#SOMOSUNAL

Política de Firma Digital y Electrónica e Identidad Electrónica

http://gestiondocumental.unal.edu.co/

Comité Nacional de Gestión y Patrimonio Documental

Secretaría General

Oficina Nacional de Gestión y Patrimonio Documental

Universidad Nacional de Colombia

Marzo 2021

POLÍTICA

Política de Firma Digital y Electrónica e Identidad Electrónica

Comité Nacional de Gestión y Patrimonio Documental

Secretaría General
Oficina Nacional de Gestión y Patrimonio Documental
Universidad Nacional de Colombia

Marzo de 2021

Índice

1 Introducción

La estrategia de implantación del documento y expediente electrónico de la Universidad Nacional de Colombia, como elemento base para evidenciar su actuación administrativa, contempla la necesidad de una política para la Firma Digital y Electrónica, así como de los certificados electrónicos.

Bajo el amparo de la normativa legal, especialmente de la Ley 527 de 1999 y el Decreto 2368 de 2012, la Universidad Nacional de Colombia puede implementar el uso de firmas y certificados electrónicos concretos, para lo cual y con el objetivo de dar una solidez jurídica y técnica a todo el sistema se requiere de unas pautas corporativas cohesionadas.

Esta Política debe garantizar el correcto uso de herramientas de Firma Digital y Electrónica con el objetivo de que permitan generar con carácter de autenticidad documentos electrónicos, expedientes electrónicos y foliados de expedientes electrónicos. Para ello esta política se fundamenta en los siguientes criterios:

- La vocación de la Universidad en que su actividad administrativa y académica pueda plasmarse en documentos y expedientes electrónicos auténticos, para poder implantar la administración sin papeles.
- Los documentos electrónicos firmados electrónicamente, en cumplimiento de lo establecido en esta política y conforme las disposiciones legales, tendrán plena validez y se considerarán originales y definitivos.
- El nivel de seguridad tecnológica, el tipo de certificado a utilizar, el formato de la firma y del sellado y los mecanismos de preservación se fijarán en función de la importancia del documento y del acto administrativo a que se refieran.
- Las firmas electrónicas contempladas por la Universidad tienen el alcance y características legales definidas en la ley 527 de 1999, por lo que tendrán efectos vinculantes y probatorios. No se contempla en ningún caso el uso de la firma escaneada en papel, como sistema de firma.

- En la medida de lo posible, las firmas electrónicas que se generan en la Universidad se harán, en origen, con el formato y nivel de seguridad requerido para su conservación durante todo el periodo de vida útil del documento al que hacen referencia. Del mismo modo, los documentos electrónicos que se reciban firmados serán sometidos a un proceso de validación y compleción de las firmas en el momento de la recepción.

En este sentido, en esta Política se desarrollan los siguientes elementos:

1. El objeto con el que se desarrolla la Política de Firma Electrónica e Identidad Electrónica de la Universidad Nacional de Colombia.

2. Los datos identificativos de la política, sus periodos de validez y su transición a nuevas políticas y la asignación de responsabilidades para su gestión.

3. La definición de los conceptos clave en materia de Firma Digital y Electrónica y que son desarrollados a lo largo de la Política.

4. La normativa y estándares internacionales a la que está sujeta la Política de Firma Electrónica e Identidad Electrónica de la Universidad y en base a la cual se desarrolla.

5. El uso de certificados digitales:

    - Certificados digitales e identidades digitales admitidos: qué certificados digitales o identidades digitales (acreditadas a través de un registro previo) pueden utilizar otras personas o entidades para relacionarse telemáticamente con la Universidad, y como se actualizará y publicará la lista de certificados admitidos.

    - Certificados digitales empleados: qué certificados digitales pueden utilizar los empleados de la Universidad, en el ejercicio de sus funciones, y qué certificados de persona jurídica están previstos para la actuación automatizada.

6. El ciclo de vida de los certificados empleados por la Universidad, identificándose cómo pueden obtenerse los certificados cuando se necesiten y cómo se llevará el control de los certificados existentes y de su eventual revocación cuando dejen de ser necesarios.

7. Los tipos y niveles de firma, es decir, el cómo y en qué formato se generan las firmas electrónicas empleadas en el ámbito de la Universidad y el proceso seguido para su

validación. También señalar que se contempla en esta Política la firma digital biométrica y la firma basada en identidad más voluntad de firma.

8. La definición del estampado cronológico cómo elemento que permite dejar evidencia de la fecha y hora en que se ha producido un acto.

9. El mantenimiento y la preservación de firmas electrónicas para garantizar la introducción en los sistemas de gestión documental de la Universidad de documentos auténticos que garanticen la preservación de su validez jurídica a largo plazo mediante procesos de restampado cronológico.

Para la elaboración de esta Política se ha tenido en cuenta las recomendaciones del Archivo General de la Nación, y también recomendaciones y estándares internacionales en materia de Firma Digital y Electrónica, expediente electrónico y foliado del mismo.

2 Objeto de la Política de Firma Digital y Electrónica e Identidad Electrónica

Esta Política tiene por objeto establecer el conjunto de criterios comunes asumidos por la Universidad Nacional de Colombia en relación con la autenticación y el reconocimiento de firmas electrónicas basadas tanto en certificados, como en otros tipos de firma como la firma biométrica. En concreto establece las directrices a seguir por la Universidad Nacional de Colombia respecto al uso de la Firma Digital y Electrónica, en el seno de las aplicaciones corporativas, para garantizar la autenticidad, integridad y conservación de los documentos firmados digitalmente.

Así mismo el objetivo de esta Política es establecer qué identidades digitales y certificados digitales de estudiantes, así como de terceros, acepta la Universidad Nacional de Colombia y qué certificados digitales utilizan los empleados de la Universidad.

En este último caso, también se establece su ciclo de vida.

Como casos particulares, se establece también la Firma Electrónica Biométrica y la Firma Electrónica basada en identificar al firmante más la gestión de evidencias de su voluntad de firma.

Por último, establece las estrategias que la Universidad Nacional de Colombia para la preservación a largo plazo de las firmas digitales y electrónicas.

3 Datos de la Política de Firma Digital y Electrónica e Identidad Electrónica

a. Identificación de la política

Los datos identificativos de la Política de Firma Electrónica e Identidad Electrónica son los que se incluyen a continuación:

1. Nombre del documento: Política de Firma Digital y Electrónica e Identidad Electrónica de la Universidad Nacional de Colombia.
2. Versión: 1.0
3. Fecha de aprobación: 26 de marzo de 2021

b. Periodos de validez y transición

La presente Política de Firma Electrónica e Identidad Electrónica de la Universidad Nacional de Colombia entrará en vigor en la fecha de su aprobación y será válida hasta que no sea sustituida o derogada por otra política posterior. Su aprobación se realizará de forma conjunta con el Modelo de Gestión de Documentos Electrónicos de Archivo de la Universidad Nacional de Colombia.

Si se estima oportuno, una nueva versión de la Política de Firma Electrónica e Identidad Electrónica de la Universidad podrá facilitar un período de tiempo transitorio para adecuar los diferentes sistemas de firma digital y electrónica y validación utilizados por la Universidad Nacional de Colombia a las especificaciones de la nueva versión.

Este período de tiempo de transición se deberá indicar en la nueva versión y superado el mismo sólo será válida la versión actualizada.

c. Identificación del gestor del documento de la política

A continuación, se incluyen los datos identificativos del gestor de la Política de Firma Electrónica e Identidad Electrónica de la Universidad Nacional de Colombia:

1. Responsable de la política: Comité Nacional de Gestión Documental y Patrimonio

2. Dirección de contacto:

Ciudad Universitaria Avenida El Dorado No. 42- 42 Edificio Archivo Histórico (500B)
Bogotá D.C., Colombia
Conmutador: (+57-1) 316 5000 Extensión: 19243 – 19246

http://gestiondocumental.unal.edu.co

4 Conceptos

Se ha creído importante incorporar un capítulo de definición de términos, aplicados en este documento, para hacer más comprensible la Política de Firma Electrónica e Identidad Electrónica de la Universidad Nacional de Colombia.

