SECCIÓN 10

INTEGRIDAD, AUTENTICIDAD Y PRUEBA

IBERARCHIVOS IBERARQUIVOS
ARCHIVO NACIONAL COSTA RICA
UNIVERSIDAD DE COSTA RICA

MÓDULO 7

Gestión y preservación de documentos digitales

SECCIÓN 10

Integridad, autenticidad y prueba

Adaptación del Archivo Nacional de Costa Rica
Versión 1, 2024

Este curso fue traducido y adaptado por la Dirección General del Archivo Nacional de Costa Rica en colaboración con la Sección de Archivística de la Universidad de Costa Rica a partir del material original del año 2011 de la Asociación Internacional de Archivos Francófonos disponible en línea en el Portal Internacional Archivístico Francófono. Se aclara que pueden existir variaciones respecto al contenido original. Para acceder al material en francés, visite https://www.piaf-archives.org/se-former/module-7-gestion-et-archivage-des-documents-numeriques.

IBERARCHIVOS IBERARQUIVOS
ARCHIVO NACIONAL COSTA RICA
UNIVERSIDAD DE COSTA RICA

Contenido

Capítulo 1. Objetivo de la sección

En esta sección en una primera parte se presentará el marco legal probatorio que, ha afectado a todos los países en lo que respecta a los documentos electrónicos, desde la experiencia que se ha vivido en Costa Rica. Este marco normativo tiene como objetivo brindar el mismo valor de prueba a los documentos en formato digital que a los documentos en formato papel, en determinadas condiciones y debido al contexto de creciente uso de Internet y las redes de comercio electrónico. Además, se presentarán los procedimientos de firma digital (criptografía de clave pública).

Un segundo apartado se refiere, en este marco, al desarrollo de la administración electrónica como lo son los programas de gobierno, aspectos generales que estructuran este desarrollo, cuestiones particulares de interoperabilidad, el trabajo realizado por el grupo InterPARES sobre la autenticidad en un entorno digital, el archivo en planes de gobierno y las propuestas para garantizar la autenticidad de los documentos a través del modelo OAIS.

Capítulo 2. El marco legal de la prueba en Costa Rica

Todos los países han avanzado de la misma manera con el establecimiento de un nuevo marco legal que otorga, bajo ciertas condiciones, el mismo valor probatorio a los documentos en formato digital que a los documentos en papel.

En Costa Rica, el marco legal para estos efectos está en vigencia desde el año 2005 y es ilustrativo del desarrollo general de los países. Por eso, siendo conocedores de esta situación, se ha optado por desarrollar aquí como ejemplo este marco costarricense en donde se destaca lo esencial.

Ley de Certificados, Firmas Digitales y Documentos Electrónicos N.º 8454 de 30 de agosto de 2005
Hasta esa fecha, en Costa Rica, era el principio de inseparabilidad entre un soporte material duradero y la información que este portal, lo que constituía la calidad de la prueba y, en particular, de la prueba preconstituida de un acto jurídico.

La Ley de Certificados, Firmas Digitales y Documentos Electrónicos Nº 8454 del 30 de agosto de 2005 ha sido reformada en dos ocasiones, según lo indica el Sistema Costarricense de Información Jurídica (SINALEVI, 2022) y desde la primera versión de la ley se establece la **equivalencia funcional** entre la firma manuscrita y la firma digital certificada.

1. Por tanto, se brinda la misma fuerza probatoria a los documentos electrónicos que a los físicos según se observa a continuación:
"Calificación jurídica y fuerza probatoria. Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos." (Ley 8454,2005,art.4)**.**

En esta ley se establece que el ámbito de aplicación de la ley, el cual rige para el sector público y privado en Costa Rica. (Art.1).

Asimismo, la ley establece una serie de excepciones, según se observa a continuación:

a) Los actos o negocios en los que, por mandato legal, la fijación física resulte consustancial.

b) Las disposiciones por causa de muerte, a excepción de lo establecido en los artículos 183 de la Ley 7732, Ley Reguladora del Mercados de Valores, de 17 de diciembre de 1997 y el artículo 95 de la Ley 8956, Ley Reguladora del Contrato de Seguros, de 17 de junio de 2011.

(Así reformado el inciso anterior por el artículo 1° de la ley N° 10181 del 5 de mayo de 2022)

c) Los actos y convenios relativos al Derecho de familia.

d) Los actos personalísimos en general.

(Nota de Sinalevi: Mediante el artículo 2 aparte X) de la ley que aprueba el Código Procesal de Familia, N° 9747 del 23 de octubre del 2019, se reformará este numeral. De conformidad con el transitorio III de la ley antes mencionada dicha modificación entrarán a regir a partir del 1° de octubre del 2024, por lo que a partir de esa fecha el nuevo texto será el siguiente: "Artículo 5- En particular y excepciones: En particular y sin que conlleve la exclusión de otros actos, contratos o negocios jurídicos, la utilización de documentos electrónicos es válida para lo siguiente:

a) La formación, formalización y ejecución de los contratos.

b) El señalamiento para notificaciones conforme a la Ley N.º 7637, Ley de Notificaciones, Citaciones y otras Comunicaciones Judiciales, de 21 de octubre de 1996.
c) La tramitación, gestión y conservación de expedientes judiciales y administrativos; asimismo, la recepción, práctica y conservación de prueba, incluida la recibida por archivos y medios electrónicos. De igual manera, los órganos jurisdiccionales que requieran la actualización de certificaciones y, en general, de otras piezas, podrán proceder sobre simples impresiones de los documentos en línea efectuadas por la autoridad judicial o aceptar las impresiones de dichos documentos en línea, aportadas por la parte interesada y certificadas notarialmente.

d) La emisión de certificaciones, constancias y otros documentos.

e) La presentación, tramitación e inscripción de documentos en el Registro Nacional.
f) La gestión, conservación y utilización, en general, de protocolos notariales, incluso la manifestación del consentimiento y la firma de las partes.

No se podrán consignar en documentos electrónicos:

a) Los actos o negocios en los que, por mandato legal, la fijación física resulte consustancial.

b) Las disposiciones por causa de muerte.

c) Los actos y convenios no jurisdiccionales relativos al derecho de familia.

d) Los actos personalísimos en general.") (Art.5)

2. En la ley se establecen además diferentes conceptos alrededor de la firma digital, tales como:

- Definición de firma digital:

  Alcance del concepto. Entiéndese por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como **identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.**

> Una firma digital se considerará certificada cuando sea emitida **al amparo de un certificado digital vigente, expedido por un certificador registrado.** (Art.8)

- Establece también, el valor **equivalente** pues explica claramente dicho concepto como se detalla a continuación.

> **Valor equivalente.** Los documentos y las comunicaciones suscritos mediante firma digital, **tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito.** En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.
>
> Los documentos públicos electrónicos deberán llevar la firma digital certificada. (Art.9)

- Determina la presunción de autoría y responsabilidad

> **Presunción de autoría y responsabilidad.** Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.
>
> No obstante, **esta presunción no dispensa el cumplimiento de las formalidades adicionales de autenticación, certificación o registro que, desde el punto de vista jurídico, exija la ley para un acto o negocio determinado**. (Art.10)

Es decir, el documento firmado digitalmente debe cumplir con todas las formalidades que se exigen para el documento en papel.

2.1. La firma criptográfica con llave pública

Esta tecnología tiene su origen en el campo de la criptografía la cual se puede definir como un proceso de protección de la información que consiste en encriptar, enmascarar o codificar los datos para que estos no puedan ser accesados por personas que no están autorizadas.

