08/2000)
- Ley 8.803 de 6 de octubre de 1999, de acceso al conocimiento de los Actos del Estado de la Provincia de Córdoba. (Boletín Oficial de 15/11/1999)
- Decreto nº 58 HCD de 21/12/2006. Reglamento general de Acceso a la información Pública (Boletín Oficial de Entre Ríos, Lunes 26/11/2007, nº 23.912 225/07)

De **COLOMBIA:**

- Ley nº 227 de 21/04/1998, por medio del cual se define y reglamenta el acceso y uso del comercio electrónico. Firmas digitales y se autorizan las entidades de certificación.
- Ley 527 de 18/08/1999, que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 del 14/07/2000 por la cual se dicta la Ley General de Archivos y otras disposiciones.
- Ley Estatutaria 1581 de 17/10/2012, con disposiciones generales para la protección de los datos personales (Diario Oficial 48587 de 18/10/2012)
- Decreto Nº 2609 de 14/12/2012, que reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y dicta otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 1747 del 11/09/2000, por el que se reglamenta parcialmente la ley 527 de 1999.
- Decreto Nº 2364 de 22/11/2012, reglamentario del artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y otras disposiciones.
- Acuerdo Nº 027-2006 del Consejo Directivo del Archivo General de la Nación de Colombia, que actualiza el Glosario del Reglamento General de Archivos.
- Guías de Papel Cero en la Administración Pública, Ministerio de Tecnologías de la Información MINTIC. *Guía 3. Documentos Electrónicos*

De **PERÚ**:

- Ley nº 27269 - de Firmas y Certificados Digitales, modificada por la Ley nº 27310.
- Ley nº 28.493 de 18/03/2005, que regula el uso del correo electrónico comercial no solicitado (SPAM) (Promulgada el 11/04/2005 y Publicada en el Diario Oficial "El Peruano" el 12/04/2005).
- Ley nº 29.733 de 02/07/2011 de Protección de Datos Personales.

- Decreto Supremo nº 019-2002/JUS, de 15/05/2002. Reglamento de la Ley de firmas y certificados digitales. Cabe aclarar que este instrumento fue derogado por el Decreto Supremo nº 052-2008/PCM. Sin embargo, de él se han tomado las definiciones de dos términos (Entidad de Certificación y Firma electrónica) por cuanto no están definidos en el nuevo decreto.
- Decreto Supremo nº 052-2008/PCM de 18/07/2008, Reglamento de la Ley de Firmas y Certificados Digitales (El Peruano, 19/07/2008)
- Decreto Supremo Nº 003-2013-JUS, que aprueba Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales
- Norma Técnica Peruana NTP 392.030-2

Cuadro comparativo n° 1 Legislación: Argentina, Colombia y Perú

TÉRMINO	**ARGENTINA**	**COLOMBIA**	**PERU**
Archivo	(*Decisión 43/96)* Colección de datos efectuada ordenada y sistemáticamente, y que ofrece garantía de su recuperación. *Ley 25.326* **Archivo, registro, base o banco de datos**: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.	*Ley 594* y *Acuerdo No. 027/2006* Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.	*D. S. nº 052-2008* Es el conjunto organizado de documentos producidos o recibidos por una entidad en el ejercicio de las funciones propias de su fin, y que están destinados al servicio. *NTP 392.030-2* Conjunto de documentos conservados por cualquier técnica, en cualquier medio actualmente conocido o recientemente desarrollado.

Archivo electrónico		*Acuerdo No. 027/2006* Conjunto de documentos electrónicos producidos y tratados conforme a los principios y procesos archivísticos.	*D. S. nº 052-2008* Es el conjunto de registros que guardan relación. También es la organización de dichos registros.
Autenticación	(*Decisión Ad. 43/96)* Procedimiento fijado por la ley que debe observar el funcionario competente designado conforme aquella, para otorgar autenticidad a un documento o a su copia.		*D. S. nº 052-2008* Proceso técnico que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.
Autoridad certificante	*Res. 555/97 Min. T.y S.S.* Persona física o jurídica que da fe – por medio de un certificado – a la atribución de claves públicas a personas físicas y/o jurídicas.	Ver: Entidad de Certificación	Ver: Entidad de Certificación
Certificado	*Res. 555/97 Min. T.y S.S.* Registro basado en la computadora, que identifica a la autoridad certificante que lo emite, nombra o identifica a quien lo suscribe; contiene la clave pública de quien lo suscribe y está firmado digitalmente por la autoridad certificante que lo emite.	*Ley 227* Es la manifestación que hace la entidad de certificación, como resultado de la verificación que efectúa sobre la autenticidad, veracidad y legitimidad de las firmas digitales o la integridad de un mensaje.	
Certificado Digital	*Ley 25.506* Documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular		*D.S.nº 052-2008 y Ley 27.269* Es el documento credencial electrónico generado y firmado digitalmente por una Entidad de Certificación que vincula un par de claves con una persona natural o jurídica confirmando su

			identidad.
Clave privada	*Res. 555/97 Min. T.y S.S.l* de dos claves, una de ellas, que se usa para crear una firma digital.	*Decreto 1747* Valor o valores numéricos que, utilizados conjuntamente con un procedimiento matemático conocido, sirven para generar la firma digital de un mensaje de datos.	*D. S. nº 052-2008* Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.
Clave pública	*Res. 555/97 Min. T.y S.S.l* de dos claves, una de ellas, que se usa para verificar una firma digital.	*Decreto 1747* Valor o valores numéricos que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador.	*D. S. nº 052-2008* Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.
Conservación	*Decisión Ad. 43/96* Mantenimiento de los datos archivados, de sus soportes relativos y de la tecnología de investigación y utilización de tales datos.	*Acuerdo No. 027-2006* **Conservación de documentos:** Conjunto de medidas preventivas o correctivas adoptadas para asegurar la integridad física y funcional de los documentos de archivo.	
Copia	*Decisión Ad. 43/96)* Versión obtenida del documento original por cualquier medio de reproducción.	*Acuerdo No. 027-2006* Reproducción exacta de un documento.	
Copia autenticada:	*Decisión Ad. 43/96* Versión del documento original legalizada por el funcionario competente siguiendo el procedimiento establecido en la ley.	*Acuerdo No. 027-2006* Reproducción de un documento, expedida y autorizada por el funcionario competente y que tendrá el mismo valor probatorio del original.	

Copia de sustitución:	*Decisión Ad. 43/96* Versión del documento original obtenida por cualquier medio de reproducción, destinada a reemplazar al original.		
Copia de resguardo: **Correo electrónico**	*Decisión Ad. 43/96* Versión del documento original obtenida por cualquier medio de reproducción, destinada a ser utilizada para evitar el manipuleo del original por razones de seguridad o protección. *Res. 555/97 Min. T.y S.S.* Medio de transmisión del documento digital a través de una red de comunicaciones, por el cual un usuario escribe su correspondencia desde su terminal (correspondencia que puede almacenarse en un banco de mensajes propio o en uno central) y solicita su transmisión a uno o varios usuarios receptores, pudiendo aquello ser transmitido a través de la red interna del Organismo, o ser encadenada a sistemas externos para lograr una transmisión remota.	*Acuerdo No. 027-2006* **Copia de seguridad:** Copia de un documento realizada para conservar la información contenida en el original en caso de pérdida o destrucción del mismo. *Guía 3. Documentos Electrónicos* El correo electrónico (e-mail) es uno de los servicios más usados en Internet que permite el intercambio de mensajes entre las personas conectadas a la red, de manera similar a como funcionaba el correo tradicional. Básicamente es un servicio que nos permite enviar mensajes a otras personas de una forma rápida y económica, facilitando el intercambio de todo tipo de archivos, dando clic en el link "adjuntar" que aparece en pantalla. Los documentos que se adjuntan comienzan a ser nombrados como documentos electrónicos de archivo, debido a que incorporan información de alto valor que sirve de soporte y evidencia para las entidades. Constituye un tipo de documento en el que con mayor frecuencia se incluyen datos de	*Ley 28.493* Todo mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión entre computadoras o cualquier otro equipo de tecnología similar. También se considera correo electrónico la información contenida en forma de remisión o anexo accesible mediante enlace electrónico directo contenido dentro del correo electrónico.

		gran valor documental.	
Criptografía Asimétrica	Ver: Criptosistema Asimétrico	*Ley 227* **Criptografía:** Es la rama de las matemáticas aplicadas que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas a su forma original.	*D.S. nº 052-2008* Es la rama de las matemáticas aplicadas que se ocupa de transformar documentos electrónicos en formas aparentemente ininteligibles y devolverlas a su forma original, las cuales se basan en el empleo de funciones algorítmicas para generar dos "claves" diferentes pero matemáticamente relacionadas entre sí. Una de esas claves se utiliza para crear una firma numérica o transformar datos en una forma aparentemente ininteligible (clave privada), y la otra para verificar una firma numérica o devolver el documento electrónico a su forma original (clave pública). Las claves están matemáticamente relacionadas, de tal modo que cualquiera de ellas implica la existencia de la otra, pero la posibilidad de acceder a la clave privada a partir de la pública es técnicamente ínfima.
Criptosistema Asimétrico	*Res. 555/97 Min. T.y S.S.* Algoritmo o serie de algoritmos que brindan un par de claves confiables (clave pública y clave privada). *Ley 25.506* 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.		
Dato **Datos de creación de la firma electrónica**	*Ley 25506* **Datos de creación de firma digital**: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.	*Decreto 2364* Datos únicos y personalísimos, que el firmante utiliza para firmar.	*NTP 392.030-2* Una descifrable representación de información en una manera formalizada apropiada para comunicación, interpretación o procesamiento.
Datos personales	*Ley 25.326* Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.	*Ley 1581* Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.	*D. S. Nº 003-2013* Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados. *Ley nº 29.733* Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
Datos	Ley 25.326:		*D. S. Nº 003-2013*

sensibles	Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. *Ley 1845 Ciudad Bs As* Aquellos datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos.		Es aquella información relativa a datos personales referidos a la características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad. *Ley nº 29.733* Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.
Documento		*Acuerdo No. 027-2006* Información registrada, cualquiera que sea su forma o el medio utilizado **Documento de archivo:** Registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones. . *LEY 594 DE 2000* ***Documento de archivo*** Registro de información producida o recibida por una	*D. S. nº 052-2008* Es cualquier escrito público o privado, los impresos, fotocopias, facsímil o fax, planos, cuadros, dibujos, fotografías, radiografías, cintas cinematográficas, microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, y otras reproducciones de audio o video, la telemática en general y demás objetos que recojan, contengan o

		entidad pública o privada en razón de sus actividades o funciones.	representen algún hecho, o una actividad humana o su resultado. Los documentos pueden ser archivados a través de medios electrónicos, ópticos o cualquier otro similar. *NTP 392.030-2* Cualquier medio que lleve en él información registrada y que puede ser tratado como una unidad. Nota 1: De acuerdo a los requerimientos funcionales de las organizaciones los documentos se pueden clasificar, organizar, ordenar e identificar en forma individual o en conjunto y en ambos casos ser tratados como unidad, sea como documentos físicos o documentos electrónicos. Nota 2: Son ejemplos de conjuntos tratados como unidad las bibliotecas, las colecciones, series documentales, los expedientes, legajos, planillas, etc., sea como documentos físicos o documentos electrónicos o una combinación de ambos.
Documento digital	*(Res. 555/97 Min. T.y S.S.)* Toda representación en forma electrónica de un hecho jurídicamente relevante susceptible de ser recuperado en forma humanamente comprensible, ello cuando: a) no se produzcan alteraciones	*ACUERDO No. 027-2006* **Documento electrónico de archivo:** Registro de la información generada, recibida, almacenada, y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital; es	*D. S. nº 052-2008* **Documento electrónico:** Es la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o