- **Casos de uso de la Firma Digital y Electrónica.** En este documento nos referimos a los casos de uso de la Firma Digital y Electrónica, a los escenarios posibles de generación de documentos electrónicos firmados. Para cada caso de uso se identificarán los sistemas de firma posibles, formatos de Firma Digital y Electrónica, los posibles niveles de firma, etc. En el caso de la Universidad Nacional de Colombia se definen siete tipos de casos de uso diferentes: Firma Digital y Electrónica de un documento electrónico, digitalización certificada de documentos en papel, copia electrónica certificada de un documento electrónico firmado electrónicamente, procesos de firma automatizada, Firma Electrónica biométrica de un documento electrónico, Firma Electrónica mediante identidad más autenticidad de la expresión de la voluntad y consentimiento de los interesados e incorporación de documentos firmados digitalmente por parte del tercero. No se contempla en ningún caso la firma escaneada como sistema de firma electrónica de la Universidad.
- **Firma digital.** De acuerdo con la Ley 527 de 1999, se entenderá como "un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".
- **Firma electrónica.** De acuerdo con el Decreto 2365 de 2012, se entenderá firma electrónica como "métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con

un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente".

- **Formato de Firma Digital y Electrónica**. Forma en que se codifican las firmas electrónicas. Los formatos más utilizados son los formatos S/MIME, CMS, XAdES, CAdES y PAdES.
- **Nivel de firma.** Con este nombre nos referiremos a si el documento tiene una única firma o múltiples firmas y en este caso si se generan en paralelo o anidadas.
- **Sistema de firma.** Con este nombre nos referimos a si la forma electrónica de un documento se ha realizado con un certificado digital del firmante o mediante firma biométrica o mediante identificación más voluntad de firma, tal y como se recoge en la Ley 527 de 1999 y el Decreto 2368 de 2012.
- **Tipos de firma**. Forma como se relaciona la Firma Digital y Electrónica con el documento firmado: dentro del mismo documento, como un documento a parte o dentro de estructuras XML.

5 Normativa aplicable y estándares internacionales

La reciente evolución en el uso del documento electrónico es el resultado de la aparición de cambios normativos que han dado impulso a las herramientas telemáticas y han equiparado, en determinadas circunstancias, los documentos en formato electrónico a los documentos en formatos más tradicionales.

Además, tanto a nivel nacional como internacionalmente, las organizaciones de estandarización técnica han definido y documentado los criterios y formatos que se utilizarán para la gestión de los documentos digitales en todos sus aspectos, garantizando la autenticidad como soporte o validez probatoria.

En este apartado se identifican el conjunto de normativas y estándares internacionales que se han tenido en cuenta para la definición de la Política de Firma Electrónica e Identidad Electrónica de la Universidad Nacional de Colombia.

a. Normativa aplicable

- Ley 527 de 1999, Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Decreto 1747 de 2000 por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales
- Decreto 2364 de 2012 Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- Ley 794 de 2003, Actos de comunicación procesal por medios electrónicos (artículo 32)
- Ley 962 de 2005, de Actuaciones administrativas por medios electrónicos (artículo 6)

b. Estándares internacionales y otras convenciones

- ETSI RFC 2315 (1998), ETSI RFC 2630 (1999), IETF RFC 3369 (2002), IETF RFC 3852 (2004): PKCS#7: Cryptographic Message Syntax (CMS)

- ETSI TS 101 733. v.1.6.3, v1.7.4 y v.1.8.1: Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)
- IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- IETF RFC 2560 (1999): X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP
- ETSI TS 101 903 v.1.2.2, v.1.3.2 y 1.4.1: XML Advanced Electronic Signatures (XAdES)
- IETF RFC 3126 (2001): Electronic Signature Formats for Long Term Electronic Signatures.
- ISO 19005 (2008): Formato de fichero PDF/A-1
- ISO/TR 18492: 2005- Long-term preservation of electronic document-based Information
- UNE-ISO/TR 13008: 2010- Información y documentación. Conversión de documentos digitales y procesos de migración.
- ETSI TS 102 176-1 V2.0.0 Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms.
- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
- ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI);
- Policy requirements for time-stamping authorities.
- ETSI TS 101 861 V1.3.1 Time stamping profile.
- ETSI TR 102 038, v.1.1.1. Electronic Signatures and Infrastructures (SEI); XML format for signature policies.
- ETSI TR 102 041, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policies report.
- ETSI TR 102 045, v.1.1.1. Electronic Signatures and Infrastructures (SEI); Signature policy for extended business model.
- ETSI TR 102 272, v.1.1.1. Electronic Signatures and Infrastructures (SEI); ASN.1 format for signature policies.

- IETF RFC 2560, X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP.
- IETF RFC 3125, Electronic Signature Policies.
- IETF RFC 3161 actualizada por RFC 5816, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- IETF RFC 5280, RFC 4325 y RFC 4630, Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
- IETF RFC 5652, RFC 4853 y RFC 3852, Cryptographic Message Syntax (CMS).
- ITU-T Recommendation X.680 (1997): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

6 Uso de certificados e identidades digitales

a. Certificados admitidos por la Universidad Nacional de Colombia

El mecanismo de Firma Digital con certificado digital se sustenta en la existencia de Autoridades de Certificación que emiten certificados digitales y permiten comprobar que un certificado concreto ha estado correctamente emitido y que continúa siendo válido en el momento de su uso, es decir de la firma digital de un documento. La relación entre la Autoridad de Certificación y la entidad que valida el certificado es una relación que se fundamenta en la confianza: los certificados serán aceptados sólo en la medida en que la entidad que lo ha de validar confíe en la honestidad de la Autoridad de Certificación.

La Universidad Nacional de Colombia depositará esa confianza en los certificados expedidos por otras organizaciones que tengan homologación del Organismo Nacional de Acreditación de Colombia (ONAC). Para la comprobación de dichos certificados la Universidad Nacional de Colombia se basará en una herramienta contratada destinada a este propósito.

b. Identidades digitales admitidas por la Universidad Nacional de Colombia

La Universidad Nacional de Colombia podrá admitir los sistemas de identificación, contemplados en el Decreto 2365 de 2012, en relación con la firma electrónica, como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

Todos los ciudadanos (tanto miembros como no miembros de la comunidad universitaria) podrán utilizar los certificados reconocidos y homologados por la ONAC.

La Universidad está suministrando a los usuarios de la Comunidad Universitaria, usuarios y contraseñas de acceso a las distintas herramientas tecnológicas de esta.

Dichas identidades digitales podrán ser utilizadas como sistema de firma basado en identidad más autenticidad de la expresión de la voluntad y consentimiento de los interesados.

c. Certificados empleados por la Universidad Nacional de Colombia

Los empleados o colaboradores de la Universidad Nacional de Colombia que deban firmar documentos digitalmente o tener acceso a determinados servicios o aplicaciones donde se requiera un alto nivel de autenticación, podrán utilizar certificados digitales. Para el caso del uso del certificado digital, la Universidad Nacional de Colombia utilizará certificados digitales de un prestador de servicios de certificación reconocido y homologado por la ONAC.

La Universidad Nacional de Colombia puede convenir con el prestador del servicio de certificación que contrate un acuerdo para que la Universidad sea un Punto de registro y pueda, por tanto, generar los certificados necesarios.

Finalmente, y en cuanto a los certificados de servidor (página web) y de persona jurídica la Universidad Nacional de Colombia utilizará los proporcionados a través del prestador contratado, si bien en el futuro podría utilizar alguno de los diversos prestadores de servicios de certificación en función, en cada momento, del nivel de instalación de las claves públicas de dichos prestadores en los navegadores utilizados por la comunidad universitaria.

Por lo que respecta al uso de certificados digitales en servidor para el intercambio seguro de información entre organizaciones se utilizará los del prestador contratado, o en su defecto, cualquiera de los emitidos por otras autoridades de certificación que ya tengan un alto nivel de instalación, de sus claves públicas, en los navegadores. Cabe señalar que, si bien estos certificados no generan actos jurídicos, se ha considerado oportuno incorporarlos a esta Política.

