

GENERACIÓN DE UN MARCO DE GOBIERNO PARA LA IMPLEMENTACIÓN Y  
GESTIÓN DE UN SISTEMA DE FIRMA ELECTRÓNICA EN LA COMPAÑÍA DE  
TELECOMUNICACIONES TIGOUNE.

JAIME JULIAN RODRIGUEZ ZARATE

UNIVERSIDAD PONTIFICIA BOLIVARIANA  
ESCUELA INGENIERÍAS  
FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y  
COMUNICACIÓN  
MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN  
MEDELLIN

2019

GENERACIÓN DE UN MARCO DE GOBIERNO PARA LA IMPLEMENTACIÓN Y  
GESTIÓN DE UN SISTEMA DE FIRMA ELECTRÓNICA EN LA COMPAÑÍA DE  
TELECOMUNICACIONES TIGOUNE.

JAIME JULIAN RODRIGUEZ ZARATE

Trabajo de grado para optar al título de Magister en Tecnologías de la información y la  
comunicación.

Asesor

CARLOS AUGUSTO CERON URBANO

Magister en Tecnologías de la información y la comunicación

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y

COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

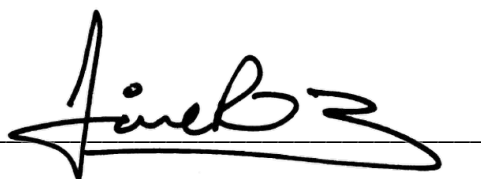
MEDELLIN

2019

## Declaración Originalidad

*“Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad”. Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.*

FIRMA AUTOR (ES)

A handwritten signature in black ink, written over a horizontal line. The signature is stylized and appears to be 'Luis B'.

Medellín 15 de enero de 2019

### **Agradecimientos**

Extiendo mis más sinceros agradecimientos principalmente a mi familia quienes me apoyaron siempre en el proceso de este proyecto de vida que ha representado escalar un peldaño a la vez en el desarrollo profesional que emprendí desde muy joven.

A mis amigos y compañeros de maestría por compartir su experiencia y conocimiento y permitirme aportarles conocimiento con la mía.

A la Universidad Pontificia Bolivariana y su cuerpo docente por su vocación y dedicación en enseñar a todos los que quisimos ser parte de esta institución.

## Contenido

<b>1</b>	<b>Introducción.....</b>	<b>20</b>
<b>2</b>	<b>Planteamiento del Problema.....</b>	<b>21</b>
2.1	<b>Problema .....</b>	<b>21</b>
2.2	<b>Justificación .....</b>	<b>22</b>
<b>3</b>	<b>Objetivos.....</b>	<b>25</b>
3.1	<b>Objetivo General. ....</b>	<b>25</b>
3.2	<b>Objetivos Específicos.....</b>	<b>25</b>
<b>4</b>	<b>Marco Referencial .....</b>	<b>26</b>
4.1	<b>Marco Contextual.....</b>	<b>26</b>
4.2	<b>Marco Conceptual.....</b>	<b>26</b>
4.2.1	Vigilancia Tecnológica. ....	27
4.2.2	Documentos digitales y digitalizados.....	27
4.2.3	Criptografía. ....	32
4.2.4	Políticas. ....	61
4.3	<b>Marco legal.....</b>	<b>65</b>
4.4	<b>Estado del arte .....</b>	<b>68</b>
<b>5</b>	<b>Metodología.....</b>	<b>73</b>
<b>6</b>	<b>Presentación y Análisis de Resultados .....</b>	<b>75</b>
6.1	<b>Marco de Gobierno .....</b>	<b>75</b>
6.1.1	Alcance de la política de implementación del sistema.....	75

6.1.2	Actores involucrados en el marco. ....	76
6.1.3	Gestión de la política de firma. ....	77
6.1.4	Identificación del documento. ....	77
6.1.5	Período de validez. ....	80
6.1.6	Identificación del gestor del documento. ....	81
<b>6.2</b>	<b>Lineamientos para implementación de un sistema de firma electrónica ....</b>	<b>81</b>
6.2.1	Criterios de selección del modelo de sistema a implementar. ....	81
6.2.2	Formatos admitidos de firma. ....	83
6.2.3	Creación de la firma electrónica. ....	85
6.2.4	Verificación de la firma electrónica. ....	88
<b>6.3</b>	<b>Lineamientos de firma electrónica. ....</b>	<b>89</b>
6.3.1	Reglas comunes y de Compromiso. ....	90
6.3.2	Requerimientos de certificados y revocación. ....	103
<b>6.4</b>	<b>Resultados de pruebas de software de firma electrónica. ....</b>	<b>107</b>
6.4.1	PKI actual TigoUne. ....	107
6.4.2	Generación de Certificado en CA de PKI Publica. ....	109
6.4.3	Generación de certificados CA privada. ....	111
6.4.4	Acrobat Reader. ....	115
6.4.5	Office 365. ....	123
<b>7</b>	<b>Conclusiones. ....</b>	<b>127</b>
<b>8</b>	<b>Trabajos Futuros. ....</b>	<b>129</b>
<b>9</b>	<b>Referencias. ....</b>	<b>130</b>

## Lista de Figuras

<i>Figura 1.</i> Documento Digitalizado Certificado. ....	31
<i>Figura 2.</i> Cifrado Asimétrico. ....	33
<i>Figura 3.</i> Uso de cifrado asimétrico en la firma de un mensaje. ....	33
<i>Figura 4.</i> Generación de Claves Asimétricas con Algoritmo RSA. ....	34
<i>Figura 5.</i> Autenticación de Mensajes. ....	35
<i>Figura 6.</i> Firmas Digitales. ....	38
<i>Figura 7.</i> Infraestructura de Clave Pública PKI. ....	41
<i>Figura 8.</i> Obtención de un Certificado Digital. ....	46
<i>Figura 9.</i> Campos de un Certificado Digital. ....	49
<i>Figura 10.</i> Firma Electrónica. ....	52
<i>Figura 11.</i> Relación de Políticas de Seguridad. ....	64
<i>Figura 12.</i> Cuadrante Mágico de Gartner para Mercado de Firma Electrónica. ....	72
<i>Figura 13.</i> Caratula de la Política. ....	79
<i>Figura 14.</i> Cuadro de Aceptaciones. ....	80
<i>Figura 15.</i> Historial de Versiones. ....	80
<i>Figura 16.</i> Reglas Comunes. ....	91

<i>Figura 17.</i> Bloque de Reglas de Verificador. ....	99
<i>Figura 18.</i> Bloque de los Requerimientos de Certificados. ....	105
<i>Figura 19.</i> Bloque de Requerimientos de Revocación. ....	106
<i>Figura 20.</i> PKI TigoUne .....	108
<i>Figura 21.</i> Proceso de Solicitud de Certificado CA Pública.....	109
<i>Figura 22.</i> Plantilla de User Signature Only.....	111
<i>Figura 23.</i> Administrador de Certificados de Usuario.....	112
<i>Figura 24.</i> Gestor de Generación de Certificados.....	113
<i>Figura 25.</i> Pasos del Gestor de Generación de Certificado. ....	114
<i>Figura 26.</i> Certificado de Usuario. ....	115
<i>Figura 27.</i> Preferencias de Adobe Reader. ....	116
<i>Figura 28.</i> Certificados de Confianza Adobe Reader. ....	117
<i>Figura 29.</i> 4 Pasos Para Importar Certificado de CA TigoUne. ....	118
<i>Figura 30.</i> Certificado Importado de CA Interna. ....	119
<i>Figura 31.</i> Configuración de Raíz de Confianza. ....	120
<i>Figura 32.</i> Creación y Aspecto de Firma Electrónica.....	121
<i>Figura 33.</i> Configuración del ID de Firma Adobe Reader. ....	122



<i>Figura 34.</i> Validación de Firmas Electrónicas Adobe Reader.....	123
<i>Figura 35.</i> Insertar Línea de Firma Office 365 .....	124
<i>Figura 36.</i> Configuración de Firma Electrónica Office 365.....	125
<i>Figura 37.</i> Validación de Firma en Office 365.....	126

**Lista de Tablas**

Tabla 1 .....	84
Tabla 2 .....	85
Tabla 3 .....	93
Tabla 4 .....	94
Tabla 5 .....	95
Tabla 6 .....	96
Tabla 7 .....	97
Tabla 8 .....	98
Tabla 9 .....	101
Tabla 10 .....	102

## Glosario

Algoritmo ElGamal: método de cifrado de datos basado en logaritmo discreto.

Algoritmo Rabin: modelo criptográfico asimétrico basado en métodos complejos de factorización

Algoritmo RSA: Algoritmo criptográfico de clave pública que es usado tanto para cifrar como para firmar digitalmente.

Autenticación: proceso mediante el cual son comprobadas las credenciales de un usuario para validar su identidad.

CA Raíz: Entidad de certificación principal que emite certificados digitales a entidades subordinadas.

CA Subordinada: Entidad de certificación que replica un certificado emitido por una CA Raíz y cuya clave de firma ha sido certificada por esta.

Certificado digital: fichero o archivo que contiene información estructurada de una persona o institución, que comprueban su identidad y es emitido por una CA.

Cifrado: Codificar con caracteres diferentes, información que solo pueda comprenderse si se cuenta con la clave para descodificarlos.

Clave privada: Clave criptográfica que solo debe ser conocida por el propietario y es usada para cifrar, descifrar o firmar un mensaje.

Clave Pública: Clave criptográfica que puede ser divulgada por el propietario o un tercero y es usada para cifrar, descifrar o comprobar la firma de un mensaje.

Confidencialidad: propiedad de reserva de la información únicamente accesible a personas autorizadas.

Criptografía: método de codificado o cifrado de información por medio de representaciones alfanuméricas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Descifrado: Proceso inverso de cifrar un mensaje, si se cuenta con la clave necesaria para ello.

Entidad certificadora (CA por sus siglas en inglés): entidad que emite y revoca los certificados, utilizando en ellos la firma digital y electrónica.

e-squiggles: Garabato electrónico, figura formada de forma digital.

Firma Digital: método criptográfico o de cifrado que permite identificar a una entidad remitente de un mensaje.

Firma Electrónica: método técnico, que permite identificar a una entidad o persona ante un sistema de información.

Gestión documental: prácticas y normas metodológicas usadas para gestionar el flujo de documentos en una organización.

Hash: algoritmo matemático que codifica un paquete de datos en una serie de caracteres con una longitud fija.

I+D+i: Investigación, Desarrollo e Innovación, es el concepto evolucionado de I+D.

Integridad: propiedad que permite garantizar que un mensaje no ha sido modificados sin autorización, desde su creación.

Kilowatio por Hora (KW/h): Unidad de medida que equivale a la energía consumida en una hora, denominada como unidad de consumo eléctrico.

Kp: Clave privada de cifrado y firma.

Ku: Clave Publica de descifrado y comprobación de firma.

Millicom: operador de telefonía móvil, con sede central en Luxemburgo, presencia en América, Europa, África y Asia.

No repudio: garantiza, que en el origen la persona o entidad envió el mensaje no puede negar que es el emisor; y en el destino, que el receptor no puede negar que recibió el mensaje.

Parámetros de Dominio: parámetros utilizados con algoritmos criptográficos como los asimétricos, que generalmente son comunes a un dominio de usuarios.

Política de seguridad: documento administrativo que establece las normas, lineamientos y compromisos de una gerencia con la seguridad de la información.

Signatario / Firmante: Parte, persona o entidad que firma un mensaje electrónico.

TigoUne: empresa colombiana que presta servicios integrados de comunicaciones.

## Acrónimos

Los siguientes acrónimos mantiene las siglas en su idioma original (Ej. Ingles)

AES: (Estándar avanzado de cifrado), método criptográfico de cifrado de información por bloques.

CMS: *Cryptographic Message Syntax*, estándar general usado para firmar documentos digitales o digitalizados.

CRL: *Certificate Revocation List*, Lista de certificados de clave pública creados revocados y firmados digitalmente por una Autoridad de Certificación.

DSA: Algoritmo estándar usado para Firma digital,

ECDSA: Algoritmo de firma digital basado en curvas elípticas, es una modificación del algoritmo DSA.

EPM: Empresas Públicas de Medellín, prestadora de servicios públicos domiciliarios como acueducto, alcantarillado, gas, energía y aseo.

ETSI: Instituto Europeo de Normas de Telecomunicaciones

FIPS: Estándares generados por el gobierno de estados unidos de américa para regular Procesamiento de la Información.

IETF: organización internacional abierta de normalización generadora de los documentos RFC.

MDC: funciones de código de detección de modificación.

NIST: Instituto nacional de estándares y tecnología de Estados Unidos.

OCSP: Protocolo de comprobación del Estado de un Certificado En línea.

ONAC: Organismo Nacional de Acreditación en Colombia, presta servicios de acreditación a otros organismos de evaluación.

PKCS: (Estándares criptográficos de clave publica) hace referencia a un grupo de estándares de criptografía de clave pública creados y divulgados por los laboratorios de RSA en California.

RFC: *Request for Comments*, son publicaciones que regulan las propuestas y los estándares de internet.

RSE: Responsabilidad Social Empresarial.

SGSI: Sistema de gestión de seguridad de la información.

TIC: Tecnologías de la información y la comunicación.

TLS: Protocolo de seguridad en la capa de transporte del modelo OSI, permite que dos partes se comuniquen con privacidad e integridad de datos.

TTA: Autoridad de marca de tiempo para certificados digitales.

W3C: El *World Wide Web Consortium* es un grupo de ámbito internacional dedicado a la estandarización de Internet

## Resumen

Las tendencias actuales en modelos de gestión e implementación de firmas electrónicas alrededor del mundo, aplicadas a procesos de negocio dentro de las compañías de tecnología de información y comunicación, requieren de la definición de marcos de gobierno y buenas prácticas que permitan la implementación y gestión de este tipo de servicios. En este trabajo se genera un marco de gobierno y buenas prácticas, a través de una política que permite la implementación y gestión de un sistema de firma electrónica en la compañía de telecomunicaciones TigoUne.

Este marco de gobierno y buenas practica se enfoca en los procesos internos del sistema de gestión de la seguridad de la información y el sistema de gestión documental, cimentándose en los conceptos elementales de confidencialidad, integridad y disponibilidad de la información. Se desarrolla a partir de un ejercicio de vigilancia tecnológica a nivel de la normatividad legal vigente en Colombia, el estado del arte o tendencias a nivel mundial de la implementación de sistemas de firma electrónica y de generación de sus políticas corporativas, firmas digitales y electrónicas, y sus arquitecturas de solución, incorporando elementos como infraestructuras de clave pública, entidades de certificación, procesos de generación de políticas corporativas y sistemas de gestión de seguridad de la información. Todo esto enfocándose en las necesidades de implementación del sistema de firma electrónica, en la compañía TigoUne.

Las fases de desarrollo de este proyecto contemplan una primera etapa de vigilancia tecnológica para recopilar información relevante para el cumplimiento del objetivo general de este proyecto, una segunda fase donde se definen los lineamientos de implementación de un sistema de firma electrónica ajustado a las necesidades de TigoUne, una tercera fase de



evaluación de los tipos de arquitecturas de aplicación del sistema de firma electrónica y una fase final de generación del documento de la política de uso e implementación de firma electrónica.

**Palabras Clave:** Firma Digital; Firma electrónica; Política organizacional; certificado digital; Infraestructura de Clave Pública.

### **Abstract**

Current trends in management models and implementation of electronic signatures around the world, applied to business processes within information and communication technology companies, require the definition of governance frameworks and good practices that allow the implementation and management of this type of services. This work generates a governance framework and good practices, through a policy that allows the implementation and management of an electronic signature system in the telecommunications company TigoUne.

This framework of governance and good practice focuses on the internal processes of the information security management system and the document management system, based on the basic concepts of confidentiality, integrity and availability of information. It is developed from an exercise of technological surveillance at the level of current legal regulations in Colombia, the state of the art or worldwide trends in the implementation of electronic signature systems and generation of corporate policies, digital and electronic signatures, and its solution architectures, incorporating elements such as public key infrastructures, certification entities, corporate policy generation processes and information security management systems. All this focusing on the needs of implementation of the electronic signature system, in the company TigoUne.

The development phases of this project includes a first stage of technological monitoring to gather relevant information for the fulfillment of the general objective of this project, a second phase where the guidelines for the implementation of an electronic signature system adjusted to the needs of TigoUne are defined. , a third phase of evaluation of the types of architectures of application of the electronic signature system and a final phase of generation of the document of the use and implementation policy of electronic signature.

**Key Words:** Digital Signature; Electronic Signature; organizational policy; digital certificate; Public Key Infrastructure.

## **1 Introducción.**

La transformación digital en las compañías de tecnología y servicios se ha convertido en una necesidad de competitividad que obliga a estas a mejorar sus procesos y sus resultados, orientadas a mejorar la eficiencia de sus productos y servicios, a la par que se busca optimizar sus costos, la protección de sus recursos digitales, y aportar de manera significativa a la sostenibilidad ambiental. Este trabajo de grado apoya la transformación digital que busca la compañía de servicios de telecomunicaciones TigoUne a través de la definición de un marco de gobierno que le permita establecer lineamientos para la implementación de sistemas de firma electrónica.

Se aborda la normativa legal vigente aplicable a firmas digitales y electrónicas para Colombia y los conceptos fundamentales de seguridad de la información referentes a firmas electrónicas, pasando por la identificación de documentos digitales y digitalizados, criptografía asimétrica, procesos de generación de firmas digitales, infraestructura de clave pública, proceso fundamental de las firmas electrónicas, el uso de certificados digitales y de las entidades de certificación. Se hace énfasis en los formatos de firmas electrónicas, los diferentes tipos y variaciones de estos en busca de la mejor alternativa de firma electrónica.

Se establece requisitos legales, administrativos y procedimentales que deben cumplirse para la elaboración de la política de firma electrónica, asociados a los lineamientos técnicos de firmas electrónicas avanzadas y certificados digitales que deben ser aplicados para la selección e implementación de sistemas de firma electrónica clasificados por tipo y necesidad.

Se muestran también pruebas de configuración y funcionamiento de dos de las más reconocidas aplicaciones de generación, edición y digitalización de documentos enfocadas a la aplicación de firmas electrónicas avanzadas y su correspondiente validación.

## 2 Planteamiento del Problema

### 2.1 Problema

A comienzos del año 2016 en la Gerencia de operaciones de infraestructura de TigoUne, se implementó un modelo de firma electrónica a través de una aplicación libre, de visualización de documentos en formato PDF que no garantiza la autenticidad, confidencialidad, integridad y no repudio de los documentos o información.

La implementación de esta herramienta de firma electrónica surgió de una necesidad puntual para darle agilidad a la gestión de documentos de asignación de activos fijos al interior de TigoUne, previo a la implementación de esta herramienta, estos documentos debían imprimirse y firmarse físicamente, generando demora en el proceso de gestión documental, desperdicio de papel, costos innecesarios en energía eléctrica, consumibles de impresión y tiempo útil por empleado.

Esta herramienta solucionó parte del problema, no obstante, dejó al descubierto un problema secundario de gran importancia, como la imposibilidad de tener integridad en el documento firmado, ya que no garantiza que el documento firmado no se pueda modificar o genere trazas sobre su alteración, también carece de autenticidad por no existir un mecanismo de comprobación de la firma del documento a través de una entidad certificadora, falta de no repudio ante la imposibilidad de validar si el individuo firmante es quien dice ser, y por último, sin ser menos importante, falta de confidencialidad, aunque estos documentos son de manejo interno de TigoUne, cuentan con datos personales de los empleados y contratistas que están protegidos por la ley Colombiana. TigoUne carece de una política específica de firma electrónica, la cual enmarque el uso de herramientas adecuadas, establezca el alcance de aplicabilidad de estas y permita derivar procedimientos acordes a las necesidades de TigoUne para la firma electrónica de documentos.