	en la etapa de memorización, de elaboración o de transmisión, para que se garantice la fidelidad e integridad de la información transmitida y b) se signe mediante firma digital. *Ley 25.506* 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.	producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos.	conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos.
Documento original	(*Decisión Ad 43/96)* Documento en su primera versión o de primera generación, cualquiera sea el soporte sobre el cual se extienda. Puede ser firmado o no firmado.	*Acuerdo No. 027-2006* Es la fuente primaria de información con todos los rasgos y características que permiten garantizar su autenticidad e integridad.	*NTP 392.030-2* Para los propósitos de la presente NTP, documento de una organización que autoriza su migración a microformas de cuyo origen y contenido es responsable.
Encargado del tratamiento:	*(Ley 1845 Ciudad Bs. As)* Persona física o de existencia ideal, autoridad pública, dependencia u organismo que, solo o juntamente con otros, realice tratamientos de datos personales por cuenta del responsable del archivo, registro, base o banco de datos.	Ley 1581 Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;	*D. S. Nº 003-2013* Es quien realiza el tratamiento de los datos personales, pudiendo ser el propio titular del banco de datos personales o el encargado del banco de datos personales u otra persona por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento de datos personales por orden

			del responsable del tratamiento cuando este se realice sin la existencia de un banco de datos personales.
Entidad de Certificación	Ver: autoridad certificante	*Ley 227* Es aquella persona que, autorizada conforme a la presente Ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.	***D-S-*** nº 019-2002/JUS Persona jurídica que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación.
Interoperabilidad		*Resolución 202 de 8/03/2010* Aptitud de los sistemas y aplicaciones, basados en Tecnologías de la Información y las Comunicaciones, y los procesos que estos soportan, para intercambiar información y posibilitar utilizar mutuamente la información intercambiada. Para el caso de redes de telecomunicaciones, la interoperabilidad es inherente a la interconexión de las mismas.	*D. S. nº 052-2008* Según el OASIS Forum Group la interoperabilidad puede definirse en tres áreas: • Interoperabilidad a nivel de componentes: consiste en la interacción entre sistemas que soportan o consumen directamente servicios relacionados con PKI. • Interoperabilidad a nivel de aplicación: consiste en la compatibilidad entre aplicaciones que se comunican entre sí. • Interoperabilidad entre dominios o infraestructuras PKI: consiste en la interacción de distintos sistemas de certificación PKI (dominios, infraestructuras), estableciendo relaciones de

			confianza que permiten el reconocimiento indistinto de los certificados digitales por parte de los terceros que confían.
Firma digital.	*(Ley 25.506)* 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. *(Res. 555/97 Min. T.y S.S.)* transformación de un mensaje empleando un criptosistema asimétrico tal que, una persona que posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante y si el mensaje ha sido modificado desde que se efectuó la transformación.	*Ley 227* Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación. **firma digital segura** es una firma digital que puede ser verificada de conformidad con un sistema o procedimiento de seguridad autorizado por la presente Ley o autorizado por las partes.	*NTP 392.030-2* A) Conjunto de datos anexados a un archivo electrónico que permite a un destinatario certificar su origen. B) Datos anexados a, o una transformación criptográfica de, una unidad de datos que permite al receptor de la unidad de datos probar el origen e integridad de la unidad de datos y proteger contra la falsificación por ejemplo, por el receptor. *Ley nº 27.269* Es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.
Firma electrónica	*Ley 25.506* Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera	*Decreto 2364* Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una	*D.S. 019/2002* Cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención

	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.	persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.	precisa de vincularse, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita.
Fuentes de acceso público irrestricto	*(Ley 1845 Ciudad Bs. As)* Exclusivamente, se entienden por tales a los boletines, diarios o repertorios oficiales, los medios de comunicación escritos, las guías telefónicas en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección o cualquier otro dato que indique de su pertenencia al grupo.		*(Ley nº 29.733)* **Fuentes accesibles para el público**. Bancos de datos personales de administración pública o privada, que pueden ser consultados por cualquier persona, previo abono de la contraprestación correspondiente, de ser el caso. Las fuentes accesibles para el público son determinadas en el reglamento.
Responsable del Tratamiento	*(Ley 1845 Ciudad Bs. As)* **Responsable del archivo, registro, base o banco de datos:** Persona física o de existencia ideal del sector público de la Ciudad de Buenos Aires que sea titular de un archivo, registro, base o banco de datos.	*Ley 1581* Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.	*D. S. Nº 003-2013* Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.
Sistema de Información.		*Ley 527* Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de	

		alguna otra forma mensajes de datos.	
Tratamiento de datos:	*Ley 25.326:* Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias. *(Ley 1845 Ciudad Bs. As)* Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relaciona-miento, evaluación, bloqueo, destrucción, registro, organización, elaboración, extracción, utilización, cotejo, supresión, y en general, el procesamiento de datos personales, así como también su cesión a terceros a través de todo tipo de comunicación, consulta, interconexión, transferencia, difusión, o cualquier otro medio que permita el acceso a los mismos.	Ley 1581 **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.	*Ley nº 29.733* **Tratamiento de datos personales***.* Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.
Usuario de datos	*Ley 25.326:* Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en	*Ley 227* **Usuario**: Dícese de la persona que sin ser suscriptor y sin	*Ley nº 27269* **Usuario final:** En líneas generales, es toda persona

	archivos, registros o bancos de datos propios o a través de conexión con los mismos. *(Ley 1845 Bs. As):* Persona física que, en ocasión del trabajo y cumpliendo sus tareas específicas, tenga acceso a los datos personales incluidos en cualquier archivo, registro, base o banco de datos del sector público de la Ciudad de Buenos Aires.	contratar los servicios de emisión de certificados de una Entidad de certificación, puede sin embargo validar la integridad y autenticidad de un mensaje de datos, con un certificado del suscriptor originador del mensaje. *Resolución 202 de 8/03/2010* **Usuario:** Persona natural o jurídica consumidora de servicios que hacen uso de las Tecnologías de la Información y las Comunicaciones.	que solicita cualquier tipo de servicio por parte de un Prestador de Servicios de Certificación Digital acreditado.

Comentarios y comparaciones

Digital / Electrónico:

Estos términos requieren un comentario inicial, ya que en los glosarios utilizados en algunos casos se utilizan como sinónimos, y otras veces con significado disímil.

Cuando se hace referencia a documento, en Argentina se lo define como digital, mientras que en Colombia como en Perú, se lo denomina electrónico. Entendemos que: el soporte de estos documentos es digital, o numérico, puesto que está constituido por series de "0" y "1"; que se encuentran en un espacio virtual, a diferencia de los documentos en soporte papel, que se están en un espacio analógico; que para acceder a ellos se requiere de equipamiento electrónico y que el procedimiento que se utiliza para gestionarlos es informático. Por lo tanto, si documento es básicamente soporte más información, consideramos que el término más correcto para definirlos es el de documento digital.

Las definiciones son bastante diferentes pero en todos los casos se refieren, sin lugar a dudas, a un mismo objeto:

En Argentina, la Resolución Nº 555/97 del Ministerio de Trabajo y Seguridad Social denomina **Documento digital** a una "representación en forma electrónica" signada mediante firma digital y la Ley 25.506 dice que es una "representación digital". En tanto,

el Acuerdo Nº 027/2006 del Consejo Directivo del Archivo General de la Nación de Colombia define **documento electrónico** como "información generada, recibida, almacenada, y comunicada por medios electrónicos", es decir, incluye en la definición no solo la representación, o sea, la generación, sino el tratamiento posterior. El Decreto Supremo nº 052-2008-PCM de Perú, por su parte, precisa que **documento electrónico** es "la unidad básica estructurada de información registrada, publicada o no, susceptible de ser generada, clasificada, gestionada, transmitida, procesada o conservada por una persona o una organización de acuerdo a sus requisitos funcionales, utilizando sistemas informáticos", con lo que incluye todo el proceso archivístico y alude al uso de sistemas informáticos en el tratamiento.

Cuando se trata de definir la firma, los tres países utilizan tanto "digital" como "electrónica" pero marcan la diferencia entre una y otra.

Cabe señalar que el ICA Multilingual Archival Terminology define **firma digital** como: "Un conjunto de números en código basado en técnicas criptográficas de llave pública y/o privada que se embebe dentro de un documento digital con el fin de garantizar que ese documento no ha sido alterado o modificado en forma alguna desde su producción y firma. También se le conoce como "firma electrónica avanzada" o por sus siglas: 'FEA' o 'FIEL'."[3]

Al comparar las definiciones de los glosarios se constata, *grosso modo*, que para Argentina se trata de la transformación de un mensaje empleando un criptosistema asimétrico y un sistema de doble claves (pública y privada) en tanto Colombia la entiende como un valor numérico que se adhiere a un mensaje de datos y que utiliza un procedimiento matemático para vincular las claves y Perú la define como firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves únicos. Si bien las definiciones son todas diferentes, incluso existen definiciones diferentes dentro de una misma nación, se observa que los tres países coinciden en que su finalidad es certificar la

[3] http://www.ciscra.org/mat/termdb/term/3032 [consultado el 29/09/2013]

autenticidad y la integridad del mensaje bajo el principio del 'no repudio', que su utilización exige un procedimiento matemático, o técnica de criptografía asimétrica, y mencionan la existencia de dos claves –privada y pública- para generar y verificar la firma.

En cuanto a la **firma electrónica**, el ICA Multilingual Archival Terminology dice que es "una marca digital que al ser agregada o ser lógicamente asociada a un documento de archivo funge como una firma sobre el mismo, y es usada por el firmante para asumir la responsabilidad u otorgar consentimiento sobre el contenido del documento de archivo".[4] El Portal de Administración Electrónica del Gobierno de España, por su parte, la define como conjunto de datos electrónicos que acompañan o que están asociados a un documento digital y cuyas funciones básicas son: identificar al firmante de manera inequívoca, asegurar la integridad del documento firmado y asegurar que el firmante no puede repudiar lo firmado.

La Ley 25.506 argentina la define como: "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 tanto, el Decreto 2364 de Colombia considera que son "Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos", y el Decreto Supremo 019/2002 de Perú, (derogado por Decreto Supremo 052/2008) precisaba que es "Cualquier símbolo basado en medios electrónicos utilizado con la intención precisa de vincularse, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita". Se puede observar que las tres definiciones especifican que son datos o símbolos electrónicos que se utilizan para identificar al autor de un documento digital y que solo la de Argentina aclara que la firma electrónica no incluye la totalidad de los requisitos que posee la firma digital.

[4] http://www.ciscra.org/mat/termdb/term/3033 [consultado el 29/09/2013]

Archivo

En los glosarios de Colombia y Perú se define archivo como conjunto de documentos e incluyen separadamente el término **Archivo electrónico.** En la legislación de Argentina, en cambio, el concepto dado para **Archivo** es, en realidad, el de **Archivo electrónico** o **digital.** Una diferencia interesante para destacar es que mientras Argentina refiere a "Colección de datos" o a "conjunto organizado de datos", Colombia alude a "conjunto de documentos electrónicos" y Perú, a "registros".

Documento /documento original:

La legislación argentina no define "documento" y se ocupa directamente de precisar los conceptos de "documento digital" (explicado más arriba) y de "documento original". Colombia, en tanto, diferencia "documento" de "documento de archivo" y la legislación peruana aclara, en la definición de "documento" que se incluyen todo tipo de soportes, entre ellos los informáticos.

En cuanto a **documento original,** debe señalarse que el término "original" es discutible cuando se hace referencia a documentos digitales y algunos especialistas en derecho informático entienden que lo correcto es hablar de "documento digital de origen". Más aún, dadas las características funcionales y de identidad de los documentos digitales, su valor radica en la autenticidad, fiabilidad y exactitud de la información, independientemente de su formato como documento. Sin embargo, los tres países que se estudian han definido este término, con algunas diferencias: en Argentina se explica que se trata del "documento en su primera versión o de primera generación, cualquiera sea el soporte sobre el cual se extienda", en Colombia se lo define como "fuente primaria de información con todos los rasgos y características que permiten garantizar su autenticidad e integridad" y la legislación peruana puntualiza que es el "documento de una organización que autoriza su migración a microformas de cuyo origen y contenido es responsable".