Durante muchos años, para poder comunicar información cifrada entre sí, las personas tenían que ponerse de acuerdo sobre una clave o llave privada (secreta) para llevar a cabo el proceso y así lo explican Banat-Berger y Huc (2010) los cuales mencionan que la información cifrada se sustenta en un descubrimiento de dos investigadores de la Universidad de Stanford, Whitfield Diffie, Martin Hellman, el mecanismo ahora se basa en la separación de la llave única en dos llaves distintas:

- una llave privada
- y una llave pública.

La llave privada se utiliza para el cifrado y la llave pública para el descifrado. Este mecanismo se conoce como criptografía de llave pública o criptografía asimétrica:

- con la llave privada utilizada para firmar
- y la llave pública utilizada para la verificación.

De hecho, el mecanismo se basa en tres elementos:

- la generación de una huella dactilar,
- firmar la huella digital con una llave privada (secreta)
- y establecer el vínculo entre la llave privada y su propietario.

2.1.1. Generando una "huella dactilar"

La huella, de tamaño generalmente fijo, se crea a partir del documento utilizando una función matemática llamada función hash:

- esta función restaura una impresión indisociable del documento del que se extrae y que tiene una longitud fija;
- la huella dactilar se envía con el documento
- a su llegada, con la misma función, el sistema calcula una huella dactilar del documento recibido y compara las dos huellas dactilares: si el resultado es el mismo, significa que existe una probabilidad muy alta de que el documento no haya sido manipulado durante la transmisión.

EJEMPLO
La más mínima modificación del archivo da como resultado la generación de una huella dactilar completamente diferente

Considere el siguiente texto: "Algoritmo MD5 (" Wikipedia, la enciclopedia libre y abierta")"

La huella de un archivo de texto que contiene solo este texto, calculada con el algoritmo MD5 es la siguiente: "d6aa97d33d459ea3670056e737c99a3d"

Modificando solo un carácter de este texto: "MD5 (" Wikipedia, la enciclopedia libre y libre")" Este sello cambia radicalmente y se convierte en: "5da8aa7126701c9840f99f8e9fa54976"

COMPLEMENTO: COMPROBACIÓN DE LA INTEGRIDAD

Es un elemento fundamental de la preservación digital, que permite asegurar que el contenido digital no se haya perdido, modificado o dañado.

Implica el uso de software para generar una suma de comprobación que representa la estructura del archivo, de manera que posteriormente se comprueban las sumas de verificación generadas en diferentes momentos para corroborar si se ha producido algún cambio.

Estas herramientas se utilizan para detectar si el contenido del archivo o su huella digital ha cambiado, pero no indica en qué parte del archivo se ha producido el cambio.

La verificación de integridad se utiliza:

- Al mover/ transferir datos: al recibir contenido como depositante o al reemplazar los medios de almacenamiento.
- Para comprobar el almacenamiento: monitorear el archivo digital a lo largo del tiempo.
- Para demostrar la autenticidad: una verificación de la integridad documentada permite mostrar a los usuarios la autenticidad del contenido digital.

La creación de varias copias de cada objeto digital permite reemplazar cualquier archivo dañado o faltante si se detecta algún problema, mantener estas copias en diferentes ubicaciones en diferentes tipos de medios de almacenamiento ayuda a mitigar el riesgo de pérdida.

Existen herramientas que permiten la comprobación de la integridad:

DROID, FITS, FIXITY y CHECKSUM BY CORZ

2.1.2. Firma de la huella dactilar con llave privada (secreta)

Durante la transmisión, el documento y su huella digital podrían haber sido robados y reemplazados por otro documento con su propia huella digital.

Esta es la razón

- la huella digital inicial está firmada con la llave privada (secreta) de su autor
- y se verifica la huella generada a la llegada con la llave pública correspondiente a la llave privada y que es destinado a ser comunicado a todo aquel que desee verificar la firma.

De este modo

- la firma también permite certificar el origen del documento: hablamos entonces de “no repudio” porque el autor no puede dejar de reconocer ser el autor del acto en la medida en que la llave pública sólo puede verificar positivamente lo que ha sido firmado por la llave privada correspondiente.

Representación sobre el mecanismo de firma. Fuente: Soporte firma

2.1.3. Establecimiento del vínculo entre la llave privada y su titular

Finalmente, queda asegurar el vínculo entre la llave privada y su propietario. Aquí es donde entran los proveedores de certificación con quienes registrará su llave pública. Así, un tercero (el proveedor del servicio) garantiza que la llave pública es efectivamente propia y, de esta forma, crea un enlace:

- ingrese la llave pública
- y su identidad.

El registro se realiza en un certificado que contiene una cierta cantidad de información, que varía según el nivel de seguridad del certificado y del proveedor de servicios:

- identidad de su propietario,
- calidad,
- llave pública,
- entre otros.

Dos elementos muy importantes son

- por un lado, el período de validez del certificado (en Costa Rica es de cuatro años),
- por otro lado, las transacciones permitidas para este certificado.

Evidentemente, el certificado se firma a su vez con la llave privada del proveedor de servicios. Esto implica que, en cuanto un sistema verifica una llave pública, comienza por verificar la firma del certificado, antes de verificar la firma del documento enviado.

Se puede agregar que el proceso de firma digital como se acaba de describir tiene como objetivo garantizar la integridad del documento durante su transferencia y dar al destinatario la certeza de la identidad del remitente.

ATENCIÓN

Este proceso no tiene por objeto garantizar la confidencialidad del documento.

Esta confidencialidad sólo podrá obtenerse si el propio documento está cifrado.

EJEMPLO
Creación de un certificado de firma digital, según su jerarquía de emisión

Jerarquía de firma digital. Fuente: Soporte firma

Este sistema relativamente complejo conduce a la creación de una infraestructura de clave pública y se ve que la verificación de una firma induce, junto con el documento propiamente dicho, la conservación

• incluidos los algoritmos de firma utilizados en el momento de la firma del documento,

• así como la de los certificados (hay que basarse en el que era válido en el momento en que se firmó el documento).

Se muestra a continuación el Diagrama de la jerarquía nacional de certificadores registrada en Costa Rica, según la Política de Certificados para la Jerarquía Nacional de Certificadores Registrados:

