San Marcos

MIEMBRO DE LA RED ILUMNO

LA NORMATIVA DE LOS DOCUMENTOS INFORMÁTICOS

LA NORMATIVA DE LOS DOCUMENTOS INFORMÁTICOS

POLÍTICAS DE FORMATOS OFICIALES DE DOCUMENTOS ELECTRÓNICOS

Aunque en nuestro país el ente rector de la documentación y archivo, es la Dirección de Archivos Nacionales, en el caso de los documentos digitales es el Ministerio de Ciencia, Tecnología y Telecomunicaciones y la Dirección de Certificadores de Firma Digital establecen una Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente. Dicha documento está fundamentado la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454.

La política que se describe a continuación establece formatos oficiales donde se dictan todas características que deben ser adaptadas por: el firmante, receptor o validador de documento electrónico en los procesos de generación o validación de la firma digital, según corresponda, y verificadas por cualquier receptor del documento electrónico en el respectivo proceso de validación de la firma digital de este.

Los formatos oficiales serán utilizados por toda entidad pública, empresa privada o particular, así como el estándar en el cual basarán sus documentos electrónicos firmados digitalmente, estos generan o consumen en sus respectivos procesos de negocio apoyados en sistemas de información. Los documentos en formatos oficiales tienen una serie de mecanismos que le garantizan al usuario mayor desempeño en los procesos y a las organizaciones o individuos que los utilizan e implementan.

DEFINICIONES Y CONCEPTOS GENERALES

Cuando se busca estandarizar un procedimiento son necesarias las definiciones que se utilizarán. En el caso de la normativa de documentos electrónicos se estudiarán las siguientes definiciones, que establece la Ley de Sistema de Archivo Nacional de Costa Rica del año 2005

Documento electrónico: cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, cualquier conjunto de datos creado, preservado, transmitido o visualizado por medios electrónicos puede ser considerado un documento electrónico.

Documento electrónico firmado digitalmente: aquel documento electrónico, cualquiera que sea su contenido, contexto y estructura, que tiene lógicamente asociada una firma digital. En otras palabras, es un objeto conceptual que contiene tanto el documento electrónico como una firma digital, sin importar que estos dos elementos puedan encontrarse representados por conjuntos de datos diferentes.

Token de sellado de tiempo: respuesta estandarizada de un Token de Sellado de Tiempo (TSA) que permite relacionar un conjunto de datos con un tiempo concreto, estableciendo así evidencia de que el dato existía antes de ese tiempo. Los token de sellado se emiten de acuerdo al RFC 3161 "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)". También se conocen con el nombre de estampas de tiempo.

Autoridad de Sellado de Tiempo (TSA por sus siglas en inglés Time Stamping Authority): sistema de emisión y gestión de token de sellado de tiempo basado en una firma digital acreditada dentro de la jerarquía nacional de certificadores registrados.

Ruta de certificación: corresponde a la cadena de certificados que soportan un certificado en particular, empezando en el certificado raíz y terminando en el certificado en cuestión, siempre dentro de la jerarquía nacional según el Sistema Nacional de Certificación Digital.

LOS MECANISMOS TRADICIONALES DE INFORMACIÓN DE REVOCACIÓN SON LAS LISTAS DE REVOCACIÓN DE CERTIFICADOS

Información de revocación: se refiere al conjunto de datos que permiten determinar la validez de un certificado en un momento dado del tiempo. Los mecanismos tradicionales de información de revocación son las Listas de Revocación de Certificados (CRLs por sus siglas en inglés) y la respuesta del Protocolo En Línea de Estado de Certificados (OCSP por sus siglas en inglés).

Listas de Revocación de Certificados (CRLs): mantiene un listado de todos los certificados que han sido revocados y del momento en que se dio su revocación. La autoridad certificadora define un tiempo de validez para la CRL, de tal forma que una vez que caduque debe ser actualizada.

Protocolo en Línea de Estado de Certificados (OCSP): protocolo de implementación de servicios de respuesta en línea del estado de un certificado en el momento en que es solicitado. Requiere de comunicación en línea con la autoridad certificadora.