Otras similitudes y diferencias

En general, las diferencias entre las definiciones no son muchas. En algunos casos, se trata simplemente de detalles, no de conceptos. Así, por ejemplo, a la copia de un documento realizada para conservar la información contenida en el original en caso de pérdida o destrucción y destinada a ser utilizada para evitar el manipuleo del original, en Argentina se la llama **Copia de resguardo** mientras que en Colombia se la denomina **Copia de seguridad.** Del mismo modo, Colombia y Perú denominan **Entidad de Certificación** a la persona facultada para prestar los servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la firma digital y, en Argentina, esta entidad recibe el nombre de **Autoridad certificante.** En cuanto a las claves utilizadas en la firma digital, los conceptos de **Clave privada** y de **Clave pública** no difieren demasiado; solamente puede señalarse, respecto de la primera, que en Argentina se hace referencia a **crear** una firma digital, mientras que Colombia y Perú utilizan el término **genera**r una firma digital.

Hay, sin embargo, algunos pocos términos que se usan con distinto significado. Así: **autenticación** es, en Argentina, un procedimiento determinado *para otorgar autenticidad a un documento* o a su copia, mientras que en Perú es un proceso que permite *determinar la identidad de la persona que firma digitalmente*, pero que no otorga certificación notarial ni fe pública.

En cuanto al término **correo electrónico**, no incluido en los glosarios colombianos, para Perú es el *mensaje que se trasmite* mediante una red de interconexión entre computadoras, mientras que para Argentina es el *medio de transmisión del documento digital*.

Finalmente, se notan algunas diferencias en el concepto de **usuario.** Colombia da dos acepciones: es la persona que hace uso de las Tecnologías de la Información y las Comunicaciones, pero también aquella que puede validar la integridad y autenticidad de un mensaje de datos, con un certificado del suscriptor originador del mensaje. Perú entiende que **usuario final** es la persona que solicita cualquier tipo de servicio por parte

de un Prestador de Servicios de Certificación Digital acreditado. En Argentina, en tanto, la ley nacional define **usuario de datos** como la persona, pública o privada que realiza el tratamiento de datos, mientras que para la Ciudad Autónoma de Buenos Aires es la persona física que, en ocasión del trabajo y cumpliendo sus tareas específicas, tiene acceso a los datos personales incluidos en cualquier archivo, registro, base o banco de datos.

ACCESO A LA INFORMACIÓN, TRANSPARENCIA, PROTECCIÓN DE DATOS Y SU INCIDENCIA EN LA EVALUACIÓN DE DOCUMENTOS

La Evaluación de documentos de archivo como proceso técnico archivístico busca establecer los plazos de retención de las series documentales con el propósito de tomar decisiones respecto de su disposición. De acuerdo con criterios técnico-archivísticos, la metodología a emplearse, el marco legal aplicable y sobre todo la experiencia del profesional de archivos, se determinan los plazos sobre los cuales se decide la conservación definitiva de los documentos o su eliminación al término de dichos plazos.

Uno de los aspectos que inciden preferentemente para determinar dichos plazos de retención es, sin duda, el marco legal, tanto para la evaluación de los documentos en soporte de papel como en soporte electrónico. En principio, los criterios para decidir si los documentos tienen valor primario o secundario no cambian, sin embargo cuando se trata de documentos en medio electrónico es necesario, a partir del marco legal que ampara su tratamiento sea como documento digital de origen o digitalizado, así como las condiciones o requisitos para otorgarle el valor legal en ese medio de conservar documentos de archivo, tomar las medidas y consideraciones (requisitos funcionales) para su conservación a largo plazo para proteger su autenticidad y permanencia mientras se les necesite.

En el contexto legal, como soporte de las decisiones para la asignación de plazos de retención, se analizó la legislación sobre acceso a la información, transparencia y

protección de datos de Argentina, Colombia y Perú.

Cuadro comparativo N° 2: Principales disposiciones normativas: acceso a la información, transparencia y protección de datos

País	Acceso a la Información (Constitución Política)	Norma de menor rango: Transparencia	Norma de menor rango: Protección de datos
Argentina	No tiene norma específica, pero en el artículo 43 encontrarnos lo relativo a la protección de datos. Ley 25.831 de 26/11/2003, sobre protección ambiental, artículo 1º derecho de acceso a la información ambiental. Decreto 1172/2003 Anexo VII, artículo 10 sobre Accesibilidad exige medidas a tomar en los archivos, obligación de quien tiene en su poder la información. Constitución de la Ciudad de Buenos Aires, el artículo 16 señala que toda persona tiene, mediante una acción de amparo, libre acceso a todo registro, archivo o banco de datos de entidades públicas o privadas		Decisión Administrativa 43/96 del Jefe de Gabinete de Ministros, Capítulo XI: Destrucción, *normas sobre la eliminación de los documentos, que debe practicarse por cualquier medio que asegure su destrucción total o parcial de datos.*
Colombia	El acceso o uso de los documentos públicos, se encentra en el artículo 74º	Norma en proyecto desde el año 2011	Ley Estatutaria Nº 1581, de 2012 por la cual se dictan disposiciones generales para la protección de datos personales.
Perú	Artículo 2, incisos 5 y 6 señala como derechos fundamentales	Ley de Transparencia N°	Ley de protección de datos personales N°

	de la persona: 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido del Juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado. 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.	27806 (13.07.2002) Decreto Supremo número 072-2003-PCM, reglamento de la Ley 27.806	29.733 (2 julio 2011)

Análisis comparado: Argentina, Colombia y Perú

La legislación comparada según Galindo Vácha: "

> Es el análisis que se lleva a cabo sobre dos o más legislaciones, o más particularmente de una institución [jurídica] en dos o más países, verificando sus características, diferencias, semejanzas, bondades y dificultades. Es la concreción o la practicidad del derecho comparado. A través de ella se intenta obtener datos y particularidades de las legislaciones extranjeras, con fines académicos o prácticos; entre los primeros, puede contenerse el estudio de las instituciones, mientras que en el segundo puede comprenderse los fines de mejoramiento de la normatividad

nacional y de política legislativa.[5]

Un estudio de legislación comparada tiene como fin principal la integración normativa de los objetos de estudio, en el presente caso se trata de la legislación de tres países en lo relacionado con el acceso a la información, la transparencia y la protección de datos personales.

Adicionalmente, dado que nuestro objeto de estudio es la evaluación documental y la legislación es fundamental para la toma de decisiones al momento de establecer los plazos de retención de los documentos, tratamos de observar la vinculación directa o indirecta entre las dos áreas de conocimiento involucradas: el Derecho y la Archivística.

Como el estudio comparado en el campo del Derecho cumple diversos objetivos, en este caso nos dirigimos al soporte legal de la evaluación documental. A decir de Galindo Vácha uno de los aspectos que trata el derecho comparado es: "…el análisis de diversas realidades jurídicas, con el ánimo de desarrollar una nueva legislación por ejemplo comunitaria o común a varios países, tomando como base diferentes realidades y necesidades".[6]

Siempre siguiendo a Galindo Vácha, nos ubicamos en los fines académicos antes que en los fines prácticos, en tanto no pretendemos modificaciones normativas, sino apoyar las decisiones de evaluación de documentos desde el campo jurídico especializado, respecto de los plazos de retención y conservación de documentos digitales de archivo.

Centrándonos en la legislación de los países en estudio, diremos que de acuerdo con el principio de jerarquía normativa, todo Estado inicia su ordenamiento jurídico con la Constitución Política, por lo que empezaremos señalando los preceptos legales, de los países que comprende nuestro estudio, vinculados con el acceso a la información, transparencia y protección de datos.

En la normativa constitucional destacaremos, puntualmente, el derecho de acceso a la

---

[5] GALINDO VÁCHA, Juan Carlos, p. 54.

[6] Idem.

información, porque entendemos constituye la institución jurídica fundamental a partir de la cual se derivan otros derechos adyacentes como son el derecho que exigen los ciudadanos de un gobierno transparente y su derecho a la protección de datos personales.

Argentina no tiene legislado en la Constitución Política el derecho de acceso a la información de manera taxativa, pero en el artículo 43 encontrarnos lo relativo a la protección de datos, señalándose el derecho de toda persona a interponer una acción de amparo. La norma indica: "Toda persona podrá interponer acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación confidencialidad o actualización de aquellos."[7] De acuerdo con la norma, jurídicamente la protección de los datos personales queda instituida desde el máximo nivel jerárquico.

A diferencia de la Constitución Nacional, la de la ciudad Autónoma de Buenos Aires, (01/10/1996) en su artículo 16 señala que toda persona tiene, mediante una acción de amparo, libre acceso a todo registro, archivo o banco de datos que conste en organismos públicos o en los privados destinados a proveer informes, a fin de conocer cualquier asiento sobre su persona, su fuente, origen, finalidad o uso que del mismo se haga. También puede requerir su actualización, rectificación, confidencialidad o supresión, cuando esa información lesione o restrinja algún derecho. El ejercicio de este derecho no afecta el secreto de la fuente de información periodística. Como podemos apreciar la norma condensa el acceso a la información y la protección de datos, aunque media una acción de amparo para acceder a la información, por tanto no es una medida jurídica directa. Asimismo le confiere atribuciones al Defensor del Pueblo (artículo 3°) para solicitar vista de expedientes, informes, documentos, antecedentes y todo otro elemento que estime útil a los efectos de la investigación, aun aquellos clasificados como reservados

[7] CONSTITUCIÓN POLÍTICA DE ARGENTINA, http://www.cepal.org/oig/doc/ArgentinaConstitucionPolitica.pdf [Consulta: 14.07.2013]

o secretos, sin violar el carácter de estos últimos. Realizar inspecciones a oficinas, archivos y registros de los entes y organismos bajo su control.

La norma en referencia señala algunas excepciones de acceso vinculadas a la defensa nacional, la seguridad interior, relaciones internacionales, perjuicio a terceros, el secreto comercial, industrial, la propiedad intelectual, etc. Esta es una restricción que se encuentra en la legislación de todos los países que regulan el acceso a la información pública.

Tanto Colombia como Perú norman constitucionalmente, de manera más directa, el acceso o uso de los documentos públicos. Para **Colombia**, según el Artículo 74º de su Constitución Política: "Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley. El secreto profesional es inviolable"[8] con lo que queda claro que el acceso no es indiscriminado, tal como sucede con otras constituciones, en tanto la ley marcará en forma expresa los casos de excepción a la regla constitucional.

El **Perú**, en el artículo 2, incisos 5 y 6 señala, toda persona tiene derecho:

> 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.
>
> 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.[9]

Como podemos comprobar tanto para Colombia como para el Perú la ley marca las restricciones al acceso, y señalan que las normas pertinentes establecerán expresamente las excepciones. En forma similar a la Constitución Argentina respecto de los datos personales, protegen la intimidad personal, lo que se inscribe en la denominada

---

[8] CONSTITUCIÓN POLÍTICA DE COLOMBIA, http://cms-static.colombiaaprende.edu.co/cache/binaries/articles-186370_constitucion_politica.pdf?binary_rand=1416 [Consulta: 14.07.2013]

[9] CONSTITUCIÓN POLÍTICA DEL PERÚ, http://www.tc.gob.pe/constitucion.pdf [consulta: 15.07.2013]

'protección de datos personales'.