## 2.2 Justificación

TigoUne cuenta actualmente con un marco de gobierno general de seguridad de la información, basada en las mejores prácticas establecidas por la norma ISO 27000, y alineada con la política global de seguridad de la información de *Millicom – Security Policy ELC*, esta política general contempla políticas asociadas como:

- Política de gestión de seguridad de la información.
- Política de Administración del riesgo de seguridad de la información.
- Política de Seguridad de la información en los procesos asociados a las personas.
- Política de Administración y protección de activos de información.
- Política de gestión de acceso.
- Política de Cifrado de información.
- Política de seguridad física y del entorno.
- Política de seguridad de las operaciones.
- Política de Seguridad en las comunicaciones.
- Política de adquisición y desarrollo de plataformas de tecnologías de información y comunicaciones.
- Política de seguridad de la información en relaciones con terceras partes.
- Política de gestión de incidentes de seguridad de la información.
- Política de continuidad de la seguridad de la información.
- Política de cumplimiento de requisitos legales y normativos de seguridad de la información.

No obstante, TigoUne carece de una política que establezca el marco y alcance de implementación de un sistema de firma electrónica.

La prioridad de mantener la confidencialidad, autenticidad e integridad en el manejo de información relevante de la compañía, contenida en los documentos contractuales, informes para presentación, formatos internos y externos para legalización, deben estar respaldadas por un marco de gobierno que establezca la adecuada implementación del sistema de firma electrónica, basada en procedimientos claros y específicos, generando mayor eficiencia en los procesos internos de la gestión documental enmarcados en la gestión de la seguridad de la información, amoldándose a las necesidades puntuales del negocio.

Con la generación de un marco de gobierno que establezca una adecuada implementación de un sistema de firma electrónica, se podrían obtener beneficios como la reducción en promedio del 30% de las impresiones de documentos físicos al año, también la reducción del consumo energético del parque de equipos de impresión el cual puede llegar a 3876 KW/h al año, Energía que consumen 2 hogares de 4 personas cada uno (Empresas Públicas de Medellín, 2017), al igual que la reducción del impacto ambiental ya que el parque de equipos de impresión de la compañía se aproxima al medio millar lo que se traduce al final de la vida útil de estos equipos, en desechos electrónicos que deben ser tratados para su destinación final.

La generación de este marco de gobierno para la implementación del sistema de firma electrónica en la compañía, aporta al incremento de la productividad de los empleados, facilita el cumplimiento de la política interna de cero papel, mitiga el riesgo de apropiación indebida de propiedad intelectual o derechos de autor, permite establecer procedimientos específicos para su implementación, proyecta el retorno de la inversión de la implementación del sistema, establece las definiciones que facilitan la integración con el sistema de gestión documental, el cual fortalece la disponibilidad, integridad, confidencialidad y acceso de la información.

Surge de esta manera la necesidad de generar un marco de gobierno para la implementación y gestión de un sistema de firma electrónica que ayude a dar solución al problema planteado, objeto de este trabajo de grado.



### **3 Objetivos**

#### **3.1 Objetivo General.**

Generar un marco de gobierno para control y uso de un sistema de firma electrónica de manejo y legalización de documentos físicos digitalizados y documentos digitales de la compañía TigoUne.

#### **3.2 Objetivos Específicos.**

1. Definir el alcance del marco de gobierno de implementación del sistema de firma electrónica en TigoUne a través de los estándares internacionales
2. Definir los lineamientos sobre los cuales se basa el marco de gobierno de implementación de del sistema de firma electrónica en TigoUne teniendo en cuenta las necesidades internas del negocio
3. Establecer las medidas de control de la implementación del sistema de firma electrónica en TigoUne a través de reglas.

## 4 Marco Referencial

A continuación, se describe el marco sobre el cual se referencia el presente proyecto.

### 4.1 Marco Contextual

La generación de un marco de gobierno que asegure una adecuada implementación de un sistema de firma electrónica se aplica a la compañía TigoUne, siendo esta, un marco referencial para la aplicabilidad al entorno de negocio de la compañía y sus procesos internos como gestión humana, nómina, compras y contratación, así también podría referenciar a compañías similares en foco de negocio, tamaño y tipo como pública, privada o mixta, que hagan parte de los grupos empresariales a nivel trasnacional de *Millicom International Cellular S.A*, operador de telefonía móvil, con sede central en Estados Unidos de América, Reino Unido y Luxemburgo, con presencia operativa en América, Europa, África y Asia, y Empresas Públicas de Medellín (EPM), empresa que presta servicios públicos de agua, energía y gas natural, propietaria del 50% de TigoUne.

El marco de gobierno será generado y aplicado para el cumplimiento de políticas generales al interior de la compañía, descritas en el apartado de la justificación, y enmarca el método de implementación del sistema de firma electrónica, de la misma forma, debe apalancar los procesos internos de la compañía, principalmente y sin limitarse a ellos, el sistema de gestión de seguridad de la información, la gestión documental y el proceso de aseguramiento de servicios de TI.

### 4.2 Marco Conceptual

Se tendrán en cuenta los siguientes conceptos que enmarcan de forma general el alcance del presente proyecto y serán la base fundamental para la generación de una política de control e

implementación de un sistema de firma digital para manejo y legalización de documentos internos y externos de la compañía TigoUne.

#### **4.2.1 Vigilancia Tecnológica.**

En los últimos años la vigilancia tecnológica ha sido pieza fundamental no solo en el ámbito de la investigación sino en el empresarial, para captar información de ciencia y tecnología tanto al interior como al exterior de las organizaciones y convertirla en conocimiento, con el fin de tomar decisiones que permitan anticiparse a cambios, encaminarse en las últimas tendencias de desarrollo e innovación y minimizar riesgos(Angelozzi & Martín, 2011).

La norma vigente UNE 166006 de 2011 Gestión de la I+D+i: Sistema de la vigilancia tecnológica e inteligencia competitiva, describe la vigilancia tecnológica como una herramienta metodológica esencial para los sistemas de gestión de investigación, desarrollo e innovación. La mejora continua que provee para la accesibilidad y gestión de conocimiento científico y técnico, así como su contexto en la aplicación de este, la vigilancia tecnológica se convierte en indispensable en la toma de decisiones para la planeación y desarrollo de un nuevo producto, servicio o proceso en una organización. Por otro lado, la tecnología está supeditada por otros factores, como pueden ser legislativos, normativos, económicos, de mercado, sociales, entre otros, que será necesario vigilar de igual manera (Aenor, 2011).

#### **4.2.2 Documentos digitales y digitalizados.**

##### **4.2.2.1 Documentos digitales.**

La FADGI (*Federal Agencies Digital Guidelines Initiative*) define un archivo digital o informático como un segmento o bloque de información almacenado, que está disponible para un programa informático. Son los homólogos de los documentos en papel, que tradicionalmente se

guardan en carpetas de archivos. Los sistemas operativos de los computadores consideran los archivos como una secuencia de bytes, mientras que el software interpreta los datos binarios, por ejemplo, caracteres de texto, píxeles de imágenes o muestras de audio (Federal Agencies Digital Guidelines Initiative, 2017).

Entre las principales características de los documentos digitales se tienen:

- Formato binario, los datos digitales se almacena en este formato, en soporte magnético, óptico, almacenamiento en discos de estado sólido local o en la nube.
- Es procesable en computador, dependiendo de la clase de soporte en que se almacena, estos datos pueden ser accedidos mediante software y por tanto puede ser procesada informáticamente.
- Son reutilizables, la información es fácil replicar y pasarla de un soporte a otro conservando un alto grado de fiabilidad, adicionalmente, varios usuarios pueden acceder a la información al mismo tiempo.
- Es interactiva, los documentos digitales cuentan con la propiedad de ser interactivos e intuitivos, pueden modificarse según la necesidad del usuario.
- Son actualizables, los datos digitales pueden ser actualizados por el autor o autores de forma fácil, generando así, versiones por cada actualización de forma rápida.
- Son navegables, el uso de enlaces en documentos de tipo http, permite que el usuario pueda acceder a los datos documentos a través de la red.
- Son respaldarles y recuperables, permiten almacenar estos datos o documentos digitales y usar herramientas de búsqueda, respaldo y recuperación.

La FADGI establece también que los documentos digitales son clasificables según el tipo de Información que contienen, de esta forma se pueden diferenciar cuatro grandes tipos de documentos digitales, los textuales, los no textuales, los multimedia e hipertexto.

- Documentos de tipo texto, este tipo de documentos contiene solo texto como libros, artículos de prensa, revistas, legislación, etc., este tipo de formato tiene la particularidad que se pueden visualizar sin problemas de formato al cambiar de computador, herramienta o programa de software, y la gran cantidad de Información que puede contener por su bajo peso en bytes.
- Documentos No textuales, son tipos de documentos que almacenan Información diferente a texto, como imágenes estáticas, sonidos o programas ejecutables.
- Documentos multimedia, son archivos digitales que mezclan documentos de tipo texto y no texto como imágenes, gráficos, sonido y programas ejecutables, estos archivos permiten la interacción con el usuario.
- Hipertextos, son documentos digitales que están conformados por una compleja estructura, compuesta de elementos con diferentes tipos de Información multimedia asociados mediante relaciones lógicas, este tipo de documentos puede ser revisado rápidamente y cuya visualización puede ser selectiva, el ejemplo más común de este tipo de documentos son las páginas web.

Un componente fundamental de este proyecto es el uso de metadatos de los documentos digitales y digitalizados, los metadatos consisten en datos altamente estructurados que contienen información relevante del contenido, calidad, condición y otras características únicas de los documentos digitales, pueden considerarse “Información sobre Información”. Algunos ejemplos

de información que se puede describir y registrar usando los metadatos son: nomenclaturas, fechas, autores, impresa, audiovisual, geoespacial, etc.

Los metadatos según su tipo y funciones pueden clasificarse en administrativos, descriptivos y estructurales. Estas categorías pueden superponerse en ocasiones y dependiendo de los datos que quieran referenciarse, no siempre tienen definidos los alcances, por ejemplo, los metadatos administrativos podrían ser considerados como metadatos descriptivos y estructurales dependiendo del nivel de detalle de la información contenida.

#### ***4.2.2.2 Documentos Digitalizados.***

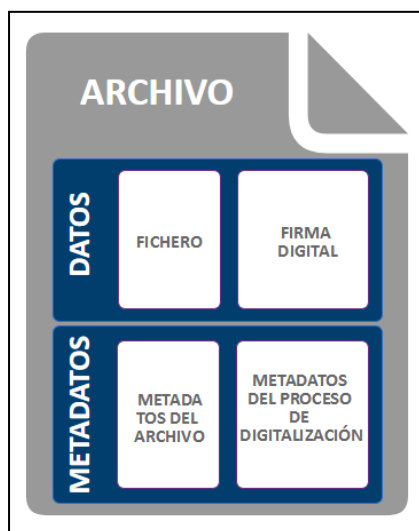
El ministerio de tecnologías de la información y las comunicaciones de Colombia (MINTIC), en la guía número 5 de digitalización certificada de documentos, define la digitalización de documentos como el proceso tecnológico que se surte para convertir un documento de tipo análogo, en uno o varios archivos que contienen la Información codificada, que corresponden de forma fiel e íntegra al documento análogo, que certifica su integridad, disponibilidad, fiabilidad y autenticidad (Ministerio de Tecnologías de la Información y la Comunicaciones. s.f).

El objetivo principal del proceso de digitalización es la generación de un archivo electrónico, es decir, un objeto digital formado por el archivo electrónico, sus metadatos y la certificación o firma relacionada al proceso de digitalización, dicha estructura de documento puede verse en la figura 1.

La composición de un documento digitalizado certificado consta de:

- Datos de contenido (fichero)
- Metadatos del documento

- Firma digital
- Metadatos del proceso de digitalización



*Figura 1.* Documento Digitalizado Certificado.

Referenciada de: Colciencias, Proyecto Diseño del Modelo de Administración Electrónica de Cero Papel en la Administración Pública.

No obstante, el documento resultante de la digitalización:

- Debe ser válido como documento digital con las características exigidas por la normatividad existente.
- Debe ser fiel copia del documento análogo y en términos proporcionales a su naturaleza, características o fines de la digitalización de este.

Algunos de los formatos más utilizados en la digitalización de documentos son los siguientes:

- GIF (*Graphics Interchange Format*).
- JPEG (*Joint Photographic Experts Group*).

- JPEG2000.
- PNG (*Portable Network Graphics*).
- TIFF (*Tagged Image File Format*).
- PDF (*Portable Document Format*).

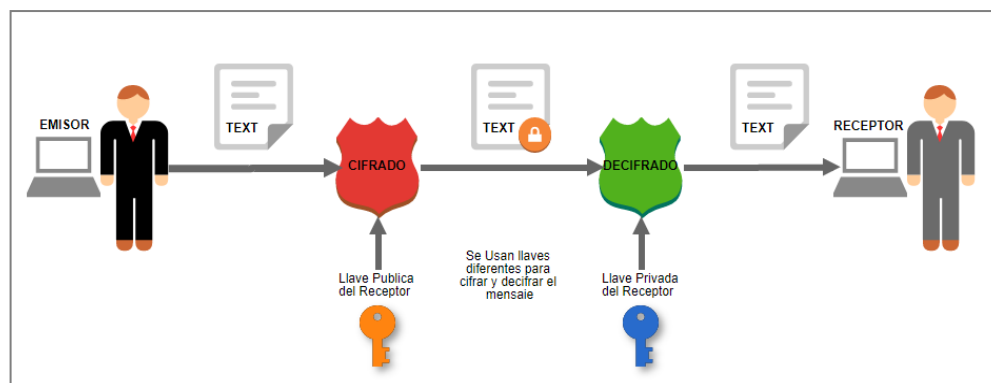
### **4.2.3 Criptografía.**

#### **4.2.3.1 Algoritmo de clave asimétrica.**

Los algoritmos asimétricos, también llamados algoritmos de clave pública, utilizan dos claves: una clave pública y una clave privada, que están matemáticamente relacionadas entre sí. La clave pública se comparte con todas las entidades que quieren participar o comunicarse con la entidad dueña de la clave; la clave privada debe permanecer en secreto y solo gestionadas por el dueño de esta. Aunque existe una relación entre las dos claves, la clave privada es poco probable que pueda determinarse a partir de la clave pública.

Los usos más importantes corresponden a la firma digital, la cual se genera utilizando la clave privada y la firma se verifica utilizando la clave pública, el cifrado que se realiza utilizando la clave pública, y el descifrado se realiza utilizando la clave privada. La figura 2 muestra el transporte de un mensaje cifrado, utilizando claves asimétricas (pública y privada del receptor) (Lucena, 2010).

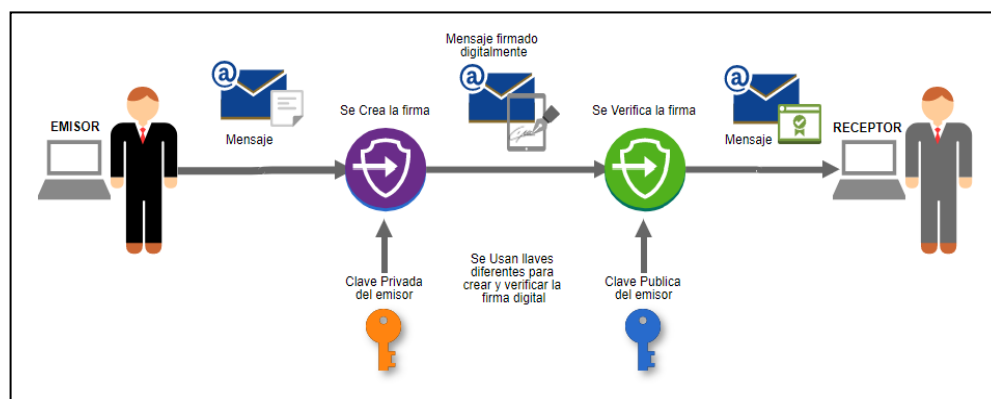




*Figura 2.* Cifrado Asimétrico.

Referenciado de: Lucena, M. (2010)

La figura 3 muestra el uso de claves asimétricas en la firma de un mensaje y su posterior verificación de firma. Por supuesto existen otros factores involucrados, de los cuales se dará más detalle en los siguientes apartados de este documento (Lucena, 2010).



*Figura 3.* Uso de cifrado asimétrico en la firma de un mensaje.

Referenciado de: Lucena, M. (2010)

En la práctica algunos de los algoritmos más utilizados son: RSA (Rivest, Shamir y Adleman), ElGamal y Rabin. La figura 4 muestra el procedimiento para la generación de las claves pública y privada del algoritmo RSA.

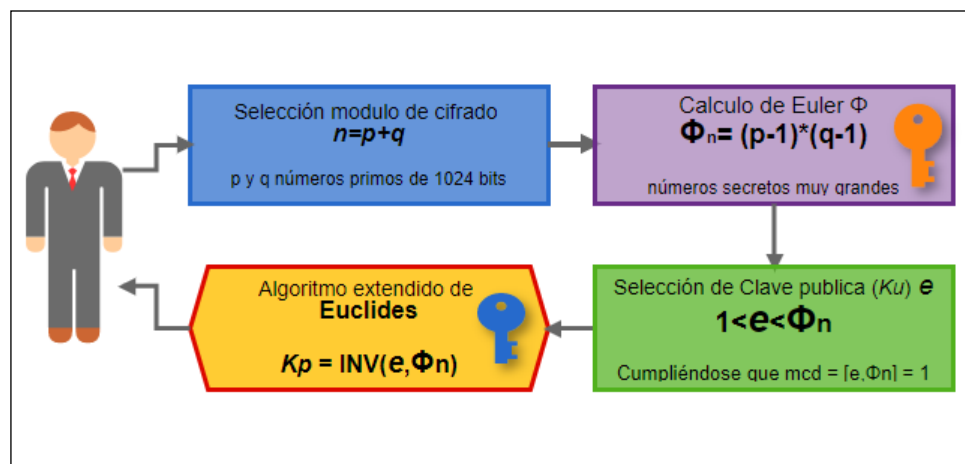


Figura 4. Generación de Claves Asimétricas con Algoritmo RSA.

Referenciado de: Lucena, M. (2010)

Los algoritmos asimétricos se utilizan principalmente como mecanismos de verificación de integridad de datos, de autenticación y de no repudio, es decir, para firmas digitales y para el establecimiento de claves. Los algoritmos asimétricos utilizan claves de mucha más longitud en bits que los algoritmos de clave simétrica, mientras que para considerar seguro un algoritmo simétrico basta con tener una clave de 128 bits, según la publicación FIPS 197 del NIST, para los algoritmos asimétricos se recomiendan claves de 2048 bits (RSA), exceptuando los algoritmos de curvas elípticas que por sus características matemáticas brindan la posibilidad de tener claves de menor tamaño y con niveles de seguridad similares a los de RSA (resistencia a ataques de fuerza bruta o estadísticos) (*National Institute of Standards and Technology*, 2001).

Los algoritmos asimétricos poseen dos características importantes. Para el cifrado de la información no requiere transmitir la clave de descifrado, lo cual permite su uso en canales de poca o ninguna seguridad.