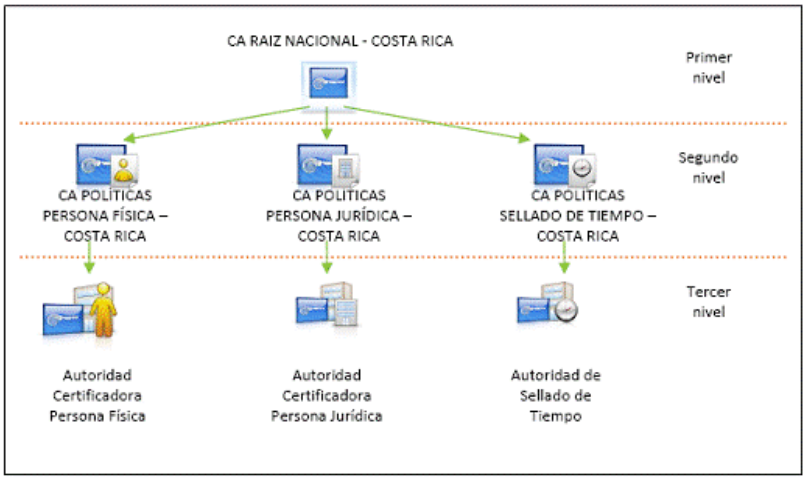


Diagrama de la jerarquía nacional de certificadores registrados

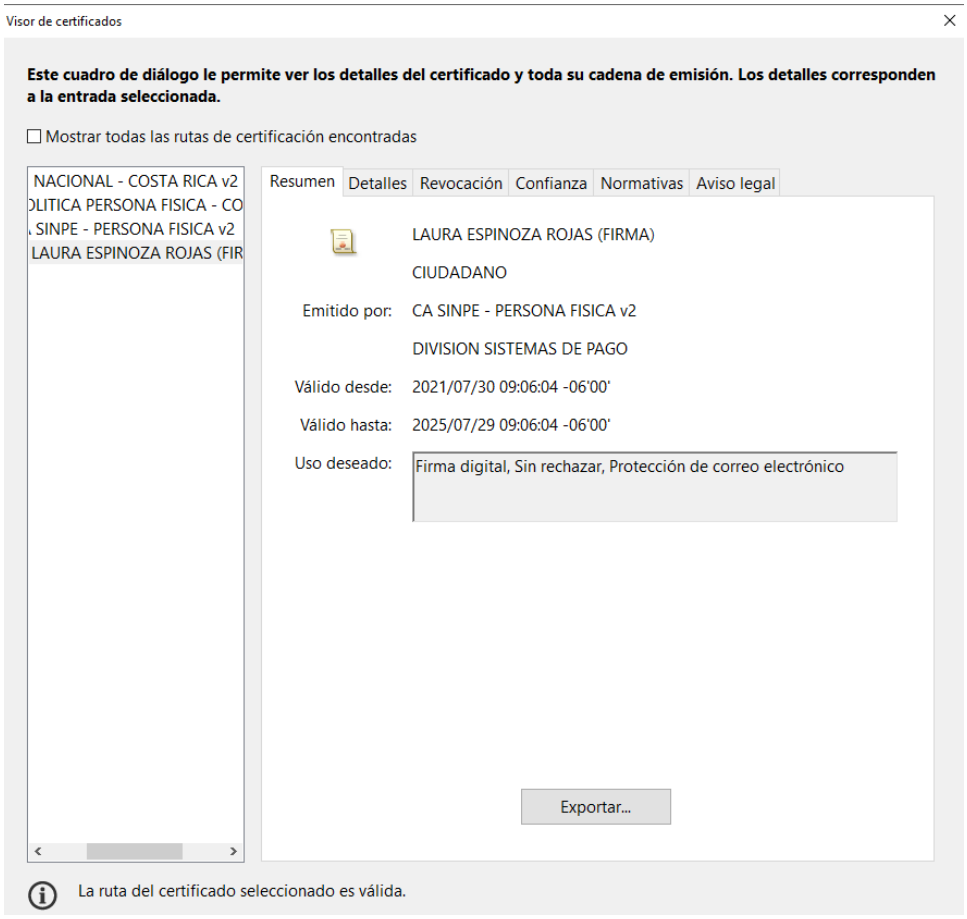
Diagrama de jerarquía nacional de certificadores registrados. Fuente: Soporte firma

COMPLEMENTO: FUNCIONAMIENTO DE LOS CERTIFICADOS

Tarjeta lectora de firma digital de Costa Rica. Fuente: Soporte firma

Tal como se utiliza en criptografía y seguridad informática, un certificado electrónico es un bloque de datos que contiene, en un formato especificado, las siguientes partes:

- un número de serie;
- la identificación del algoritmo de firma;
- la designación de la autoridad de certificación emisora del certificado;
- el período de validez tras el cual será suspendido o revocado;
- el nombre del titular de la clave pública;
- la identificación del algoritmo de cifrado y el valor de la clave pública constituida por un par de claves asimétricas
- información adicional opcional;
- la identificación del algoritmo de firma y el valor de la firma digital



Interfaz de visibilidad de los certificados de firma digital

2.2. Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 33018

Este reglamento es emitido por el Poder Ejecutivo de Costa Rica (20 de marzo de 2006).

- sirve para reglamentar y dar cumplimiento a la ejecución de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, número 8454
- respeta el carácter y la jerarquía de reglamento general, en los términos del artículo 6 de la Ley General de la Administración Pública, frente a los demás reglamentos particulares o autónomos en la materia.

Es decir que está por debajo de las leyes de la República y por encima de los reglamentos particulares o autónomos que pueda emitir alguna institución sobre este tema.

¿Qué dice este reglamento?

Contiene un glosario sobre los términos que se utilizarán en el marco nacional de firma digital certificada, determina que el contenido, condiciones de emisión, suspensión, revocación y expiración de los certificados digitales, serán los que se señalan en la Norma INTE /ISO 21188 en su versión vigente y las políticas que al efecto emita la Dirección de Certificadores de Firma Digital.

Establece también las obligaciones de los usuarios de los certificados digitales, p**lazo de suspensión de certificados, revocación por cese de actividades de un certificador, reconocimiento jurídico** de los certificados digitales expedidos por certificadores registrados ante la Dirección de Certificadores de Firma Digital, **comprobación de idoneidad técnica y administrativa** para obtener la condición de certificador registrado.

Habla también sobre **las formalidades de la solicitud** del certificador que quiera registrarse como tal, la **caución** que deben tener los sujetos privados que quieran dar el servicio, entre otros aspectos. Asimismo, establece las **funciones,** atribuciones y responsabilidades de los certificadores registrados.

Por otra parte, establece también las responsabilidades y funciones de la Dirección de Certificadores de Firma Digital -perteneciente al Ministerio de Ciencia, Tecnología y Telecomunicaciones-, como órgano administrador y supervisor del Sistema Nacional de Certificación Digital, esta Dirección también debe contar con un **Comité Asesor de Políticas,** y por último -este reglamento- menciona las diferentes sanciones en que puede incurrir un certificador.

2.3. Conclusiones relativas al marco legal

El sistema legal vigente permite desmaterializar gradualmente los procesos comerciales a lo largo de la cadena. **Los conceptos de autenticación e integridad, acordes con los peligros de la tecnología digital cuando se utilizan redes, son fundamentales y son las tecnologías de criptografía de clave pública las que se utilizan para cumplir con estos requisitos.** Se establecen infraestructuras que permiten asegurar los intercambios, las transacciones y el flujo de datos intercambiados.

> De esta manera, el Estado costarricense es el principal promotor de la firma digital certificada con relevancia jurídica, de acuerdo con la ley N° 8454 y pertenece al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT); además es el órgano administrador y supervisor del **Sistema Nacional de Certificación Digital.** La entidad que quiera emitir

certificados digitales debe estar registrada ante la Dirección de Certificadores de Firma Digital, y garantizar el cumplimiento de las más estrictas normas de seguridad y operación, **para que los documentos electrónicos firmados digitalmente tengan el mismo valor legal que los documentos físicos.**

Para registrar una Autoridad Certificadora se debe garantizar la competencia legal y técnica, para este efecto la Dirección de Certificadores de Firma Digital, se apoya en el Ente Costarricense de Acreditación (ECA), que es el responsable de evaluar el cumplimiento de los requisitos técnicos y acreditar la Autoridad Certificadora.

Autoridades Certificadoras: La gestión para ser Autoridad Certificadora se divide en dos fases: En la primera fase, el solicitante implementa y garantiza la operación de la infraestructura de llave pública de acuerdo con la ley y su reglamento. En la segunda fase, gestiona su autorización o registro ante la Dirección General de Certificados y Firmas Digitales (DGDCFD).