Cuadro comparativo N° 3: Resumen comparativo (área constitucional)

País	Alcance normativo	Comentario
Argentina	No contiene norma específica sobre acceso a la información. Constitución de la Ciudad Autónoma de Buenos Aires, artículo 16 es puntual respecto del acceso a todo registro, archivo o banco de datos	El acceso a la información se establece como derecho a la protección de datos. Mecanismo para accionar: acción de amparo
Colombia	Art. 74 Acceso a la información y derecho del secreto profesional	Comprende la inviolabilidad del secreto profesional lo que no incluye Argentina y Perú en este aspecto constitucional de derecho a la información.
Perú	Art. 2 incisos 5 y 6 Acceso a solicitar y recibir información y protección de la intimidad respecto de servicios informáticos y especializados	Incluye la información que se sirve por medios electrónicos, concretamente se vincula con la protección de la intimidad personal, respecto de información que se encuentran en los bancos de datos.

A la luz de los preceptos legales referidos, abordaremos seguidamente los dispositivos legales específicos que se derivan de los principios constitucionales, motivo de nuestro estudio, en la legislación especializada respectiva.

Sobre el acceso a la información, no obstante que la Constitución argentina omite regularlo de manera expresa, encontramos legislado este derecho en normas expresas como la Ley 25.831 de 26/11/2003, sobre protección ambiental, que en su artículo 1º señala los presupuestos mínimos de protección ambiental para garantizar el derecho de acceso a la información ambiental que se encontrase en poder del Estado y entes autárquicos y empresas prestadoras de servicios públicos, sean públicas, privadas o mixtas.

Entendemos que al no estar normado directamente el acceso a la información, por la vía del precedente constitucional vinculante, el acceso a la información se recoge en la

normativa de menor rango que en esencia lleva el mismo objetivo de facilitar la información a los ciudadanos reconociendo su derecho a solicitarla. La norma en referencia entonces, regula un derecho por el cual la ciudadanía puede obtener información en poder de las autoridades públicas, esto es el derecho a recibir información ambientalmente relevante por parte de la administración pública que está obligada a publicitarla sin requerimiento previo. Este tipo de legislación hace algunas precisiones, pero mayormente coincide con las exigencias de acceso a la información de manera genérica y la transparencia. Doctrinariamente la legislación sobre acceso a la información ambiental comprende propiamente: el estado de los elementos del medio ambiente, factores, salud de las personas, etc., por lo tanto se dirige a un sector muy específico de información.

De otro lado el Decreto 1172/2003 de 3/12/2003, Anexo VII en su artículo 10 sobre Accesibilidad, exige medidas de archivos a la que está obligado quien tiene en su poder la información, quien debe realizar una adecuada organización, sistematización y disponibilidad, asegurando un amplio y fácil acceso, debiendo además generar, actualizar y dar a conocer información básica, con el suficiente detalle para su individualización, a fin de orientar al público en el ejercicio de su derecho.

La Ley 104 de la Ciudad Autónoma de Buenos Aires (19/11/98) artículo 1°, establece el derecho de toda persona a recibir información completa, veraz, adecuada y oportuna, de cualquier órgano perteneciente a la Administración Central, Descentralizada, Entes Autárquicos, Organismos Interjurisdiccionales integrados por la Ciudad Autónoma de Buenos Aires, Empresas y Sociedades del Estado, Sociedades Anónimas con participación Estatal mayoritaria, Sociedades de economía mixta, todas aquellas otras organizaciones empresariales donde el Estado de la Ciudad tenga participación en el capital o en la formación de las decisiones societarias, del Poder Legislativo, Judicial, entes Públicos no Estatales, en cuanto a su actividad administrativa, y de los demás órganos establecidos en el Libro II de la Constitución de la Ciudad de Buenos Aires. (Conforme texto Artículo 1º de la Ley número 1391, BOCBA número 2011 del 26 de agosto de 2004) Esta norma de mayor amplitud comprende prácticamente todos los archivos públicos de la Ciudad Autónoma de

Buenos Aires. Y en el artículo 2° puntualmente indica el tipo de información a proveerse, esta es: la información contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital, o en cualquier otro formato y que haya sido creada u obtenida por el órgano requerido que se encuentre en su posesión y bajo su control.

Se considera como información a los efectos de esta ley, cualquier tipo de documentación que sirva de base a un acto administrativo, así como las actas de reuniones oficiales. El órgano requerido no tiene obligación de crear o producir información con la que no cuente al momento de efectuarse el pedido.

Notamos que la enumeración de los tipos documentales incluye de manera expresa los documentos digitales.

Colombia, dentro de los alcances de la norma constitucional y la legislación archivística vigente, expide el Acuerdo AGN N° 004 (15/03/2013), sobre Acceso, Consulta y Visualización de Fondos Documentales, que en su artículo 14 establece la consulta en línea de los instrumentos de descripción documental de los archivos históricos públicos o privados, se insta a las organizaciones que los conservan a desarrollar procesos de descripción documental que faciliten la consulta, mediante la aplicación de las normas de descripción documental del Consejo Internacional de Archivos, también se hace lo propio respecto de los documentos administrativos, contratos y otras series documentales, así como con los expedientes compuestos, debiendo las organizaciones públicas desarrollar procesos de descripción documental para la consulta en línea, siempre que los documentos no tengan carácter reservado de acuerdo con la Constitución o la Ley. La norma señala que cuando se trata de expedientes electrónicos se implementarán los medios tecnológicos para su registro y control que permitan la generación de un índice electrónico que asegure su integridad y completitud. En cuanto a la compatibilidad e interoperabilidad, se indica que en la adopción de tecnologías de la información y comunicaciones, en la producción, organización, conservación, control, acceso y preservación de los documentos de archivo, se deberá garantizar la compatibilidad de las

herramientas tecnológicas, e interoperables con el sistema de gestión documental entre entidades públicas y cumplir con las normas expedidas por el Archivo General de la Nación (AGN), en el mismo sentido se establece que los sistemas deben permitir la transferencia de información al Sistema del AGN y a los archivos generales territoriales.

Perú tiene legislado el Acceso a la información a partir de la Constitución Política de 1993 tal como ya lo hemos expresado líneas arriba. Teniendo como base el marco legal constitucional se emitieron normas de menor nivel jerárquico de manera secuencial y progresiva. Así, el Decreto Supremo nº 018-2001-PCM de acceso a la información, fue el punto de partida respecto de la legislación que vino más adelante; este dispositivo legal en su artículo 2º señala los siguientes criterios: El procedimiento deberá permitir que el acceso a la información pueda realizarse por escrito, otros medios físicos, medios electrónicos o magnéticos de acuerdo a lo solicitado y a la capacidad de la dependencia. De no indicarse el medio por el cual se entregará la información, la entidad utilizará el medio escrito, salvo que se acuerde con el interesado la utilización de otro medio de entrega de la información. Este decreto supremo fue el antecedente de la Ley de Transparencia N° 27.806 (13/07/2002) en el que encontramos una disposición vinculada con nuestro foco de atención, la Evaluación Documental cuando señala que la eliminación de documentos se realizará en aplicación de procedimiento establecido, con la autorización del Archivo Nacional y en el artículo 18° de la ley se enfatiza que ningún caso la entidad de la Administración Pública podrá destruir la información que posea. Además la entidad de la Administración Pública deberá remitir al Archivo Nacional la información que obre en su poder, en los plazos estipulados por la Ley de la materia. El Archivo Nacional podrá destruir la información que no tenga utilidad pública, cuando haya transcurrido un plazo razonable durante el cual no se haya requerido dicha información y de acuerdo a la normatividad por la que se rige el Archivo Nacional.

El artículo 10 de la ley establece que las entidades de la Administración Pública tienen la obligación de proveer la información requerida si se refiere a la contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital, o en cualquier otro

formato, siempre que haya sido creada u obtenida por ella o que se encuentre en su posesión o bajo su control.

Respecto de los documentos electrónicos o digitales la Ley 27.927 de 13/01/2003, que modifica la Ley 27.806 Ley de Transparencia y Acceso a la información Pública establece la responsabilidad del Estado de crear y mantener registros públicos de manera profesional para que el derecho a la información pueda ejercerse a plenitud. En ningún caso la entidad de la Administración Pública podrá destruir la información que posea.

La norma debió mencionar la obligación de las entidades del Estado de 'crear o producir y mantener documentos públicos de manera profesional', no registros debido a que no es el término más exacto cuando se refiere a los archivos, como es el caso; sin embargo rescatamos la norma regulatoria que exige el tratamiento profesional, entendemos archivístico, de los documentos de la Administración Pública, tal como se precisa varios años después con la norma que agrega otros artículos al reglamento de la ley de transparencia, como veremos seguidamente.

El Decreto Supremo número 072-2003-PCM, reglamento de la Ley 27.806 de Transparencia y Acceso a la Información Pública (07/08/2003), en el artículo 15° legisla sobre la entrega de la información solicitada en las unidades de recepción documentaria. Al respecto, la solicitud de información que genere una respuesta que esté contenida en medio magnético o impresa, será puesta a disposición del solicitante en la unidad de recepción documentaria o el módulo habilitado para tales efectos, previa presentación de la constancia de pago en caso de existir costo de reproducción. Recientemente el Decreto Supremo N° 070 que modifica el anterior, agrega el artículo 25 sobre digitalización de documentos, en el sentido que ésta, la información, su organización y conservación se realizarán obligatoriamente conforme a la normativa sobre la materia y las políticas y lineamientos emanadas del Sistema Nacional de Archivos, debemos advertir que a la fecha que esto escribimos, el AGN, organismo rector del Sistema, no ha emitido norma alguna sobre el tema.

Cuadro comparativo N° 4: Resumen comparativo (Área de transparencia)

País	Alcance normativo	Comentario
Argentina	No contiene norma específica sobre transparencia de la función pública. El tema se inserta en normas como: Ley 25.831 sobre protección ambiental dirigida a los documentos de ese sector, cuyos postulados se inscriben en la obligación de transparentar la información sobre el tema que poseen. El Decreto 1172/2003, Anexo VII en su artículo 10 sobre Accesibilidad, exige medidas de archivos a la que está obligado quien tiene en su poder la información pública. Ley 104 de la Ciudad Autónoma de Buenos Aires, regula el acceso a la información contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital.	Normas de menor nivel jerárquico a la Constitución Política, regulan el derecho de los ciudadanos a recibir información de los organismos en posesión de documentos públicos. Se destaca la norma sobre protección medio ambiental, pero circunscrita a los documentos de ese género. No obstante existe normativa local importante (teniendo en cuenta que se trata de un país con estados federales) que puntualiza en la necesidad de mantener archivos en buen estado para cumplir con la transparencia y que incluye los documentos digitales.
Colombia	No cuenta con una ley regulatoria de la transparencia. Se aprobó una norma sobre transparencia en el año 2012, pero fue declarada inexequible por el Tribunal Constitucional, actualmente la norma no se encuentra reglamentada ni en vigencia, por tanto no es posible considerarla para su análisis jurídico. El Acuerdo AGN N° 004 (15/03/2013), Acceso, Consulta y Visualización de Fondos Documentales se centra en documentos históricos, e incluye la interoperabilidad para facilitar el acceso en línea de los documentos.	Al no contar con un texto normativo exclusivamente dirigido a la transparencia y facilidades de acceso a la información, de carácter público, entendemos que el AGN suple de alguna manera el vacío normativo, sin embargo debemos precisar que trata del acceso a los documentos históricos lo que se refiere básicamente a la investigación y luego incide en los documentos administrativos incorporando el concepto de interoperabilidad para facilitar el acceso a los documentos o expedientes de carácter público. Existe un proyecto de Ley de transparencia que atenderá el vacío normativo.
Perú	Primer antecedente normativo a partir de la Constitución Política, Decreto Supremo nº 018-2001-PCM, incluye documentos electrónicos o magnéticos.	Las normas regulatorias sobre transparencia y rendición de cuentas derivan de los principios constitucionales anotados líneas

	Ley 27806, refiere la eliminación de documentos al cumplimiento de los plazos de retención. Ley 27.927 modifica la Ley 27.806 establece la responsabilidad del Estado de crear y mantener registros públicos de manera profesional. Decreto Supremo N° 070-2013-PCM, artículo 25 sobre digitalización de documentos de acuerdo con la normativa del Sistema Nacional de Archivos (SNA)	arriba. El Decreto Supremo 070-2013-PCM supera una omisión respecto del rol de los archiveros y del SNA en la efectividad de la transparencia y rendición de cuentas.