En la autenticación de mensajes, la cual se tendrá en cuenta principalmente para el desarrollo del presente proyecto, utiliza las funciones hash que permite obtener una firma digital o resumen a partir de un mensaje, dicha firma es mucho más pequeña en bits que el mensaje original, y es poco probable encontrar otro mensaje que posea la misma firma o más específicamente su valor de resumen (Hash).

A continuación, se explica a modo de ejemplo la figura 5. B posee la clave Pública  $K_u$  de A, B quiere validar la autenticidad del mensaje enviado por A; A genera el resumen hash 1, cifra el Hash 1 con su clave privada  $K_p$  para generar una firma digital y envía a B el mensaje junto con la firma; B genera por su cuenta el hash 2 del mensaje firmado y descifra la firma con la clave pública  $K_u$  de A; B compara hash 2 con el hash 1 descifrado para comprobar la autenticidad e integridad del mensaje.

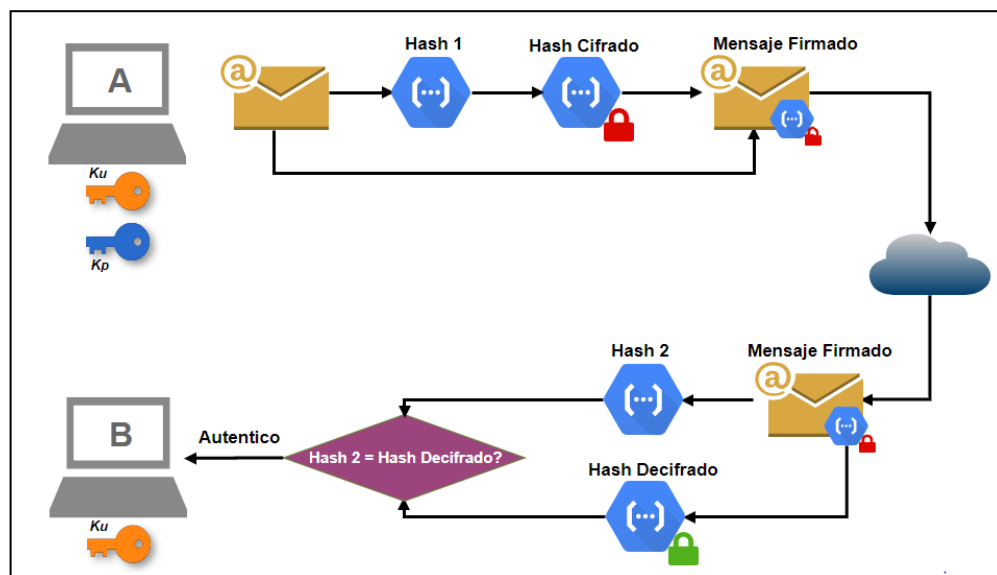


Figura 5. Autenticación de Mensajes.

Referenciada de: Lucena, M. (2010).

Para poder hablar de algunas garantías del uso seguro de algoritmos asimétricos es necesario describir los parámetros de dominio semilla, estos son una cadena de bits que se usa como entrada para un proceso de validación o generación de parámetros de dominio; Los parámetros de dominio son parámetros utilizados con algoritmos criptográficos como los asimétricos, que generalmente son comunes a un dominio de usuarios.

El Estándar publicado en el NIST en 2013, FIPS 186-4 especifica los métodos para la generación de parámetros de dominio y pares de claves privadas y públicas, la selección de tamaños de clave y funciones hash, y la generación y verificación de firmas digitales. El estándar también proporciona métodos para obtener garantías de validez de parámetros de dominio, validez de clave pública y posesión de la clave privada.

Según lo anterior podemos decir que el uso de algoritmos asimétricos brinda a los usuarios ciertas garantías como:

- Asegurar la validez de la clave pública, proporciona confianza en la entidad con la que se establece comunicaciones, es decir, la entidad es quien dice ser.
- Asegurar la validez de los parámetros de dominio, proporciona confianza en que los parámetros de dominio son matemáticamente correctos.
- Asegurar que la posesión de clave privada proporciona confianza, es decir, que el tenedor de la clave privada es realmente el dueño de esta.

#### ***4.2.3.2 Firma Digital.***

El NIST en su estándar FIPS 182-4 define la firma digital como el resultado de una transformación criptográfica de datos, que cuando se implementa correctamente, proporciona un

mecanismo para verificar la autenticación de origen, la integridad de los datos y el no repudio de la parte firmante.

Una firma digital podría definirse entonces como un análogo electrónico de una firma escrita que puede utilizarse para probar al destinatario o a un tercero que el mensaje fue firmado por el remitente, una propiedad conocida como no repudio. También se pueden emplear la firma digital para validar la integridad y autenticidad de los datos o programas almacenados de modo que estas se pueda verificar en un momento posterior.

Cada signatario posee un par de claves públicas y privadas. La generación de firmas sólo puede ser realizada por el poseedor de la clave privada (firmante o signatario). Sin embargo, cualquiera puede verificar la firma empleando la clave pública del firmante. La seguridad de un sistema de firma digital depende del mantenimiento en secreto de la clave privada de un signatario. Por lo tanto, los usuarios deben protegerse contra el robo, pérdida o exposición de sus claves privadas (Barker et al., 2005).

La figura 6 representa la generación y verificación de firmas digitales.

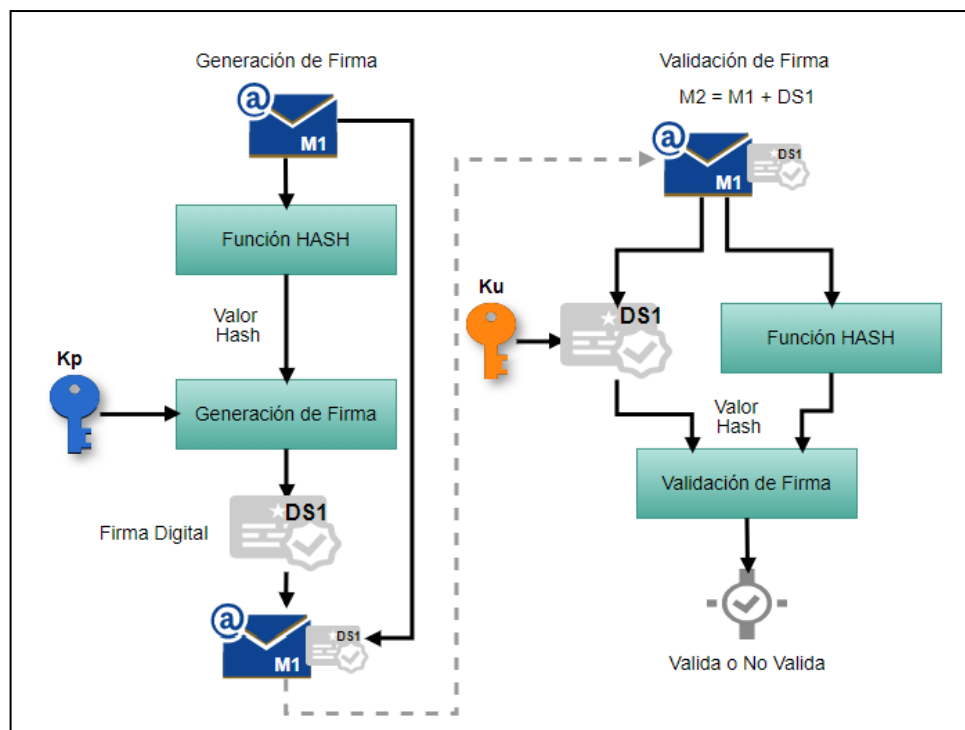


Figura 6. Firmas Digitales.

Referenciada de NIST SP 800-175B.

Generación de Firma, a partir de la figura 6:

- Una función hash es usada en el proceso de generación de firma para obtener un valor hash el cual es una versión condensada de los datos (M1) a firmar.
- El valor de hash junto con la clave privada (Kp) del firmante se utilizan para generar la firma digital (DS1)
- La firma digital (DS1) y los datos (M1) se envían al destinatario (receptor).
- Proceso de verificación de la firma, a partir de la figura 6:
- Se genera el valor hash del mensaje recibido (M1) usando la misma función hash que utilizó el emisor.
- Se extrae el hash de la firma y se comparan con el hash calculado del mensaje recibido. Si

los dos hashes son iguales, se valida si el mensaje recibido es integro y autentico.

- Si el hash extraído de la firma y el hash calculado a través del mensaje son iguales significa que el documento no ha sido deliberada o accidentalmente modificado (Barker, 2016).

El NIST también establece estándares para la generación de firmas digitales descritas en el documento FIPS PUB 186-4 (*Federal Information Processing Standards Publication 186-4*), Esta norma define los métodos para la generación de firma digital que se pueden utilizar para la protección, y para la verificación y validación de las firmas digitales. Las siguientes son las tres técnicas que están aprobadas por el NIST (National Institute of Standards and Technology, 2013).

1. Algoritmo de firma digital - DSA: incluye criterios para la generación de parámetros de dominio de seguridad, estos dominios son conformados por un conjunto de entidades que soportan un sistema de gestión de claves criptográfica, para la generación de claves públicas y privadas, y la generación y verificación de firmas digitales.
2. Algoritmo de firma digital RSA: se especifica en la Norma Nacional Americana (ANS) X9.31 y la *Public Key Cryptography Standard (PKCS) # 1*. FIPS 186-4 aprueba el uso de implementaciones de una o ambas de estas normas y especifica requerimientos adicionales.
3. firma digital por curvas elípticas - ECDSA se especifica en ANS X9.62. FIPS 186-4 aprueba el uso de ECDSA y especifica los requisitos adicionales (*National Institute of Standards and Technology, 2013*).

De acuerdo a la Ley 527 de 1999 del congreso de la república de Colombia, la firma digital es una cadena de caracteres que se agrega a un mensaje de datos y que al aplicar un

procedimiento matemático, relaciona la clave privada del remitente al texto del mensaje, permite determinar que esta cadena de caracteres se ha obtenido exclusivamente con la clave del remitente o firmante y que el mensaje inicial no ha sido alterado después de efectuado el proceso de transformación (Congreso de Colombia, 1999)

#### ***4.2.3.3 Infraestructura de Clave Pública.***

La infraestructura de clave pública (PKI), es un componente fundamental en un sistema de firma electrónica, una PKI es una infraestructura de seguridad que crea y gestiona certificados de clave pública para facilitar el uso de la criptografía de clave pública (es decir, clave asimétrica) (Barker, Barker & Lee, 2005). Para lograr este objetivo, una PKI debe realizar dos tareas básicas:

1. Generar y distribuir certificados de clave pública para vincular claves públicas a Información, después, valida la exactitud de la vinculación entre estas dos.
2. Mantener y distribuir información de estado del certificado, para certificados no expirados.

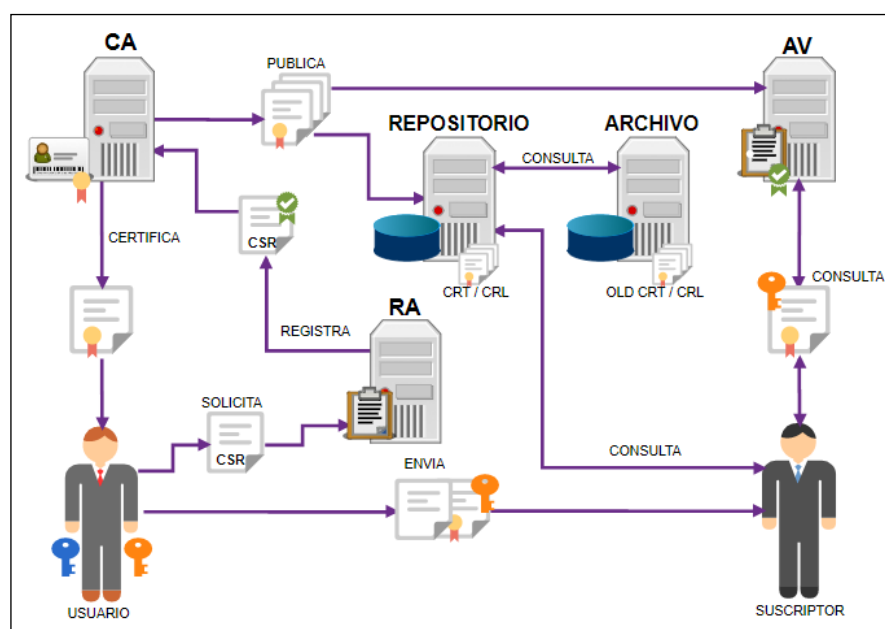
La principal actividad de la PKI es brindar confianza entre las entidades que la utilizan, Las tareas principales de la PKI, incluye vincular claves públicas a entidades a través de los certificados Digitales y mantener esta información actualizada. Si los componentes que ejecutan estas tareas básicas se implementan mal, afectara la disponibilidad del servicio en cual se aplica, incluso llegando a afectar la confianza en el servicio. Por ejemplo, con la apropiación indebida de la clave privada de la CA, aun así, la confiabilidad de la PKI no se vería afectada.

El uso de certificados digitales para entidades finales garantiza la disponibilidad de las claves públicas, los cuales pueden ser distribuidos a través de protocolo TLS (Seguridad en capas



de transporte por sus siglas en inglés), y son validados a través del servicio de PKI, Sin embargo, las claves privadas se mantienen bajo el control y administración exclusiva del propietario de esta (es decir, el usuario que está autorizado a utilizar la clave privada).

Una PKI contiene unos elementos funcionales básicos como autoridades de certificación (CAs), autoridades de registro (RAs), repositorios de datos o bases de datos (DBs) y archivos, como se muestra en la figura 7 dentro de una PKI existen dos tipos de usuarios, los dueños de certificados y las partes confiantes (Barker, Barker & Lee, 2005).



*Figura 7. Infraestructura de Clave Pública PKI.*

Referenciada de: NIST *Special Publication 800-21 2nd edition*

- Autoridad de certificación (CA), es similar a un notario. La CA confirma la identidad de las partes que solicitan un certificado Digital. Las entidades involucradas en una comunicación como por ejemplo aquellas que envían y reciben pagos electrónicos u otro tipo de comunicaciones confían en la CA. Si la CA brinda confianza a una entidad determinada, a través de la PKI todas las entidades que confían en la CA confiarán en la

entidad determinada. Por ello es importante que la CA y la RA validen las entidades antes de brindarles confianza a través de un Certificado Digital.

- Autoridad de registro (RA), es una entidad en la que la CA confía, para registrar o garantizar la identidad de los usuarios de ella misma o de otras CA.
- Repositorio, es una base de datos de certificados digitales activos para un sistema de CA. La función principal del repositorio es proporcionar datos que permitan a los usuarios confirmar el estado de los certificados digitales para individuos y empresas que reciben mensajes firmados digitalmente. Estos destinatarios de mensajes se llaman partes que confían. Las CA publican certificados y CRL (listas de certificados revocados por sus siglas en inglés) en repositorios.
- Archivo, es una base de datos de información que se utilizará para resolver disputas futuras. La función del archivo es almacenar y proteger la información suficiente para determinar si se debe confiar en una firma digital en un documento "antiguo".
- Certificado de clave pública, es un certificado emitido por la CA para cada identidad, confirmando que la identidad es objeto de confianza ante la CA. Un certificado digital normalmente incluye la clave pública, información sobre la identidad de la parte que contiene la clave privada correspondiente, el período de vigencia para el certificado y la propia firma digital de la CA. Además, el certificado puede contener otra información sobre la parte firmante o información sobre los usos recomendados para la clave pública.
- Suscriptor, es una entidad individual o comercial que tiene un contrato con una CA para recibir un certificado digital que verifica una identidad para la firma digital de mensajes electrónicos.
- Listas de revocación de certificados (CRL), que son listas de certificados que han sido

revocados y que también son emitidas y procesadas por las CA. La lista generalmente está firmada por la misma entidad que emitió los certificados. Los certificados pueden ser revocados, por ejemplo, si se ha perdido la clave privada, si la clave privada ha sido robada, si el propietario deja la compañía o agencia, si el nombre del dueño cambia. Las CRL también documentan el estado histórico de revocación de los certificados. Es decir, se puede suponer que una firma fechada es válida si la fecha de la firma se encontraba dentro del período de validez del certificado.

- Usuarios de PKI, son organizaciones o individuos que usan PKI, pero no emiten certificados. Confían en los otros componentes de la PKI para obtener certificados y para verificar los certificados de otras entidades con las que hacen transacciones o negocios. Una persona u organización puede ser una parte confiable y un titular de certificado para diversas aplicaciones.

Ahora bien, si se llegase a perder, es objeto exposición o robo, de una clave privada que se utiliza para generar firmas digitales, el propietario ya no podría garantizar la autenticidad e integridad de los documentos que firmo digitalmente, incluso ya no podría generar firmas digitales con esta clave privada.

Si se cuenta con un llavero de claves, que a su vez utiliza una clave privada y esta es objeto de robo o pérdida (por ejemplo, una clave utilizada para el transporte de claves), el acceso al llavero protegido por esa clave ya no será posible. Para garantizar que no se pierda el acceso a los datos críticos, las PKI suelen realizar copias de seguridad de la clave de administración, para que su recuperación sea posible. Si bien la recuperación de claves se enfoca al objetivo principal de una PKI (es decir, la distribución de claves públicas), la fiabilidad de una PKI puede depender en gran medida de la seguridad de la función de copia de seguridad y recuperación. Los servicios

de recuperación de claves implementados de forma segura mejorarán la usabilidad y fiabilidad de las aplicaciones basadas en PKI, pero una implementación insegura pondrá en peligro la confidencialidad de cualquier aplicación o servicio dependiente de PKI.

Para darle tratamiento al riesgo anterior podría diseñarse un componente de PKI para satisfacer todos estos requisitos, pero esto no es una práctica común. Para la escalabilidad, las PKI implementan generalmente con un conjunto de componentes complementarios, cada uno enfocado en aspectos específicos del proceso PKI.

- Servidores OCSP (*Online Certificate Status Protocol*) para distribuir información de estado del certificado en forma de respuestas OCSP;
- Servidores de recuperación de claves para respaldar material de clave privada.

Servidores de credenciales móviles para distribuir el material de clave privada y los certificados correspondientes.

Se puede decir entonces que, una implementación PKI particular debe incluir la funcionalidad de CAs y RAs, pero los requisitos pueden ser asignados a cualquier número de componentes. Las características proporcionadas por los repositorios, los servidores OCSP, los servidores de recuperación de claves y los servidores de credenciales de *roaming* (móvil) son opcionales en una implementación de PKI (Barker, Barker & Lee, 2005).