Gestión de un certificado de Sellado de Tiempo: La emisión del certificado de sellado de tiempo lo realiza una Autoridad de Sellado de Tiempo (TSA), la cual debe estar registrada ante la DGDCFD, cumpliendo con las regulaciones de la "Política de sellado de tiempo del sistema nacional de certificación digital"

Gestión de un certificado de Persona Física y Persona jurídica: Los certificados de persona física y los certificados de persona jurídica son emitidos por una Autoridad Certificadora autorizada o registrada por el MICITT.

Por tanto, el Banco Central de Costa Rica tiene constituida una Autoridad Certificadora para la emisión de certificados de firma digital para personas físicas (CA SINPE - Persona Física) y otra para la emisión de certificados para personas jurídicas (CA SINPE- Persona Jurídica). Ambas autoridades certificadoras pertenecen a la Jerarquía Nacional de Certificadores Registrados y están debidamente inscritas y autorizadas para su operación por la Dirección de Certificadores de Firma Digital del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), ente responsable de la administración y supervisión del sistema nacional de certificación digital.

En otro orden de ideas, la noción de interoperabilidad también será central para que los sistemas de información de los socios puedan dialogar a través de formatos de datos estandarizados, como XML, por ejemplo, que se ha vuelto imprescindible en este entorno. Este idioma permite modelar los procesos, los intercambios y asegurar que se establezca un lenguaje común entre los diferentes actores.

Capítulo 3. El establecimiento de la administración electrónica

La evolución de la legislación relacionada con el derecho probatorio ha reconocido el valor de la evidencia contenida en documentos electrónicos, reflejando así la creciente importancia de los medios digitales en el ámbito legal y administrativo.

Este avance es global y persigue proporcionar la confianza jurídica necesaria para impulsar el comercio electrónico en todos los países.

Como resultado, surge lo que se conoce como administración electrónica, marcando un cambio hacia la virtualización de los procesos comerciales. Este proceso suele comenzar con la implementación de transmisiones y servicios en línea, seguido por la adopción de la firma digital. Esta transformación conlleva la generación de documentos digitales que requieren ser conservados, al igual que sus contrapartes en papel lo eran en el pasado

3.1. El desarrollo de la administración electrónica en Costa Rica

En Costa Rica el gobierno digital o administración electrónica se ha impulsado en diferentes momentos y a la vez se han generado y/o utilizado diferentes documentos como bien señala Romero Pérez (2018) a continuación.

3.1.1. Reuniones internacionales:

- Carta Iberoamericana de Gobierno Electrónico. Adoptada por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, Chile, noviembre 2007.
- Segunda conferencia ministerial sobre la sociedad de la Información en América Latina y el Caribe, EL Salvador, febrero 2008.
- Carta Iberoamericana de calidad de la gestión pública. Adoptada XVIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, El Salvador, octubre 2008.

3.1.2. Leyes costarricenses:

- No. 7169 Promoción de desarrollo científico y tecnológico 26 junio 1990
- No. 8220 Protección al ciudadano del exceso de requisitos y trámites administrativos 4 marzo 2002
- No. 8454 Certificados, firmas digitales y documentos electrónicos 30 agosto 2005
- No. 9046 Traslado del sector telecomunicaciones del Ministerio de Ambiente, Energía y Telecomunicaciones al Ministerio de Ciencia y Tecnología 25 julio 2012
- No. 9943 Creación de la agencia nacional de Gobierno Digital 11 de mayo de 2021

3.1.3. Decretos Ejecutivos:

- No. 31681 Creación de la Comisión Nacional de Tecnologías de la Información y la Comunicación 20 enero 2004
- No. 33147 Ministerio de la Presidencia crea la Comisión Intersectorial de Gobierno Digital para diseñar y planificar políticas públicas en este campo. 8 mayo 2006
- No. 34093 del 10 de octubre del 2007 Hace una reforma a la Comisión Intersectorial de Gobierno Digital
- No. 34413 del 1 de abril del 2008 Realiza una reforma integral del Decreto Ejecutivo No. 33147-MP que creó la Comisión Intersectorial de Gobierno Digital.
- No. 34702 del 6 de mayo del 2008. Realiza una reforma parcialmente a los artículos 2 y 4 del decreto ejecutivo No. 33147 citado.
- No. 35139 Ministerio de la Presidencia- Ministerio de Planificación Creación Comisión Intersectorial de Gobierno Digital, a cargo del Ministerio de Planificación 6 abril 2009
- No. 34704 Promoción del Teletrabajo en las Instituciones Públicas 31 julio 2009
- No. 35776 Ministerio de Planificación- Gobernación y Justicia Promoción del modelo de interoperabilidad en el sector público 1 marzo 2010
- No. 36176 Ministerio de Planificación. Reforma del artículo 1 del decreto ejecutivo No. 35139 4 octubre 2010.
- No. 38276 MIDEPLAN- MICITT del 18 de marzo del 2014 Fomento del gobierno abierto en las instituciones púbicas; y, creación de la comisión intersectorial de gobierno abierto. (pp.161-163)

3.1.4. Otros documentos:

- Plan Nacional de Ciencia, Tecnología e Innovación 2015-2021 (PNCTI) (Gobierno de Costa Rica, 2015) que establece la incorporación del eje de transformación digital dentro de los proyectos intersectoriales y que plantea que al pensar en una gran temática como la innovación y modernización de la gestión pública, dos son los elementos que pueden conllevar a una mejor gestión pública, tanto a nivel de sector público centralizado y descentralizado, como a nivel local o municipal: gobierno abierto y gobierno electrónico (Gobierno de Costa Rica, 2015).
- Política Nacional de Sociedad y Economía basadas en el Conocimiento (PNSEBC), que en su quinto pilar de tecnología digital, plantea el fomento de las tecnologías digitales como catalizador del conocimiento (Gobierno de Costa Rica, 2017).
- Directriz 019-MP-MICITT Desarrollo del Gobierno Digital del Bicentenario, emitida el 21 de agosto de 2018.
- Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0 2018-2022, promovida por la Presidencia y el Micitt.
- Reglamento del Expediente Digital Único en Salud, aprobado por La Junta Directiva de la Caja Costarricense de Seguro Social, en la sesión 8954, celebrada el 29 de enero de 2018.

Actualmente, en Costa Rica se pueden hacer trámites con la firma digital certificada en 60 instituciones públicas diferentes, de alrededor de 350 que tiene el Estado. (mifirmadigital, 2022).

En el índice de desarrollo de gobierno digital de la Organización de las Naciones Unidas ONU, (2021) Costa Rica se posicionó por primera vez en la sección de “Muy Alto Nivel de Desarrollo de Gobierno Digital”, colocándose en la posición #7 de América y #56 a nivel mundial.

Además, la Organización para la Cooperación y el Desarrollo Económico (OCDE, 2020) destaca avances de Costa Rica en transformación digital que serán clave para acelerar la recuperación post pandemia del COVID-19.

3.2. Aspectos de la administración electrónica

Los conceptos de administración electrónica, gobierno abierto, gobierno digital y gobierno inteligente y su interrelación se encuentran actualmente en pleno proceso de debate y construcción, no solo en América Latina y el Caribe, sino en todo el mundo.