7 Ciclo de vida de los certificados digitales empleados por la Universidad

Cuando la Universidad Nacional de Colombia contrate al prestador de servicios de certificación de una empresa reconocida, será esta Autoridad de Certificación la responsable de definir las políticas de gestión de los certificados digitales que emite y por tanto es quien define la vigencia de los certificados, la manera como se revocan, se renuevan, se validan, etc.

A efectos de adoptar los procedimientos establecidos por el prestador de servicios de certificación para operar el Punto de Registro se han establecido procedimientos internos que identifican las actividades que se realizan y sus responsables, así como los procedimientos a seguir por los usuarios para la solicitud, renovación, revocación, etc. de sus certificados digitales.

7.1 Empleados o colaboradores

Los certificados digitales de empleado o colaboradores de la Universidad se emiten y revocan en función de las necesidades del puesto de trabajo y lo gestiona la Dirección Nacional de Estrategia Digital.

La solicitud se genera por parte del responsable del servicio o departamento de la Universidad y previa certificación de dicha vinculación con la Universidad por parte de la Dirección Nacional de Personal Académico y Administrativo.

En el caso de que el certificado digital sea de empleado con cargo (en el mismo certificado digital, aparte de informar sobre la vinculación del empleado con la Universidad, específica qué cargo tiene esta persona. Está pensado para cargos como el Síndico, Rector, Secretaria General, etc., además deberá acompañar la solicitud una certificación por parte de la Dirección Nacional de Personal Académico y Administrativo, en la que certifique el cargo de la persona que solicita dicho certificado.

En el caso de que un empleado de la Universidad tenga una incidencia como puede ser la pérdida del certificado, el usuario deberá solicitar la revocación a través del

responsable de su servicio o departamento, que es quien redirigirá el trámite a la Dirección Nacional de Estrategia Digital.

La Universidad Nacional de Colombia, a través de la Dirección Nacional de Estrategia Digital, lleva un inventario de los certificados que dispone. El inventario de certificados digitales incluye la información necesaria para su gestión, como el número de certificado, el tipo de certificado, el emisor del certificado, la persona o aplicación que gestiona el certificado, así como la fecha de caducidad del certificado, entre otros datos.

Periódicamente se realiza un control proactivo desde la Dirección Nacional de Estrategia Digital y de forma coordinada con la Dirección Nacional de Personal Académico y Administrativo, para proceder a la revocación de certificados resultantes de cambios de cargos de los empleados o bajas de estos.

En el momento en que la Dirección Nacional de Estrategia Digital detecta que un certificado incluido en el inventario está a punto de caducar (3 meses antes de este hecho), bien porqué recibe un e-mail de la empresa certificadora o bien porqué accede a la herramienta suministrada por esta, lo comunica al responsable del servicio o departamento quien informa al titular del certificado, sea este de vinculación con la Universidad o de cargo. Será el responsable del servicio o departamento quien pedirá a la Dirección Nacional de Estrategia Digital su renovación o no siguiendo los mismos procedimientos establecidos para la solicitud de un nuevo certificado digital.

Los certificados digitales de empleado se emiten y revocan a solicitud de estos, y con el consentimiento del responsable del Servicio, en la Dirección Nacional de Estrategia Digital.

7.2 Técnicos

En el caso de los certificados técnicos, el proceso de solicitud es el siguiente: el área que precisa de dicho certificado lo solicita a la Dirección Nacional de Estrategia Digital, que es quien, con una aplicación específica hace la solicitud y descarga del certificado digital y posteriormente ordena su instalación en el servidor y en la o las aplicaciones que corresponda.

En este caso es también la Dirección Nacional de Estrategia Digital quien lleva un inventario de los certificados técnicos que la Universidad dispone. El inventario de certificados digitales incluye la información necesaria para su gestión, como el número de certificado, el tipo de certificado, el emisor del certificado, la aplicación que gestiona el certificado, así como la fecha de caducidad del certificado, entre otros datos.

En el momento en que la Dirección Nacional de Estrategia Digital, detecta que un certificado incluido en el inventario está a punto de caducar (3 meses antes de este hecho), este deberá decidir si se debe renovar o no. En caso de que se deba renovar será la misma Dirección Nacional de Estrategia Digital quien procede a su renovación.

8 Estampado cronológico (time stamping o Sello de tiempo)

Las características principales del estampado cronológico son:

- El estampado cronológico es un sello electrónico generado por un tercero de confianza en base a un certificado digital especialmente destinado al efecto.
- Evidencia de la fecha y hora en que se ha producido un acto. Se utiliza conjuntamente con un documento en cualquier formato y que puede estar firmado electrónicamente. El estampado cronológico puede hacer referencia a:
    - Firma del documento: el estampado cronológico está asociado a la Firma Digital.
    - Creación del documento: el estampado cronológico está asociado al documento.
- Mediante un proveedor de estampado cronológico, se sellará la fecha y hora del instante en el que se ha realizado el acto. El proveedor será el proveedor de servicios de certificación de referencia.

El proceso consiste en crear una evidencia electrónica sobre una Firma Digital: se calcula el resumen criptográfico del documento y/o sus firmas electrónicas (en el caso del restampado cronológico), es decir, una operación matemática que se aplica al conjunto de información sobre el que emitir el estampado cronológico y obtiene una cadena de bits denominada "hash" la cual se cifra con la clave privada del certificado de estampado cronológico utilizado para hacer la operación. Se retorna esta firma conjuntamente con la fecha y hora de la operación, así como información sobre el certificado de estampado cronológico utilizado para hacer la firma.

9 Sistemas, tipos y niveles de firma

En este apartado se recopilan los aspectos relacionados con la Firma Digital y Electrónica en el marco de la Universidad Nacional de Colombia, incluyendo los diferentes usos de la Firma, tanto Digital como Electrónica en el ámbito de los sistemas de la Universidad Nacional de Colombia. Los objetivos que persigue la Universidad Nacional de Colombia con la implantación de la Firma Digital y Electrónica son fundamentalmente dos:

- Dotar a la Universidad Nacional de Colombia de un sistema para el control, el uso y la conservación de la documentación original firmada digital y electrónicamente, gestionada en el desarrollo habitual de su actividad política y administrativa.
- Garantizar la gestión adecuada de los documentos de la Universidad Nacional de Colombia, asegurando la autenticidad, la fiabilidad, la integridad y la disponibilidad futura a lo largo de su ciclo de vida, basado en un software informático que ofrece una capa de gestión de documentos y archivo común.

Una vez formulados estos objetivos básicos, hay que tener presente la definición de los Sistemas de Firma Digital y Electrónica, la Universidad podrá usar:

- **Firma Digital basada en el uso de un certificado digital**. Es el sistema de firma digital en la que, en base a la clave privada de un usuario, se cifra el resumen criptográfico del documento a firma, y se añade a esta firma información del certificado utilizado para la firma, la fecha de la firma, la política de firma, etc.
- **Biométrica**. El sistema consiste en la captación de las evidencias biométricas del firmante, así como del contexto de la firma (hash del documento, momento de la firma, lugar, etc.), en un dispositivo especializado. Dicha información se cifra con una clave pública de un tercero de confianza, y se almacena o bien en el propio documento firmado o bien en un repositorio de firmas. La validación de las firmas se efectúa en el momento de conflicto. En caso de conflicto, la Universidad podrá aportar ante el juez el documento, así como su firma (evidencias cifradas) y será el juez quien solicitará el descifrado de las evidencias al tercero de confianza, y a partir de dichas evidencias y del hash del documento se podrá probar la identidad del firmante, la integridad del documento y la vinculación de este con el documento.