#### **4.2.3.4 Entidades Certificadoras o Certificación.**

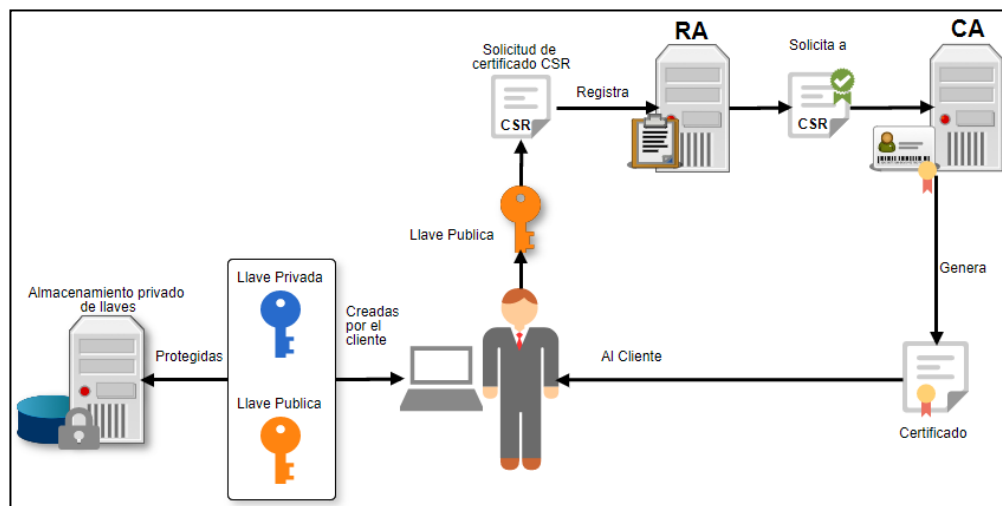
Entidad certificadora CA es aquella que garantiza la autenticidad y no repudio de una firma digital, confirma la identidad de las partes involucradas, es la responsable de emitir y revocar certificados digitales, es un tipo particular que presta servicios de certificación que

legítima a una entidad o persona ante terceros que confían en sus certificados y la relación que debe existir entre la identidad de un usuario y su clave pública. Los métodos para obtener estas garantías se especifican en la publicación especial (SP) del NIST (SP) 800-89, recomendación para obtener la aplicación garantizada de la firma digital, Esta norma incluye requisitos para obtener las garantías necesarias para la validez de las firmas digitales a través de sus certificados.

Las entidades de certificación tienen las siguientes funciones específicas:

- Generación de pares de claves: la CA puede generar un par de claves de forma independiente o conjunta con el cliente.
- Emisión de certificados digitales: se puede considerar que la CA es el equivalente PKI de una agencia de pasaportes: la CA emite un certificado luego de que el cliente proporciona las credenciales para confirmar su identidad. Luego, la CA firma el certificado para evitar la modificación de los detalles contenidos en el certificado.
- Publicación de certificados: la CA debe publicar certificados para que los usuarios puedan encontrarlos. Hay dos formas de lograr esto, una de ellas es publicar certificados en el equivalente de un directorio telefónico electrónico o repositorio. la otra es enviar su certificado a las personas o entidades que cree que podrían necesitarlo de una manera u otra.
- Verificación de certificados: la CA pone a disposición su clave pública en la red para ayudar a la verificación de su firma en el certificado digital de los clientes.
- Revocación de certificados: en ocasiones, la CA revoca por algún motivo el certificado emitido, por vencimiento de la fecha o la pérdida de confianza en el cliente. Después de la revocación, la CA mantiene la lista de todos los certificados revocados que están disponibles.

Como se muestra en la figura 8, la CA acepta la aplicación de un cliente para certificar su clave pública. La CA, luego de verificar debidamente la identidad del cliente, emite un certificado digital a ese cliente.



*Figura 8. Obtención de un Certificado Digital.*

Referenciada de: NIST (SP) 800-89

Así como cobra importancia el poder certificar la autenticidad de una firma digital, también es importante establecer el momento en que se generó una firma digital, a menudo es una consideración crítica. Un mensaje firmado que incluye supuestamente el tiempo de firma no proporciona ninguna garantía de que la clave privada se utilizó para firmar el mensaje. Con el uso apropiado de las marcas de tiempo aplicadas a firmas digitales, es posible incrementar la confianza en el mensaje y la entidad o parte que lo generó, a partir de los datos de TTA (*Trusted Timestamp Authority*), también a partir de los datos suministrados por la entidad de verificación, o en su defecto, los datos de la entidad certificadora incluidos en el mensaje firmado, el firmante

podrá proporcionar cierto nivel de seguridad sobre el momento en que se firmó el mensaje (Barker, 2009).

La Ley 537 de 1999, en el artículo 2 describe a las entidades de certificación o certificadoras como aquella entidad o persona que, autorizada conforme a la ley, está autorizada para generar y firmar certificados en relación con las firmas digitales de terceros que confían, también debe ofrecer o permitir los servicios de registro y estampado de tiempo y fecha de la emisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales (Congreso de Colombia, 1999).

Las entidades de certificación son el elemento fundamental del sistema PKI. Estas hacen posible su aplicación y, por consiguiente, aportan a mantener la seguridad y la autenticidad de la información enviada (Zubite, 2002).

Las entidades de certificación son el respaldo fundamental y jurídico de una firma digital, al validar vinculación entre una clave pública con una persona o entidad que ha firmado un mensaje digital.

En la normatividad colombiana se definen dos clases de entidades certificadoras, la cerrada y la abierta. La entidad certificadora cerrada es aquella que presta servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad certificadora y el suscriptor, sin que haya una contraprestación económica por ello. Y la entidad certificadora abierta es aquella que presta servicios propios de las entidades de certificación, que contemplan:

- Que su uso no es restringido al intercambio de mensajes entre la entidad certificadora y el suscriptor, o
- Que recibe contraprestación económica por éstos. (Presidencia de la república de Colombia, 2000).

#### ***4.2.3.5 Certificados de Clave Pública X.509.***

El formato de certificado de clave pública X.509 se ha convertido en un mecanismo flexible y potente. Se puede usar para transmitir una amplia variedad de información. Gran parte de esa información es opcional, y el contenido de los campos obligatorios también puede variar. Es importante que las áreas encargadas o personas que implementen una PKI comprendan las opciones que enfrentan y sus consecuencias.

El certificado de clave pública X.509 está protegido por una firma digital de la entidad certificadora que lo emite. Los usuarios de certificados saben que el contenido de un archivo o documento no han sido manipulados desde que se generó la firma en el momento de verificar el certificado. Los certificados contienen un conjunto de campos comunes y también pueden incluir un conjunto opcional de extensiones.

Hay diez campos comunes: seis obligatorios y cuatro opcionales. Los campos obligatorios son: el número de serie, el identificador del algoritmo de firma del certificado, el nombre del emisor del certificado, el período de validez del certificado, la clave pública y el nombre del sujeto. El sujeto es la parte que controla la clave privada correspondiente. Hay cuatro campos opcionales: el número de versión, dos identificadores únicos y las extensiones. Estos campos opcionales solo aparecen en los certificados de las versiones 2 y 3.



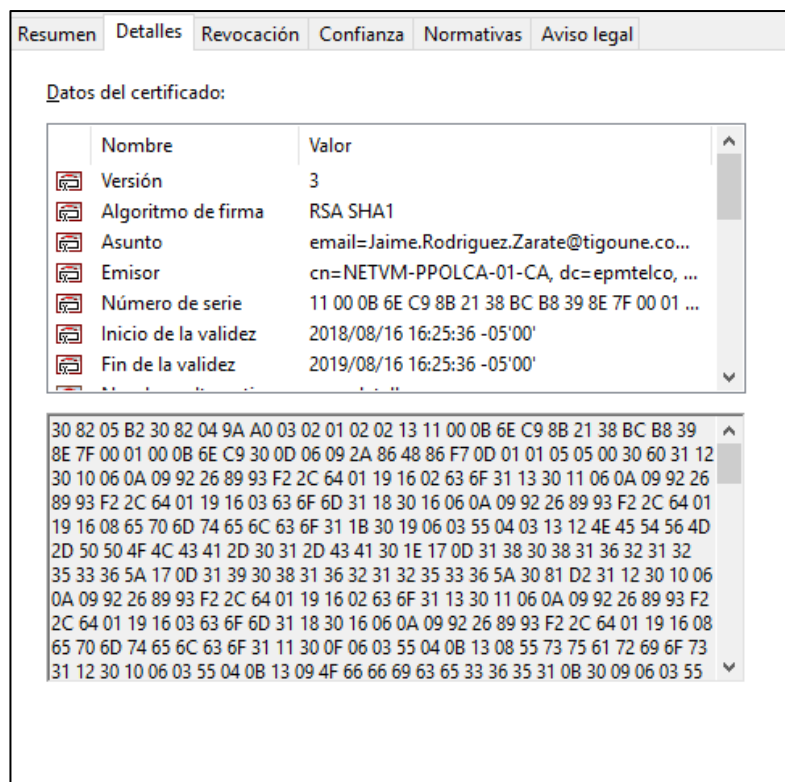


Figura 9. Campos de un Certificado Digital.

Las especificaciones técnicas podrán estudiarse con más detalle en los documentos del IETF como el estándar RFC 3161 y su actualización RFC 5816, Internet X.509 *Public Key Infrastructure Time-Stamp Protocol (TSP)*, RFC 2560, X.509 *Public Key Infrastructure Online Certificate Status-Protocol-OCSP* y las RFC 5280, RFC 4325 y RFC 4630, Internet X.509 *Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile*.

La sintaxis básica del certificado de X.509 v3 se puede detallar en el Anexo A. Para el cálculo de firmas, los datos que se van a firmar se codifican utilizando las reglas de codificación del estándar ASN.1 (DER) X.690. La codificación ASN.1 DER es una etiqueta de codificación de valor para cada elemento.

En cuanto a la forma de almacenar los certificados digitales es preciso especificar el formato el cual debe ser adecuado para cumplir con la confidencialidad, autenticidad e integridad de la información de los usuarios para ello se cuenta con el formato PKCS # 12 v1.1 el cual describe una sintaxis de transferencia para información de identidad personal, que incluye claves privadas, certificados y extensiones. Las máquinas, aplicaciones, navegadores, sitios de Internet, etc., que admiten este estándar permitirán a un usuario importar, exportar un único conjunto o bloque de información de identidad personal. Esta norma admite la transferencia directa de información personal en varios modos de privacidad e integridad, el detalle de esta norma podrá estudiarse al detalle en el RFC7292.

#### **4.2.3.6 *Firma Electrónica.***

Según el glosario del NIST en su publicación NISTIR7298 una firma electrónica es el proceso de aplicar cualquier marca en formato electrónico con la intención de firmar un objeto de datos.

Se puede decir entonces que una firma electrónica es un conjunto de datos o mecanismo técnico electrónico, consignados junto a otros datos o asociados con ellos que identifica a una persona, siempre y cuando sea confiable y apropiable (Certicámara, s.f).

Cualquier persona nueva en esta área puede confundirse fácilmente sobre lo que constituye una firma electrónica y cómo se comparan los diferentes tipos de firmas electrónicas, en términos de poder probatorio y legalidad.

En un nivel básico, cualquier marca en un documento electrónico se puede utilizar para capturar la intención del firmante, de aprobar o aceptar el contenido de ese documento. La forma de la "marca" o cómo fue creada no es en realidad importante. Lo importante es poder comprobar quién hizo la marca y que el documento firmado electrónicamente no se modificó posteriormente.

Entre los más conocidos, existen cuatro tipos de firma electrónica diferenciados por el nivel de complejidad de cada uno de ellos:

Firmas de clic, incluyen casillas de verificación, e-squiggles, imágenes escaneadas y nombres escritos. En este tipo de firma electrónica, no se establece algún tipo de protección criptográfica del documento. Con estas firmas no es posible establecer una evidencia confiable de quién firmó los datos, o incluso, brindar protección al documento para evitar o registrar alteraciones. Esta firma puede transferirse fácilmente de un documento a otro, entre las más conocidas son las que se pueden aplicar con la aplicación Adobe Acrobat Reader.

Firmas Electrónicas Básicas, este tipo de firma involucran al firmante que aplica en el documento, su marca de firma a mano y luego este está protegido con una firma digital, se aplica cada vez que el usuario aplica una marca de firma electrónica y vincula criptográficamente esta marca al documento, por lo general la firma digital aplicada es una firma común o de organización, adicionalmente protege el documento de cualquier cambio posterior, lo que garantiza la integridad de los datos. Esta es una firma a largo plazo que incluye una marca de tiempo, no obstante, este tipo de firma puede requerir, o no, que el usuario tenga un certificado válido de una entidad certificadora, con la desventaja que la identidad del firmante no es verificable directamente desde el documento firmado.

Firmas electrónicas avanzadas y calificadas, Las firmas electrónicas avanzadas (AES) y las firmas electrónicas calificadas (QES), brindan el más alto nivel de confianza y seguridad porque utilizan claves de firma únicas para cada firmante. Esto vincula directamente la identidad del usuario con el documento firmado de modo que cualquier persona puede verificarlo por sí misma utilizando un lector de PDF estándar de la industria.

La ventaja de utilizar AES y QES es que muestran exactamente quién firmó el documento.

QES es una versión más confiable de AES porque requieren los más altos niveles de seguridad para la protección de la clave de firma del usuario y también un proceso de registro formal para que el usuario verifique su identidad mediante una entidad de certificación (*signhub*. S.f).

En la figura 10 se observa gráficamente y en términos generales como podría estar compuesta una firma electrónica en un documento digital o digitalizado.

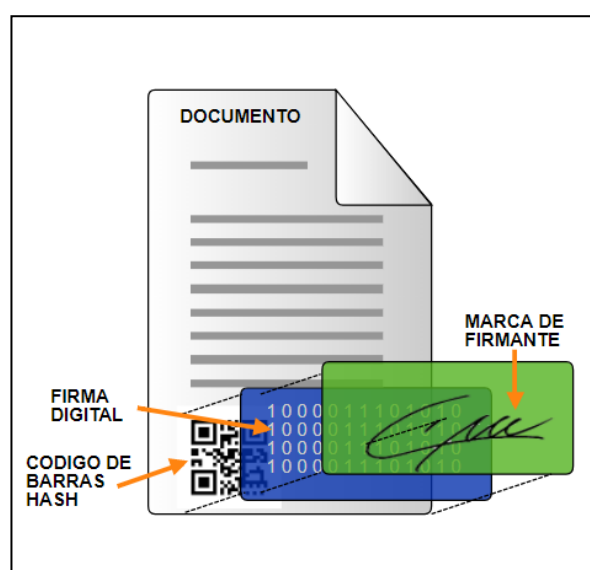


Figura 10. Firma Electrónica.

Referenciado de: <https://www.signinghub.com/electronic-signatures/>

La diferencia entre una firma electrónica y una digital radica en que la firma digital es el resultado de un algoritmo matemático que genera un resumen o hash de un documento o conjunto de datos, concepto que fue abordado en el numeral 4.2.3.2 de este documento; La firma electrónica es más robusta e implica el uso de una PKI, la firma electrónica puede ser legalmente reconocida en tramites comerciales y personales, ya que atribuye a la firma de un marco

normativo que le otorga su validez jurídica y debe contener en su esencia una firma digital junto a otros datos como una imagen, un archivo pdf, un código de barras o una firma digitalizada, siendo esta última una representación gráfica de una firma manuscrita y fácilmente obtenible con un escáner y puede ser insertada en cualquier otro documento, una firma digitalizada no tiene por si sola una validez legal.

Para realizar la firma electrónica de un documento, necesariamente se deben emplear sistemas de información o software que cumplan con tal función.

Algunos de los usos que se les puede dar a las firmas electrónicas son:

- Tramites de impuestos y aduanas nacionales en línea.
- Certificación de transferencias entre sistemas de información
- Generación de certificados laborales.
- Recepción de notificaciones electrónicas.
- Firma de correspondencia electrónica.
- Firma de comprobantes de pago y facturas electrónicas (signhub. S.f).

Para todos estos casos es necesario contar con un certificado digital de una entidad certificadora interna de la compañía o externa según su implementación en documentos de uso interno o externo.

#### ***4.2.3.7 Estándar de firmas electrónicas avanzadas.***

Las normas ETSI TS 101 903, ETSI TS 101 733 y ETSI TS 102 778-3 definen los formatos para firmas electrónicas avanzadas que permanecen válidas durante largos períodos de tiempo, cumplen con la Directiva Europea sobre un marco comunitario para la firma electrónica e

incorporan información complementaria útil en casos comunes de uso. Actualmente, usa la notación de sintaxis abstracta 1 (ASN.1) y se basa en la estructura definida en RFC 2630 *Cryptographic Message Syntax*.

Basados en la estructura de datos XML se pueden encontrar varios tipos de firma electrónica avanzada como:

- Firma electrónica avanzada XML (XAdES) (XAdES-BES): proporciona autenticación básica e integridad y cumple con los requisitos legales para firmas electrónicas avanzadas según lo definido en la Directiva europea. Pero no proporciona el no repudio de su existencia. Este formulario agrega elementos a la sintaxis de procesamiento de firma electrónica, estos elementos son descritos en las notas del grupo W3C en el documento *XML Advanced Electronic Signatures (XAdES) (World Wide Web Consortium W3C, 2003)*.
- Firma electrónica avanzada XAdES-EPES: en esencia es una en formato XAdES-BES al que se le agrega información sobre la política establecida de firma, como, por ejemplo, información sobre el certificado utilizado y la entidad certificadora que lo emitió (*World Wide Web Consortium W3C, 2003*).
- Firma electrónica avanzada XML con sello de tiempo (XAdES-T): Incorpora sello de tiempo para brindar protección contra el repudio. Esta forma agrega el campo *SignatureTimeStamp* + al formulario XAdES dentro del elemento *UnsignedSignatureProperties* (*World Wide Web Consortium W3C, 2003*).
- Firma electrónica avanzada XML con datos de validación completos (XAdES-C): Incorpora referencias al grupo de datos que respaldan la verificación de la firma electrónica, es decir, incorpora las referencias a la ruta de certificación y su información

de estado de revocación asociada. Este formulario es útil para aquellas situaciones en que dicha información es archivada por una fuente externa, como un proveedor de servicios. Este formulario agrega los campos *CompleteCertificateRefs* y *CompleteRevocationRefs* dentro del elemento *UnsignedSignatureProperties* en el formulario XAdES-T (*World Wide Web Consortium W3C, 2003*).

- Firma electrónica avanzada XML con datos de validación extendidos (XAdES-X): Incluye marca de tiempo en las referencias de los datos de validación o en el elemento *ds:Signature* y los datos de validación antes mencionados. Este sello de tiempo contrarresta el riesgo de que las claves utilizadas en la cadena de certificados o en la información de estado de revocación se vean comprometidas. Como se ha dicho, esta forma tiene dos implementaciones alternativas. El primero agrega el campo *RefsOnlyTimeStamp* al elemento *UnsignedSignatureProperties* y el segundo agrega el campo *SigAndRefsTimeStamp* al elemento *UnsignedSignatureProperties* en el formulario XAdES-C (*World Wide Web Consortium W3C, 2003*).
- Firma electrónica avanzada XML con incorporación de datos de validación ampliados a largo plazo (XAdES-XL): Incluye los datos de validación para aquellas situaciones en las que los datos de validación no se almacenan en otro lugar a largo plazo. Este formulario agrega el campo *CertificadosValues* y *RevocationValues* al elemento *UnsignedSignatureProperties* en XAdES-X
- Firma electrónica avanzada XML con incorporación de datos de validación de archivo (XAdES-A): Incluye sellos de tiempo adicionales para archivar firmas de manera que estén protegidos si los datos criptográficos se debilitan. Esta forma agrega el campo *ArchiveTimestamp* + al elemento *UnsignedSignatureProperties* en XAdES-XL.

Según la RFC 5126 CMS *Advanced Electronic Signatures* de 2008, los siguientes son los formatos de firma electrónica basados en sintaxis de mensajes criptográficos CMS, que hacen parte de la firma electrónica avanzada.