En cuanto a la protección de datos **Argentina** cuenta con la Ley N° 25.326 de Protección de Datos Personales que fue promulgada con observaciones el 30/10/2000. Luego vino el Texto actualizado con las modificaciones de La ley 26.343 BO 9/01/2008 publicado en el Boletín Oficial (2/11/2000) Posteriormente se dictaron medidas reglamentarias y complementarias como el Decreto 1558/2001 (29/11/2001) Reglamento de la Ley en referencia, la Disposición 7/2005 D N de protección de datos Personales, Clasificación de Infracciones y Graduación de sanciones; y la Disposición 11/2006 D N de protección de datos Personales, Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados que desarrollan de manera amplia la materia que nos ocupa.

En su Artículo 1° la Ley en referencia indica su objeto refiriéndose a la protección integral de los datos personales que se encuentran en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos; públicos o privados. Asimismo se señala que la ley es aplicable a personas de existencia ideal, es decir a la persona jurídica.

Entre los principios de la norma, como también prevén las de los países de Colombia y Perú que luego abordaremos, destacamos el indicado en el Artículo 9°, Seguridad de los datos. Por este principio el responsable o usuario del archivo – que a nuestro modo de ver puede o debería ser un profesional de archivo – de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida,

consulta o tratamiento no autorizado y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Además se prohíbe el registro de datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad. Por lo que apreciamos, las medidas de seguridad son rígidas con la finalidad de proteger la información y su confidencialidad que es otro de los principios que marca la Ley.

En el Capítulo IV, Artículo 21, se exige que todo registro de archivos de datos comprenda información, entre otras especificaciones, sobre las características y finalidad del archivo; medios utilizados para garantizar la seguridad de los datos y el tiempo de conservación de los datos. En el artículo 22 sobre archivos, registros o bancos de datos públicos se indica que las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial, debiendo indicar igualmente lo señalado en el numeral anterior respecto de los registros de carácter privado. Se adiciona la necesidad de contar con estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán; los órganos responsables del archivo, precisando dependencia jerárquica.

En cuanto al Control la norma es muy precisa, encargándose al órgano correspondiente (entiéndase el Órgano de Control de la entidad) realizar todas las acciones necesarias para el cumplimiento de los objetivos con la finalidad de que, entre otras acciones, se dicten las normas y la reglamentación para el desarrollo de las actividades propias de la Ley como realizar un censo de archivos, registros o bancos de datos y mantener el registro permanente de los mismos; y controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. Asimismo se podrá solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran; controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el

Registro creado por la misma ley.

En cuanto al Decreto 1558/2001 (29/11/2001) Reglamento de la Ley destacamos el artículo 29° numeral 5 que establece las funciones de la Dirección Nacional de Protección de Datos Personales, además de las que surgen de la Ley Nº 25.326. Esta dirección está encargada de dictar normas y procedimientos técnicos, entre otros, los relativos al tratamiento y condiciones de seguridad de los archivos, registros y bases o bancos de datos públicos y privados;

Una norma complementaria, que desde nuestro punto de vista es de suma importancia, es la Disposición 11/2006 Dirección Nacional de Protección de Datos Personales, sobre Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados, publicada en el Boletín Oficial (22/09/2006) que establece en cuanto a Medidas de Seguridad de Nivel Básico que los archivos, registros, bases y bancos de datos que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas, disponiendo del Documento de Seguridad de Datos Personales en el que se especifiquen, entre otros, los procedimientos y las medidas de seguridad a observar sobre los archivos, registros, bases y bancos que contengan datos de carácter personal, el que debe estar actualizado y ser revisado cuando se produzcan cambios en el sistema de información. Esto nos lleva a pensar en las eventuales evaluaciones de documentos, que necesariamente deberán registrarse.

Las medidas son muy específicas y técnicas, como los registros de incidentes de seguridad, notificación, gestión y respuesta ante los incidentes de seguridad; procedimientos para efectuar las copias de respaldo y de recuperación de datos, etc.

En el caso de la autenticación se pide utilizar contraseña, que será asignada por el responsable de seguridad de acuerdo a un procedimiento que garantice su confidencialidad; control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados; se deberán adoptar medidas de prevención a efectos de impedir amenazas de software malicioso, etc., así

como garantizar una adecuada Gestión de los Soportes que contengan datos de carácter personal (identificación del tipo de información que contienen, almacenamiento en lugares de acceso restringidos, inventarios, autorización para su salida fuera del local en que están ubicados, destrucción de la información en desuso, etc.). Estas medidas corresponden al ámbito tecnológico informático pero también a la archivística propiamente.

En lo que se refiere a Medidas de Seguridad de Nivel Medio se debe contar con el Instructivo de seguridad para identificar al Responsable (u órgano específico) de Seguridad; y se realizarán auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos

En lo que corresponde a Medidas de Seguridad de nivel crítico los archivos, registros, bases y bancos de datos que contengan datos personales, definidos como "datos sensibles", además de las medidas de seguridad de nivel Básico y Medio, deberán distribuir soportes que contengan archivos con datos de carácter personal —incluidas las copias de respaldo—, cifradas (o utilizar cualquier otro mecanismo) para garantizar que no puedan ser leídos o manipulados durante su transporte; se deberá disponer de un registro de accesos. Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como mínimo por el término de un tres (3) años. Cabe señalar que en este caso preciso se cuenta con un término de prescripción legal que deberá ser aplicado en el momento de tomar decisiones sobre su conservación o eliminación como resultado de la evaluación documental.

Por otro lado, las copias de respaldo debe ser situadas fuera de la localización y disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.

También respecto de la protección de datos, **Colombia** cuenta con la Ley Estatutaria

No.1581 de 18/10/2012 por la cual se dictan disposiciones generales para la protección de datos personales. La norma señala que se trata de desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política sobre protección de datos personales.

La norma establece excepciones a la protección de datos personales, no siendo de aplicación: "a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico; Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley; b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; d) A las bases de datos y archivos de información periodística y otros contenidos editoriales; e) A las bases de datos y archivos regulados por la Ley 1266 de 2008; f) A las bases de datos y archivos regulados por la Ley 79 de 1993".

En el artículo 11.- Suministro de la información, se señala: "La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos".

Como podemos apreciar se protege específicamente la autenticidad de los datos.

El Gobierno Nacional establecerá la forma en la cual los Responsables del Tratamiento y Encargados del Tratamiento deberán suministrar la información del Titular, atendiendo a la naturaleza del dato personal.

Convenimos que el responsable directo del tratamiento de los datos debería ser un

archivero, esta situación no se encuentra estipulada en ninguna norma de su género, pero es lo que correspondería.

El artículo 12, respecto del encargado del tratamiento de los datos establece que el Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en ese artículo y, cuando el Titular lo solicite, entregarle copia. Además sus responsabilidades están señaladas en el TÍTULO VI.- Deberes de los responsables del tratamiento y encargados del tratamiento: "Los Responsables del Tratamiento deberán cumplir los siguientes deberes: a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data; b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular; c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada; d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible; f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada; g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento; h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley; i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular."

En el artículo 18 se señalan los Deberes de los Encargados del Tratamiento.-[destacamos solamente los incisos vinculados, de alguna manera a nuestro objeto de estudio: la evaluación documental]: "a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data; b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no

autorizado o fraudulento; c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley; j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella."

La norma colombiana incide especialmente en las medidas de seguridad de los datos y en las responsabilidades que asume quien se encarga del tratamiento de los datos.

Perú cuenta con la ley de protección de datos personales N° 29.733 (02/07/2011) la cual, en su artículo 18°, legisla sobre el derecho de información del titular de datos personales, en ese sentido el titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados, entre otros temas, así como ser informado sobre el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello. Además el artículo 28° que regula las obligaciones (Del Titular y encargado de datos personales) en el inciso 6 permite suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto; o (inciso 7) suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.

En la misma forma que la ley colombiana se asignan una serie de responsabilidades al responsable del tratamiento de los datos a partir del artículo 28° de la ley, entre otros: Efectuar el tratamiento de datos personales, solo previo consentimiento informado, expreso e inequívoco del titular de los datos personales, salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14 de la Ley; no recopilar datos personales por medios fraudulentos, desleales o ilícitos; recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido; no utilizar los datos

personales objeto de tratamiento para finalidades distintas de aquellas que motivaron su recopilación, salvo que medie procedimiento de anonimización o disociación; almacenar los datos personales de manera que se posibilite el ejercicio de los derechos de su titular; suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto; suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación, etc.

La norma peruana no llega a la precisión lograda por la norma colombiana respecto de las medidas de seguridad en la conservación de los datos. Sin embargo veremos a continuación que el reglamento hace las especificaciones de las medidas de seguridad agenciándose de la norma ISO 17799.

La ley en referencia ha sido reglamentada por el DS.003-2013 que en su artículo 39° regula sobre la generación y mantenimiento de los registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes.

Se aclara que estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros [Exigencias de autenticidad], una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros. En el artículo 40° relativo a la conservación, respaldo y recuperación de los datos personales, establece que los ambientes en los que se procese, almacene o transmita la información deberán ser implementados, con controles de seguridad apropiados, tomando como referencia las recomendaciones de seguridad física y ambiental recomendados en la “NTP ISO/IEC 17799 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información.” en la edición que se encuentre vigente. Adicionalmente, se deben contemplar los mecanismos de respaldo de seguridad de la información de la base de datos personales con un

procedimiento que contemple la verificación de la integridad de los datos almacenados en el respaldo, incluyendo cuando sea pertinente, la recuperación completa ante una interrupción o daño, garantizando el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño. El artículo 45° respecto del traslado de documentación no automatizada, textualmente dice: "Siempre que se proceda al traslado físico de la documentación contenida en un banco de datos, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado. Más adelante en el artículo 69° sumillado como Improcedencia de la supresión o cancelación, se regula sobre la supresión, indicándose que ésta no procederá cuando los datos personales deban ser conservados en virtud de razones históricas, estadísticas o científicas de acuerdo con la legislación aplicable o, en su caso, en las relaciones contractuales entre el responsable y el titular de los datos personales, que justifiquen el tratamiento de los mismos.

Debemos destacar en las Disposiciones Complementarias Finales, la Primera, referente a la interoperabilidad entre entidades públicas. Respecto de la definición, los alcances y el contenido de la interoperabilidad, y los lineamientos para su aplicación y funcionamiento en concordancia con las normas de protección de datos personales, encarga a la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI de la Presidencia del Consejo de Ministros, en su calidad de ente Rector del Sistema Nacional de Informática. La interoperabilidad entre entidades se regulará en cuanto a su implementación en el marco de lo dispuesto por el numeral 76.2.2 del inciso 76.2 del artículo 76 de la Ley Nº 27444, Ley del Procedimiento Administrativo General, Constitución Política, art. 2, inc. 6.

Cuadro comparativo N° 5: Resumen comparativo (Área protección de datos)

País	Alcance normativo	Comentario
Argentina	Ley N° 25.326 de Protección de Datos Personales Decreto 1558/2001 (29/11/2001)	Desarrolla el ercer párrafo del Art. 43 de la Constitución Política Reglamentación de la ley nº

		25.326 Clasificación de Infracciones y Graduación de sanciones Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados
	Disposición 7/2005 D N de protección de datos Personales Disposición 11/2006 D N de protección de datos Personales	
Colombia	Ley Estatutaria No.1581 protección de datos personales. El artículo 12, señala las responsabilidades para el tratamiento de los datos.	Las responsabilidades en el tratamiento de los datos personales se regulan de manera extensa.
Perú	Ley N° 29.733, en su artículo 18° legisla sobre el derecho de información del titular de datos personales. Artículo 28° responsabilidades en el tratamiento de datos personales. Artículo 40° relativo a la conservación de datos personales. Medidas para la Interoperabilidad entre entidades públicas. Encarga a la Oficina de E-Gobierno	Al igual que la norma colombiana se pone especial atención en la seguridad de los datos personales y responsabilidades en el tratamiento de los datos.