- **Firma Electrónica basada en la identidad digital y la expresión de la voluntad y consentimiento de los interesados.** El sistema consiste en que en el momento en que una persona va a firmar un documento, se le pide usuario y la contraseña de acceso a los sistemas de información de la Universidad. En caso de que la identificación sea correcta, se le muestra una segunda pantalla donde se le informa de que va a firmar un documento. En esta pantalla le aparece un mensaje que le indica que consiente en la firma del documento siguiente y se le informa del nombre del documento a firmar, el formato, el resumen criptográfico del documento a firmar, la fecha y la hora de la firma y la IP desde donde está accediendo el usuario y se le pide que, introduzca una segunda contraseña específica de firma. Esta segunda contraseña se le ha proporcionado al usuario a través de la relación presencial en algún momento previo a la firma del documento. En el caso de que introduzca correctamente esta segunda contraseña se genera una evidencia y se guarda esta en un repositorio seguro de evidencias. La evidencia constará de la siguiente información:
    - Nombre y apellidos del firmante.
    - Nombre del usuario.
    - Fecha y hora de la firma.
    - Nombre del fichero firmado.
    - Resumen criptográfico del documento.
    - Método de resumen criptográfico utilizado.
    - IP del ordenador desde el que se firma.
    - e-mail de confirmación de firma que se ha mandado al firmante una vez este ha introducido la segunda contraseña, la de firma.

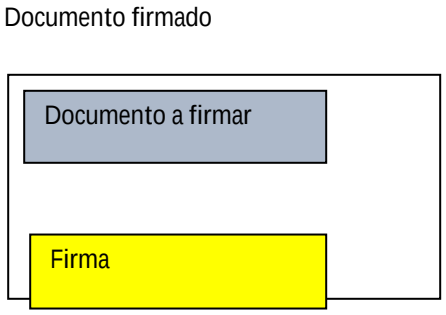
  Finalmente, una vez firmado el documento, le aparece al firmante una pantalla donde se le informa que se ha efectuado correctamente la firma y se manda un e-mail al firmante con la información de la firma.

  A continuación, se incorpora la información de la firma (XML con la información que se ha guardado en el repositorio seguro de evidencias) dentro del documento a firmar y se procede a la firma del documento con un certificado digital de persona jurídica de la Universidad para garantizar la integridad de este. Dicha firma será con estampado cronológico.

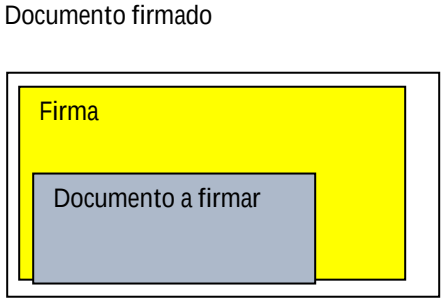
  En caso de conflicto, la Universidad podrá aportar: el documento firmado con el XML incorporado y la información guardada en el repositorio seguro de firmas.

9.1 Tipos de firma

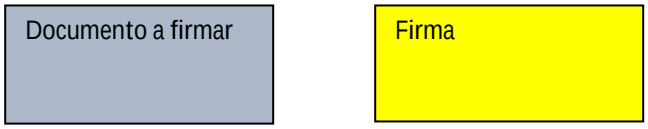
- **Firma *attached***: los datos de firma residen en el documento firmado. Por tanto, el mismo documento dispone de toda la información para comprobar la autenticidad e integridad del documento, así como la información necesaria para la validación de la firma. Hay que diferenciar entre dos tipos diferentes de firma *attached*:
  - **Enveloped (incrustada)**, en este caso el documento firmado está compuesto por el contenido del documento a firmar más la firma de este contenido.



  - **Enveloping (envolvente)**, en este caso el documento firmado es la firma del documento a firmar y dentro de esta firma está el propio documento a firmar.



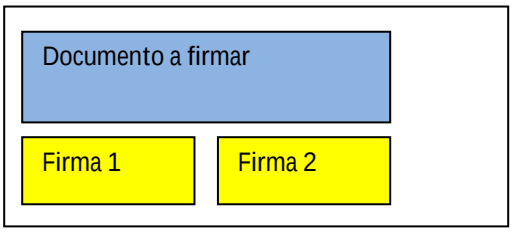
- **Firma *detached***: los datos de firma residen fuera del documento a firmar, pero asociados a éste. Los datos de la firma se mantendrán por separado durante todo el ciclo de vida del documento. Para validar la firma hay que crear un documento de evidencia electrónica que contenga de forma conjunta el documento y sus datos completos de la firma.



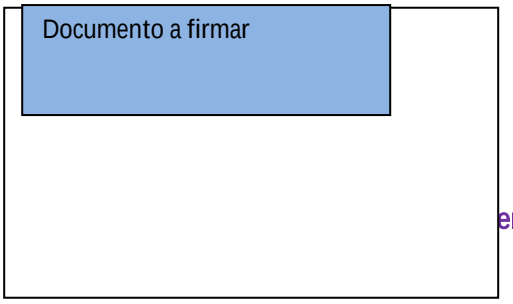
9.2 Nivel de firmas

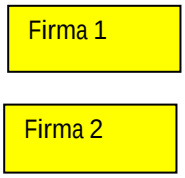
- **Firma simple**: el documento contiene una única firma.
- **Firma múltiple**: el documento contiene dos o más firmas. Esta firma múltiple consiste en que varios firmantes firmen el documento consecutivamente. Esta firma se puede aplicar sobre el documento original cada vez, lo que se identifica como firma **paralela**, o sobre el documento firmado, que se identifica como firma **anidada**.

Documento firmado con firma paralela:



Documento firmado con firma anidada:





La firma múltiple se utilizará en diversas situaciones en el marco de los procedimientos de la Universidad Nacional de Colombia, como por ejemplo en la firma de documentos electrónicos por más de una persona o en el reestampado cronológico (ver apartado 11.1) ya firmados para actualizar la validez legal del documento a lo largo del tiempo, antes de que pueda quedar en entredicho la validez criptográfica de la Firma Digital.

9.3 Formatos de firma

Partiendo de los conceptos básicos sobre firma, descritos anteriormente, a continuación, se describen los formatos de Firma Digital que va a utilizar la Universidad Nacional de Colombia en el marco de esta Política de Firma Electrónica e Identidad Electrónica.

9.3.1 Firma Digital con política de firma y estampado cronológico

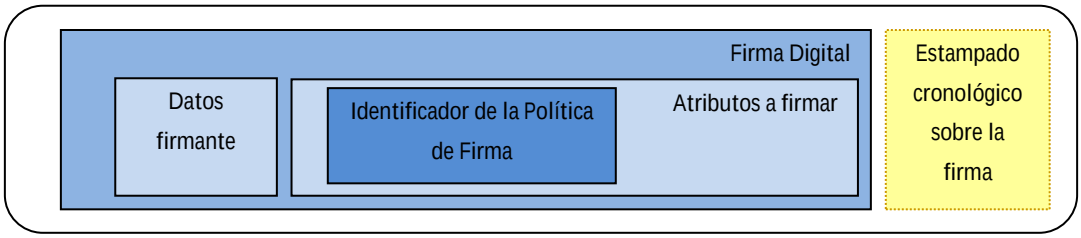
Este será el formato de firma digital para los documentos electrónicos y foliados de expedientes que se tengan que guardar menos que el tiempo de caducidad del certificado digital utilizado para generar el estampado cronológico asociado a la firma digital. En el caso de múltiples firmas, se tendrá en cuenta:

- En paralelo: primera fecha de caducidad del estampado cronológico dentro de las distintas firmas.
- Anidadas: fecha de caducidad del estampado cronológico de la última firma.

Formato de firma derivado de la firma digital con identificador de Política de Firma, también conocida EPES, con la incorporación de un estampado cronológico de tiempo que sitúa la firma digital en un momento determinado del tiempo.