El gobierno abierto tiene como objetivos principales: i) mejorar los niveles de transparencia y acceso a la información mediante la apertura de datos públicos (para ejercer control social sobre los gobiernos y demandar rendición de cuentas) y la reutilización de la información del sector público (para promover la innovación y el desarrollo económico); ii) facilitar la participación de la ciudadanía en el diseño e implementación de las políticas públicas (e incidir en la toma de decisiones); y iii) favorecer la generación de espacios de colaboración e innovación entre los diversos actores, particularmente entre las administraciones públicas, la sociedad civil y el sector privado, para codiseñar o coproducir valor público, social y cívico (Enriquez y Saénz, 2022, pp. 15).

Sobre el gobierno digital, sus áreas de acción son:

- Cercano: busca mejorar la interacción entre los ciudadanos y el Estado a través de servicios de alta calidad.

- Eficiente: desarrolla las bases de los sistemas de gestión que simplifican y unifican los procesos transversales a cada organismo del Estado para que brinde mejores servicios.
- Inteligente: aprovecha los datos, información y conocimiento como activos de gobierno para optimizar los servicios públicos, brindar experiencias de servicios integrados y proactivos, fortalecer la interacción con el ciudadano y la cocreación de políticas públicas.
- Integrado: busca la integración tecnológica entre los diferentes organismos del Estado, así como la integración entre el Estado, la ciudadanía, la industria y la academia. Potencia la integración tecnológica y la interoperabilidad de los datos como base del desarrollo y la evolución de los sistemas de gestión.
- Confiable: vela por responder a los riesgos, amenazas y desafíos que surgen con el desarrollo de las tecnologías digitales. Se enfoca en generar y hacer disponibles marcos que proporcionen seguridad y confianza en la aplicación y evolución del gobierno digital. (Enríquez y Sáenz, 2022, pp. 15)

Para esto se requiere de elementos como la interoperabilidad y la seguridad de las transacciones virtuales.

COMPLEMENTO

En el sitio web Pura vida digital (2018-2022), se pueden encontrar diferentes servicios dirigidos al ciudadano que se pueden realizar a distancia.

https://www.gob.go.cr/

3.3. La cuestión de la interoperabilidad para el archivo

¿Qué es importante recordar?

La **interoperabilidad** se traduce concretamente en la capacidad de las entidades administrativas dotadas de aplicaciones informáticas **de intercambiar datos y servicios** con otras entidades o con los ciudadanos.

Esto implica, por ejemplo, poder crear, administrar y transmitir datos desde una aplicación A, que se ejecuta en un sistema operativo determinado y en una computadora determinada, y reutilizar estos datos en una aplicación local B o remoto, operando en el mismo o en otro sistema operativo y generalmente en otro ordenador, cada uno de los dos contextos técnicos es susceptible de evolucionar de acuerdo con varias limitaciones independientemente el uno del otro.

Para hacer esto posible en un **marco de entidad múltiple** que intercambian información en forma digital, es necesario:

- que la estructura de datos sea neutral e independiente de una aplicación o paquete de software en particular.
- que la descripción de estos datos sea una descripción estandarizada, reconocida por las diferentes entidades y usuarios.

Estas dos orientaciones técnicas, motivadas por la necesidad de interoperabilidad, facilitan enormemente el archivo de esta información.

Para ser interoperable, como se acaba de mostrar, es necesario permanecer neutral en relación con una aplicación particular y estandarizar la descripción de los datos como señalan Franco Espiño y Pérez Alcazar (2014) en el *Modelo de Gestión de Documentos y Administración de Archivos* (MGD) para la Red de transparencia y Acceso a la Información (RTA), promovido por la Unión Europea, como requerimientos esenciales en el diseño de la arquitectura y de una plataforma de interoperabilidad en la región, se señalan los siguientes:

No centralidad. Para permitir una adaptación de los componentes de las plataformas a las características de los sistemas de información ya existentes y respetar la autonomía de los países y regiones para establecer reglas internas de funcionalidad.

Bienes públicos regionales. Para preservar los derechos de propiedad y uso de la solución de interoperabilidad como patrimonio común de conocimiento, huyendo del uso de patentes privadas.

Cooperación y reusabilidad. Para posibilitar que cada país entrante en dicho estudio de investigación avance, con los menores costes y esfuerzos posibles, en el proceso de automatización e interoperabilidad.

Mecanismos de consenso para definir y adoptar estándares. Para otorgar un valor formal a la definición de estándares, mediante previo consenso, y generar confianza. (pp.8)

3.4. Dimensiones de la interoperabilidad

En cuanto a la interoperabilidad, es comúnmente aceptado hacer referencia a tres dimensiones: técnica, semántica y organizativa, pero según (Franco Espiño y Pérez Alcazar, 2014) al hablar sobre gestión de documentos y administración de archivos, es oportuno hacer hincapié en la necesidad de comprender la interoperabilidad desde otra dimensión, como es la de su durabilidad o permanencia en el tiempo.

- I**nteroperabilidad técnica.** Referida a la garantía de que los componentes tecnológicos están preparados para la colaboración. Es la dimensión que debe permitir mecanismos comunes de transferencia de datos.
- **Interoperabilidad semántica.** Referida a la garantía de que el significado de la información puede ser entendida por cualquier aplicación. Es la dimensión que habilita a los sistemas a combinar la información de fuentes externas y procesarla adecuadamente.
- **Interoperabilidad organizativa.** Referida a la garantía de colaboración de las organizaciones que desean intercambiar información. Es la dimensión que asegura la coordinación y alineamiento de los procedimientos que intervienen en la provisión de servicios.
- **Interoperabilidad en el tiempo.** Referida a la garantía de interacción entre elementos que correspondan a diversas oleadas tecnológicas. Es la dimensión que asegura la adecuada recuperación y conservación de la información en soporte electrónico. (pp. 9)

La interoperabilidad en el tiempo es un dominio que figura en el Esquema Nacional de Interoperabilidad, aprobado en 2010 por el Gobierno de España.

EJEMPLO

Los estándares abiertos garantizan y facilitan la interoperabilidad. Se desarrollan en un proceso transparente y de colaboración, están disponibles de forma gratuita, o con un coste razonable, y pueden ser implementados por los particulares. Algunos ejemplos de estándares abiertos son: TCP/IP, HTTP, HTML, ODF, JSON RESTful, Oauth, etc.

COMPLEMENTO

Para más información puede consultar las regulaciones y directrices que ha girado el Gobierno de España, como parte del Esquema Nacional de Interoperabilidad. Por ejemplo: la Guía de aplicación de la Norma Técnica de Interoperabilidad para Documento Electrónico y el Manual de Usuario "Esquemas XML para el intercambio de documentos electrónicos y expedientes electrónicos".

Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html

3.5. Concepto de autenticidad en un entorno digital: trabajo del grupo InterPARES

Este grupo de trabajo interdisciplinario, instalado en la Universidad de British Columbia y encabezado por la profesora Luciana Duranti, buscó inicialmente (InterPARES 1, 1999-2002) definir las reglas y principios necesarios para demostrar que un documento digital presenta un carácter de autenticidad.

A lo largo del tiempo, se han desarrollado varios proyectos InterPARES (etapas: 2, 3 y 4), este último InterPARES Trust llamado Itrust (2012-2019), consistió en un "proyecto de investigación interdisciplinario multinacional que explora cuestiones de confianza y confiabilidad de los registros y datos en entornos en línea.

Su objetivo es generar los marcos teóricos y metodológicos para desarrollar políticas, procedimientos, reglamentos, normas y legislación locales, nacionales e internacionales, con el fin de garantizar la confianza ciudadana basada en evidencias de buen gobierno, una economía digital fuerte y una memoria digital persistente.

