

## **Firma** electrónica avanzada

*Alicia Barnard Amozorrutia*

El artículo 4, fracción XXXII de la Ley General de Archivos (la Ley) define a la firma electrónica avanzada como:

Conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa. (DOF del 15 de junio de 2018).

La Ley de Firma Electrónica Avanzada señala, en su artículo 2, esta misma definición. (DOF del 11 de enero de 2012). Por su parte, el Código de Comercio considera a la firma electrónica avanzada un instrumento confiable si cumple por lo menos con los siguientes requisitos:

- Los datos de creación de la firma en el contexto en que son utilizados corresponden exclusivamente al firmante.
- Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante.
- Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma.

- Respecto a la integridad de la información de un mensaje de datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma. (DOF última reforma con cantidades actualizadas al 30 de diciembre de 2019).

La Ley de Firma Electrónica Avanzada también establece en su artículo 15 la disposición sobre la conservación:

Las dependencias y entidades, así como los sujetos obligados deberán conservar en medios electrónicos, los mensajes de datos y los documentos electrónicos con firma electrónica avanzada derivados de los actos a que se refiere esta Ley, durante los plazos de conservación previstos en los ordenamientos aplicables, según la naturaleza de la información.

Lo anterior es congruente con las disposiciones que la Ley General de Archivos establece respecto de las vigencias de los documentos de archivo. Esta Ley se refiere a la firma electrónica avanzada en los siguientes artículos:

Artículo 48. Los sujetos obligados que, por sus atribuciones, utilicen la firma electrónica avanzada para realizar trámites o proporcionar servicios que impliquen la certificación de identidad del solicitante, generarán documentos de archivo electrónico con validez jurídica de acuerdo con la normativa aplicable y las disposiciones que para el efecto se emitan.

En este caso, la definición de la firma electrónica avanzada señala que su uso surte los mismos efectos que una firma autógrafa, por lo que una vez que la misma sea incluida en un documento de archivo ya cuenta con esa validez jurídica, la cual, según las definiciones señaladas, surte los mismos efectos que la firma autógrafa.

Artículo 63. Los sujetos obligados desarrollarán medidas de interoperabilidad que permitan la gestión documental integral, considerando el documento electrónico, el expediente, la digitalización, el copiado auténtico y conversión; la política de firma electrónica, la intermediación de datos, el modelo de datos y la conexión a la red de comunicaciones de los sujetos obligados.

Toda vez que la interoperabilidad implica la interacción de objetivos comunes que sirven para obtener beneficios mediante la compartición de información a través de intercambio de datos entre sus sistemas tecno-

lógicos (Comisión Europea, 2017), las medidas de interoperabilidad que requieran desarrollarse demandan del consenso de los sujetos obligados para compartir la información conforme a lo establecido en el artículo mencionado, con la participación de los responsables de la política de gobierno digital a través del Consejo Nacional de Archivos.

Al contar con las disposiciones jurídico-normativas sobre la firma electrónica avanzada que incluyen la vigencia de esta, no existe argumento que ponga en entredicho su uso en los documentos de archivo que se encuentran activos o semiactivos. Sin embargo, conviene detenerse en la preservación de documentos de archivo con firma electrónica en archivos con valor histórico o patrimonial.

La autenticación de documentos de archivo ha sido una constante a lo largo de la historia. Los sellos, las estampillas, los símbolos y las firmas notariales se han utilizado para denotar la autenticidad de los documentos en medios tradicionales como el papel. Sin embargo, estos medios ya no se pueden aplicar en los documentos electrónicos de archivo.

Respecto de la autenticación, Luciana Duranti<sup>24</sup> apunta que se sustenta en el conocimiento directo, prueba material, inferencia y deducción del documento de archivo. Comenta que en el ambiente digital, la autenticación de los documentos electrónicos de archivo se puede hacer a través de una cadena legítima de custodia, la cual sigue siendo un medio importante para autenticar un documento electrónico de archivo, pero también se puede hacer mediante una cadena de custodia digital de la información preservada y los cambios que muestran datos específicos de un estado, fecha y tiempo particular, que puede ser utilizada para demostrar su autenticidad. (Pearce-Moses R. , 2018; Pearce-Moses R., 2018). Duranti, advierte una tercera opción para la autenticación, la declaración que hace un experto quien se sustenta en la confianza del sistema de gestión documental, así como en los procesos y procedimientos por los cuales se produce y conserva el documento de archivo.