La representación gráfica de este formato de firma, identificado como AdES-T es la siguiente:

AdES-T



La Firma Digital con política explícita (XAdES-T o PAdES-T), debe contener todos los elementos que se listan a continuación de los cuales todos, excepto el último, corresponden al formato XAdES-EPES o PAdES-EPES:

- Los datos firmados por el usuario, como por ejemplo un documento electrónico
- El tipo de contenido firmado: ContentType
- El resumen criptográfico del mensaje: MessageDigest
- El certificado empleado para firmar: ESSSigningCertificate o OtherSigningCertificate
- La fecha y hora alegada de la firma: SigningTime (Opcional)
- Las pistas sobre el contenido firmado: ContentHints (Opcional)
- La identificación del contenido: ContentIdentifier (Opcional)
- La referencia a los contenidos: ContentReference (Opcional)
- La indicación del tipo de compromiso: CommitmentTypeIndication (Opcional)
- La localización del firmante: SignerLocation (Opcional)

- Los atributos del firmante: SignerAttributes (Opcional)
- El estampado cronológico sobre el contenido: ContentTimestamp (Opcional)
- Contrafirma: Countersignature (Opcional)
- Identificación de la política de firma: SignaturePolicyIdentifier
- Estampado cronológico: SignatureTimeStamp

9.3.2 Firma Digital de archivo

Este será el formato de Firma Digital para los documentos electrónicos y foliados de expedientes que se tengan que guardar más del tiempo de caducidad del certificado digital utilizado para generar el estampado cronológico asociado a la Firma Digital. En el caso de múltiples firmas, se tendrá en cuenta:

- En paralelo: primera fecha de caducidad del estampado cronológico dentro de las distintas firmas.
- Anidadas: fecha de caducidad del estampado cronológico de la última firma.

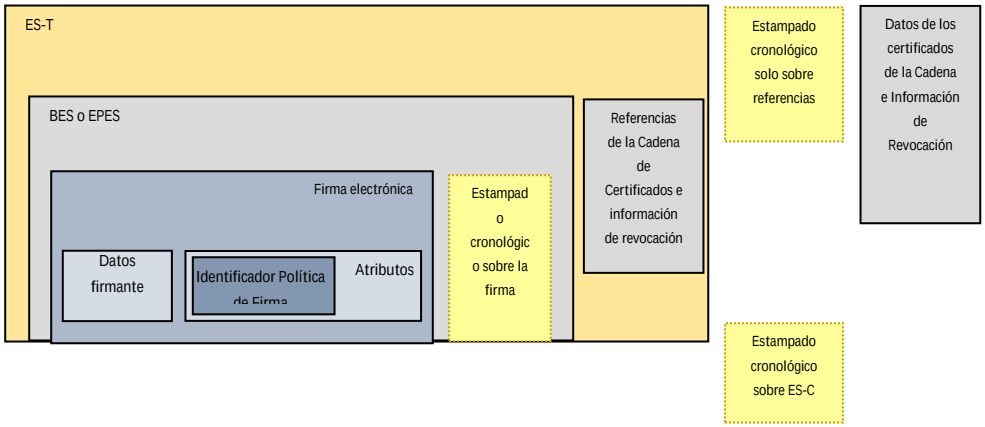
Existen dos formatos: AdES-A y PAdES-LTV

9.3.2.1 Firma AdES-A: XAdES-A y CAdES-A

La Firma Digital de archivo (AdES-A) parte del formato de Firma Digital extensa (XL), que incluye todos los elementos de verificación de la vigencia del certificado para poder repetir la validación de manera autónoma. Sobre este formato extenso de firma, añade un estampado cronológico, previendo el reestampado cronológico sucesivo de manera periódica. Este es el formato de firma más completo y está pensado expresamente para los documentos que se quiere garantizar la disponibilidad a lo largo del tiempo.

Firma Digital de Archivo (ES-A)

C



- La Firma Digital XML: Signature
- El certificado utilizado para firmar: SigningCertificate o KeyInfo:X509Data
- La fecha y hora alegada de la firma: SigningTime (Opcional)
- El formato del objeto de datos firmado: DataObjectFormat (Opcional)
- La indicación del tipo de compromiso: CommitmentTypeIndication (Opcional)
- El lugar de producción de la firma: SignatureProductionPlace (Opcional)
- El rol del firmante: SignerRole (Opcional)
- El estampado cronológico sobre el contenido: AllDataObjectsTimeStamp o IndividualDataObjectsTimeStamp (Opcional)
- La contrafirma: Reference o CounterSignature (Opcional)
- Identificación de la política de firma: SignaturePolicyIdentifier
- Estampado cronológico: SignatureTimeStamp
- Referencias completas de certificados: CompleteCertificateRefs
- Referencias completas de revocación: CompleteRevocationRefs
- Referencias completas de certificados de atributos: AttributeCertificateRefs
- Referencias completas de revocación de atributos: AttributeRevocationRefs

- Estampado cronológico sobre la firma completa: SigAndRefsTimeStamp
- Estampado cronológico sobre las referencias de certificados y revocaciones: RefsOnlyTimeStamp
- Valores de certificados: CertificateValues
- Valores de revocación: RevocationValues
- Valores de certificados de atributo: AttrAuthoritiesCertsValues
- Valores de revocación de certificados de atributo: AttributeRevocationValues
- Estampado cronológico de archivo: ArchiveTimeStamp

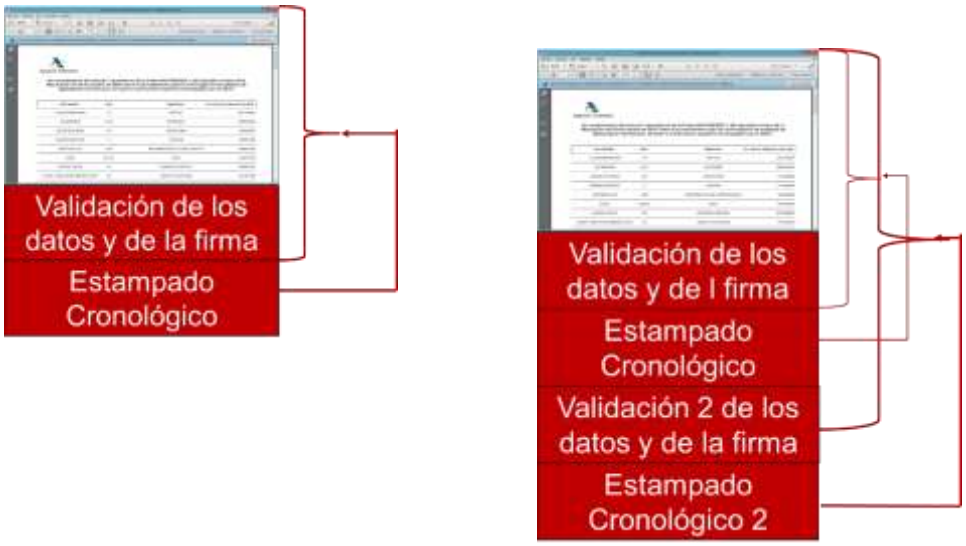
9.3.2.2 Firma PAdES-LTV

La Firma Digital de larga duración (Long Term Validation) es un formato específico de la familia PAdES. La firma más básica, la PAdES Basic además está especificada en una ISO, la ISO 32000-1. La firma PAdES EPES incluye la Firma Digital del documento (en formato CAdES-BES), con estampado cronológico (recomendado) y una respuesta de validación de un servicio OCSP (recomendado). Puede incluir además motivos de firma, el lugar de la firma y datos de contacto del firmante. Incluye además la política de firma.

Sobre estas firmas se puede construir una firma PAdES-LTV que incluye para la verificación de las firmas y del contenido, de que las Autoridades de Certificación en el momento de la validación eran correctas, la respuesta del servicio de validación OCSP y un estampado cronológico sobre esta verificación de firmas.

Se puede añadir a la firma, posteriormente un nuevo comprobante de verificación que garantiza que la verificación que se hizo en su momento continúa siendo válida y se añade un nuevo estampado cronológico para proteger las firmas y sus validaciones.

Ejemplo:



9.3.3 Firma Electrónica biométrica

Este será un formato específico, de firma electrónica para los documentos electrónicos que se generan presencialmente ante un tercero y en el que se guardan cifrados, conjuntamente con el resumen criptográfico del documento, la siguiente información:

- Datos biométricos de la persona que firma manuscritamente el documento, entre ellos:
    - Detalle temporal de la realización de la firma (inicio, final y duración en milisegundos).
    - Detalle de la traza, en relación con la velocidad, aceleración y presión del trazo en toda su figura.