Las realidades obtenidas de la legislación revisada otorga un marco normativo en las áreas señaladas, que nos permiten visualizar las necesidades normativas para nuestro propósito: la evaluación documental, en la medida que nos permitirá tomar decisiones sobre los valores de los documentos (primario o secundario para su conservación en determinados plazos de retención) teniendo en cuenta las posibilidades de su recuperación en el largo plazo cuando los documentos se encuentran en soporte electrónico.

Apoyo legal para la toma de decisiones en evaluación documental

La normativa analizada a partir de las constituciones políticas y normas específicas sobre acceso a la información, transparencia y protección de datos, fundamentan la toma de decisiones en la evaluación de los documentos digitales de archivos en la medida que se sustenta por un lado, la conservación de los documentos de archivo para facilitar la información a los usuarios, por lo que las decisiones de eliminación deberán contemplar la

vigencia de los documentos para efectos de rendición de cuentas y necesidades de información de los usuarios o administrados; y por otro lado, en la permanencia de la autenticidad de los documentos mientras se les necesite. Ambos temas son fundamentales para el servicio de información toda vez que los documentos deberán ser accesibles en condiciones que permita su uso de información, administrativo o jurisdiccional.

Las normas sobre estos temas, si bien aplican a los documentos en soporte de papel, comprometen aún más a los archiveros cuando de documentos digitales se trata, por lo que la toma de decisiones para optar por la destrucción de documentos en determinados plazos de retención, será siempre muy comprometida, no es sencillo pero tampoco imposible precisar cuál es la información de interés para el administrado y que además solicitará basándose en el marco regulatorio vigente de acceso a la información pública. Mucho dependerá de la experiencia y solvencia profesional del evaluador: el archivero.

Asimismo las normas relativas a la protección de datos examinadas nos llevan al mismo resultado, con la diferencia que en este caso el interés del titular de los datos es directo, en esta situación no está en juego el interés de la sociedad sino básicamente del titular de los datos. Cualquier decisión de destrucción deberá ser consultada y/o corroborada por el interesado directo, aquél a quien los datos pertenecen.

COMPARACION DE CONCEPTOS Y APLICACIONES SOBRE FIRMA DIGITAL

La premisa para la realización de este análisis fue lograr tener una aproximación de los avances que se han efectuado sobre firma digital en los países estudiados y poder realizar una comparación de la legislación vigente. Para ello se tomaron las siguientes normativas:

ARGENTINA

- Ley 25.506 de 14/11/2001: sobre Firma digital
- Decreto Nº 2628/2002: reglamenta la Ley Nº 25.506/2002 y contiene, además, consideraciones generales y autoridad de aplicación.
- Decreto 409/2005: sobre Autoridad de Aplicación.
- Decreto Nº 658/2002: que modifica la normativa que regula las formas de

presentación de declaraciones juradas ante la Administración Federal de Ingresos Públicos. En su artículo 1º reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, estableciendo que las declaraciones juradas podrán ser presentadas firmadas en papel o por medios electrónicos.

COLOMBIA

- Ley 527 de 18/08/1999, que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.
- Decreto 1747/2000: por el cual se reglamenta parcialmente la Ley 527.
- Decreto N° 2364/2012: por medio del cual se reglamenta el artículo 7 de la Ley 527/1999, sobre la firma electrónica y se dictan otras disposiciones.
- Decreto 805/2013 Reglamenta art. 173 del Decreto 19/2012.

PERU

- Ley nº 27269 del 8/05/2000 - Ley de Firmas y Certificados Digitales, modificada por la Ley nº 27310/2000.
- Ley 27.291/2000, que modificó el Código Civil, permitiendo la utilización de medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica, sobre todo en el área de contratos.
- Decreto Supremo nº 019-2002/JUS, Reglamento de la Ley de firmas y certificados digitales N° 27269

Cuadro comparativo N°6: Análisis comparativo temático

CONCEPTO	**ARGENTINA** **LEY 25.506**	**COLOMBIA** **LEY 527**	**PERU** **LEY 27.269**
	Artículo 2. Se entiende por firma digital al resultado de aplicar a un documento digital	Artículo 2. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y	Artículo 3. La firma digital es aquella firma electrónica que utiliza una técnica de

Firma 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. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.	que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación	criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.
Ámbito de Aplicación	En todo el territorio Argentino Artículo 47. Utilización por el Estado Nacional. El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes. Artículo 48**.** Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y	Artículo 1. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos. Artículo 10. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.	Artículo 2. La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

	control por parte del interesado, propendiendo a la progresiva despapelización.		
Excepciones	Artículo 4. Exclusiones. Las disposiciones de esta ley no son aplicables: a) A las disposiciones por causa de muerte; b) A los actos jurídicos del derecho de familia; c) A los actos personalísimos en general; d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes	Artículo 1. La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos: a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales; b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.	Artículo 2. La presente ley se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.
Validez de la Firma Digital	Artículo 9. Validez. Una firma digital es válida si cumple con 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, según el artículo 16 de la presente, por un certificador licenciado.	Artículo 7. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si: a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación; b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.	Artículo 5. Obligaciones del titular de la firma digital. El titular de la firma digital tiene la obligación de brindar a las entidades de certificación ya los terceras con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas.

		Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma.	
Requerimiento de la Firma	Artículo 3. Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.	Artículo 6. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información que este contiene es accesible para su posterior consulta	Artículo l. La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad.
Certificados Digitales	Artículo 13. 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. Artículo 14. Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos 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:	Artículo 29. Características y requerimientos de las entidades de Certificación. Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones: a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación; b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de	Artículo 6. Certificado digital. El certificado digital es el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula una parte claves con una persona determinada confirmando su identidad. Artículo 7. Contenido del certificado digital. Los certificados digitales emitidos por las entidades de certificación deben contener al menos: **1.** Datos que identifiquen indubitablemente al suscriptor. **2.** Datos que identifiquen a la Entidad de Certificación. **3.** La clave pública. **4.** La metodología para

	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.	certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley; c) Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto. - Artículo declarado EXEQUIBLE por la Corte Constitucional mediante Sentencia C-662-0023 de 8 de junio de 2000, Magistrado Ponente Dr. Fabio Morón Díaz.	verificar la firma digital del suscriptor impuesta a un mensaje de datos. **5.** Número de serie del certificado. **6.** Vigencia del certificado. **7.** Firma digital de la Entidad de Certificación.
Decretos Reglamentarios de la Ley Madre	**Decreto Nº 2628/2002** reglamenta la Ley Nº 25.506/2002 y, entre otras cosas, contiene consideraciones generales y autoridad de aplicación**.** Artículo 1°. La presente reglamentación regula el empleo de la firma electrónica y de la firma digital y su eficacia jurídica. En los casos contemplados por los artículos 3°, 4° y 5° de la Ley N° 25.506 podrán utilizarse los siguientes sistemas de comprobación de	**Decreto Nº 2364 de 2012** reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. *Firma electrónica:* Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como	**Decreto Supremo N° 019-2002** Artículo 1. Aprobar el Reglamento de la Ley de Firmas y Certificados Digitales - Ley N’ 27269, que consta de tres (3) Títulos, cincuenta (50) Artículos y dos (2) Disposiciones Finales. **Artículo 2**. Designar al instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) como la autoridad administrativa competente, conforme a lo

	autoría e integridad: a) Firma electrónica, b) Firma electrónica basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación. c) Firma digital basada en certificados digitales emitidos por certificadores licenciados en el marco de la presente reglamentación, d) Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos: 1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero. 2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación.	cualquier acuerdo pertinente. **Decreto 1747 de 11/09/2000,** reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales."	establecido en el Artículo 15'de la Ley N'27269 Normas Generales CAPITULO 1 Artículo 1º. - Objeto El Reglamento regula, para el sector público y privado, la utilización de firmas electrónicas en mensaje de datos y documentos electrónicos, generadas bajo la Infraestructura Oficial de Firma Electrónica comprendiendo el régimen de acreditación y supervisión de las entidades de certificación, así como do las entidades de registro o verificación, establecidas en la Ley No. 27269 - Ley de Firmas y Certificados Digitales, modificada en su Artículo 11o. por la Ley N' 27310. Cuando en el Reglamento haga referencia a la Ley, debe entenderse referida a la Ley N' 27269, Ley de Firmas y Certificados Digitales. Cuando se mencione el Reglamento debe entenderse referido al presente Reglamento, de la Ley N' 27269. Las firmas electrónicas aprobadas por la autoridad administrativa competente, tienen, desde su aprobación los mismos efectos que las firmas generadas bajo la Infraestructura Oficial de

			Firma Electrónica conforme a lo establecido en el Reglamento.
Autoridad Competente	**Ley 25506** Artículo 29**.** La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros **Decreto Nº 409/2005:** establece que la Subsecretaría de la Gestión Pública actuará como autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital.	**Ley 527** Artículo 41. La Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación, y adicionalmente tendrá las siguientes funciones: 1. Autorizar la actividad de las entidades de certificación en el territorio nacional. 2. Velar por el funcionamiento y la eficiente prestación del servicio por parte de las entidades de certificación. 3. Realizar visitas de auditoría a las entidades de certificación. 4. Revocar o suspender la autorización para operar como entidad de certificación. 5. Solicitar la información pertinente para el ejercicio de sus funciones. 6. Imponer sanciones a las entidades de certificación en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio. 7. Ordenar la revocación de certificados cuando la entidad de certificación los emita sin el cumplimiento de las formalidades legales. 8. Designar los repositorios y entidades de certificación en los eventos previstos en la ley.	**Decreto Supremo N° 019-2002 Jus** Artículo 1. Aprobar el Reglamento de la Ley de Firmas y Certificados Digitales - Ley N’ 27269, que consta de tres (3) Títulos, cincuenta (50) Artículos y dos (2) Disposiciones Finales. Artículo 2º Designar al instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) como la autoridad administrativa competente, conforme a lo establecido en el Artículo 15 de la Ley N’27269.

		9. Emitir certificados en relación con las firmas digitales de las entidades de certificación. 10. Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y prácticas comerciales restrictivas, competencia desleal y protección del consumidor, en los mercados atendidos por las entidades de certificación. 11. Impartir instrucciones sobre el adecuado cumplimiento de las normas a las cuales deben sujetarse las entidades de certificación. - Artículo declarado EXEQUIBLE por la Corte Constitucional mediante Sentencia C-662-0046 de 8 de junio de 2000, Magistrado Ponente Dr. Fabio Morón Díaz.	
Libros de Comercio	**Decreto Nº 658/2002:** modifica la normativa que regula las formas de presentación de declaraciones juradas ante la Administración Federal de Ingresos Públicos. Artículo 1. reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica, estableciendo que las declaraciones juradas podrán ser presentadas firmadas en papel o por medios electrónicos o magnéticos que aseguren su autoría e inalterabilidad.	**Decreto 805** del 24/04/2013 Reglamenta art 173 del Decreto 19 del 2012. Artículo 2. *Libros de comercio en medios electrónicos.* Se entiende por libros de comercio en medios electrónicos, aquellos documentos en forma de mensajes de datos, de conformidad con la definición de la Ley 527 de 1999, mediante los cuales los comerciantes realizan los registros de sus operaciones mercantiles, en los términos del presente decreto. El registro de los libros de comercio en medios	**Ley 27.291**, de 2/06/2000, que modificó el Código Civil, permitiendo la utilización de medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica, sobre todo en el área de contratos. (Promulgada el 23/06/2000 y Publicada en el Diario Oficial "El Peruano" 24/06/2000).

		electrónicos deberá surtirse ante la cámara de comercio del domicilio del comerciante, de conformidad con las plataformas electrónicas o sistemas de información previstos para tal efecto mediante las instrucciones que, sobre el particular imparta la Superintendencia de Industria y Comercio. En todo caso, deberán sujetarse a lo dispuesto en este decreto y en el inciso 2° del artículo 56 del Código de Comercio, de manera que se garantice la inalterabilidad, integridad y seguridad de la información, así como su conservación en forma ordenada.	