- CAdES-BES: Es el formato básico que cumple los requisitos legales de la Directiva para firma electrónica avanzada, contiene los datos del usuario, una colección de atributos obligatorios como se definen en CMS y en ESS (*Enhanced Security Services*).
- CAdES-T (*timestamp*): en esencia es el mismo formato base con incorporación de información del campo de sello de tiempos para resguardar la información de un posible repudio.
- CAdES-C (complete): en esencia es un formato CAdES-T al que se le han agregado datos sobre los certificados y CRL's utilizadas para que puedan ser validados fuera de línea y su verificación posterior.
- CAdES-X (extended): En esencia es un CAdES-C al que se le adicionan datos sobre la fecha y hora específicamente de los datos adicionados sobre certificados y CRL's.
- CAdES-X-L (*extended long-term*): En esencia es un CAdES-X al que se le han agregado los certificados y las referencias de verificación de los certificados que se usaron. Proporciona la opción de validación fuera de línea a largo plazo, incluso si la referencia original ya no esté disponible.
- CAdES-A (archivado): En esencia es un formato CAdES-X-L con la particularidad que adiciona los metadatos asociados a políticas de nueva firma por vencimiento de la anterior. El escenario ideal para este formato de firma son aquellos documentos cuya validez sea muy elevada: hipotecas, títulos universitarios, escrituras, de más de 15 años.



Otro formato específico para la firma electrónica avanzada es el PAdES descrito en la ETSI 102 778 y la cual especifica el soporte para firmas digitales en formato PDF 1.7 (ISO 32000-1) con el objetivo de poder adicionar firmas electrónicas avanzadas en los documentos en formato PDF.

Concretamente, PAdES (ETSI TS 102 778) 1,2 y 3 define los siguientes formatos:

- PAdES-CMS: Define una firma CMS/PKCS#7 descrito en le RFC3852 y basada en ISO 32000-1, admite firmas en serie, recomienda la inclusión de una marca de tiempo de firma, la inclusión de información de revocación, esta firma protege la integridad del documento y autentica al firmante, La firma puede incluir opcionalmente las "razones" para la firma, al igual que una descripción de la ubicación de la firma, puede incluir opcionalmente la información de contacto del firmante.
- PAdES-BES: define una firma electrónica avanzada en formato PDF basada en CAdES-BES como se especifica en el estándar TS 101 733 con la opción de una marca de tiempo de firma (CAdES-T). Las características proporcionadas por este perfil son muy similares al perfil PAdES como se especifica en la TS 102 778-2. Se usa CAdES en lugar de CMS.
- PAdES-EPES: especifica una firma PDF avanzada basada en CAdES-EPES como se especifica en el estándar TS 101 733. Este perfil es el mismo que el perfil PAdES-BES con la adición de un identificador de política de firma y, opcionalmente, una indicación de tipo de compromiso. Las características proporcionadas por este perfil son muy similares al perfil PAdES-CMS como se especifica en el estándar TS 102 778-2. Se usa CAdES en lugar de CMS y el perfil proporciona una guía para evitar incrustar información potencialmente duplicada.

- PAdES-LTV: Este perfil admite la validación a largo plazo de las firmas de PDF. También se puede usar junto con los perfiles PAdES-CMS, PAdES-BES o PAdES-EPES. Este perfil es aplicable a cualquier parte que confíe en una firma durante un período prolongado (por ejemplo, más tiempo que la vigencia del certificado de firma). Con este formato de firma en documentos PDF se consiguen características similares a las de las firmas en formato CAdES-XL y CAdES-A anteriormente descritos.
- PAdES-XML: conglojera un grupo de formatos que describen como utilizar las firmas XAdES en los documentos de tipo PDF. Específicamente, se diferencia en que los documentos firmados en formato XAdES sean documentos netamente XML y que los estos correspondan a formularios XFA (*XML Forms Architecture*).

#### ***4.2.3.8 Criterios para implementación de firma electrónica.***

Los sistemas de firma electrónica se pueden clasificar en tres tipos básicos de herramientas de software, que van desde suites de código abierto gratuitas hasta unidades alojadas localmente. Las características también pueden ser criterios de categorización, ya que ciertos programas no hacen más que ofrecer la firma digital, mientras que otros son más robustos y permiten a los usuarios escribir a mano los documentos, escribir firmas e incluso personalizar algunas marcas:

*Programas de firma electrónica locales.* Estos están cubiertos con una sola licencia y están alojados en servidores locales del cliente. Califican como los más costosos, debido al hecho de que requieren una configuración compleja y, ocasionalmente, alguna instalación de hardware.

*Programas de firma electrónica de software como servicio (SaaS).* Estos generalmente se pagan por mes y están alojados en servidores del proveedor. La empresa cliente no es responsable

de la instalación, actualización y mantenimiento, todo esto hace parte del servicio prestado por el proveedor.

*Programas de firma electrónica de código abierto.* La mayoría de estos ofrecen planes básicos gratuitos, y califican como los más asequibles debido a su acceso universal y al hecho de que el cliente no necesita actualizarlos o pagar por el mantenimiento.

Para adoptar una solución de firma electrónica, una compañía debe:

1. *Examinar* el proceso comercial, administrativo o técnico actual que se está considerando para la transformación y emplear documentos electrónicos, formularios o transacciones, identificando las necesidades y demandas de los clientes o usuarios, así como los riesgos existentes asociados con el fraude, error o mal uso.
2. *Evaluar* el nivel de riesgo del proceso comercial, administrativo o técnico y las transacciones de acuerdo con los estándares establecidos en el NIST. Estos niveles de riesgo son: no aplicable, bajo, medio y alto.
3. En función del nivel de riesgo determinado, *identificar* el estándar de requisitos de autenticación correspondiente.
4. *Evaluar* cómo cada alternativa de firma electrónica puede cumplir con los estándares requeridos y puede minimizar el riesgo en comparación con los costos incurridos al adoptar una alternativa.
5. *Revisar* y evaluar la tecnología de firma electrónica propuesta, y enviar la evaluación a las partes interesadas como la Dirección de TI y Seguridad de la Información para su revisión y recomendación al CIO.
6. *Desarrollar* planes para retener y eliminar la información, asegurando que pueda estar continuamente disponible para quienes la necesiten, para el control gerencial de datos confidenciales y para el cumplimiento de estos planes.

7. *Consultar* Guías de gestión de registros como por ejemplo las publicaciones referentes a identificación y autenticación de usuarios del NIST.
8. *Desarrollar* estrategias de gestión para proporcionar la seguridad adecuada para el acceso físico a los registros electrónicos.
9. *Determinar* si las regulaciones o políticas nacionales son adecuadas para respaldar las transacciones electrónicas a través de firmas digitales y electrónicas y el mantenimiento de registros.
10. *Validar* y confirmar que el sistema alcanza el nivel de seguridad requerido, que el proceso de autenticación cumpla con los requisitos de autenticación del sistema como parte de los procedimientos de seguridad necesarios como la certificación y acreditación.
11. *Implementar* la tecnología seleccionada para el sistema de firma electrónica.

#### **4.2.3.9** *Uso de aplicaciones de firma electrónica.*

El software de firma electrónica brinda a los usuarios la capacidad de reunir firmas en documentos compartidos electrónicamente, eliminando la necesidad de documentos físicos para registrar firmas. El software de firma electrónica facilita la distribución de documentos legalmente sensibles para la recolección de firmas electrónicas. Las organizaciones utilizan el software de firma electrónica para cifrar documentos, como contratos de venta o trámites de empleo, para los cuales a menudo se requieren firmas de clientes, empleados o socios. El software de firma electrónica se integra con frecuencia con aplicaciones de terceros, incluidas las de ventas, los sistemas ERP, las suites de gestión de recursos humanos y las suites de la cadena de suministro, para facilitar los esfuerzos de gestión de cotizaciones, contratos y proveedores. Los estándares de seguridad incorporados que cumplen con los requisitos legales locales y gubernamentales agilizan aún más el proceso de intercambio de documentos legales y garantizan

la legitimidad y las ramificaciones legales de las firmas realizadas a través del software de firma electrónica.

Para calificar su inclusión en la categoría Firma electrónica, un producto de software o aplicación debe:

- Permitir que los usuarios tanto del remitente como del destinatario firmen documentos en una variedad de dispositivos y sistemas operativos
- Cifre y asegure las comunicaciones y documentos compartidos entre los usuarios de la solución
- Rastrea el estado del documento y notifica a los usuarios cuando se requieren acciones (firmar, aprobar, etc.)
- Permitir a los usuarios definir roles de usuario y derechos de permisos tanto internamente como para usuarios externos (contratistas, socios, clientes, etc.)
- Ofrezca capacidades de almacenamiento y creación de documentos integrados o integre con soluciones de software de terceros que brinden funciones de creación o almacenamiento de documentos.

#### **4.2.4 Políticas.**

##### ***4.2.4.1 Políticas Organizacionales.***

Según Richard L. Daft (2011) en su libro Teoría y Diseño Organizacional, una política organizacional se puede definir como un proceso organizacional natural para resolver las diferencias entre los grupos de interés organizacionales. La política es el proceso por el cual se establecen acuerdos y negociar, que se utiliza para superar las pugnas y las diferencias de opinión. la política organizacional involucra las actividades de establecer, desarrollar y dar uso al

poder y otros recursos asociados para influir en las demás partes implicadas y obtener el resultado deseado cuando existe probabilidad de incertidumbre o desacuerdo acerca de las elecciones (p. 510).

Podría decirse que una política organizacional es un lineamiento o directiva que debe entenderse y acatarse por todos los miembros de la organización posterior a su proceso de divulgación, esta debe estar compuesta por aquellas normas, alcance y responsabilidades de cada área de la organización, al igual que debe establecer las guías para orientar las acciones pertinentes de dicha política, también puede decirse que las políticas organizacionales son lineamientos de ámbito general y de la cual se pueden derivar procesos y procedimientos para la toma de decisiones, sobre otros procedimientos o algún problema concurrente dentro de la organización. Dado lo anterior, las políticas organizacionales son criterios de cumplimiento que complementan el logro de los objetivos estratégicos de las compañías y facilitan la implementación de las estrategias para el cumplimiento de estos.

Existen dos tipos de políticas organizacionales, las generales y las específicas, las generales son aquellas que impactan de forma transversal a todos los niveles organizacionales, son de alto impacto o criticidad, entre las que se pueden clasificar como generales están, políticas de presupuesto, políticas de compensación, política de calidad, política de seguridad integral. Las políticas organizacionales específicas son aquellas que impactan procesos puntuales o específicos y están acotadas por su alcance, pueden ser ejemplo de estas, la política de ventas, política de compras, política de seguridad de la información y políticas de inventario.

Para generar una política organizacional ya sea general o específica se deben seguir los siguientes pasos:

1. Diseño y Desarrollo de la política
2. Revisión y aprobación

3. Divulgación a la organización
4. Mantenimiento y mejora continua

#### ***4.2.4.2 Política de Firma Electrónica.***

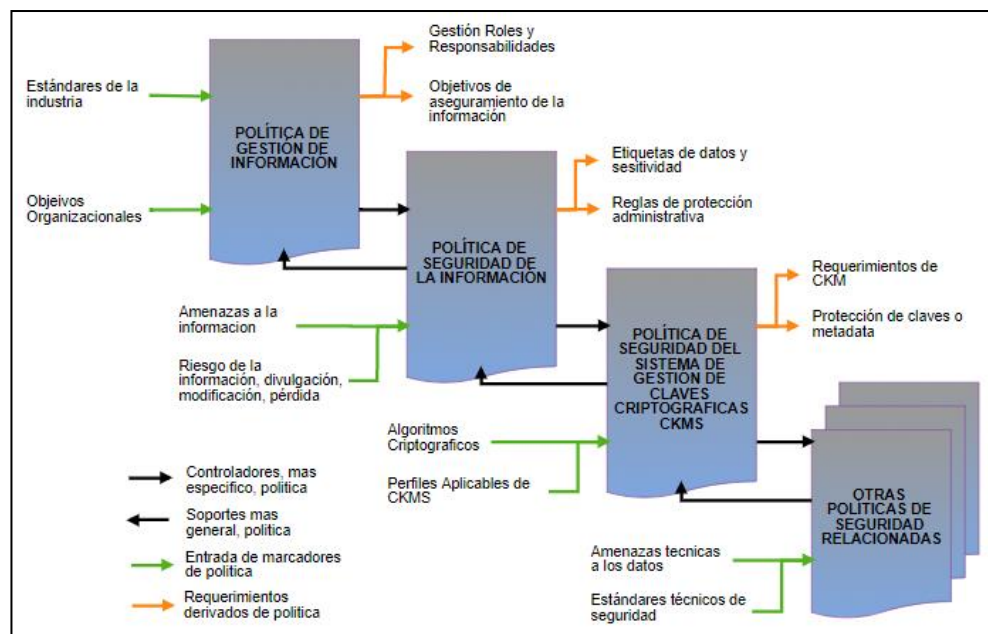
Una organización puede tener diferentes políticas que cubren diferentes aplicaciones o categorías de información.

Una organización a menudo crea y depende de políticas en capas, con políticas de alto nivel que abordan problemas en el nivel de administración de información y políticas de nivel inferior que abordan reglas específicas para la protección de datos. Una política de seguridad física se puede especificar en un documento y se puede especificar una política de seguridad de comunicación en otro documento. Los sistemas informáticos a menudo se construyen de acuerdo con su propia política de seguridad informática.

Las capas de políticas (por ejemplo, administración de información, seguridad de información, seguridad física, seguridad informática, seguridad de comunicaciones y seguridad de claves criptográficas) se interrelacionan de muchas maneras. Las capas intermedias e inferiores de una jerarquía de políticas deben proporcionar más detalles sobre la implementación y la aplicación que la capa superior. Por ejemplo, una política de gestión de la información de la organización que especifique que la información debe estar protegida contra la divulgación no autorizada debe dar lugar a una política de seguridad de la información que especifique la restricción del acceso y el uso de la información sólo a personas adecuadamente identificadas y autorizadas.

La figura 11 proporciona un ejemplo de las políticas que se pueden usar y sus relaciones (Barker, Smid, Branstad & Chokhani, 2013).

Un marco de gobierno como política de firma electrónica hace parte del conglomerado de normas de seguridad, de organización, técnicas y legales que por su composición debe establecer cómo se generan, verifican y gestionan firmas electrónicas, junto con las características exigibles a los certificados de firma.



*Figura 11. Relación de Políticas de Seguridad.*

Referenciada de: NIST SP 800-130, p.18.

El hecho de instaurar políticas de firma electrónica genera la confianza de las partes involucradas en la seguridad del uso de las firmas electrónicas, al sentar unas bases sólidas reconocidas para el intercambio y operación sobre las firmas. Contar con política de firma electrónica por una parte determina los datos que debe incluir el firmante y por otra parte define los datos que debe validar el verificador para comprobar su veracidad. (Universidad Europea de Madrid, 2012).



En una mirada global, una política de firma electrónica es un documento que contiene una serie de lineamientos referentes a la firma electrónica, dispuestas entorno a los conceptos de generación y validación de esta, en un contexto ya sea administrativo, contractual, jurídico, legal o técnico, determinando las normas y obligaciones de todas las partes interesadas en dicho proceso. La finalidad de este proceso es determinar la validez de la firma electrónica para una transacción en particular, definiendo los datos que deberá agregar el firmante en el proceso de generación de la firma, y los datos que deberá tener en cuenta el verificador en el proceso de validación de esta.

### **4.3 Marco legal**

En Colombia se cuenta con la Ley 527 en la que se establece y reglamenta el acceso y uso de los mensajes de datos, en el comercio electrónico y las firmas digitales, y se determinan las entidades de certificación, esta ley reconoce dos tipos de firma: la firma electrónica y la firma digital (Congreso de Colombia, 1999).

El decreto 2364 de 2012 de la presidencia de la república, define la firma electrónica como procedimientos de contraseñas, datos biométricos, códigos, o claves criptográficas privadas, que consiguen identificar a una persona o entidad, asociados con un mensaje de datos, con la condición de que este sea confiable y apropiado conforme los fines de uso de la firma.

Las particularidades de la firma digital hicieron que el congreso de la república de Colombia le otorgara la presunción de confiabilidad, la cual hace que no sea necesario el acuerdo previo entre las partes involucradas, pues se dan de manera predeterminada.

Para que una firma digital en Colombia sea válida, se necesita de la intervención de un tercero de confianza llamado entidad de certificación, quien valida la identidad de quien registra como dueño de la firma digital. Es de esta forma como interviene en este modelo un tercero, que,

aplicando procedimientos idóneos y específicos, valida de manera detallada y exhaustiva la identidad de las personas o entidades.

Resulta fundamental la intervención de una entidad prestadora de servicios de certificación y también se encuentra definida en el artículo 2 de la ley 527 como aquella entidad que, faculta conforme a esta ley, está autorizada para generar certificados en relación con las firmas digitales de las personas o entidades, ofrecer servicios de registro y estampado de tiempo y fecha de la transacción de mensajes de datos, así como cumplir otras funciones inherentes a las comunicaciones basadas en las firmas digitales (Congreso de Colombia, 1999). Dicho sea de paso, lo anterior permite avalar la identidad de los firmantes a través de tres atributos de seguridad de la información y teniendo en cuenta el proceso de generación de la firma electrónica:

- La autenticidad, es el atributo con el que se puede verificar quién es su autor, es decir, quién es la persona que se compromete jurídicamente hablando, en un mensaje de datos firmado digitalmente.
- La integridad, es el atributo mediante el cual el destinatario de dicho mensaje de datos podrá validar si la información ha sido o no alterada en la transacción del mensaje de datos, esto es útil para verificar la originalidad del mensaje de datos, puntualmente al amparo de los artículos 8 y 9 de la Ley 527.
- El no repudio, es el atributo que determina que la persona o entidad que firmo el mensaje de datos es quien dice ser, para evitar que el firmante se retracte o refute dicho hecho.

La ley colombiana le ha otorgado a la firma digital estos especiales atributos probatorios dado que, en medio del proceso de emisión de la firma digital, interviene un tercero que garantiza

la identidad del titular de la firma o firmante ya sea una persona o entidad.

Podría decirse entonces que la ley Colombiana reconoce tanto la firma digital como la firma electrónica y que, si bien estas pueden generar los mismos efectos legales como mecanismos de autenticación, también pueden existir grandes diferencias en la carga probatoria de los atributos de seguridad jurídica antes mencionados, en especial por la intervención de la entidad de certificación.

A continuación, se describen otras normas que regulan la ley 527 de la firma digital en Colombia.

Decreto 1747 del 2000: “Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados digitales y las firmas digitales” (Presidencia de la república de Colombia, 2000, p.1).

Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones: a) Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación; b) Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley. (Congreso de Colombia, 1999, p.11).

Parágrafo 1 del artículo 1 de la Ley 588 de 2000: “Las notarías y consulados podrán ser autorizados por la Superintendencia de Industria y Comercio como entidades de certificación, de conformidad con la Ley 527 de 1999” (Congreso de Colombia, 2000, p.1).

Resolución 26930 de 2000 de la Superintendencia de Industria y Comercio: “Por la cual

se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores” (Superintendente de Industria y Comercio, 2000, p.1).

Ley 1341 de 2009 “por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC), se crea la Agencia Nacional de Espectro y se dictan otras disposiciones” (Congreso de Colombia, 2009, p.1).

#### **4.4 Estado del arte**

La dinámica del avance de la tecnología de los últimos años en el campo de las comunicaciones, electrónico y digital ha transformado el comercio, la industria, en el sector de servicios domésticos y móviles prestados por entidades públicas y privadas, lo que ha propiciado una tendencia mayor y un incremento en la necesidad de interactuar a través de transacciones electrónicas por medio de la red, para ello se debió cimentar esta transformación en conceptos de firma digital e infraestructuras que la soportasen de forma segura.