  Los datos biométricos se recogen con elementos específicos de captura permitiendo al firmante la visualización del documento a firmar en el mismo acto de firma.
- Otra información que pueda resultar relevante para el proceso de firma o el documento firmado como puede ser la identificación del software y hardware de captura de firma o la localización GPS del elemento hardware de captura de firma.

El cifrado de información se realiza con la clave pública de un certificado digital específico de firma electrónica biométrica cuya clave pública se almacena en los servidores de la Universidad. La clave privada, es custodiada por un tercero de confianza que se le requerirá cuando sea necesario verificar una firma biométrica, en caso de reclamación o litigio.

En este formato de firma puede haber más de una firma biométrica sobre el documento, pero siempre serán en paralelo. En cualquier caso, una vez finalizadas todas las firmas biométricas y cifradas la información mencionada anteriormente se guardará de forma conjunta con el documento y, para garantizar su integridad, se realizará sobre el mismo una firma electrónica automática de certificado digital de persona jurídica de la Universidad Nacional de Colombia completada con estampado cronológico.

Por lo tanto, la validez jurídica de la firma electrónica biométrica está vinculada al documento y a las evidencias biométricas que se guardan dentro del mismo documento de forma cifrada aportando la firma electrónica y el estampado cronológico únicamente evidencias de integridad y no de autenticidad. En caso de conflicto, una vez descifrados los datos por parte del tercero de confianza que custodia la clave privada del certificado de cifrado, se deberá generar un peritaje de los datos biométricos guardados en el documento y compararlos con una nueva toma de datos biométricos de la persona a la que supuestamente corresponden los datos biométricos y que deberá realizarse bajo condiciones similares, en cuanto a elementos hardware y software, con las que se realizó la firma a verificar.

En este sentido, el tercero de confianza que custodie la clave privada del certificado digital de cifrado deberá contar, o deberá proporcionarse en el momento del peritaje de la firma biométrica, de un cliente ligero de la aplicación de generación de firmas biométricas, así como de la aplicación que permita el descifrado en interpretación de los datos biométricos.

9.3.4 Firma Electrónica basada en la identidad digital y la expresión de la voluntad y consentimiento de los interesados.

Este será otro formato específico de firma electrónica para los documentos electrónicos que se generan telemáticamente con alguna persona de la comunidad universitaria y que no tenga certificado digital.

Dentro del documento firmado, se guarda la información de la firma, la cual es un XML con la siguiente información:

- Nombre y apellidos del firmante.
- Nombre del usuario.
- Fecha y hora de la firma.
- Nombre del fichero firmado.
- Resumen criptográfico del documento.
- Método de resumen criptográfico utilizado.
- IP del ordenador desde el que se firma.
- e-mail de confirmación de firma que se ha mandado al firmante una vez este ha introducido la segunda contraseña, la de firma.

Esta información también se guarda en un repositorio seguro de firmas basada en la identidad digital y la expresión de la voluntad y consentimiento de los interesados.

El documento con la información de la firma, el XML, se firma digitalmente con un certificado electrónico de persona jurídica de la Universidad Nacional de Colombia, específico para la firma de este tipo de firmas.

En este formato de firma puede haber más de una firma basada en la identidad digital y la expresión de la voluntad y consentimiento de los interesados sobre el documento, las cuales pueden ser en paralelo, si el resumen criptográfico es del documento original o anidadas si el resumen criptográfico incluye la firma XML guardada en el documento una vez firmado por primera vez. Para cada firma basada en la identidad

digital habrá una firma XML y una Firma Digital, con estampado cronológico, con el certificado de persona jurídica de la Universidad Nacional de Colombia.

Por lo tanto, la validez jurídica de la firma basada en la identidad digital y la expresión de la voluntad y consentimiento de los interesados está vinculada al documento y a las evidencias de firma XML que se guardan dentro del mismo documento, así como en el repositorio de evidencias de firma, aportando la Firma Digital y el estampado cronológico únicamente evidencias de integridad y no de autenticidad. En caso de conflicto, se podrá aportar como prueba, el proceso seguido, la política de firma, la evidencia guardada en el documento, la evidencia guardada en el repositorio seguro, la firma con el certificado de persona jurídica y el estampado cronológico que deberá coincidir aproximadamente con la fecha que consta en la evidencia de firma (XML).

10 Validación de firmas

Para garantizar la validez jurídica de los documentos electrónicos firmados, cualquier documento que entre o se genere en la Universidad Nacional de Colombia y que contenga una Firma Digital y/o un estampado cronológico, previamente a su almacenaje en el gestor documental, es necesario validarlo.

Para validarlo se utilizará alguno de estos sistemas:

- Para documentos en PDF que no se carguen en el momento de su recepción a la plataforma, se utilizará el servicio de validación de PDF que aporta el propio Adobe PDF.
- La plataforma de validación y los procedimientos que ésta establezca en cada momento.
- Mediante el proceso antes especificado para las firmas electrónicas biométricas.

En los casos de las firmas electrónicas, sólo en aquellos casos en que el proceso de validación de todas las firmas electrónicas sea satisfactorio se procederá a almacenar el documento electrónico dentro del gestor documental de la Universidad Nacional de Colombia.

Para el caso de las firmas biométricas, se procederá a almacenar el documento electrónico en el gestor documental de la Universidad Nacional de Colombia directamente sin ninguna validación adicional, al ser los sistemas de captación de este tipo de firma ya seguros y no existir un proceso automatizado de validación.

Para el caso de las firmas basadas en la identidad digital y la expresión de la voluntad y consentimiento de los interesados, se procederá a almacenar el documento electrónico en el gestor documental de la Universidad Nacional de Colombia directamente sin ninguna validación adicional, al ser los sistemas de captación de este tipo de firma ya seguros y no existir un proceso automatizado de validación.

En el caso de que sea necesaria la preservación de la validez jurídica del documento más allá del tiempo de vida del certificado digital utilizado para generar cualquier firma asociada a este documento, o del estampado cronológico asociado a la o las firmas electrónicas se procederá a completar la firma o firmas electrónicas en el caso de que estas no sean ya firma de archivo, es decir -A o -LTV. El completado ser realizará a formato de firma de archivo.

Para el caso de las firmas biométricas se procederá a la Firma Digital del documento con un certificado de persona jurídica en formato –A o –LTV.

11 Mantenimiento y preservación de las firmas electrónicas

La Firma Digital otorga validez jurídica a los documentos electrónicos. No obstante, esta validez está sujeta a ciertos riesgos que deben gestionarse debidamente para garantizar una validez jurídica indefinida del documento en soporte electrónico. Estos riesgos son:

1. **Caducidad del certificado digital con el que se firma un documento electrónico.** Puede cuestionarse la validez de un documento electrónico a partir del día que caduque el certificado digital que lo firmó, si no se puede acreditar con total garantía la fecha en que se generó dicha firma, la cual debe ser evidentemente posterior a la fecha de emisión del certificado digital y anterior a la fecha de revocación o caducidad del certificado digital. Para garantizar el momento en que se generó la Firma Digital, ésta puede completarse con un estampado cronológico emitido por una Autoridad de Certificación. En el caso de la Universidad Nacional de Colombia estaremos hablando de realizar firmas de archivo, XAdES-A para documentos XML y PAdES-LTV para documentos PDF.

2. **Validez del certificado digital en el momento de generarse la Firma Digital.** Puede cuestionarse la validez de un documento electrónico si no existe evidencia suficiente de que el certificado digital estaba vigente el día que se generó la Firma Digital, es decir, no estaba revocado. Para guardar la evidencia de que un certificado digital en una fecha determinada, la de la firma, no estaba revocado puede completarse la firma con la información de la validación de este aspecto contra la Autoridad de Certificación emisora del certificado en el momento emisión de la firma. En este sentido hay que tener en cuenta que las autoridades de certificación, en el momento en que un certificado digital caduca, eliminan las evidencias de revocación de su lista de revocados por lo que si no se guarda la evidencia mencionada una vez caducado el certificado no existirá la certeza de que el certificado con el que se generó la firma no estaba revocado en el momento de generarla. En el caso de la Universidad Nacional de Colombia para garantizar este caso estaremos hablando de firmas AdES-A o PAdES-LTV.