ITrust es una asociación de investigación que comprende más de cincuenta universidades y organizaciones, nacionales y multinacionales, públicas y privadas, en América del Norte, América Latina, Europa, África, Australasia y Asia (la Alianza Internacional). Los investigadores son expertos en archivística, gestión de registros, diplomacia, derecho, tecnología de la información, comunicación y medios, periodismo, comercio electrónico, informática de la salud, ciberseguridad, gobernanza y garantía de la información, análisis forense digital, ingeniería informática y política de la información.

(InterPARES 3 Proyect, 2022) posee una base de datos terminológica del proyecto y de ella se extrae el significado para este trabajo de los términos de auténtico y autenticidad como se detalla a continuación:

auténtico

Junto con confianza y exactitud es uno de los elementos que conforman la confianza de un documento de archivo; consiste en la acreditación de un documento de archivo de ser lo que pretende ser sin alteraciones o corrupciones. Los documentos auténticos son los que han mantenido su identidad e integridad al paso del tiempo gracias a la evidencia de su carácter, requisitos o circunstancias inherentes. *(Ver también: autenticación, evaluación de autenticidad , presunción de autenticidad , requisito de autenticidad , requisitos básicos de autenticidad, requisitos de referencia)*

Términos traducidos:

autenticidad

s., La confiabilidad de un registro como registro; es decir, la calidad de un registro que es lo que pretende ser y que está libre de manipulación o corrupción. *(Ver también: evaluación de la autenticidad , autenticación, requisito de autenticidad , requisitos de autenticidad de referencia , requisitos de autenticidad de referencia , presunción de autenticidad,) n.,* La cualidad de ser auténtico, o con derecho a aceptación. Por estar autorizado o debidamente autorizado, por ser lo que profesa en origen o autoría, por ser genuino. 1Requisitos de referencia que respaldan la producción de copias auténticas de registros electrónicos: las condiciones mínimas necesarias para permitir que el conservador certifique la autenticidad de las copias de registroselectrónicos. Requisitos de referencia que respaldan la presunción de autenticidad de los registros electrónicos: las condiciones que sirven como base para la evaluación de la autenticidad de los registros electrónicos por parte del conservador. (párrs.1-2)

COMPLEMENTO

Las extensas investigaciones llevadas a cabo durante InterPARES 1, en tres años en este contexto dieron como resultado la definición de un conjunto de catorce principios y criterios.

1. Tratar los documentos de archivo de una manera específica en lugar de considerarlos como objetos digitalizados en general; es decir, tratarlos como documentos creados o recibidos y clasificados en el ejercicio de las actividades laborales.
2. Centrarse en documentos de archivo electrónicos auténticos: Un documento de archivo electrónico genuino es un documento que es lo que debe ser y que está libre de alteraciones o modificaciones. Por tanto, probar la autenticidad de un documento de archivo electrónico implica establecer su identidad y demostrar su integridad en condiciones de referencia y condiciones mínimas de autenticidad. Cuando se trata de un registro de archivo electrónico, se considera esencialmente completo e inalterado si el mensaje que pretende transmitir para lograr su propósito no se modifica.

3. Reconocer y tener en cuenta que el mayor riesgo para la autenticidad de los documentos de archivo electrónicos se produce durante su transmisión en el espacio (por ejemplo, la transmisión entre personas, sistemas o programas de aplicación) o en el tiempo (por ejemplo, si se almacenan fuera de línea o si el hardware o software utilizado para su procesamiento, comunicación o mantenimiento sea actualizado o reemplazado).
4. Reconocer que la preservación de documentos de archivo electrónicos auténticos es un proceso continuo que comienza con su creación y cuyo objetivo es la transmisión de documentos de archivo electrónicos auténticos en el espacio y el tiempo (Cadena de custodia ininterrumpida).
5. Basarse en el concepto de confiabilidad en el mantenimiento y preservación de documentos de archivo y específicamente en el concepto de un sistema confiable de gestión de documentos de archivo y en el rol del custodio como un repositorio confiable.
6. Basarse en el reconocimiento de que no es posible conservar un documento de archivo electrónico de la misma forma que un objeto físico almacenado; solo podemos conservar la capacidad de reproducirlo.
7. Reconocer que los elementos constitutivos físicos e intelectuales de un documento de archivo electrónico no deben coincidir necesariamente y que el concepto de elemento constitutivo digital es distinto del concepto de elemento de forma documental.
8. Especificar las condiciones requeridas para que una copia de un documento de archivo electrónico se considere equivalente al original: en principio, el original de un documento de archivo electrónico es el primer documento completo y efectivo. Sin embargo, en el entorno electrónico, ningún documento sobrevive en su forma original. Cualquier copia que sea fiel al contenido y a la forma documental del original debe ser considerada como una copia fiel del original, equivalente al original en cuanto a las consecuencias del mismo. Cualquier copia certificada como auténtica por un agente a quien se le haya confiado esta responsabilidad es tan válida como el original.
9. Integrar la evaluación de los documentos de archivo electrónicos en el proceso de conservación en curso.
10. Integrar la descripción de archivo en el proceso de conservación en curso: la descripción de archivo debe proporcionar una certificación general de la autenticidad de los documentos de archivo electrónicos y de su relación con otros documentos en el contexto del fondo al que pertenecen, siguiendo las condiciones mínimas requeridas.
11. Indicar explícitamente que el proceso de conservación debe estar completamente documentado, como medio principal de protección y evaluación de la autenticidad a largo plazo.
12. Reconocer explícitamente que el principio tradicional de presunción de autenticidad de los documentos de archivo utilizados en el curso normal de las actividades comerciales debe ir acompañado, en el caso de los documentos de archivo electrónicos, de la prueba de que no han sido manipulados de manera inapropiada.
13. Reconocer que el responsable debe evaluar cómo mantener la autenticidad de los documentos de archivo electrónicos. La evaluación de la autenticidad de los documentos se realiza antes de que se transfieran al custodio y es parte del proceso de evaluación, mientras que el mantenimiento de la autenticidad de las copias de los documentos se lleve a cabo después de la transferencia hecha a partir del proceso de preservación a largo plazo.
14. Hacer una distinción clara entre la protección de la autenticidad de los documentos del archivo digital y la autenticación del documento.