En cuanto a la firma electrónica como medio de autenticación tecnológico Duranti dice que protege el contenido bit a bit (*bitwise*) donde cualquier cambio de un bit significa un valor diferente presentado en la pantalla o

24 Duranti, L. (2010). "De la Diplomática Digital a la Forense de Registros Digitales", en *Archivaria*. No. 68, pp. 39-66. <https://archivaria.ca/index.php/archivaria/article/view/13229>

la acción tomada en un programa o base de datos. La firma electrónica también verifica el origen de documento de archivo (identidad), y hace que sea indisputable e incontestable (no repudiable). Al estar habilitada mediante infraestructuras de llave pública (PKI), asegura la autenticidad de la información a través del espacio, pero no del tiempo, debido a que está sujeta a obsolescencia y constituye un problema de preservación.

Duranti comenta que en otros países se le ha dado un valor legal a la firma electrónica y que la autoridad y la no disputabilidad de una firma digital dependen de un verificador que tiene acceso a la llave pública del firmante, quien consigue cierta seguridad de que ésta le pertenece. Uno de los medios indispensables para proporcionar la seguridad de la interacción del firmante y el receptor es la autoridad certificadora, responsable de emitir el certificado de firma electrónica que acompaña al documento electrónico de archivo. Esta autoridad autentica la propiedad y características de una llave pública. (Duranti, 2009).

Para Duranti, una firma digital está asociada a una persona física o jurídica y con un documento específico. Consecuentemente, dos documentos de archivo no podrán tener la misma firma digital, no obstante que sea emitida por la misma persona. Además, una firma digital no comunica su significado y significancia con la misma inmediatez del sello tradicional. La firma digital adjuntada y transmitida con un documento de archivo es simplemente el resultado *hash* que se manifiesta como una secuencia de números incomprensible (Duranti, 2009). Lo anterior implica que en la preservación en el largo plazo se conservarán tantas firmas electrónicas avanzadas como documentos firmados en un solo expediente que ameritarán tratamiento específico en cada caso.

La encriptación, como la que se utiliza en una firma electrónica avanzada, se define como la conversión de datos en un código secreto o de texto plano a texto cifrado para que sea transmitido a través de una red pública. (Pearce-Moses R., 2018). El manual de preservación de la Digital Preservation Coalition menciona que la encriptación puede ser aplicada en varios niveles desde un documento de archivo hasta un disco completo. En la actualidad existe una cantidad importante de algoritmos y cada uno mezcla la información en forma diferente. La fortaleza del método de encriptación está influenciada por el tamaño de la llave. La encriptación de 256 bites

será más segura que la encriptación de 128 bites, por ejemplo. El manual indica que la encriptación es solamente efectiva cuando el tercero no tiene acceso a llave de encriptación, sin embargo, puede suceder que un tercero haga uso de ésta con o sin conocimiento del firmante. También, cuando las medidas de seguridad son encriptadas para un repositorio o sistema de preservación en el largo plazo, éstas pueden perder efectividad al paso del tiempo si no son actualizadas y manejadas con agilidad. El Manual señala que existe una carrera entre las técnicas de encriptación y los métodos para romperlas. Además, el material encriptado solo puede ser accesible al paso del tiempo en un repositorio o sistema de preservación en el largo plazo si la organización maneja las llaves, la pérdida o destrucción de estas llaves harán inaccesible los datos. (Digital Preservation Coalition, 2015).

Lo anterior ha tenido como propósito alertar sobre la problemática que existe para preservar documentos electrónicos de archivo con valor histórico o patrimonial. Por tanto, toda vez que las disposiciones jurídicas vigentes no establecen disposición alguna sobre el tratamiento archivístico de la firma electrónica avanzada, en su fase histórica, es factible que a través del Consejo Nacional de Archivos se establezcan lineamientos respectivos. En principio retirar la firma electrónica avanzada de un documento de archivo con valor histórico es el mecanismo idóneo, en su lugar, puede ser útil la sustitución de otro mecanismo de autenticación del propio sistema o repositorio como lo recomienda el manual mencionado. También el retiro de la firma electrónica avanzada, junto con la inclusión de metadatos de pista de auditoría periódicamente actualizables que confirmen su retiro, fecha y hora de que el documento fue firmado y transmitido, así como las correspondientes actualizaciones de auditoría.