Comentarios y consideraciones

Firma Digital: De las definiciones de firma digital de Argentina, Colombia y Perú, podemos expresar que todas ellas dejan asentado que se trata de procedimientos matemáticos que garantizan que la firma pertenezca a su iniciador y que solamente esa persona es el conocedor de su clave.

Ámbito de aplicación: Las normativas de los países hacen mención a que la ley es aplicable a todo el territorio nacional, pero cada país tiene particularidades respecto de las instituciones que encuentran directamente involucradas.

Excepciones: Argentina y Colombia dejan especificado en su ley madre las excepciones, no así la normativa del Perú que no especifica.

Validez de la Firma: Todos los países dan plena validez a la firma digital si se siguen rigurosamente los procedimientos de seguridad descriptos en la normativa.

Requerimiento de la Firma: todos manifiestan que la firma digital tiene la misma validez

que la firma ológrafa.

Certificados Digitales: todas las normativas manifiestan el indispensable certificado digital para dar validez a la firma.

Autoridad Competente: En Argentina la autoridad de aplicación de la ley es la Jefatura de Gabinete de Ministros y la Subsecretaría de la Gestión Pública actuará como autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital. En Colombia **l**a Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación. En tanto, Perú designa al Instituto Nacional de Defensa de la Competencia y Ia Protección de la Propiedad Intelectual (INDECOPI) como la autoridad administrativa competente.

Libros de Comercio: hay coincidencias en otorgar plena validez de la firma digital en los documentos inherente al comercio.

Reglamentaciones: los tres países estudiados tienen respectivos decretos reglamentarios, los que cumplen debidamente la función de arbitrar modalidades para la aplicación de la ley.

Refexiones finales

Como es sabido, en la historia de la civilización humana, los registros eran asentados principalmente en soporte papel. Hoy en día es una constante la evolución de tecnologías en el campo de la informática, por esto, "la forma" en que se expresan los actos humanos cobra una principal figura. El documento que es el objeto de estudio por la archivología muestra un cambio con respecto al soporte que contiene la información, es decir que el documento prescinde de la forma, por lo cual el formato no altera la naturaleza del mismo.

Los profesionales de la archivología, como custodios del patrimonio documental, debemos ser cautos en el tratamiento que le demos a estos soportes, reclamar que los medios informáticos garanticen perdurabilidad, seguridad en el almacenado, asimismo exigir que

la información pueda ser transferida sin ningún tipo de riesgo, es decir que los programas sean compatibles. En este sentido vale tener bien en cuenta las leyes sobre la responsabilidad del fabricante de hardware y software.

Una cuestión primordial es saber discernir el tipo de documentos que podemos informatizar, para esto vale tener presente las legislaciones vigentes de cada país que deben ser respetadas.

Con respecto a la firma digital, habrá que estar atentos a los nuevos aportes de la tecnología; que sin dudas, en un futuro inmediato será aceptada en todas las legislaciones del mundo; hasta que eso suceda, cuando tengamos que proceder al uso de la misma, deberemos estar seguros que contamos con el respaldo legal pertinente para cada caso.

Es importante que cada país continúe desarrollando estrategias para la utilización de estas nuevas tecnologías, la falta de recaudos hará que los avances en el mundo lo sorprendan y teniendo en cuenta el carácter general del fenómeno, que abarca todas las áreas y sectores de la sociedad, harán que dicho Estado retroceda socialmente.

DIGITALIZACIÓN PARA SUSTITUCIÓN

El espacio físico es un problema en la gran mayoría de los archivos. Por ello, la sustitución de los documentos en soporte papel por otro también analógico pero de menores dimensiones (el microfilm) o por la imagen digitalizada, parece ser en principio una solución. Sin embargo, estos soportes presentan inconvenientes, ligados fundamentalmente a los requisitos que demanda su conservación en el largo plazo.

Más allá de las cuestiones técnicas, que no forman parte del objeto de estudio en esta oportunidad, la existencia de normativa que autorice el cambio de formato y otorgue validez legal al nuevo soporte es fundamental para poder llevar a cabo un programa de digitalización.

Con ese objetivo, se realizó una comparación de la legislación de Argentina, Colombia y

Perú, que versa sobre la posibilidad de digitalizar, o utilizar otro soporte distinto al papel; y que estos documentos digitalizados o en microformas -dependiendo de la terminología y la época de la legislación- pueden suplir a los originales en soporte papel sin que ello lleve a la pérdida de un derecho o al incumplimiento de una obligación.

Es de señalar que este tema está legislado en los tres países en estudio, si bien los instrumentos legales no son abundantes. Concretamente, se trabajó con:

De **ARGENTINA**

LEY 24.624 del 28/12/1995

Decisión Administrativa 46/1996

De **COLOMBIA**

Ley 527 agosto de 1999

Ley 594 del 14/07/2000

De **PERÚ**

Decreto Legislativo 681 de 1991

Ley 26.612 del 10/05/1996

Decreto Legislativo 827 del 31/05/1996

Ley 28.186 del 04/03/2004

Análisis

En **Argentina,** el Decreto 447, del 07/08/1974, autorizó a los propietarios de publicaciones periódicas inscriptas en la Dirección Nacional del Derecho de Autor a microfilmar sus ediciones para disminuir el espacio que requiere su conservación, aclarando que dicha acción debe ser comunicada a la citada Dirección y que los microfilms deben quedar a disposición de dicha entidad. Este instrumento es el antecedente legal más antiguo encontrado respecto de la sustitución de documentos en papel por otro formato de

menor tamaño, en este caso una microforma.

Más de veinte años después, la Ley 24.624, en su artículo 30, establece que luego de digitalizar un documento financiero, de personal, de control, administrativo y comercial de la Administración Pública Nacional, cumplimentadas las normas de seguridad correspondientes, los originales en soporte papel pierden su valor jurídico. Por lo tanto y al carecer de valor, estos documentos ya digitalizados deben ser destruidos siguiendo las pautas que se establecen en la decisión administrativa 46/96. Esta disposición aclara que no pueden ser destruidos los documentos considerados de interés social o histórico.

El texto completo del Artículo 30 de la *Ley 24.624 es el siguiente:*

> ARTICULO 30. — Sustitúyese el artículo 49 de la Ley N° 11.672, COMPLEMENTARIA PERMANENTE DE PRESUPUESTO (t.o. 1995) por el siguiente:
>
> La documentación financiera, la de personal y la de control de la Administración Pública Nacional, como también la administrativa y comercial que se incorpore a sus Archivos, podrán ser archivados y conservados en soporte electrónico u óptico indeleble, cualquiera sea el soporte primario en que estén redactados y construidos, utilizando medios de memorización de datos, cuya tecnología conlleve la modificación irreversible de su estado físico y garantice su estabilidad, perdurabilidad, inmutabilidad e inalterabilidad, asegurando la fidelidad, uniformidad e integridad de la información que constituye la base de la registración.
>
> Los documentos redactados en primera generación en soporte electrónico u óptico indeleble, y los reproducidos en soporte electrónico u óptico indeleble a partir de originales de primera generación en cualquier otro soporte, serán considerados originales y poseerán, como consecuencia de ello, pleno valor probatorio, en los términos del artículo 995 y concordantes del Código Civil.
>
> Los originales redactados o producidos en primera generación en cualquier soporte una vez reproducidos, siguiendo el procedimiento previsto en este artículo, perderán su valor jurídico y podrán ser destruidos o dárseles el destino que la autoridad competente determine, procediéndose previamente a su anulación.
> La documentación de propiedad de terceros podrá ser destruida luego de transcurrido el plazo que fije la reglamentación transcurrido el mismo sin que se haya reclamado su devolución o conservación, caducará todo derecho a objetar el procedimiento al cual fuera sometida y el destino posterior dado a la misma.
> La eliminación de los documentos podrá ser practicada por cualquier procedimiento que asegure su destrucción total o parcial, con la intervención y supervisión de los

funcionarios autorizados.
Facúltase al JEFE DE GABINETE DE MINISTROS a reglamentar las disposiciones del presente artículo."

En la Decisión administrativa 43/96 leemos:

Capítulo XI: De la Destrucción.
a) La eliminación de los documentos deberá ser practicada por cualquier medio que asegure su destrucción total o parcial, de modo que no puedan ser utilizados los datos o la información contenida en ellos.

b) El procedimiento a seguir será el siguiente: Ubicados y seleccionados los documentos a ser eliminados, y verificado por el funcionario, que los mismos hayan sido anulados conforme lo establece esta reglamentación, se labrará un Acta de Destrucción en la que se consignará: Número de Acta. / Descripción de la documentación que será destruida, indicando en cada caso el tipo documental de que se trate y en el caso de los expedientes, su número identificatorio y el de cada uno de sus agregados acumulados. / Identificación del organismo en el que se originó la documentación, del poseedor de la misma o del que resulte responsable legal de ella. / Lugar, fecha y hora de iniciación y finalización del proceso de destrucción. / Nombre y firma de los funcionarios intervinientes.

c) El Contador General de la Nación, mediante la Disposición pertinente, determinará el funcionario autorizado para intervenir y supervisar el desarrollo del proceso de destrucción de los documentos.

d) Todo original cuyo contenido sea considerado de interés social o histórico en los términos de la Ley Nº 15.930 y sus Decretos Reglamentarios, no podrá ser destruido total o parcialmente. El interés social o histórico deberá ser determinado en todos los casos por los funcionarios responsables legalmente de la documentación mediante Resolución fundada.

Capítulo XII: De la Conservación y Seguridad.
a) Los documentos originales en soporte electrónico u óptico indeleble deben conservarse en archivos de seguridad adecuadamente protegidos de los agentes atmosféricos y biológicos que pudieran afectarlos por el plazo legal establecido, siendo responsabilidad de los funcionarios a cargo de su guarda el procurar los medios y las técnicas más apropiadas para el cumplimiento de tal fin. Se considerarán archivos adecuadamente protegidos los que cumplan con las normas nacionales e internacionales establecidas al respecto.

b) El Órgano Rector dispondrá de un archivo de seguridad adecuadamente protegido de los agentes atmosféricos y biológicos donde se conservarán los

documentos originales en soporte electrónico u óptico indeleble. Al mismo tiempo, se grabarán DOS (2) copias de resguardo; una de ellas, será depositada en un archivo de seguridad con las características mencionadas, en una entidad pública escogida al efecto, distinta al órgano rector, y la otra, se utilizará para el manejo diario. El Secretario de Hacienda determinará mediante la Resolución pertinente cuál será la entidad pública en la que se conservará la primera copia de resguardo a que se hace mención en el presente párrafo. Esta copia de resguardo podrá utilizarse como copia de sustitución, en el caso de destrucción, parcial o total de su original.

Capítulo XIII: Disposiciones Varias.
a) Se podrán obtener copias autenticadas a partir de los originales en soporte electrónico u óptico indeleble. La certificación de autenticidad se hará de conformidad a los procedimientos legales vigentes para la Administración Pública Nacional, identificando el soporte del que procede la copia.

En **Colombia**, la Ley 527 establece que los libros y papeles podrán ser conservados en cualquier medio técnico que garantice su reproducción exacta, fija también que los documentos que deben ser conservados -según plazos establecidos- deberán serlo en el formato en el que se hubieran generado. Por lo tanto si el documento fue creado originalmente en papel el documento digitalizado no puede sustituirlo a la hora de la selección. Tampoco pueden eliminarse documentos que posean valor histórico por más que hayan sido digitalizados como lo establece la ley 594.