Dado lo anterior, nace el concepto de firma digital de una oferta en tecnología para acercar lo que se denomina el trabajo cibernético a la firma manuscrita que garantiza los trámites hechos en la red.

En 1976 el concepto de clave pública fue concebido por Diffie y Helman cuando se define que la firma digital es un conglomerado de información asociados a un mensaje que permite asegurar la integridad del mensaje y la identidad del firmante. En 1977 R. Rivest, A Shamir y L. Adleman del Instituto Tecnológico de Massachusetts proponen el que hasta hoy es el método más utilizado de clave pública denominado RSA, este método en esencia obedece a los mismos principios de la firma autográfica (Zayas & Milagro, 2013). En 1985 es publicada la tesis “*A public key cryptosystem and a signature scheme based on discrete logarithms*” con la que se

sentó la base del algoritmo de firma digital adoptado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, como el estándar de firmas digitales (DSS) establecido en 1991. En mayo 1995 estableció la primera ley de regulación de firma digital a nivel mundial y fue la denominada “*Utah Digital Signature Act*” en el estado de Utah de los Estados Unidos de América, el objetivo era propiciar transacciones a través de mensajes electrónicos y firmas digitales.

Nace entonces el concepto de criptografía de clave pública la cual desempeña un papel importante en la prestación de servicios de seguridad de la información, abarcando los atributos fundamentales de confidencialidad, autenticidad, integridad y las firmas digitales, especialmente a través del uso de infraestructura de clave pública (PKI), la cual tiene sus propias características técnicas descritas en los capítulos anteriores, sin embargo, requiere de elementos adicionales que permiten una gestión y operación adecuada como:

- Políticas de seguridad para establecer las reglas con las cuales deben funcionar los sistemas de criptografía.
- Herramientas para generar, almacenar y administrar certificados y sus claves asociadas.
- Procedimientos para dictar cómo se generan y distribuyen las claves y certificados digitales.

Continuando con el estado del arte en el ámbito técnico y en cuanto a la evolución de la infraestructura de clave pública (PKI), el estándar X.509v3 proporciona una base útil para definir formatos de datos y procedimientos para la distribución de claves públicas a través de certificados firmados digitalmente por las CA. Sin embargo, X.509v3 no incluye un perfil para

especificar los requisitos de soporte para muchos de los subcampos, extensiones o valores de datos del certificado digital.

Dentro del ámbito administrativo en el contexto nacional, algunas Compañías y entidades que han implementado sistemas de firma electrónica o digital son: Superintendencias (sociedades, Financiera y Salud), Banco de la Republica, Fondo Nacional del Ahorro, Ministerio de Hacienda, Ministerio de comercio, industria y turismo (Cercicámara, s.f).

El departamento de impuestos y aduanas nacionales DIAN, implementó en febrero de 2016 una política de que regula la firma electrónica para los documentos digitales de la facturación electrónica en Colombia. Esta política establece los principales criterios técnicos para el sistema de la firma electrónica, que proporcionan la seguridad, autenticidad y confiabilidad de todos los procesos que apoyan la implementación de la factura electrónica en Colombia, y los elementos comunes para el mutuo reconocimiento de firmas electrónicas. En esta política de la DIAN también se menciona la firma digital de facturas electrónicas como firma electrónica avanzada (Dirección de impuestos y aduanas nacionales, 2016).

En el ámbito mundial se puede encontrar bases de políticas de firmas electrónicas emitidas bajo conceptos similares, tales como la política de firma electrónica del Departamento de Impuestos y Aduanas Nacionales DIAN, la política de firma electrónica y certificados de la administración general de estado en España y la política de firma electrónica de la Universidad Europea de Madrid.

En cuanto a software especializado a nivel mundial, según el cuadrante mágico de Gartner, Los mejores productos de software de firma electrónica están posicionados según la satisfacción del cliente y la presencia en el mercado y se clasifican en cuatro categorías:

Los productos posicionados en el cuadrante líder tienen puntajes sustanciales en la presencia del mercado y tienen una alta calificación por parte de los usuarios. Los líderes

incluyen: Adobe Sign, DocuSign, RightSignature, OneSpan Sign, HelloSign, SignNow, PandaDoc y SignEasy

Los usuarios de aplicaciones del sector de High Performance según la figura otorgan buenas calificaciones a estas aplicaciones, pero aún no han alcanzado la presencia en el mercado de los líderes. Entre estas se incluyen: Sertifi, DocVerify, Legalesign, eSign Genie, GetAccept, Signable, SignRequest, eversign y InsureSign

Los denominados *contenders* tienen una posición importante en el mercado y recursos, pero no han recibido una calificación lo suficientemente satisfactoria por parte del usuario que los sitúa por debajo del promedio o aún no reciben un número significativo de revisiones para validar la solución. Los contendientes incluyen: Nitro Productivity Suite, LiveCycle Digital Signatures ES4, dotloop y PDFfiller

Las soluciones de nicho no tienen la presencia de los líderes en el mercado. Es posible que hayan sido calificados positivamente por Satisfacción del cliente, pero aún no han recibido suficientes críticas para validarlos. Los productos de nicho incluyen: AssureSign, SigningHub, Secured, Smartwaiver, Scribe, Signority, Oneflow, Docsmore y KeepSolid Sign (Gartner peer insights, 2018).

En la figura 12 se muestra gráficamente la posición de cada una de estas aplicaciones de firma electrónica en el cuadrante mágico de Gartner

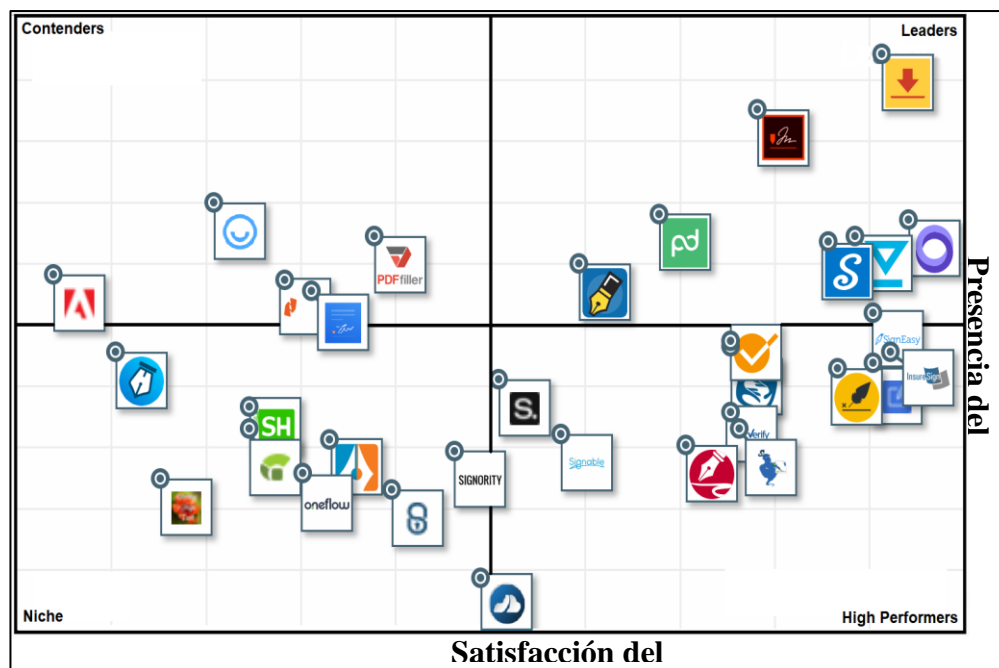


Figura 12. Cuadrante Mágico de Gartner para Mercado de Firma Electrónica.

Referenciado de <https://www.gartner.com/reviews/market/electronic-signature>



## 5 Metodología

La metodología por implementar en la generación de una política de firma digital para TigoUne es de tipo cuantitativa e involucra las siguientes fases:

1. Vigilancia Tecnológica: Recolección de información del estado del arte, donde se referencien leyes, normas y estándares que reglamenten el uso de las firmas electrónicas, las posibles políticas organizacionales generadas de uso de dichas firmas, búsqueda de las mejores prácticas de implementación de sistemas de gestión de seguridad de la información y la implementación de sistemas de firma electrónica al interior de entidades o compañías a nivel nacional.

También se referencian las tendencias mundiales en cuanto a procedimientos implementados y aplicaciones que los soportan en la adecuada implementación de un sistema de firma electrónica ajustado a las necesidades de compañías similares en tipo, enfoque a TigoUne.

2. Arquitectura de la solución: Se estudian en esta fase, los modelos de arquitectura que aplicarían para la implementación de un sistema de firma electrónica que cumpla con las necesidades del negocio de TigoUne y que sean aplicables a los procesos internos ya descritos en este documento y que garanticen las principales características de seguridad de la información
3. Definición de procedimientos: En esta fase se define el alcance de la política, donde se establecen las consideraciones generales del documento, se identifican las referencias normativas nacionales, estándares internacionales y los actores involucrados, los formatos admitidos, el método de generación y verificación de la firma a través de entidades certificadoras privadas y públicas, también se define en esta fase el tipo de estampado de

la fecha que debe tener la firma electrónica que a su vez haría parte de un sistema de firma electrónica o PKI.

4. Generación del marco de gobierno de firma electrónica: En esta fase se establece la identificación del documento para su posterior validación, también se define el periodo de validez, gestor o ente generador del documento, cuadro de control de cambios del documento. En esta fase también se define los usos, las reglas comunes que le apliquen, los formatos admitidos tanto para la generación de la firma como los algoritmos permitidos, su validación, estampado de tiempo a través de certificado y confianza.

## **6 Presentación y Análisis de Resultados**

Como resultado de la ejecución de las fases de metodología aplicada a este trabajo, en donde la primera fase da como resultado concreto la definición del marco conceptual, legal y estado del arte, la segunda fase da como resultado el estudio de la arquitectura actual de TigoUne descrita en el apartado 6.4.1 de este documento, la utilizada por Certicámara S.A con la aplicación TrustedX del fabricante *Safelayer Secure Communications S.A*, la cual se puede ver en el anexo “H”, tomada del documento original del fabricante y la arquitectura de la aplicación de código abierto @firma del gobierno de España, la cual se puede ver en el anexo “I”, tomada también de los documentos oficiales del servicio de identificación de España. Para la tercera y cuarta fase se definen los criterios que debe cumplir el documento de la política para implementar un adecuado sistema de firma electrónica que cumpla con las necesidades de la compañía de telecomunicaciones TigoUne.

### **6.1 Marco de Gobierno**

El documento resultado de este trabajo define la política interna de implementación de un sistema de firma electrónica para TigoUne junto con las reglas para la creación y validación de firmas, con las cuales podrán determinarse la validez de estas bajo un contexto legal, contractual o administrativo.

#### **6.1.1 Alcance de la política de implementación del sistema.**

La definición del presente marco de gobierno describe los criterios generales para la implementación de un sistema de firma electrónica y las condiciones administrativas y técnicas para la generación y validación de las firmas electrónicas. Este marco será aplicado de manera implícita para implementar sistemas de firma electrónica de documentos digitales y digitalizados

en el contexto de procesos internos legales, contractuales técnicos y administrativos en la compañía de telecomunicaciones TigoUne cumpliendo las políticas internas de seguridad de la información.

### **6.1.2 Actores involucrados en el marco.**

Las partes involucradas en el presente marco se describen a continuación:

- Firmante: persona o colaborador de la compañía que tiene a su disposición un dispositivo o sistema de creación de firma electrónica y que actúa en nombre propio.
- Operador de Servicios de firma electrónica: Área de la compañía encargada de administrar, operar y mantener los sistemas de firma electrónica, ya sean locales, como servicio o de código abierto.
- Prestador de servicios de firma electrónica: es la persona natural o jurídica que presta servicios de sistemas de firma electrónica en los tres modelos, locales, como servicio y de código abierto.
- Prestador de servicios de certificación: es la entidad comercial, pública o privada que emite certificados electrónicos, valida o verifica una firma electrónica teniendo en cuenta las condiciones descritas en este marco de firma electrónica.
- Emisor de la política de firma: Compañía o área de la compañía que se encarga de generar y gestionar el documento de política de implementación de un sistema de firma electrónica, por el cual se debe regir el Operador de servicios de firma electrónica, el firmante y el ente verificador en los procesos de generación y validación de la firma electrónica.

### **6.1.3 Gestión de la política de firma.**

El documento de la política de implementación del sistema de firma electrónica de TigoUne, que se obtiene como resultado de este trabajo, se elaboró sobre los formatos establecidos al interior de la compañía, formalizado y comunicado a todos los integrantes de la compañía TigoUne y sus filiales, incluyendo proveedores y contratistas, de igual forma, deberá permanecer publicado y actualizado en la intranet de la compañía, en formato digital PDF previamente firmado y aprobado por la Vicepresidencia de Operaciones y la Gerencia de Seguridad de la información.

Los cambios que apliquen a la política de firma electrónica serán acordados entre las partes interesadas, así como el periodo de tiempo necesario para la adecuación de las herramientas ofimáticas y sistemas de información.

Cundo se requiera actualizar la política, se deberá indicar en el control de cambios del mismo documento y en forma secuencial, la fecha del cambio, el aprobador del cambio, el validador del cambio y sus correspondientes firmas.

La Gerencia de seguridad de la información es la responsable de la generación y actualización de esta política de seguridad, la Vicepresidencia de Operaciones será informada de la publicación y los cambios, por su parte las demás áreas de la compañía serán las responsables de revisar los cambios y hacerla cumplir.

### **6.1.4 Identificación del documento.**

Según el proceso de gestión documental, el formato definido para oficializar políticas, procedimientos y lineamientos de TigoUne, debió incluir de forma clara los datos de identificación del documento de la siguiente forma:

- Título del documento.

- Área de la compañía quien genera el documento (Gerencia, Direccion y Vicepresidencia).
- Versión del documento.
- Fecha de generación del documento.
- Código consecutivo (opcional).
- Declaración de confidencialidad.
- Declaración de Cumplimiento.

En la figura 13 se muestra la identificación del documento de la política.

Según la política de gestión documental de TigoUne el documento de la política de implementación de sistemas de firma electrónica en TigoUne, debió contener un cuadro de aceptaciones donde se relacionaron los datos de las personas que elaboraron el documento, las que lo revisaron y por ultimo las que lo aprueban, en la figura 14 se muestra dicho cuadro.

Adicional a los datos anteriores el documento debió contar con un cuadro de control de cambios y versiones llamado *Historial de Versiones*, donde se especificaron:

- Versión del documento, en números consecutivos
- Fecha del cambio
- Descripción del cambio

En la figura 15 se muestra el historial de versiones del documento de la política



Figura 13. Caratula de la Política.

<b>5. Aceptaciones</b>				
Los siguientes actores participaron en la estructuración del presente documento:				
Elaborado por		Entidad	Fecha	
Jaime Julian Rodríguez Zarate		TigoUne	12/10/2018	
Revisado por		Cargo	Fecha	
Natacha Rodríguez		Supervisor de seguridad de la Información	12/10/2018	
Jaime Julián Rodríguez Zárate		Supervisor Ofimática	12/10/2018	
Felipe Ruiz Rivillas		Director de Seguridad de la Información y Continuidad de Negocio	12/10/2018	
Aprobado por		Cargo	Firma	Fecha
Teresa Reyes		VP Operaciones		
Felipe Ruiz Rivillas		Director de Seguridad de la Información y Continuidad de Negocio		

Figura 14. Cuadro de Aceptaciones.

<b>6. Historial de versiones</b>		
Versión	Fecha del Cambio	Descripción
1	12/10/2018	Creación de la política

Figura 15. Historial de Versiones

### 6.1.5 Período de validez.

La vigencia del documento de la política para la implementación de sistemas de firma electrónica en TigoUne comenzara a partir de la divulgación de la misma previa al proceso de



aprobación por parte de la alta dirección, hasta la publicación de la siguiente modificación o actualización, la nueva versión de la política definirá e identificara las partes en que la nueva política sustituye la anterior.

Esta política deberá ser revisada como mínimo cada año para actualizarla según la política general de seguridad de la información y la gestión documental, así como para incluir actualizaciones en formatos, estándares y normatividad que se encuentren vigentes a la fecha de revisión.

#### **6.1.6 Identificación del gestor del documento.**

Se define a la Dirección de Seguridad de la Información y Continuidad de Negocio de la Vicepresidencia de Operaciones de TigoUne, como responsable de la política y su gestión. Internamente a nivel de la dirección se especificarán a las personas responsables a través de una matriz RACI previa a la divulgación de esta.

### **6.2 Lineamientos para implementación de un sistema de firma electrónica**

Como resultado del análisis conceptual, legal y técnico de lo que comprende la firma electrónica, se definieron los siguientes lineamientos para el marco de gobierno objeto de este trabajo de grado.

#### **6.2.1 Criterios de selección del modelo de sistema a implementar.**

Se deben tener en cuenta diez puntos fundamentales para seleccionar un adecuado sistema de firma electrónica para TigoUne. Estos hacen parte de factores decisivos para la implementación, administración y uso con un nivel de riesgo bajo, lo que repercute en todos los aspectos de los procesos internos de TigoUne, para garantizar una costo-eficiencia y un rápido retorno de la inversión a continuación se enumeran dichos criterios.

1. **Sellado de Documentos:** Asegurarse de que el sistema a implementar garantice que el documento se pueda sellar contra los cambios, ya sea accidentales o como resultado de una acción premeditada de alteración del documento. Solo las firmas digitales basadas en la tecnología de infraestructura de clave pública (PKI) pueden sellar realmente un documento. Cualquier otro tipo de solución se puede falsificar fácilmente.
2. **Cumplimiento:** Se deben revisar las regulaciones nacionales para la industria y asegurarse de que la solución cubra todos esos requisitos, cada regulación o ley tiene sus propios requisitos específicos relacionados con los documentos electrónicos.
3. **Compatibilidad con múltiples aplicaciones:** asegurar que las aplicaciones con las que se generan documentos que se necesiten firmar sean compatibles con la solución que se seleccione.
4. **Transportabilidad:** asegurar que los documentos puedan ser validados por otros usuarios tanto internos como externos según la necesidad del proceso, ya sea con CA reconocida privada o pública, sin tener que recurrir a otras aplicaciones de terceros.
5. **Firmas Gráficas:** Se requiere tener la capacidad de poder utilizar diferentes firmas gráficas (por ejemplo, iniciales, firma manuscrita completa). Las firmas gráficas aseguran que la firma se note visualmente y tenga un impacto psicológico.
6. **Registro de usuarios:** asegurar que el sistema seleccionado sea capaz de actualizar de manera automática y sin problemas los perfiles de usuario del directorio activo. En el momento en que se implemente el sistema o solución, los usuarios podrán comenzar a firmar documentos electrónicamente sin tener que acudir a un asistente o generar un requerimiento a la mesa de servicios de TI.
7. **Múltiples firmas:** asegurar que el sistema ofrezca características que permitan que varias personas puedan firmar un documento, algunas soluciones de firma electrónica no

permiten alterar el documento una vez que se aplica la firma, esto es bueno en términos de sellar el documento, pero restrictivo en la funcionalidad.