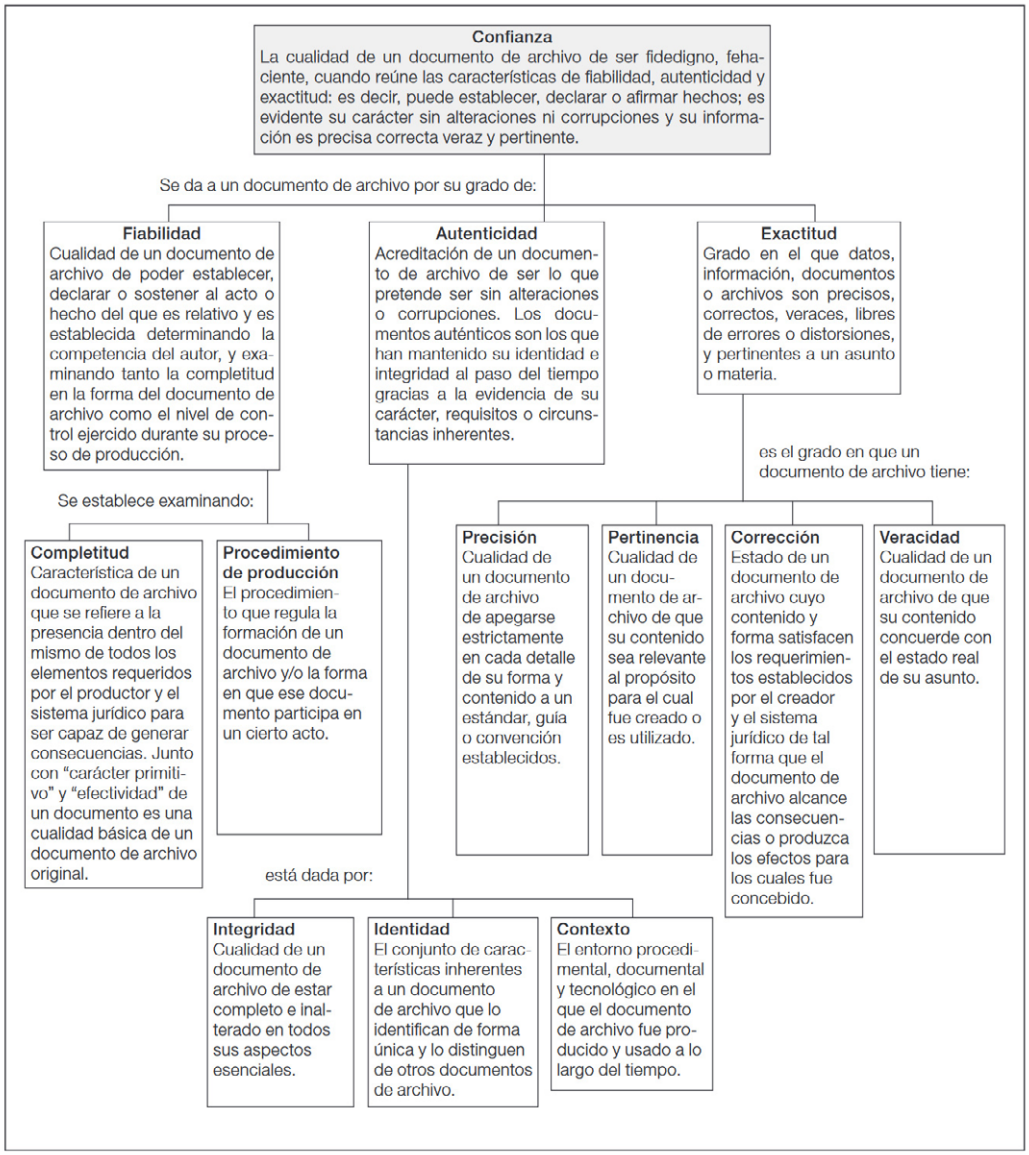
Actualmente, los retos de resguardar documentos en la nube, también plantean nuevos desafíos para los archivistas, pues la preservación digital se ha convertido en un servicio a brindar para muchos sectores.

Según Thibodeau et al. (2017) referente a la Preservación como servicio de confianza conocido por sus siglas PaaST, menciona que este presenta requisitos funcionales y de datos para la preservación digital, además, amplía los hallazgos de los anteriores InterPARES de dos maneras. En primer lugar, la investigación de InterPARES se ha centrado en documentos digitales, pero los requisitos de PaaST están formulados para ser aplicables a la preservación de prácticamente cualquier tipo de información digital, no solo documentos. En segundo lugar, aunque el tratamiento anterior de preservación en InterPARES era abstracto y conceptual, los requisitos de PaaST se articulan para apoyar la implementación e incluso la producción de software para la preservación.

Según el PaaST, la autenticidad es "la capacidad de un Registro para comunicar el mensaje que se pretendía proporcionar en el contexto en el que fue un Registro" (p.66), y está relacionada a la vez con "Una evaluación de la autenticidad nos permite determinar si la posibilidad de reconocer el significado de un Registro se ha visto afectado por el paso del tiempo. Idealmente, no debería serlo" (p.66).

De esta manera, autenticidad y preservación, están vinculados, puesto que una adecuada preservación digital va a permitir conservar la autenticidad del documento. A la vez InterPARES PaaST brinda listas de verificación de aspectos de preservación y autenticidad con las cuales llevar un adecuado entorno de conservación, en donde se ve el entorno como un todo que:

> incluye tanto el conjunto de Objetivos de Preservación que son conservados bajo las mismas Normas de Conservación y las infraestructuras tecnológicas y herramientas utilizadas en su conservación. El Entorno de Preservación puede incluir hardware y software separados, diferentes e independientes utilizados por diferentes Proveedores de Servicios de Preservación. Las capacidades que ofrece un solo proveedor se denominan Entorno de Preservación Local. (p.2)



ONTOLOGÍA. Confianza de un documento de archivo. Elaborado por Banard A, Voutssas J, 2014, en el Glosario de Preservación Archivística Digital. P. 231

3.6. Archivar en planes gubernamentales

Es importante que los gobiernos planifiquen acciones específicas para el archivo digital y electrónico, en el caso de Costa Rica estas acciones se encuentran contempladas dentro de la Ley 8454, el cual es el principal marco normativo de la firma digital, certificados y documentos electrónicos, estos documentos además deben resguardarse según la Ley 7202 del Sistema Nacional de Archivos, con lo que se ligan, ambas normativas y se complementan, por lo cual no pueden verse de forma independiente una de la otra.

CONSEJO: MODELO OAIS Y LOS ESTÁNDARES ASOCIADOS

El Modelo de Referencia OAIS: Sistema de Información de Archivo Abierto es actualmente una norma ISO. Sin embargo, fue desarrollada originalmente por el *Consultative Committee for Space Data Systems* (CCSDS), un grupo de trabajo de las agencias del espacio a nivel mundial que está enfocado en los datos terrestres y del espacio, con la finalidad de constituirse en un **modelo de referencia** que definiera los procesos necesarios para preservar y acceder a los objetos de información de forma efectiva y a largo plazo, y establecer un lenguaje común que los describa, entre otros aspectos, para la preservación de la información como señalan Cruz Mundet y Díez Carrera (2014) "Las funciones de las que se ocupa son: el ingreso, la instalación, la gestión de datos, el acceso y la difusión; es decir todo el ciclo de vida de la preservación digital"(p.132)

Además, existen otros modelos de preservación digital tal como: PREMIS para metadatos, OAIS, DAMM proporciona una forma de categorizar diferentes enfoques para permitir a las organizaciones a entender las diferencias y para seleccionar la mejor solución para ellos en términos de preservación de la información, el DoD.5015.2 el cual a su vez se deriva de estándares creados en la Universidad de la Columbia Británica en el Canadá. MoReq (Modelo de requisitos para la gestión de documentos de archivo), que, sin ser un modelo de preservación, es llamativo ya que abarca aspectos que son útiles para la misma.

Además, en Australia se creó un modelo conocido como el "Records Continuum" (Continuo de los documentos de archivo), este modelo se opone al más utilizado, basado en el concepto del "ciclo de vida" de los documentos de archivo. El modelo del *records continuum* propone que la gestión del documento es un proceso continuo desde el momento de su creación y los conceptos relativos a dicha gestión pertenecen a cuatro "dimensiones"

Por su parte, InterPARES, ha trabajado en un modelo de aproximación a la preservación digital denominado "Cadena de Preservación" (Chain of Preservation), el cual establece que los documentos de archivo digitales deben ser cuidadosamente manejados a lo largo de toda su existencia para asegurar que sean accesibles y legibles a lo largo del tiempo (Barnard Amozorrutia, 2013).