Formato de Firma Digital: especificación donde se define la estructura y codificación de un documento firmado digitalmente.

COMUNIDAD DE USUARIOS Y APLICABILIDAD

Esta política tiene como objetivo guiar a las diferentes entidades públicas y privadas que deseen proveer o consumir servicios en Internet con mecanismos de firma digital, a los proveedores y desarrolladores de soluciones de software con mecanismos de firma digital, a los usuarios de los servicios o soluciones antes mencionados y a los ciudadanos que deseen conocer o utilizar mecanismos de firma digital en general.

CUMPLIMIENTO

Las entidades públicas, empresas privadas o particulares que deseen implementar soluciones con mecanismos de firma digital, tanto para soluciones internas, interinstitucionales, o para los servicios ofrecidos a sus clientes o administrados, deberán cumplir con los lineamientos establecidas en ésta política. Lo anterior con el fin de generar y procesar documentos mediante el uso de formatos oficiales, según el conjunto de responsabilidades que les corresponda (firma digital y/o validación de la firma digital).

ESPECIFICACIÓN DE LOS FORMATOS OFICIALES

USO DE FORMATOS AVANZADOS

En el Sistema Nacional de Certificación Digital, se conocerán como formatos avanzados todos aquellos formatos de firma digital que definen de manera estandarizada los atributos suficientes para garantizar la verificación de la validez del documento en el tiempo. Además debe estar auspiciados por alguna entidad internacional reconocida, y que sus especificaciones técnicas sean de acceso público.

Esta definición se basa en los estándares promulgados por el Instituto de Estándares de Telecomunicaciones Europeo (ETSI por sus siglas en inglés), a partir de la Directiva 1999/93/EC emitida por la Unión Europea.

Los formatos oficiales de los documentos electrónicos firmados digitalmente en Costa Rica serán solo aquellos que la Dirección de Certificadores de Firma Digital determine. Se define que los formatos oficiales de los documentos electrónicos firmados digitalmente en Costa Rica serán aquellos construidos con base en los formatos avanzados emitidos como normas técnicas y estándares por la ETSI, en un nivel de especificación que contemple la inclusión de todos los atributos necesarios para garantizar la verificación de su validez en el tiempo de manera incuestionable.

Sin importar las diferencias en codificación y forma inherentes a cada especificación, los niveles de configuración de los formatos avanzados aquí mencionados cumplen con las siguientes características determinantes para su selección:

- Permiten la utilización de algoritmos criptográficos robustos
- Respetan el principio de neutralidad tecnológica
- Son estándares abiertos
- Pueden ser empleados en escenarios multiplataforma
- No están sujetos a un determinado producto licenciado
- Cuentan con una adecuada documentación técnica
- Permiten la incorporación de múltiples firmas en un documento electrónico
- Implementan los principios de un mecanismo de firma confiable
- Garantía de la autenticidad del documento electrónico
- Garantía de la integridad del documento electrónico
- Ubicación fehaciente del documento electrónico en el tiempo
- Especifican mecanismos estandarizados para garantizar la preservación
- Verificación de la validez de las firmas digitales del documento electrónico en el tiempo
- Inclusión de sellos de tiempo en el documento electrónico
- Inclusión de la ruta de certificación en el documento electrónico
- Inclusión de la información de revocación en el documento electrónico.

EN EL CICLO DE VIDA DE UN DOCUMENTO ELECTRÓNICO FIRMADO DIGITALMENTE SE IDENTIFICAN DOS CONJUNTOS DE RESPONSABILIDADES

RESPONSABILIDADES

En el ciclo de vida de un documento electrónico firmado digitalmente mediante el uso de un formato oficial, se identifican dos conjuntos de responsabilidades relacionados con mecanismos de firma digital: la firma digital y la verificación de validez de la firma digital. Para la emisión de un documento electrónico firmado digitalmente, y para la recepción o verificación de su validez, se establecen una serie de actividades que deben realizarse para garantizar que la firma digital asociada tenga valor en el tiempo.