En conclusión, la preservación en el largo plazo de documentos electrónicos de archivo, autenticada mediante medios tecnológicos de encriptación, como la firma electrónica avanzada, requiere de un análisis específico.

### Fuentes de información

- Comisión Europea. (2017). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones*. Marco Europeo de Interoperabilidad-Estrategia de Aplicación. Comisión Europea. <https://eur-lex.europa.eu/legalcontent/ES/TXT/HTML/?uri=CELEX:52017DC0134&from=EN>

- Digital Preservation Coalition. (2015). *Manual de Preservación Digital*. <https://www.dpconline.org/docs/digital-preservation->
- Duranti, L. (2010). De la Diplomática Digital a la Forense de Registros Digitales en *Archivaria*. No. 68, pp. 39-66. <https://archivaria.ca/index.php/archivaria/article/view/13229>
- Pearce-Moses, R. (. (2018). *InterPARES Trust Terminology*. <https://interparere Trust Terminology>

## Fondo documental público

*María Marván Laborde*

La definición básica de “fondo documental” hace referencia a un conjunto de documentos organizados en un archivo en el que se establece el origen o la procedencia de los documentos que contiene. Los documentos y archivos son producidos por alguien, una persona física, o jurídica, una organización que puede ser pública o privada. El nombre de un fondo documental nos permite la identificación clara de qué institución es la que tiene ese conjunto de documentos ordenados.

La Ley General de Archivos (LGA) ha establecido la procedencia como uno de sus principios fundamentales por la importancia que tiene poder identificar a cual institución pertenece cierto documento. Valga aclarar que no se utiliza la pertenencia en el sentido de posesión o propiedad sino, exclusivamente, en el sentido de procedencia. Desde que en México se aprobó en 2002 la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) se ha establecido una batalla cultural para convencer a funcionarios y servidores públicos que la información, los documentos y por tanto los archivos no son propiedad ni del funcionario ni de la institución. En sentido estricto pertenecen al público, a la sociedad, a los gobernados y por ello es obligación garantizarles el acceso a ellos. Sin embargo, si son estos funcionarios y servidores públicos quienes tienen la responsabilidad legal, administrativa y en ciertas ocasiones, inclusive penal, para garantizar que todas y cada una de las acciones de gobierno queden documentadas, en archivos ordenados y disponibles para la sociedad. Es su obligación documentar lo que se hace

y cómo se hace aun cuando no se disponga de recursos públicos para su ejecución.

En las instituciones del Estado, es una obligación de funcionarios y servidores públicos dejar constancia de sus acciones en documentos, porque a través de la evidencia documental puede evidenciarse la transparencia en las acciones tomadas por los gobernantes, y en última instancia es la única garantía para que exista un sistema efectivo de rendición de cuentas.

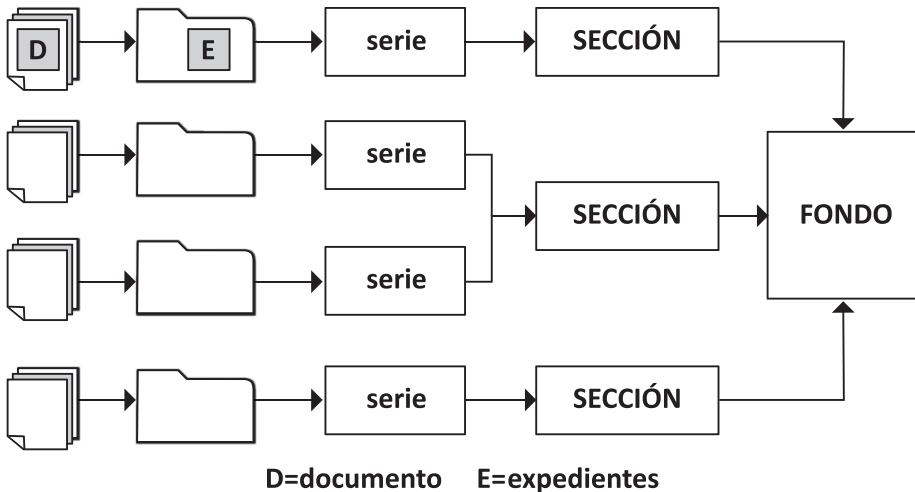
Establecer qué es un fondo documental nos exige definir qué es un documento de la manera más amplia posible. Un documento es todo registro material de información, con independencia del soporte en el que se encuentre (papel, digital, electrónico, videográfico etc.). Un documento se convierte en archivístico una vez que está ordenado para su conservación y fácil localización, con la finalidad de guardar memoria de las acciones y procedimientos que una persona física o jurídica lleva a cabo en función de sus atribuciones y competencias.