3. **Obsolescencia tecnológica de la longitud de las claves criptográficas contenidas en el certificado digital y con las que se generan las firmas electrónicas.** Un documento electrónico puede dejar de tener validez jurídica a partir del día en que se ponga en duda la seguridad de las claves criptográficas con las que se firmó. En este

escenario podrían reproducirse de forma incontrolada firmas generadas con las claves puestas en duda y, por lo tanto, todas las firmas generadas con la tecnología obsoleta se pondrían en duda. Para resolver este aspecto se requiere de claves criptográficas de mayor longitud y generar nuevas refirmas a partir de firmas que permitan incorporar estos estampados cronológicos. En el caso de la Universidad Nacional de Colombia estaremos hablando de realizar firmas de archivo, AdES-A o PAdES-LTV.

Será por lo tanto muy importante que en el momento de pasar de un expediente papel a un expediente electrónico, el cual contendrá documentos electrónicos firmados, tener en cuenta las tablas de retención para saber cuánto tiempo se deberán conservar estos documentos y a partir de esta información definir el tipo de firma a incorporar a los documentos de este expediente.

11.1 Restampado cronológico de firmas electrónicas

El objetivo principal de esta función es garantizar la Firma Digital a lo largo del tiempo.

El proceso de restampado cronológico consiste en renovar la firma de fecha y hora, añadiendo un nuevo eslabón a la cadena de evidencias electrónicas a la Firma Digital que ya está en el documento.

Para poder aplicar dicho proceso es necesario que las firmas estén en un formato que permita añadir dichas evidencias de tiempo. Estas son las firmas del tipo XAdES-A, CAdES-A o PAdES-LTV. En el caso de que una firma no esté en estos formatos, previo al restampado cronológico deberemos completar la firma a uno de los formatos anteriormente definidos.

Este será un proceso que se llevará a término:

- En el momento en que esté a punto de caducar el último estampado cronológico aplicado a la Firma Digital a preservar.
- Excepcionalmente, cuando se detecte una posible obsolescencia tecnológica de los algoritmos o de las claves utilizadas para firmar el documento.

Partiremos, tal y como se ha comentado en el punto anterior del supuesto de que los documentos tendrán ya una firma del tipo longevo: XAdES-A o PAdES-LTV. Sobre

estas firmas se incorporará un nuevo estampado cronológico, puesto que su estructura permite dicha posibilidad. Este nuevo estampado cronológico estará ya generado con un certificado reciente, con un período de validez superior al actual en la firma a resellar, con una longitud de clave que no estará comprometida y con un algoritmo que no esté sujeto a la obsolescencia criptográfica del algoritmo en el momento de su emisión.

En definitiva, el restampado cronológico consiste, pues, en mantener la validez de la firma incorporando nuevo material criptográfico, concretamente firmas de fecha y hora, en la misma estructura de la Firma Digital.

11.2 Mantenimiento de la validez jurídica de las firmas en la subetapa de vigencia

El proceso de mantenimiento de las firmas electrónicas en la Universidad Nacional de Colombia será el siguiente, para el caso de aquellos documentos que deban guardarse más allá de la validez del estampado cronológico incorporado a la Firma Digital de este:

1. En el caso de firmas generadas dentro del entorno de la Universidad Nacional de Colombia, es decir que las firmas se hayan generado mediante las herramientas de firma de este, se procederá en fase de tramitación a la generación de las firmas electrónicas ya en formato preservable, es decir en formato de firma de archivo, para documentos XML las firmas se transformarán a XAdES-A, como podría ser el caso del foliado del expediente, y para los documentos PDF se generará una Firma Digital en formato PAdES-LTV.

2. En el caso de firmas que provienen de plataformas externas: otras organizaciones, administraciones públicas, herramientas de cliente, etc. se procederá en su caso a completarlas hasta un formato preservable. Dicho proceso de completación se realizará previo cierre y foliado del expediente. Para documentos XML las firmas se pasarán a XAdES-A, como podría ser el caso del foliado del expediente, y para los documentos PDF se generará una Firma Digital en formato PAdES-LTV.

3. En el caso de que no sea posible generar para algún documento una firma preservable, se procederá lo antes posible a foliar el expediente con un índice en

formato XML con una firma XAdES-A, de forma que sea el foliado del expediente el que garantice la validez jurídica de la Firma Digital del documento.

12 Casos de uso de la Firma Digital y Electrónica.

Previo a la descripción de los casos de uso identificados de Firma Digital y Electrónica, es interesante comentar un concepto clave en este entorno de la documentación electrónica, y que no es otro que el expediente administrativo, ya completamente electrónico y su foliado, también electrónico. Para ello se define:

- Se entiende por expediente administrativo el conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.
- Los expedientes tendrán formato electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos, así como un índice numerado de todos los documentos que contenga cuando se remita. Asimismo, deberá constar en el expediente copia electrónica certificada de la resolución adoptada.
- Cuando en virtud de una norma sea preciso remitir el expediente electrónico, se enviará completo, foliado, autentificado y acompañado de un índice, asimismo autentificado, de los documentos que contenga. La autenticación del citado índice garantizará la integridad e inmutabilidad del expediente electrónico generado desde el momento de su firma y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

Por lo tanto, el índice del expediente se guardará en un fichero XML, que deberá estar firmado con certificado de persona jurídica de la Universidad Nacional de Colombia. Esta firma será en formato XML, y más concretamente firma XAdES-A. Después de definir los conceptos de expediente electrónico y de foliado del mismo, se describen los escenarios identificados:

12.1 Firma Digital de un documento electrónico

Permite firmar electrónicamente documentos en soporte electrónico en cualquier momento de su ciclo de vida, ya sean documentos creados o generados electrónicamente por otras aplicaciones.

Las principales características de este escenario son:

- Se realiza la firma sobre un documento original en soporte electrónico.
- El documento original y las firmas se deben incorporar al sistema.
- Para asegurar la integridad y la autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario en el caso de firmas usando certificados digitales del firmante, validarla y completarla, utilizando un servicio o Autoridad de Validación.
- Hay que incorporar al sistema, la evidencia de validación, que en nuestro caso será la firma completada, la cual será en el caso de XML el mismo documento con firma attached y en el caso de PDFs el mismo documento con firma attached
- El documento electrónico estará en cualquier formato de los aceptados por la Universidad Nacional de Colombia, preferiblemente PDF y XML, siempre que sea necesario garantizar su preservación a lo largo del tiempo.
- El documento se podrá firmar diversas veces y por diferentes usuarios.
- Se firmará con el sistema de Firma Digital basada en certificado electrónico del firmante.
- Se podrá firmar en paralelo y/o de forma anidada.
- En el caso de documentos que no se deban guardar más allá de la validez del estampado cronológico que utilice la Universidad Nacional de Colombia, la firma se generará en formato AdES-T o si no es posible, se completará a este formato.
- En el caso de que los documentos se deban guardar más allá de la validez del estampado cronológico que utilice la Universidad Nacional de Colombia, la Firma Digital se generará o se completará a AdES-A. Para los documentos PDF será PAdES-LTV o XAdES-A en caso de firmas dettached y para los documentos XML será XAdES-A.

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- Sistema de firma:
    - Con certificado electrónico: Para las firmas generadas por la Universidad Nacional de Colombia: Certificado de empleado o Certificado de persona jurídica. Los estudiantes y las empresas podrán utilizar cualquier certificado definidos en el punto 6.1 del presente documento.

- Formatos: PAdES. Inicialmente en formato PAdES-T. En el caso de preservación se completará la firma a formato PAdES-LTV.
- Estampado de cronológico: Sí
- Nivel de firma: Simple, Múltiple (anidada o paralelo)
- Tipo de firma: Attached

12.2 Digitalización segura de documentos en papel: copia segura electrónica.

Las principales características de este escenario son:

- Consiste en la Firma Digital de un documento digitalizado, en formato PDF, para crear una copia segura electrónica.
- La firma es necesaria para garantizar la integridad y evidencias de autenticidad del documento digitalizado, así como la fecha de dicha digitalización.
- El personal de la Universidad Nacional de Colombia que digitaliza la documentación es el responsable de firmar electrónicamente el documento digitalizado, y debe estar habilitado para hacerlo.
- Los documentos digitalizados se firman incorporando un estampado cronológico. Se genera una firma PAdES-T
- Para asegurar la integridad y las evidencias de autenticidad de la firma recibida de la aplicación de creación de firmas, será necesario validarla.
- En el caso de que los documentos se deban guardar más allá de la validez del estampado cronológico que utilice la Universidad Nacional de Colombia, la Firma Digital se generará o se completará a PAdES-A.