El lugar y la manera en que se codifican estos atributos en el documento electrónico corresponden con lo indicado en las especificaciones de la ETSI mencionadas anteriormente.

FIRMA DIGITAL DEL DOCUMENTO ELECTRÓNICO

De acuerdo a la normativa establecida por el Sistema Nacional de Certificación Nacional del año 2005, en Costa Rica, referente a la firma digital indica que cuando se firma digitalmente un documento electrónico, será responsabilidad del sistema o sistemas que implementan los mecanismos de firma digital incluir los atributos descritos a continuación (siempre respetando el estándar que corresponda):

- Nombre del atributo, descripción del atributo, etapas de proceso posibles para la inclusión del Atributo en el Documento.
- Resumen hash encriptado (digest). Mecanismo criptográfico que permite garantizar la integridad y autenticidad del documento. Emisión Certificado del firmante, copia del certificado del firmante que permite verificar la autoría del documento.
- Emisión Tokens de sellado de tiempo. Los tokens de sellado de tiempo que se utilizan de manera estandarizada en los formatos oficiales son para determinar la existencia de un conjunto de datos en un momento determinado del tiempo (por ejemplo, para garantizar que el certificado no estaba vencido al momento de la firma), y no necesariamente para identificar el momento de realización de la firma por parte del firmante ni del momento de la recepción del documento por parte de un receptor del mismo.

Pueden utilizarse otros tokens de sellado de tiempo, adecuadamente controlados y documentados en las herramientas, para tales fines. Solicitados a una TSA de la jerarquía del Sistema Nacional de Certificación Digital, tales como los siguientes emisión, recepción o validación, rutas de certificación, cadenas de certificados que ubiquen el certificado del firmante y de los sellos de tiempo en la jerarquía del Sistema Nacional de Certificación Digital. Además, de la emisión, recepción o validación, información de revocación, respuestas de valide del certificado del firmante, de los sellos de tiempo y de todos los certificados de sus respectivas rutas de certificación.

EMISIÓN, RECEPCIÓN O VALIDACIÓN

VERIFICACIÓN DE LA VALIDEZ DE LA FIRMA DIGITAL EN EL DOCUMENTO ELECTRÓNICO

Continuando con la Normativa de registro de firma digital, cuando se verifica la validez de un documento electrónico firmado digitalmente en el formato oficial, es imperativo que se realicen las siguientes validaciones de los diferentes atributos que el documento contiene:

- Nombre del atributo
- Descripción de la actividad de validación
- Resumen hash encriptado (digest). Verificar que el hash encriptado corresponda con el documento electrónico
- Certificado del firmante. Verificar que la firma del documento corresponda con el certificado del firmante
- Tokens de sellado de tiempo. Verificar que los tokens de sellado de tiempo son de fechas previas a la fecha de vencimiento de los certificados del firmante o de las rutas de certificación e información de revocación según corresponda, y así garantizar que todos los certificados y cadenas eran vigentes y válidas cuando se usaron
- Rutas de certificación. Verificar que todos los certificados del documento correspondan a certificados de la jerarquía del Sistema Nacional de Certificación Digital
- Información de revocación. Verificar que todos los certificados del documento eran válidos (vigentes y no revocados) en el momento de su inclusión en el documento

CONSIDERACIONES ADICIONALES PARA LA INCLUSIÓN DE LOS ATRIBUTOS

Tal y como se desprende de la presente política y de los estándares a los que hace referencia, los atributos “Resumen hash encriptado (digest)” y “Certificado del firmante” solo pueden agregarse en presencia de cada uno de los firmantes titulares de los certificados que realizan un ejercicio de firma sobre el documento electrónico.

Los restantes atributos, “Tokens de sellado de tiempo”, “Rutas de certificación” e “Información de revocación”, pueden agregarse posterior al ejercicio de firmado del/de los firmantes del documento, ya sea al momento de la recepción o durante la validación del documento. Esto último es cierto siempre y cuando los certificados de los firmantes, y los certificados de la jerarquía, no hayan vencido ni tampoco hayan sido revocados.