ATENCIÓN

No todos los sistemas requieren las mismas necesidades de archivo, de ahí la definición de un nivel mínimo y un nivel superior (requisitos adicionales) en términos de durabilidad, integridad y seguridad.

Bibliografía

Asamblea Legislativa. (2005, octubre 13). Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=55666&nValor3=60993&strTipM=TC

Asamblea Legislativa. (2021, setiembre 9). Ley sobre letra de cambio y pagaré electrónicos. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_articulo.aspx?param1=NRA&nValor1=1&nValor2=95870&nValor3=128143&nValor5=3&strTipM=FA

BANAT-BERGER F., HUC C., DUPLOUY L., *L'Archivage numérique à long terme, les débuts de la maturité?* (Primera obra de síntesis sobre el archivo digital en lengua francesa) Paris, La Documentation française, 2009

BANAT-BERGER F., HUC C., Module 7 - Gestion et archivage des documents numériques. Portail International Archivistique Francophone. 2011. https://www.piaf-archives.org/se-former/module-7-gestion-et-archivage-des-documents-numeriques (Se identifica en el texto como PIAF)

Barnard, A y Voutssas, J (2014). Glosario de Preservación Archivística Digital Versión 4.0. Universidad Nacional Autónoma de México. https://iibi.unam.mx/archivistica/glosario_preservacion_archivistica_digital_v4.0.pdf

Barnard Amozorrutia, A. (. (2013). Archivos electrónicos.Textos y contextos II. Puebla, México: Universidad Autónoma de Puebla. Recuperado de http://www.interpares.org/display_file.cfm?doc=ip3_mexico_dissemination_bc_barnard-et_al_archivos-electr%C3%B3nicos_2013.pdf

Cruz Mundet, J. R., y Díez Carrera, C. (2014). La normalización dela preservación digital permanente: análisis del modelo de referencia OAIS. Revista del Archivo Nacional, 129-154. Recuperado de http://www.dgan.go.cr/ran/index.php/RAN/article/view/91/45

Enriquez, A., y Saénz, C. (2022). Gobierno digital. Pieza clave para la consolidación de estados democráticos en los países del SICA. Recuperado de https://repositorio.cepal.org/bitstream/handle/11362/47811/1/S2200164_es.pdf

Franco Espiño, B., y Pérez Alcazar, R. (2014). Directrices –Interoperabilidad. Modelo de Gestión de Documentos y Administración de Archivos (MGD) para la Red de transparencia y Acceso a la Información (RTA). Recuperado de https://www.archivonacional.go.cr/web/dsae/administracion_electronica_interoperabilidad.pdf

InterPARES Proyect. (2022, octubre 21). Auténtico y autenticidad. Recuperado de http://www.interpares.org/ip3/ip3_terminology_db.cfm?team=15

mifirmadigital. (2022, octubre 21). *¿Qué puedo hacer?* Recuperado de https://www.mifirmadigital.go.cr/

Ministerio de Ciencia, Tecnología y Telecomunicaciones MICITT. (2013, mayo 20). Política de Certificados para la Jerarquía Nacional de Certificadores Registrados. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74874&nValor3=92603&strTipM=TC

Organización de las Naciones Unidas ONU. (2021). Índice de Desarrollo. Récupéré sur https://www.un.org/es/

Organización para la cooperación y el Desarrollo Económico OCDE. (2020). Informe sobre las Perspectivas Económicas de América Latina. Recuperado de https://www.comex.go.cr/sala-de-prensa/comunicados/2020/octubre/cp-2534-ocde-destaca-avances-de-costa-rica-en-transformaci%C3%B3n-digital/

Poder Ejecutivo. (2006, abril 21). Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos Nº 33018. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=56884&nValor3=103000&strTipM=TC

Presidencia (2022, octubre 21). Costa Rica lanza Agencia Nacional de Gobierno Digital Recuperado de https://www.presidencia.go.cr/comunicados/2021/11/costa-rica-lanza-agencia-nacional-de-gobierno-digital/#:~:text=En%20el%20%C3%BAltimo%20%C3%ADndice%20de,y%20%2356%20a%20nivel%20mundial

Pura vida digital. (2018-2022). https://repositorio.cepal.org/bitstream/handle/11362/47811/1/S2200164_es.pdf.

Romero Pérez, J. E. (2018). La administración electrónica pública. Revista de Ciencias Jurídicas (149), 105-132. Recuperado de https://revistas.ucr.ac.cr/index.php/juridicas/article/download/39570/40111/

Sistema Costarricense de Información Jurídica SINALEVI. (2022, octubre 21). SCIJ Sistema Costarricense de Información Jurídica. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=55666&nValor3=60993&strTipM=TC

Thibodeau, K. et al. (2017). Preservación como servicio de confianza (PaaST). Requisitos funcionales y de datos para la preservación digital. InterPARES TRUST. Recuperado de http://interparestrust.org/assets/public/dissemination/PreservationasaServiceforTrust1_0.pdf?_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wapp&_x_tr_sch=http

Est ora maximus patu vivastr idinte dicae iam hui crissum intium escerumur im hinatiquis, scere, movidetis Mulvist fue culiam faus, Ti. Viverterta partant ervis, quam dem occiisquam rehenes traves con Etre temunum is cont Cate caperit. Scierortum hem publicaper hil vidiu ia crectus sedeferet vil halis maximmo rbitrat uussoltus inculius num orurnum vid contesimis. Opio, patus, con sulicae non sum ium consum quam iac reistri puliissum mactum senirit; iam diem, ius. At et nestem det Cat es in dendiem terfirmis iu inatimis rei ilin sed num tiquam ciensup erioret videm hinprit, claribus sentem, Cas omner inat.

Ceressa pra o hactus ta popublica de con dien Ita menatam, novideme mo ina, comne is re fora, consitant, comaximil hordin serfes acienica; C. Tam misquit? Patus; et? Nihicat orudam potis nost achum et? Mulius, dium ena, pro, nulutertam loc vervica ucont.

Lium iurenih ilius, ubitiss enterei convo, quam ad det; inat, Cupiestilius patissum tum or larbis strobsentua novignos, cone dum vit cerum orte interum opublin tiocus omantem diem nors inveri potalar idemei fatiam eto cae consulv idelum incur. Grae confeci puline cres cidiis eo, pubis orteriorunte im orte in serbis, se rei cone que entis; nos C. Ridem turi, spio pul tes vilnemquo iu vastenatio num et furbefa cerceri ssulos patide quam areo et, que ego con nitis conem inatque egerat, quid sus hocam et ac faci pultum pos essulici et, faudam nihin vit. Vivit? iam. Eperter befectum pes coticon susatim esissum quides et L. Hocrum menatum dem in se inatumus verehemquam nius deribus sum haleris verum opultuam intimore ericatu ssimilius consultum eo vidiurore, no. Lus esse mortusu lissultum etraetis. M. Rae terdiis trumur inprox num, fac recondam omnit.

Ehebatumusa remum ta Sci postro iam cae num ati, Cat, nosside licitam propopo publibus es porae ac ta cre cons Ad potistinat, perede tiente, cris. Iquossul hosus, quod C. Adduc rem P. Nihilie millesi gnatili, nernihica; C. Batam, que adhucon sulabessici spio cae, nos Ahacrus cone esum is hocciem in senterione aperracia L. Habeffreis;


IBERARCHIVOS
IBERARQUIVOS


ARCHIVO NACIONAL
COSTA RICA


UNIVERSIDAD DE
COSTA RICA