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- Tipo de certificado: Certificado de empleado o de persona jurídica homologado por la ONAC
- Formatos: PAdES. Inicialmente en formato PAdES-T. En el caso de preservación se completará la firma a formato PAdES-LTV.
- Estampado cronológico: Sí

- Nivel de firma: Simple
- Tipo de firma: Attached.

12.3 Copia electrónica certificada de un documento electrónico firmado electrónicamente.

Permite obtener copias electrónicas de documentos originales firmados electrónicamente aplicando un cambio de formato. Este sería por ejemplo el caso de la migración de formatos en caso de obsolescencia tecnológica.

Las principales características de este escenario son:

- A partir de un documento original firmado electrónicamente se obtiene una copia (por ejemplo, PDF/A u otro formato de preservación), certificada digitalmente, para guardarla en el archivo electrónico.
- La copia del documento electrónico deberá estar en un formato normalizado y estandarizado, antes de firmarla.
- El documento se firmará automáticamente una única vez con un certificado de persona jurídica a nombre de la Universidad Nacional de Colombia.

Finalmente, concretando el tipo de firma se establecen las siguientes características o requerimientos:

- Tipo de certificado: Certificado de persona jurídica homologado por la ONAC.
- Formatos: Dependerá del formato final. Si es PDF/A se generará en formato PAdES-LTV.
- Estampado cronológico: Sí
- Nivel de firma: Simple
- Tipo de firma: Attached.

12.4 Procesos de firma automatizada

Permite la firma de diversos documentos de forma automática con un nivel importante de garantías jurídicas. No requiere la intervención del firmante en el proceso de firma ya que sólo puede ser realizada con certificados de persona jurídica.

Las principales características de este escenario son:

- Firma de diversos documentos de forma automática.
- El documento electrónico podrá estar en cualquier formato de los aceptados (PDF y XML).
- Se guardará en el repositorio seguro del servidor de la Universidad Nacional de Colombia, tanto los certificados digitales como sus correspondientes claves públicas que deben permitir generar procesos de firma automatizada.

Una vez descritas las características concretas de este escenario, se enumeran los criterios de aplicación y actuación:

- Este escenario está pensado para aquellas tareas en las que se deben firmar diversos documentos de forma automatizada con garantías jurídicas.
- Se utilizará un certificado de persona jurídica, que firmará los documentos en nombre de la aplicación y de la Universidad Nacional de Colombia.
- Existirá una evidencia de que el responsable del certificado guardado en el repositorio seguro de la Universidad Nacional de Colombia ha autorizado la firma automatizada.

Finalmente, concretando el tipo de firma se establecen las siguientes características o requerimientos:

- Tipo de certificado: Certificado de persona jurídica.
- Formatos: Para documentos XML: XAdES-T y para su conservación, XAdES-A. Para documentos PDF: PAdES-T y para su conservación PAdES-LTV.
- Estampado cronológico: Sí.
- Nivel de firma: Simple.
- Tipo de firma: Attached.

Este es un escenario que abarca diversos ámbitos que se podrían llegar a identificar como subescenarios diferentes, como pueden ser:

- Firma automatizada en procesos de digitalización masiva.
- Reestampado cronológico de documentos para actualizar su validez criptográfica.

- Para procedimientos de intercambio de información entre organizaciones y con administraciones.

12.5 Firma electrónica biométrica de un documento electrónico

Permite firmar electrónicamente documentos en soporte electrónico en cualquier momento de su ciclo de vida, ya sean documentos creados o generados electrónicamente por otras aplicaciones.

Las principales características de este escenario son:

- Se realiza la firma sobre un documento original en soporte electrónico.
- La firma forma parte del mismo documento.
- Los documentos originales con sus firmas se deben incorporar al sistema.
- El propio sistema garantiza la integridad y la autenticidad de la firma y por lo tanto no será necesario validarla.
- En el caso de que el documento se tenga que guardar a lo largo del tiempo la firma que se generará con el certificado de persona jurídica será de archivo.
- El documento electrónico estará en formato PDF.
- El documento se podrá firmar diversas veces y por diferentes usuarios.
- Se podrá firmar tanto en paralelo como en anidado.
- En el caso de que los documentos se deban guardar durante períodos largos de tiempo, la Firma Digital que se generará con el certificado de persona jurídica será PDF-LTV.

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- Tipo de certificado: Para el cifrado de los datos biométricos y el resumen criptográfico del documento, el certificado de cifrado guardado en los servidores de la Universidad. Para las firmas generadas con el certificado de persona jurídica: Certificado de persona jurídica a nombre de la Universidad Nacional de Colombia.
- Formatos:
    - Firma biométrica: firma específica.

- Firma con certificado de persona jurídica: PAdES. en formato PAdES-LTV.

- Estampado cronológico: Sí (para la firma con el certificado de persona jurídica)
- Nivel de firma: Simple, Múltiple (anidada o paralelo)
- Tipo de firma: Attached.

12.6 Firma electrónica basada en la identidad digital y la expresión de la voluntad y consentimiento de los interesados

Permite firmar electrónicamente documentos en soporte electrónico en cualquier momento de su ciclo de vida, ya sean documentos creados o generados electrónicamente por otras aplicaciones.

Las principales características de este escenario son:

- Se realiza la firma sobre un documento original en soporte electrónico.
- La firma forma parte del mismo documento.
- Los documentos originales con sus firmas se deben incorporar al sistema.
- El propio sistema garantiza la integridad y la autenticidad de la firma y por lo tanto no será necesario validarla.
- En el caso de que el documento se tenga que guardar a lo largo del tiempo la firma que se generará con el certificado de persona jurídica será de archivo.
- El documento electrónico estará en formato PDF.
- El documento se podrá firmar diversas veces y por diferentes usuarios.
- Se podrá firmar tanto en paralelo como en anidado.
- En el caso de que los documentos se deban guardar durante períodos largos de tiempo, la Firma Digital que se generará con el certificado de persona jurídica será PDF-LTV.

Finalmente, concretando el tipo de firma, se establecen las siguientes características o requerimientos:

- Tipo de certificado: Para las firmas generadas con el certificado de persona jurídica: Certificado de persona jurídica a nombre de la Universidad Nacional de Colombia.

- Formatos:
    - Firma con usuario: XML guardado en el PDF y datos guardados en el repositorio de firmas.
    - Firma con certificado de persona jurídica: PAdES. en formato PAdES-LTV.
- Estampado cronológico: Sí (para la firma con el certificado de persona jurídica)
- Nivel de firma: Simple, Múltiple (anidada o paralelo)
- Tipo de firma: Attached.

12.7 Incorporación de documentos firmados digitalmente por parte del tercero

En el caso en el que el tercero entregue un documento firmado electrónicamente por él, será necesario:

- Validar las firmas electrónicas del documento.
- En el caso de que las firmas no sean AdES-T o AdES-A/LTV se procederá a completarlas hasta uno de estos niveles en función del tiempo que se deba guardar el documento.
- A continuación, se procederá a incorporar al sistema, el documento con sus firmas completadas.

Finalmente, concretando el tipo de firma se establecen las siguientes características o requerimientos:

- Tipo de certificado: Cualquier certificado definido en el punto 1.3.1 del presente documento.
- Formatos: Para documentos XML: XAdES-T y para su conservación, XAdES-A. Para documentos PDF: PAdES-T y para su conservación PAdES-LTV.
- Estampado cronológico: Aconsejado. Una vez completada la firma: Sí
- Nivel de firma: Simple, Múltiple (anidada o paralelo)
- Tipo de firma: Attached.