En términos generales, se exige que los documentos sirvan para probar o demostrar ciertos hechos, asimismo guardan evidencia histórica de lo que se hace y cómo se hace. Los documentos han migrado del papel a soportes electrónicos, ya sea por que fueron creados en un medio electrónico, o bien porque estos han sido digitalizados para conservarse en medios diferentes al papel, lo cual permiten almacenar grandes cantidades de información ocupando menos espacio físico. El valor documental es independiente del material en el que se soporta la información siempre que sea legible a simple vista o bien recuperable por medio de un aparato diseñado para tal fin como es el caso de los documentos electrónicos alojados en una memoria que requieren de una computadora para poder leerlos o reproducirlos. Para conseguir la utilización provechosa de un documento, éste necesita estar ordenado en un archivo y ser plenamente identificado para su fácil localización.

Las instituciones producen grandes volúmenes de documentos y cantidades ingentes de información. La cantidad de información y documentos producidos no son por sí mismos un indicador de una gestión transparente, ni de la capacidad de rendir cuentas. La información que no está ordenada es como si no existiera, y de ahí parte la importancia de entender las categorías de la archivística para tener un lenguaje común.

El fondo documental es la categoría superior en un archivo. Lo primero que nos indica es la procedencia de un determinado documento. Un fondo está conformado por más de una sección, que hace referencia a una atribución genérica de una institución, lo que normalmente conocemos como una unidad administrativa. A su vez, la serie se compone de secciones que hacen referencia a una función específica dentro de esa unidad administrativa. La serie se compone de un conjunto de expedientes, cada uno de ellos debe estar referido a un asunto en particular. Los expedientes contienen los documentos que dan cuenta de todas y cada una de las acciones que se tomaron para la realización de ese asunto en particular. Así pues, la categoría que llamamos fondo documental correspondería a la clasificación de una determinada institución y solo una.

Figura 1. Categorías archivísticas



Fuente: José Antonio Ramírez Deleón. *Metodología para el diseño y formulación de sistemas de clasificación y ordenación archivística*. Cuadernos Metodológicos 3. INAI-AGN, p. 35.

Dentro de un fondo pueden contenerse archivos de trámite, de concentración e históricos. Esta clasificación hace referencia al ciclo de vida de los documentos. En México, cada secretaría de Estado tiene su propio fondo documental. Cuando un expediente, con todos los documentos que contiene, pasa del archivo administrativo al archivo histórico —después de una previa depuración por los profesionales de la archivística— normalmente migra físicamente de la secretaría en la que “nació” para

llegar al Archivo General de la Nación (AGN). Es precisamente cuando esto sucede que se convierte en un dato absolutamente relevante tener bien identificados todos los documentos con la institución de la cuál proceden, de otra forma en el AGN sería sumamente complicado identificar si ciertos documentos pertenecen a la Secretaría de Hacienda y Crédito Público o a la Secretaría de Gobernación. Sin la identificación de los fondos documentales, la labor de los historiadores sería mucho más ardua y compleja. Un investigador que quiere reconstruir ciertos aspectos de la historia de la salud en México, por ejemplo, difícilmente le interesarán documentos de la Secretaría de Comunicaciones y Transportes, probablemente se concentre en el fondo que corresponde a la Secretaría de Salud y quizá también en el fondo del Instituto Mexicano del Seguro Social, después de 1946 que fue fundado. En pocas palabras, los archivos históricos no servirían para preservar la memoria histórica de una nación, si no supiéramos —de manera fácil y sencilla— la procedencia de una serie, expediente o documento.

### *Fuentes de información*

- Cámara de Diputados. (2018). *Ley General de Archivos*. DOF. [http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA\\_150618.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA_150618.pdf)
- Deleón, J. (2011). *Metodología para el diseño y formulación de sistemas de clasificación y ordenación archivística*. Cuadernos Metodológicos 3. INAI-AGN.