8. Fácil de usar: elegir un sistema que sea fácil de usar, debe ser intuitivo al usar la menor cantidad de clics posible para firmar y sellar un documento y minimizar la participación de la mesa de servicios de TI.
9. Sin gestión de TI: asegurar que el sistema seleccionado esté operativo desde el momento en que se implementa en ambiente de producción en la red corporativa o dominio y que cumple el requisito de "cero administración" conservando una alta disponibilidad, la intervención de las áreas de TI para mantenimiento y operación del sistema per se, debe ser mínima.
10. Costo total: proyectar el costo total de propiedad (TCO) como mínimo a tres años y tener en cuenta el costo inicial del producto, implementación, certificados digitales (que pueden ser un costo anual recurrente) y soporte para la aplicación con la que se va a firmar. Este punto es importante ya que no siempre se considera todo el TCO al comprar una solución de firma electrónica.

### **6.2.2 Formatos admitidos de firma.**

Para el alcance de este marco de gobierno, se establece la utilización de firmas electrónicas avanzadas dada la definición en el numeral 4.2.3.7 de este documento y en los siguientes formatos:

XAdES según la especificación técnica ETSI TS 101 903, en sus versiones 1.2.2, 1.3.2 y 1.4.1 como fundamento base para la generación de la firma electrónica y en cualquiera de sus variantes especificadas en el numeral 4.2.3.7 de este documento.

CADES firma electrónica avanzada CMS que define perfiles específicos de datos firmados con CMS para su uso con firma electrónica avanzada enmarcadas en la especificación técnica ETSI TS 101 733, en sus versiones 1.6.3, 1.7 y 1.8.1. así como la Directiva Europea 1999/93/CE.

PADES, Firma electrónica avanzada en formato PDF involucra extensiones a PDF y al estándar ISO 32000-1, que especifica perfiles precisos para la firma electrónica avanzada bajo la Directiva Europea 1999/93/CE, y la norma ETSI TS 102 778-3, las variantes de este formato se describen en el numeral 4.2.3.7

En la tabla 1 se muestra el análisis de uso de los formatos de firma electrónica mas comunes.

Tabla 1

*Análisis del Uso de los Formatos de Firma Electrónica*

<u>XAdES</u>	<u>CADES</u>	<u>PADES</u>
- Provee una completa solución XML.	- Permite la firma de cualquier dato, incluido el PDF.	- Contiene firmas dentro del PDF
- Firma cualquier dato incluidos PDF y binario	- representa la firma como datos binarios.	- Soporta datos XML
- Soporta empaquetado XML o archivos separados	- A menudo requiere personalización de aplicaciones o firma genérica fuera de la aplicación	- Incluido dentro del estándar ISO PDF.
- A menudo requiere personalización de aplicaciones o firma genérica fuera de la aplicación	- Soporta aplicación de múltiples firmas en paralelo o serial	- Incluye la firma y verificación en el software PDF, no se requiere programación personalizada.
- Soporta aplicación de múltiples firmas en paralelo o serial	- La apariencia de la firma depende de la aplicación que la proporcione	- Admite el llenado de formularios en serie y firmas para flujos de trabajo de aprobación.
- Dependiendo de la aplicación, soporta la inclusión de una imagen de firma, o firma visual	- Proporciona validez a largo plazo	- Soporta la inclusión de una imagen de firma, o firma visual
- Proporciona validez a largo plazo		- Proporciona validez a largo plazo

En la tabla 2 se muestran las variantes de los formatos admitidos de firma electrónica para el presente trabajo.

Tabla 2  
*Formatos admitidos de firma electrónica*

Formatos de firma		
Notación		
<u>ASN.1</u>	<u>XML</u>	<u>PDF</u>
PKCS#7 v.1.5	XAdES	PDF
CMS	XAdES-T	PAdES-Basic
CMS-T	XAdES-C	PAdES-BES
CAdES	XAdES-X	PAdES-EPES
CAdES-A	XAdES-XL	PAdES-LTV
CAdES-T	XAdES-A	PAdES B-Level
CAdES-C	XAdES B-Level	PAdES T-Level
CAdES-X	XAdES T-Level	PAdES LT-Level
CAdES-XL	XAdES LT-Level	PAdES LTA-Level
CAdES B-Level	XAdES LTA-Level	
CAdES T-Level		
CAdES LT-Level		
CAdES LTA-Level		

Como requisito mínimo los sistemas de información y herramientas ofimáticas utilizadas tanto para firmar como para verificar las firmas, deben emplear la variante BES o EPES de cada uno de estos formatos admitidos.

De ser necesario generar firmas que permitan validación a largo plazo, se deberá implementar una derivación de los anteriores formatos que incorpore propiedades adicionales con la extensión X o XL como se especifica en el apartado 4.2.3.7 y que incorporen información sobre revocación de certificados.

### **6.2.3 Creación de la firma electrónica.**

Para la generación de la firma electrónica, los sistemas encargados de generar las firmas deberán cumplir:

1. El usuario podrá utilizar un certificado emitido tanto por una CA interna o privada para firmar documentos de procesos internos, como también por una CA pública o reconocida para los casos de firmas de documentos contractuales o que impliquen representación legal de TigoUne.
2. En caso de que los certificados empleados para firmar por parte del usuario deban ser generados por la CA interna deberán estar respaldada por la CA raíz y comprobados en la cadena de certificación
3. Los certificados emitidos por las CA para las firmas electrónicas deben estar en formato X.509v3 o superior, con la sintaxis básica de estructura que se muestra en el anexo A.
4. El formato de almacenamiento de certificados debe cumplir como mínimo con el estándar PKCS#12, este requerimiento está orientado al almacenamiento de los certificados en la CA, en el DA o en la máquina del usuario.
5. El algoritmo de la firma del certificado debe ser SHA2 o SHA-256 para minimizar el riesgo de ataques de fuerza bruta
6. El tamaño mínimo para las llaves pública y privada asociadas a los certificados digitales es de 2048 bits.
7. El usuario debe contar con la posibilidad de agregar la firma manuscrita digitalizada y con la posibilidad de agregarla o integrarla a la estructura de la firma electrónica.
8. La firma electrónica deberá contener características como estampado de tiempo, motivo de la firma, ubicación e información de contacto y el estado de revocación
9. El usuario deberá contar con la posibilidad de comprobar la información que va a firmar ya sea con una vista previa del documento o con alguna alternativa que pueda tener el usuario para comprobar el contenido del documento a firmar.

10. Previo a realizar la firma el sistema seleccionado para la firma electrónica comprobará el estado del certificado y la cadena de certificación.

Dado el caso en el que no sea posible ejecutar alguno de los pasos anteriores o su resultado no sea efectivo, no se debe permitir continuar con el proceso de generación de la firma.

Como producto final del proceso de generación de firma, se debe obtener un archivo con una firma electrónica con alguno de los formatos indicados en la tabla 2.

Las pruebas de estos requisitos podrán observarse en el apartado 6.6 de este capítulo.

La mayoría de los métodos para crear una firma electrónica involucran una cantidad de tecnologías, credenciales u objetos digitales, y procesos. Es preciso establecer que para el presente caso se debe sobreponer los enfoques de seguridad a las tecnologías existentes, estos enfoques proporcionan distintos niveles de seguridad, autenticación, integridad de registros y protección contra repudio.

Para la creación de una firma electrónica el sistema a utilizar para la generación debe utilizar firmas digitales basadas en criptografía asimétrica sobre una infraestructura de clave pública PKI que proporcione un alto nivel de seguridad en dicha firma, según lo descrito en los apartados 4.2.3.2 y 4.2.3.3. del marco teórico del presente documento.

Además, el uso de firmas electrónicas estará permitido en TigoUne y tendrá la misma validez y efecto que el uso de una firma manuscrita y debe cumplir con los siguientes requisitos en el establecimiento de la política o marco de gobierno.

1. La firma electrónica es exclusiva de la persona que la usa.
2. La firma electrónica tendrá la capacidad de ser verificada.
3. La firma electrónica deberá estar bajo el control exclusivo de la persona que la usa.

4. La firma electrónica debe estar vinculada a los datos del documento de tal manera que, si los datos se modifican después de la firma electrónica, la firma electrónica queda invalidada.
5. La firma electrónica debe estar vinculada a los datos de la cuenta de red del usuario en el dominio de TigoUne, bajo el cumplimiento de las políticas de seguridad descritas en el apartado 2.2 de este documento.

#### **6.2.4 Verificación de la firma electrónica.**

La verificación de la firma electrónica debe ser un proceso mediante el cual se valida la identidad del firmante, la validez del certificado, la integridad del documento firmado, y el estado de revocación o la caducidad del certificado digital. Para la comprobación de la validez de la firma electrónica se debe centrar en el certificado digital.

El certificado digital debe estar activo, si el certificado no es válido o ya está vencido, la firma no puede ser validada.

De ser necesario, la entidad certificadora privada de TigoUne deberá agregarse a la lista de confianza que contenga el sistema a implementar para las firmas electrónicas si se llegase a requerir.

Se deben verificar a su vez los sellos de tiempo de las firmas electrónicas, incluyendo los periodos de validez de los sellos de tiempo, esta verificación se realizará solo si son implementados los sellos de tiempo en las firmas electrónicas a través de una TSA incorporada a la PKI de TigoUne.

Para la verificación de las firmas a través de aplicaciones o sistemas de firma electrónica, este debe verificar el cumplimiento de los estándares descritos en la generación de la firma, entre ellos debe verificarse:



1. Estándares para la representación del certificado: X509v3.
2. Estándares para formatos de firma: XAdES, CAdES y PAdES o las derivaciones de estas especificadas en el anexo G.
3. Se reconocerán los siguientes niveles de conformidad: los especificados en el apartado 4.2.3.7 de este documento.
4. Estándares para los contenedores de firmas asociados: Perfil base de ASIC (ETSI TS 103174 v.2.2.1).
5. Estándares para la validación de certificados OCSP y CRL.

Los sistemas o herramientas para la firma electrónica deben mostrar en pantalla el resultado de la validación de las firmas electrónicas y el contenido del documento para que sea de fácil verificación por parte del usuario.

Para el alcance de este trabajo, se utilizaron certificados que fueron emitidos por la CA privada o local de TigoUne, solo se podrá validar la firma dentro del dominio de la compañía para documentos firmados en el cumplimiento de procesos internos de la compañía, de igual forma se usó un certificado emitido por una entidad pública reconocida como Certicámara para simular la firma de un documento que por sus características legales y jurídicas debería ser firmado con la representación de la compañía.

### **6.3 Lineamientos de firma electrónica**

Los siguientes lineamientos se deben aplicar según la norma relacionadas en el anexo G y estándares conexos, los cuales establecen determinados parámetros de la estructura base, que deben contener información relevante de la firma electrónica.

### **6.3.1 Reglas comunes y de Compromiso.**

Las reglas comunes al igual que las reglas de compromiso consisten en las reglas de validación que se aplican a tipos de compromiso dados en la firma electrónica y son atributos de la sintaxis de la firma electrónica que deben cumplirse dependiendo del formato utilizado, estas reglas comunes y reglas de compromiso definen los atributos que son comunes a todos los involucrados en la firma electrónica. Estas reglas se definen en términos de condiciones de confianza para los certificados digitales, marcas de tiempo y atributos adicionales.

Las reglas comunes y de compromiso en la sintaxis de la firma electrónica están comprendidas por las reglas del operador de servicios de Firma electrónica, reglas del verificador, reglas del sellado de tiempo, reglas de uso de algoritmos y reglas de confianza descritas a continuación.

En la figura 16 se muestra un ejemplo de la estructura básica de las reglas comunes en la sintaxis de la firma electrónica con formato en notación ASN.1.

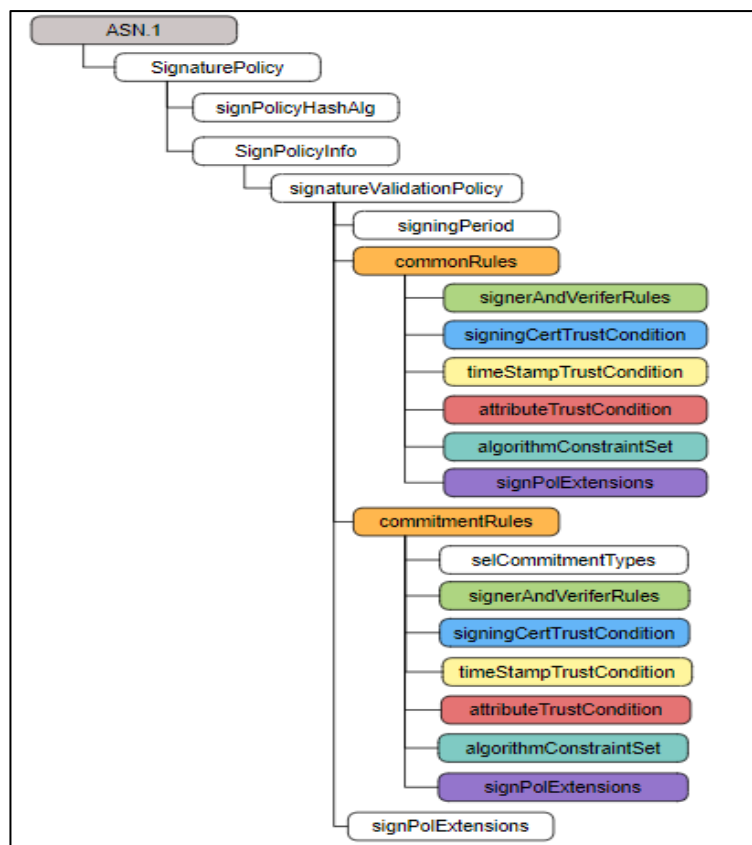


Figura 16. Reglas Comunes

### 6.3.1.1 Reglas del Firmante.

Para efectos de la implementación de un sistema de firma electrónica en TigoUne y de verificación de la sintaxis, las reglas del firmante son asumidas por el operador de servicios de firma electrónica, dando cumplimiento al numeral 8 del apartado 6.2.1 de este documento.

A excepción de las demás reglas descritas, las reglas del firmante en este caso no podrán ser verificables a través de la sintaxis, en este caso, el firmante debe asegurarse de conocer y acatar las políticas de seguridad de la información de TigoUne, así como aportar de forma activa a la conservación de la confidencialidad, integridad y disponibilidad de la información relevante para TigoUne, haciendo especial énfasis en las políticas de gestión de accesos que apoyan el componente de repudio en el ámbito legal.

### **6.3.1.2 Reglas del Operador de Servicios de Firma Electrónica.**

Estas reglas se basan en la aplicación del formato de firmas, utilizando el estándar descrito en el apartado 6.2.2 de este capítulo.

Para Formatos XAdES: El anexo B contiene la estructura detallada que debe tener una firma electrónica en este formato para que pueda ser validada por el sistema a implementar para firmas electrónicas.

El operador de servicios de firma electrónica debe asegurarse que el sistema de firma electrónica tenga la capacidad de emplear el formato XAdES de tal forma que la firma generada en formato XML pueda referenciar el documento firmado a través de una URI que hará las funciones de localizador del documento (*XAdES Detached*), o que pueda incorporar la firma y el documento en una sola estructura XML, en donde la firma debe ubicarse después del documento (*XAdES Enveloped*).

El operador de servicios de firma electrónica debe asegurarse que se cuente con la información necesaria para la estructura de la firma en las siguientes etiquetas del Objeto *SignedProperties* de la estructura XML de la firma, a continuación, se describen en la tabla 3 dichas etiquetas.

Tabla 3

## Reglas Obligatorias Para el Formato XAdES

## Sintaxis

<u>Objeto</u>	<u>Campo</u>	<u>Etiqueta</u>	<u>Descripción</u>	<u>Identificador de dato</u>
SignedProperties	SignedSignatureProperties	SigningTime	debe contener la fecha y la hora que deben ser las configuradas para el sistema de firma electrónica proveniente del TSA o del repositorio de certificados que puede ser el DA que a su vez deberá estar sincronizado con el reloj atómico de internet.	<xd:SigningTime>2018-10-05T19:20:47Z
		SigningCertificate	debe contener las referencias del certificado y los algoritmos usados de seguridad para cada certificado.	<xsd:element name="SigningCertificate" type="CertIDListType"/> Contiene la secuencia de identificadores y resúmenes de certificado
<u>Objeto</u>	<u>Campo</u>	<u>Etiqueta</u>	<u>Descripción</u>	<u>Identificador de dato</u>
SignedProperties	SignedDataObjectProperties	SignaturePolicyIdentifier	debe identificar la política de firma según se establece el proceso de la firma electrónica.	<xsd:element name="SignaturePolicyIdentifier" type="SignaturePolicyIdentifierType"/> Contiene la secuencia de identificadores y resúmenes de la política
		DataObjectFormat	debe definir el formato del archivo firmado, ya sea utilizando el XAdES Enveloped o el XAdES Detached.	<xsd:element name="DataObjectFormat" type="DataObjectFormatType"/> Contiene la secuencia de identificadores y resúmenes del tipo de formato del documento

Nota. Referenciado de ETSI TS 101 903, versión 1.2.2, versión 1.3.2 y versión 1.4.1, el identificador del dato es código estándar que puede ser común en cualquier firma de este formato.

las siguientes etiquetas descritas en la tabla 4 serán consideradas opcionales para el empleo de cada firma electrónica según las necesidades de cada área de TigoUne.

Tabla 4

## Reglas Opcionales Para el Formato XAdES

## Sintaxis

Objeto	Campo	Etiqueta	Descripción	Identificador de dato
SignedProperties	SignedSignatureProperties	SignatureProductionPlace	Debe describir la locación geográfica donde se realizó la firma del archivo.	<xsd:element name="SignatureProductionPlace" type="SignatureProductionPlaceType" minOccurs="0"/>
		SignerRole	Debe describir el rol de la persona que firma el archivo.	<xsd:element name="SignerRole" type="SignerRoleType" minOccurs="0"/> Contiene la secuencia de identificadores y resúmenes de certificado del firmante
SignedProperties	SignedDataObjectProperties	CommitmentTypeIndication	Debe describir la acción del firmante sobre el archivo firmado. Aprobación, recepción o certificación.	<xsd:element name="CommitmentTypeIndication" type="CommitmentTypeIndicationType"/> Contiene la secuencia de identificadores y resúmenes de la acción del firmante sobre el documento
		AllDataObjectsTimeStamp	Debe contener el dato de sello de tiempo, que debe estar antes del tiempo de la generación de la firma.	<xsd:element name="AllDataObjectsTimeStamp" type="XAdESTimeStampType" minOccurs="0" maxOccurs="unbounded"/>
		IndividualDataObjectsTimeStamp	Debe contener el dato de sello de tiempo, que debe estar antes del tiempo de la generación de la firma.	<xsd:element name="IndividualDataObjectsTimeStamp" type="XAdESTimeStampType" minOccurs="0" maxOccurs="unbounded"/>

Nota. Referenciado de ETSI TS 101 903, versión 1.2.2, versión 1.3.2 y versión 1.4.1, el identificador del dato es código estándar que puede ser común en cualquier firma de este formato.

Para el uso de este formato se debe incluir los certificados de atributos para certificar el rol del firmante, es decir si se opta por usar el elemento *SignerRole* debe incorporar el atributo *CertifiedRoles* que debe contener la codificación de los datos del certificado digital del firmante en base-64.

Para Formatos CADES: El anexo C contiene la estructura detallada que debe tener una firma electrónica en este formato para que pueda ser validada por el sistema a implementar para firmas electrónicas.