El escenario descrito es una medida existente para atender el riesgo de que, al tratar de hacer una firma digital en formato oficial, los servicios de respuesta en línea o los repositorios de información de revocación no estén disponibles. Lo anterior con el objetivo de que dicha eventualidad no límite la creación de firmas digitales en documentos electrónicos, a los que posteriormente pueden incluirse todos los atributos adicionales que permiten la verificación de la validez de la firma digital del documento electrónico a largo plazo.

NORMAS Y PROCEDIMIENTOS DE TRABAJO DE ARCHIVO DE LOS DOCUMENTOS INFORMÁTICOS

Según el Sistema Nacional de Certificación Digital del año 2005, es necesario cuando se inicie un expediente para un determinado cliente se creará la carpeta correspondiente, que contendrá todos los ficheros de trabajo que genere la tramitación del asunto. Para ello se seguirán los siguientes pasos:

- Abrir una carpeta a nombre del cliente en cuestión en el disco duro del servidor: unidad H: carpeta "Clientes".
- Dentro de la carpeta del cliente, abrir una subcarpeta correspondiente al área de trabajo: Auditoría, Contable, Fiscal, Laboral, Mercantil y Civil.
- Dentro de la carpeta de área de trabajo, abrir otra que se denominará con el código de expediente.
- El código de expediente se confecciona del siguiente modo:
  - El número correlativo del expediente dentro del período anual seguido de las dos últimas cifras del año en que se inicia el expediente (p. ej. 243/00).
  - Código de tipo de servicio (p. ej. AUCA para una auditoría de cuentas anual). Así, los ficheros de trabajo incluidos en el expediente de auditoría de cuentas anual del Club de Equitación Alcor, al que corresponde el número de expediente 243/00, estarán ubicados en la ruta de acceso.

Este sistema de archivo pretende que los documentos (ficheros de trabajo) estén clasificados siguiendo unos criterios que nos indiquen:

» El cliente para el que se está trabajando.

» El área de trabajo al que pertenece ese expediente.

» El número de expediente y el tipo de servicio que le corresponde.

Es importante que todos los clientes tengan aquellas carpetas que correspondan a las áreas de trabajo en las que se les prestan determinados servicios.

CADA EXPEDIENTE TENDRÁ SU CORRESPONDIENTE REGISTRO EN LA BASE DE DATOS

Cada expediente tendrá su correspondiente registro en la base de datos inventario, en la cual se vinculará mediante un campo de hiperenlace dicho registro con la ruta de la carpeta específica que le corresponda en el disco duro.

Los archivos de trabajo (generalmente de tipo .doc –Word– o tipo .xls –Excel–) recibirán un nombre que represente sin ambigüedad su contenido:

» Dictamen, Recurso, Liquidación, Estudio, Informe.

Se añadirá, si es preciso, su grado de elaboración: Notas, Borrador, Definitivo. Todos documentos de trabajo que sean susceptibles de servir como modelo de posteriores documentos se archivarán en la carpeta "Plantillas", en la subcarpeta correspondiente a área de trabajo, indicando el tipo de trabajo genérico del que se trata. Es recomendable convertir los archivos de tipo .doc en plantillas de Word (.doc) y los archivos de tipo xls. en plantillas de Excel (.xlt).

DESCRIPCIÓN DE LOS DOCUMENTOS: EL INVENTARIO

La descripción de los documentos constituye la operación que culmina el trabajo archivístico y coincide en su finalidad con la de los propios documentos: suministrar información.

Los archivos existen por la necesidad de obtener información precisa para distintas finalidades; la función básica del inventario en cuanto instrumento de descripción consiste en garantizar un acceso lo más rápido y eficiente posible a los documentos archivados. El inventario tiene como propósito describir las unidades documentales, tanto si se trata de un expediente como de una agrupación de documentos referidos al mismo asunto.