Se transcriben a continuación los artículos correspondientes de las leyes 527 y 594

Ley 527
ARTICULO 12. CONSERVACION DE LOS MENSAJES DE DATOS Y DOCUMENTOS. Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:
1. Que la información que contengan sea accesible para su posterior consulta.
2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y
3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.
No estará sujeta a la obligación de conservación, la información que tenga por única finalidad facilitar el envío o recepción de los mensajes de datos.
Los libros y papeles del comerciante podrán ser conservados en cualquier medio

técnico que garantice su reproducción exacta.

Ley 594
ARTÍCULO 19. Soporte Documental. Las entidades del Estado podrán incorporar tecnologías de avanzada en la administración y conservación de sus archivos, empleando cualquier medio técnico, electrónico, informático, óptico o telemático, siempre y cuando cumplan con los siguientes requisitos:
Organización archivística de los documentos.
Realización de estudios técnicos para la adecuada decisión, teniendo en cuenta aspectos corno la conservación física, las condiciones ambientales y operacionales, la seguridad, perdurabilidad y reproducción de la información contenida en estos soportes, así como el funcionamiento razonable del sistema.
PARÁGRAFO 1. Los documentos reproducidos por los citados medios, gozarán de la validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por las leyes procesales y se garantice la autenticidad, integridad e inalterabilidad de la información.
PARÁGRAFO 2. Los documentos originales que posean valores históricos no podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio.

Perú es el país que posee más normas en las que se contempla el tema que estamos analizando. El decreto legislativo 681 dispone que los plazos de conservación de documentos en soporte papel se deben respetar para los documentos micrograbados; el artículo 16 de este decreto faculta la destrucción de documentos de archivos particulares que fueron microfichados y establece mismo valor y tratamiento a documentos en soporte papel que a los michofichados.

La ley 26.612 en su artículo 6 establece que los documentos y libros financieros deben ser conservados como mínimo 10 años, en su formato original en papel o en microfilm. Por su lado el decreto administrativo 827 en su artículo 3 dispone que mientras el documento esté en trámite y por doce meses posteriores, debe conservarse en su soporte original pero luego puede ser sustituido por la microforma; el artículo 5° fija que los documentos que no tengan valor histórico pueden ser conservados en su micro forma.

Finalmente la ley 28.186 establece que no pueden eliminarse documentos referidos a tributos, hasta que el mismo no prescriba, aun cuando se hubieren conservado mediante microformas.

Los textos legales referidos son los siguientes:

Decreto Legislativo 681
Artículo 8°.- Los medios portadores de las microformas, obtenidos con arreglo a lo dispuesto en esta Ley, sustituyen a los expedientes y documentos originales micrograbados en ellos, para todos los efectos legales.
Estos medios han de ser archivados, clasificados, codificados y ordenados con las mismas o mejores condiciones de seguridad y métodos exigibles a los archivos convencionales de documentos en papel.

Siempre que las disposiciones legales exijan la conservación de documentos y archivos por cierto plazo o hasta un término señalado, se entiende que tal obligación puede cumplirse mediante el mantenimiento de los archivos de microformas obtenidos conforme a esta ley.

La fecha en que el documento fue micrograbado, que consta en el acta de cierre de la grabación, extendida por quien da fe de ella, se reputa como fecha cierta.
Artículo 16°.- Es facultativo de sus propietarios la eliminación de documentos de los archivos particulares, una vez incorporadas sus microformas a los correspondientes microarhivos. Se prohíbe la incineración.

Toda persona, antes de eliminar los originales de la documentación que ha sido micrograbada, tiene la obligación de seleccionar, separar y conservar aquellas piezas que tengan valor histórico o cultural.

Para este efecto, antes de proceder a la eliminación de un lote de documentos, lo avisará por escrito al director del archivo regional o local, adjuntando un catálogo de aquéllos. El director, en un plazo de tres meses, puede señalar qué documentos deben ser entregados al archivo.

El propietario de ellos puede oponerse si considera que son documentos confidenciales cuya publicidad puede perjudicarlo.

Vencido el plazo, podrá disponer de los documentos, salvo de los señalados como históricos por el director del archivo.

Ley 26.612
Artículo 6.- Sustitúyase el artículo 189o del Decreto Legislativo No 770, Ley General de Instituciones Bancarias, Financieras y de Seguros, por el siguiente texto:

Artículo 189.- Las empresas y entidades del Sistema Financiero están obligadas a conservar sus libros y documentos por un plazo no menor de diez años. Si dentro de ese plazo, se promueve acción judicial o administrativa contra ellas, la obligación en referencia subsiste en tanto dure el litigio o procedimiento, respecto de todos los

documentos que guarden relación con la materia controvertida. Para los fines de lo dispuesto en este artículo, puede hacerse uso de las microformas bajo la modalidad de microfilm, de documento informático u otro medio análogo, de conformidad con el Decreto Legislativo No 681, normas modificatorias y complementarias.

Decreto legislativo 827
Artículo 3°._ Las dependencias públicas que se acojan a lo establecido por el presente dispositivo, quedan obligadas a mantener al alcance del público, los expedientes originales en trámite hasta después de 12 meses de su terminación.

Vencido el plazo mencionado en el párrafo anterior, los expedientes y documentos que por obligación legal o por conveniencia del servicio tengan que ser conservados, pueden ser sustituidos por las correspondientes microfornas mantenidas en microarchivos autorizados conforme al presente Decreto Legislativo.

Artículo 5°._ La documentación del Archivo Nacional de la República, así como de los Archivos Regionales y Archivos Locales cuya conservación en original no se considere necesaria para preservar su valor histórico y cultural, puede ser sustituido por las correspondientes microformas, con las precauciones y conforme a las pautas que, para tal efecto se señala el Ministerio de Justicia.

Aun cuando la dependencia pública decida mantener los documentos en originales, queda obligada a tomar microformas de ellos, las mismas que deberán conservarse en el local aparte, protegidas de todo riesgo de siniestro como medida de seguridad.

Ley 28.186
Artículo 1.- Conservación de documentos con contenido tributario
No podrán destruirse, aun cuando se hubieren conservado mediante microformas, de acuerdo al Decreto Legislativo Nº 681, normas modificatorias, ampliatorias y reglamentarias, los originales de los documentos, información y antecedentes de las operaciones o situaciones que constituyan hechos generadores de obligaciones tributarias así como toda otra documentación relacionada con hechos que determinen tributación, mientras el tributo no esté prescrito.

Apreciaciones:

Del análisis realizado surge que la principal diferencia entre la legislación estudiada reside en la conservación o no del documento en su soporte original, una vez que fue microfilmado o digitalizado. En efecto, en Argentina pierden su valor y *deben* ser eliminados; en tanto en Perú *pueden* eliminarse ya que el documento digital tiene valor jurídico, excepto los referidos a tributos y en Colombia se *debe conservar* el soporte en

que fue creado el documento original.

Por otra parte, toda la legislación consultada deja en claro que los documentos que poseen valor histórico deben conservarse ya sea en soporte papel o copias en soporte digital.

EVALUACIÓN DE DOCUMENTOS DIGITALES

En Argentina y en Perú no existe ningún instrumento legal específico y concreto relacionado con el procedimiento de evaluación de documentos digitales.

En Colombia, en 2012 se publicó la Directiva Presidencial 04 de Eficiencia Administrativa y Políticas de Cero Papel y, a instancias del Ministerio de Tecnologías de la Información, se aprobó el proyecto SINAE -Sistema Nacional de Archivos Electrónicos - como un programa especial del Archivo General de la Nación para garantizar la preservación del patrimonio documental digital y promover la estandarización de la gestión de documentos electrónicos en el Estado. En ese marco, se han dictado una serie de dispositivos, guías y lineamientos, los que se han complementado con diferentes instancias de formación destinadas a funcionarios públicos y entidades articuladas a través del Sistema Nacional de Archivos. El Archivo General de la Nación ha dictado, también en 2012, las Circulares Externas Nº. 002 (Adquisición de herramientas tecnológicas de Gestión Documental) y Nº. 005 (Procesos de Digitalización y Comunicaciones Oficiales Electrónicas en la Iniciativa Cero Papel) y prevé comenzar a realizar algunos estudios de caso sobre la aplicación de Tablas de Retención Documental en documentos de archivo digitales. Sin embargo, hasta la actualidad no existe ninguna aplicación práctica y todo se reduce al aspecto normativo.

CONCLUSIONES

El estudio realizado nos permite llegar a las siguientes conclusiones:

Si bien hay similitudes, existen diferencias muy importantes en la normativa de los tres países estudiados respecto de los temas analizados, tanto en la jerarquía de normas como en su precisión.

En general, puede afirmarse que se ha detectado cierta madurez liderando las corrientes estratégicas en cuanto a las legislaciones y en todos los países existe legislación que defiende a los consumidores y exige seguridad a los fabricantes de software.

En lo que respecta la terminología utilizada, las diferencias entre las definiciones no son muchas. Salvo algunas palabras específicas, se trata simplemente de detalles, fruto de la práctica legal de cada lugar y no de conceptos.

Los tres países cuentan con normativa sobre acceso a la información de manera directa o indirecta. Colombia y Perú establecen este derecho de manera expresa en sus normas constitucionales correspondientes. Sobre transparencia solo el Perú ha emitido norma expresa, y sobre protección de datos tanto Colombia como Perú cuentan con una norma dirigida a tal fin. Debemos precisar que en cuanto a la jerarquía de normas sobre los temas abordados, no se presenta de manera uniforme, debido a que partiendo de las Constituciones Políticas, encontramos que en Argentina, este nivel normativo se asigna en la protección de datos mientras que en los otros dos países el principio constitucional ha sido desarrollado en una norma especializada.

Solo el Perú cuenta con una norma sobre Transparencia, expresamente dirigida a tal fin, la que incluye la rendición de cuentas. Argentina incluye el tema en la una norma sobre Medio Ambiente, por tanto está dirigida a este tipo de información, mientras que Colombia aun la tiene en proyecto.

Sobre protección de datos, Argentina legisla sobre este derecho a nivel constitucional, tiene una Ley específica, norma reglamentaria y complementarias, en las que destacamos las medidas respecto de su tratamiento, confidencialidad, seguridad y control.

Las tres normas analizadas sobre protección de datos, la argentina y la colombiana como la peruana inciden preferentemente en la seguridad de la información y las medidas de conservación de los datos personales, así como en las responsabilidades de los encargados del tratamiento de los datos.

En cuanto al valor probatorio del documento digital, si bien es cierto que la legislación no es numerosa, no es menos cierto que este tipo de documentos se encuentra legislado en los tres países estudiados.

No queda duda alguna de que los soportes de un sistema computarizado de información poseen valor probatorio, siempre que se ajusten a las indicaciones dadas por las respectivas normativas.

Sin dudas la revolución digital aumentará la competitividad y el desarrollo económico de los países, es decir que la riqueza se desmaterializa en beneficio de señales electrónicas que pueden intercambiarse a gran velocidad.

El conocimiento y la información necesaria para la realización de un acto jurídico son fácilmente accesibles. Las formas tradicionales de intercambio, de seguridad y de conservación de los documentos resultan superadas por las posibilidades ofrecidas por las nuevas tecnologías de la información, las cuales cambian nuestras vidas constantemente sin que nos demos cuenta, modificando las actividades y las profesiones.

La justicia sin dudas mejorará en sus procedimientos, ya que estos documentos harán más rápidas la toma de decisiones.

Los mecanismos de autenticación permiten que todas las actividades se desarrollen plenamente y en forma segura. La firma digital, con los sistemas de claves pública y privada, la utilización de certificados, sin dudas asegura que la información enviada pertenece a quien dice ser.

Sigue pendiente el estudio y definición de los plazos de retención de los documentos digitales, cuidando de su autenticidad y conservación durante el plazo que los usuarios los requieran legalmente así como su destino final para el uso de los investigadores.