Es decir, identifica los expedientes que componen cada una de las series documentales con el propósito de acceder a los documentos más relevantes para una consulta específica. Ante la necesidad de efectuar una búsqueda documental, el inventario ha de permitir obtener respuestas rápidas y precisas acerca de cuestiones puntuales:

- "¿qué expedientes tiene en curso X y Cía?"
- "¿cuántos expedientes se están tramitando en el Registro Económico?",
- "¿cuántos expedientes se han iniciado este año en el área laboral?".

Asimismo, ha de reflejar el contenido de cada expediente –el trámite o asunto específico al que hace referencia– y su localización física en el archivo, esto permitirá un acceso selectivo a la información ya que la base de datos localizará los registros que respondan a una consulta determinada buscando la información por un solo campo o cruzando la información de diferentes campos. El inventario tiene como propósito describir las unidades documentales, tanto si se trata de un expediente como de una agrupación de documentos referidos al mismo: Campos de la base de datos.

- Número de expediente.
- Estado (en curso/cerrado).
- Código del cliente.
- Nombre o razón social del cliente.
- Área de trabajo: secciones del cuadro de clasificación (contable, fiscal, laboral…).
- Tipo de servicio: series del cuadro de clasificación.
- Procedimiento o asunto.
- Organismo (en que se tramita).
- Fecha de inicio.
- Fecha de finalización.
- Signatura tipográfica.
- Notas u observaciones.
- Autor (responsable de la tramitación).

En la Ley del Sistema de Archivo Nacional se establece que toda organización está en la obligación de ejecutar las políticas que emanen de la Junta Administrativa del Sistema Nacional de Archivos. De esta forma, se puede concluir que el archivo es la herramienta más eficaz para elaborar un inventario, es una base de datos en la que cada expediente se halle descrito en los términos precisos para garantizar una información. Con esto, se puede lograr un acceso selectivo a la información, ya que la base de datos localizará los registros que respondan a una consulta determinada buscando la información por un solo campo o cruzando la información de diferentes campos.

En esta base de datos o inventario del archivo, el cuadro de clasificación trabaja como un sistema de indización, o sea como un conjunto de palabras o términos que tienen como objetivo simplificar y representar el contenido de los documentos para recuperarlos posteriormente.

BIBLIOGRAFÍA OBLIGATORIA

Guirado, J. (2007). *Casos prácticos para la gestión organización de despachos profesionales*. Madrid, España. Edición Grupo Especial Directivos ISBN 97884993602826

BIBLIOGRAFÍA DE CONSULTA

Asamblea Legislativa de la República de Costa Rica. (2002). *Ley General de Control Interno* No. 8292, publicada en el Diario Oficial, La Gaceta No. 169, del 4 de setiembre de 2002.

Asamblea Legislativa de Costa Rica. (2005). Ley N° 8454 de Certificados, Firmas Digitales y Documentos Electrónicos LEYES.

Contraloría General de la República. (2009). *Normas generales de control interno para el Sector Público, emitida mediante resolución* No. 2-2009-CO-DFOE, del 26 de enero de 2009, publicado en el Diario Oficial La Gaceta N° 26 del 6 de febrero 2009.

Guirado, J. (2007). *Casos Prácticos para la Gestión Despachorial de Despachos Profesionales*. Madrid, España. Editorial Especial Directivos Grupo Wolters Kluwer.

Ministerio de Ciencia y Tecnología. (2012). Sistema Nacional de Certificación Nacional. [Fecha de consulta 26 de junio del 2016]. Recuperado de http://www.firmadigital.go.cr/

Normas Internacionales de Auditoría (NIA). (2011). Fundación del Comité de Normas Internacionales de Contabilidad, IASCF.

Organización Internacional para la Estandarización. Ginebra, Suiza. [Fecha de consulta: 26 de junio 2016]. Recuperado de http://www.iso.org/iso/home.html

Peters, T. (2005). Educación. La esencia. (Vol. 3). Gaithersburg, MD Editorial.

Sanz, C. (2012). Las comisiones de valoración de documentos de archivo y otros instrumentos corporativos Madrid. Revista No 51. Nuevas Tecnologías. Galicia.