El operador de servicios de firma electrónica debe asegurarse que el sistema de firma electrónica tenga la capacidad de emplear el formato CADES de tal forma que la firma generada pueda ser de tipo *Signed Attached* con los datos del archivo embebidos en el cual el resultado es un archivo que contenga el documento original y la firma. Cuando el tamaño del archivo a firmar sea de un tamaño que convierta el archivo resultante, en uno que sea poco práctico en la gestión documental, se debe utilizar la firma de tipo *Signed Detached* el cual debe incluir el hash del documento original en la firma.

El operador de servicios de firma electrónica debe asegurarse que, al utilizar este formato, las etiquetas descritas a continuación en la tabla 5 sean obligatoriamente firmadas:

Tabla 5

### Reglas Obligatorias Para el Formato CADES

#### Sintaxis ASN.1 CMS ESS

<u>Tipo de Objeto</u>	<u>Etiqueta</u>	<u>Descripción</u>	<u>Identificador del dato</u>
Cryptographic Message Syntax	ContentType	Especifica el tipo de contenido que se va a firmar.	ContentInfo ::= SEQUENCE { contentType, content [0] EXPLICIT ANY DEFINED BY contentType }
The CMS Attributes	MessageDigest	Identifica el cifrado del contenido firmado OCTET STRING en encapContentInfo	MessageDigest ::= OCTET STRING
Enhanced Security Services (ESS)	SigningCertificate, SigningCertificate v2	Permite el uso de algoritmos de seguridad SHA1 para la primera etiqueta y SHA2 para la segunda.	SigningCertificate ::= SEQUENCE { certs SEQUENCE OF ESSCertID, policies SEQUENCE OF PolicyInformation OPTIONAL }
The CMS Attributes	SigningTime	Contiene la fecha y la hora que deben ser las configuradas para el sistema de firma electrónica proveniente del TSA o del repositorio de certificados que puede ser el DA que a su vez deberá estar sincronizado con el reloj atómico de internet.	SigningTime ::= Time  Time ::= CHOICE { utcTime, generalizedTime }

The ASN.1 Attributes	SignaturePolicyIdentifier	Debe Identificar la política sobre la que se establece el proceso de la firma electrónica.	SignaturePolicyIdentifier ::= CHOICE { signaturePolicyId, signaturePolicyImplied -- not used in this version }
Enhanced Security Services (ESS)	ContentHints	describir el formato del documento original firmado	ContentHints ::= SEQUENCE { contentDescription UTF8String (SIZE (1..MAX)) OPTIONAL, contentType ContentType}

Nota. Referenciada de RFC 3125, ETSI TS 101 733, en sus versiones 1.6.3, 1.7 y 1.8.1, el identificador del dato es código estándar que puede ser común en cualquier firma de este formato.

las siguientes etiquetas descritas en la tabla 6 serán consideradas opcionales para el empleo de cada firma electrónica según las necesidades de cada área de TigoUne.

Tabla 6

## Reglas Opcionales Para el Formato CADES

### Sintaxis ASN.1 CMS ESS

<u>Tipo de Objeto</u>	<u>Etiqueta</u>	<u>Descripción</u>	<u>Identificador del dato</u>
Enhanced Security Services (ESS)	ContentReference	es un enlace de un SignedData a otro. Puede usarse para vincular una respuesta al mensaje original al que se refiere, o para incorporar por referencia un SignedData en otro. El atributo de referencia de contenido será un atributo firmado.	ContentReference ::= SEQUENCE { contentType, signedContentIdentifier ContentIdentifier, originatorSignatureValue OCTET STRING }
Enhanced Security Services (ESS)	ContentIdentifier	proporciona un identificador para el contenido firmado, para usar cuando una referencia pueda ser requerida más tarde para ese contenido	ContentIdentifier ::= OCTET STRING
The ASN.1 Attributes	CommitmentTypeIndicator	Debe describir la acción del firmante sobre el archivo firmado. Aprobación, recepción o certificación.	CommitmentTypeIndicator ::= SEQUENCE { commitmentTypeId CommitmentTypeIdentifier, commitmentTypeQualifier SEQUENCE SIZE (1..MAX) OF CommitmentTypeQualifier OPTIONAL}
The ASN.1 Attributes	SignerLocation	Debe describir la locación geográfica donde se realizó la firma del archivo	SignerLocation ::= SEQUENCE { -- at least one of the following shall be present: countryName [0] DirectoryString OPTIONAL, -- As used to name a Country in X.500 localityName [1] DirectoryString OPTIONAL, -- As used to name a locality in X.500 postalAddress [2] PostalAddress OPTIONAL }
The ASN.1 Attributes	SignerAttributes	Debe describir el rol de la persona que firma el archivo.	SignerAttribute ::= SEQUENCE OF CHOICE { claimedAttributes [0] ClaimedAttributes, certifiedAttributes [1] CertifiedAttributes }
The ASN.1 Attributes	ContentTimeStamp	Debe contener el dato de sello de tiempo, que debe estar antes del tiempo de la generación de la firma.	ContentTimeStamp ::= TimeStampToken



---

Nota. Referenciada de RFC 3125, ETSI TS 101 733, en sus versiones 1.6.3, 1.7 y 1.8.1, el identificador del dato es código estándar que puede ser común en cualquier firma de este formato.

---

*Para Formatos PAdES:* la estructura que debe tener una firma electrónica en este formato para que pueda ser validada por el sistema a implementar para firmas electrónicas, deberá estar construida sobre la base del formato *CADES Signed Detached*.

Para este formato, solo se podrán utilizar algoritmos RSA y deberá contener obligatoriamente los atributos descritos en la tabla 7:

Tabla 7

### Reglas Obligatorias Para el Formato PAdES

#### Sintaxis ASN.1 CMS ESS

<u>Tipo de Objeto</u>	<u>Etiqueta</u>	<u>Descripción</u>	<u>Identificador del dato</u>
Cryptographic Message Syntax	ContentType	Especifica el tipo de contenido que se va a firmar.	ContentInfo ::= SEQUENCE { contentType, content [0] EXPLICIT ANY DEFINED BY contentType }
The CMS Attributes	MessageDigest	Identifica el cifrado del contenido firmado OCTET STRING en <i>encapContentInfo</i>	MessageDigest ::= OCTET STRING
Enhanced Security Services (ESS)	SigningCertificate, SigningCertificate v2	Permite el uso de algoritmos de seguridad SHA1 para la primera etiqueta y SHA2 para la segunda.	SigningCertificate ::= SEQUENCE { certs SEQUENCE OF ESSCertID, policies SEQUENCE OF PolicyInformation OPTIONAL }
The ASN.1 Attributes	SignaturePolicyIdentifier	Debe Identificar la política sobre la que se establece el proceso de la firma electrónica.	SignaturePolicyIdentifier ::= CHOICE { signaturePolicyId, signaturePolicyImplied -- not used in this version }

---

Nota. Referenciada de RFC 3125, ETSI TS 101 733, en sus versiones 1.6.3, 1.7 y 1.8.1, el identificador del dato es código estándar que puede ser común en cualquier firma de este formato.

---

Debido al uso interno que se denota en esta política las etiquetas

*CommitentTypeIndicator*, *SignerAttributes* y *ContentTimeStamp* descritas en la tabla 8 deberán

ser firmadas y serán consideradas opcionales para el empleo de cada firma electrónica según las necesidades de cada área de TigoUne.

Tabla 8

Reglas Opcionales Para el Formato PAdES  
 Sintaxis ASN.1 CMS ESS

<u>Tipo de Objeto</u>	<u>Etiqueta</u>	<u>Descripción</u>	<u>Identificador del dato</u>
The ASN.1 Attributes	CommitmentTypeIndicator	Debe describir la acción del firmante sobre el archivo firmado. Aprobación, recepción o certificación.	CommitmentTypeIndication ::= SEQUENCE { commitmentTypeIndicator CommitmentTypeIdentifier, commitmentTypeQualifier SEQUENCE SIZE (1..MAX) OF CommitmentTypeQualifier OPTIONAL }
The ASN.1 Attributes	SignerAttributes	Debe describir el rol de la persona que firma el archivo.	SignerAttribute ::= SEQUENCE OF CHOICE { claimedAttributes [0] ClaimedAttributes, certifiedAttributes [1] CertifiedAttributes }
The ASN.1 Attributes	ContentTimeStamp	Debe contener el dato de sello de tiempo, que debe estar antes del tiempo de la generación de la firma.	ContentTimestamp ::= TimeStampToken

Nota. Referenciada de RFC 3125, ETSI TS 101 733, en sus versiones 1.6.3, 1.7 y 1.8.1, el identificador del dato es código estándar que puede ser común en cualquier firma de este formato.

Para identificar el lugar en el documento se debe reemplazar el uso de la etiqueta *SignerLocation* especificada en el formato CADES por la entrada *Location*.

### 6.3.1.3 Reglas del verificador.

Para las firmas electrónicas avanzadas se define en este marco la validación de dicha firma a través del certificado digital del firmante, la estructura de bloques básica de la sintaxis para la verificación de las firmas electrónicas se muestra en la figura 17, incluye la etiqueta *SigninCertificate* de la estructura de la firma, y la información de la etiqueta de *SignaturePolicy*.

Independientemente del formato descritos en el apartado 6.2.2 que se utilice para la firma electrónica, la verificación de la firma debe enfocarse en la validación de la información de las etiquetas *SigningTime*, *SigningCertificate* y *SignaturePolicy*.

Para los documentos o archivos que deban contener más de una firma electrónica se seguirá el proceso anterior teniendo en cuenta la etiqueta *CounterSignature*.

Las reglas del verificador deben identificar los atributos sin firmar del CMS que deben estar presentes en esta política, en el anexo D se encuentra la estructura de la sintaxis tanto de las reglas de firmante con las del verificador.

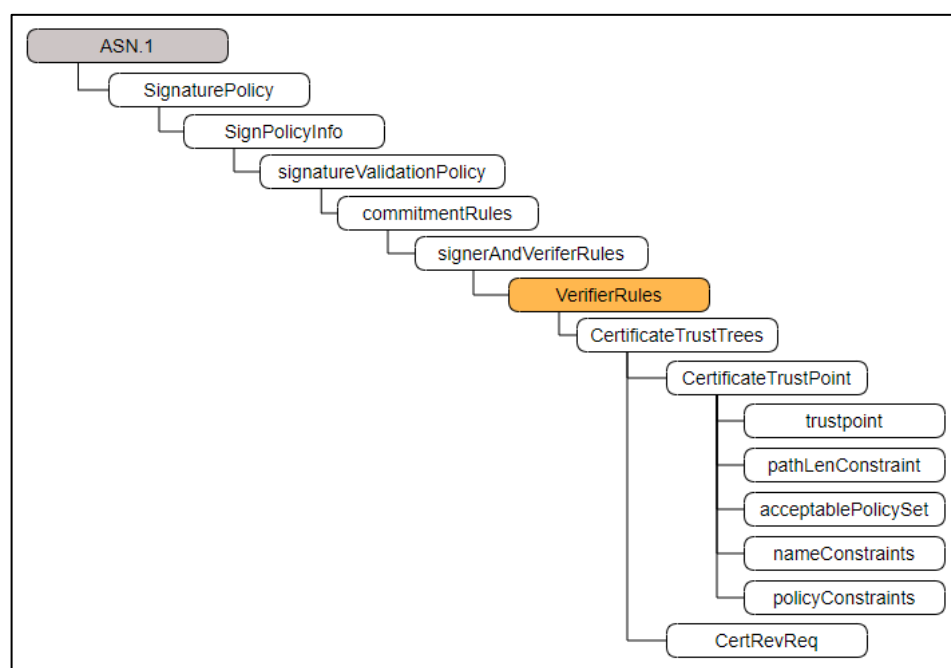


Figura 17. Bloque de Reglas de Verificador.

Referenciado de ETSI TR 102 272, Anexo D

#### **6.3.1.4 Reglas para los sellos de tiempo.**

Se debe contar con una autoridad de sellado de tiempo TSA en la PKI que genere y regule los sellos de tiempo para las firmas electrónicas avanzadas que utilicen los formatos con la extensión X, XL y C según lo indicado en el apartado 6.2.2 de este documento

Se debe aplicar el sello de tiempo para asegurar que los datos del documento, firma y certificados se generen en una fecha valida, para el presente marco de gobierno, el sellado de tiempo debe cumplir con las recomendaciones especificadas en la RFC5816, Internet X.509 PKI Protocolo de estampado de tiempo (TSP).

El sellado de tiempo aplica para formatos de firma avanzada identificada con esta característica, se debe implementar según las necesidades de firma electrónica de cada área de TigoUne, basados en las variaciones especificadas de cada formato de firma descritas en el apartado 4.2.3.7 de este documento.

La información del sellado de tiempo podrá ser agregada tanto por la persona que firma el archivo, como por el remitente del archivo o un tercero como la CA, y deben quedar especificadas como características no firmadas en el campo *SignatureTimeStamp* de la sintaxis de la firma.

En caso de utilizarse las variaciones de formato de firma que implican sellado de tiempo, debe quedar registrado con una diferencia mínima entre este y el dato en el campo *SigningTime* y no deberá superar el tiempo de vencimiento del certificado del firmante.

El sello de tiempo debe contener como mínimo los siguientes elementos:

- Fecha y Hora en formato de tiempo universal coordinado (UTC)
- Identificación de la autoridad que emite el sello de tiempo, clave publica para verificación del sello de tiempo, longitud en bits de la clave, algoritmo de firma digital y el hash usado

para el estampado del tiempo.

- Datos de referencia del archivo o documento que requiere el sello de tiempo.
- Firma digital de los puntos anteriores junto con la clave pública y formato de firma empleados.

### 6.3.1.5 Reglas de uso de algoritmos.

El presente marco de gobierno para la implementación de sistemas de firma electrónica en TigoUne, establece el uso de algoritmos específicos para los formatos de firma XAdES, CAdES, PAdES y sus variaciones y de acuerdo con lo especificado en ETSI TS 102 176-1 “*Electronic Signatures and Infrastructures (ESI), Algorithms and Parameters for Secure Electronic Signatures*” y sus posteriores actualizaciones según se muestra en la tabla 9.

Tabla 9

Algoritmos de Firma Electrónica

ETSI TS 102 176-1

<u>Índice del algoritmo de firma</u>	<u>Nombre corto del algoritmo de firma</u>	<u>Llaves y parámetros de generación de algoritmos</u>	<u>Normativas de Referencia</u>
2.01	rsa	rsagen1	RFC 3447
2.02	dsa	dsagen1	FIPS Publication 186-2 [6], ISO/IEC 14888-3:2006
2.03	ecdsa-Fp	ecgen1	ANSI X9.62
2.04	ecdsa-F2m	ecgen2	ANSI X9.62
2.05	ecgdsa-Fp	ecgen1	ISO/IEC 15946-2 (2002):
2.06	ecgdsa-F2m	ecgen2	ISO/IEC 15946-2 (2002):

Nota. Referenciado de ETSI TS 102 176-1 “*Electronic Signatures and Infrastructures (ESI), Algorithms and Parameters for Secure Electronic Signatures*”

Para la generación de HASH se considera la aceptación de codificación en base 64, siguiendo las recomendaciones de Sintaxis de firma XML y versión de procesamiento 1.1 de W3C, y para la generación de la firma electrónica se aceptarán algoritmos RSA-SHA1 como base y sujeto a posterior actualización a algoritmos más seguros como RSA-SHA256 y RSA-SHA512, este último se implementará para firmas electrónicas longevas.

La tabla 10 muestra la lista de recomendación de uso de funciones hash.

Tabla 10

Lista de Recomendación de Funciones Hash  
ETSI TS 102 176-1

<u>Índice de función hash</u>	<u>Nombre corto de la función hash</u>	<u>Fecha de adopción</u>	<u>Normativas de Referencia</u>
1.01	sha1	01.01.2001	ISO/IEC 10118-3 and FIPS Publication 180-2
1.02	ripemd160	01.01.2001	ISO/IEC 10118-3
1.03	sha224	2004	FIPS Publication 180-2
1.04	sha256	2004	ISO/IEC 10118-3 and FIPS Publication 180-2
1.05	whirlpool	2004	ISO/IEC 10118-3
1.06	sha384	31.03.2007	FIPS 180-2
1.07	sha512	31.03.2007	FIPS 180-2

Nota. Referenciado de ETSI TS 102 176-1 “*Electronic Signatures and Infrastructures (ESI), Algorithms and Parameters for Secure Electronic Signatures*”

### **6.3.1.6 Reglas de confianza.**

Para el presente marco de gobierno para la implementación de sistemas de firma electrónica en TigoUne, se determina que los certificados usados para las firmas deben ser emitidos por la entidad certificadora interna de la compañía, para firmar documentos de interés de procesos internos, estos certificados deben generar una relación clara e inequívoca con el usuario o firmante interno de la compañía y a su vez deben ser almacenados en los controladores de dominio para que tengan relación directa con el Directorio Activo (DA).

Para los casos puntuales en los que se requiera el uso de certificados reconocidos y emitidos por una CA igualmente reconocida o publica, dichos certificados podrán ser aceptados de entidades como Certicámara y Verisign, sin perjuicio de uso de alguna otra entidad certificadora pública o privada reconocida.

### **6.3.2 Requerimientos de certificados y revocación.**

A continuación, se describen los requerimientos que se deben aplicar para los certificados válidos y su correspondiente revocación, estos requisitos se centran en los campos *CertificateTrustTrees* y *CertRevReq* de la sintaxis de la firma electrónica.

#### **6.3.2.1 Requerimientos de certificados.**

El certificado a emplear deberá ser de tipo X509 v3, y debe contener los siguientes atributos:

- Versión.
- Número serial del certificado.
- Identificador del algoritmo utilizado por la CA para firmar.
- Entidad Certificadora que lo emite (CA).
- Periodo de validez (Fecha inicial, Fecha final).
- Nombre del usuario o entidad, (titular) dispuesto con los identificadores *Distinguished Name* (DN), comprendido por el *Common Name* (CN), *Organizational Unit* (OU), *Organization* (O) y *Country* (C).
- datos de la clave pública del usuario o entidad.
- Algoritmo usado para la generación de la clave pública.

- Clave pública del usuario o entidad.
- ID único del emisor del certificado (opcional).
- ID único del usuario o entidad (opcional).
- Extensiones de datos que apliquen (opcional).
- Algoritmo utilizado para firmar el certificado digital.
- Firma digital del certificado.

Desde el punto de vista de la sintaxis se debe emplear los siguientes campos para el certificado:

El campo *CertificateTrustTrees* en la sintaxis de la firma, debe identificar un conjunto de certificados auto-firmados para los puntos de confianza utilizados en el inicio del procesamiento de la ruta del certificado y las condiciones iniciales para la validación de la ruta del certificado como se define en la sección 4 de la RFC 2459, utilizada para definir la política de validación del certificado de firma, los certificados de la TSA y los certificados de atributos, como lo muestra la figura 18.

- El campo *trustPoint* debe contener información del certificado auto-firmado para la CA que se utiliza como punto de confianza para el inicio del procesamiento de la ruta del certificado.
- El campo *pathLenConstraint* debe contener el número máximo de certificados de CA que pueden estar en una ruta de certificación.
- El campo *pathLenConstraint* debe estar siempre presente en la sintaxis de la firma, su valor debe ser mayor o igual a cero y debe establecer el límite de la longitud de la ruta de certificación.



- El campo *acceptablePolicySet* debe identificar el conjunto inicial de políticas de certificado, en la sintaxis cada política de certificado debe ser identificada con un ID.
- El campo *nameConstraints* debe contener todos los nombres de los sujetos en los certificados posteriores en una ruta de certificación, para este campo no se deben especificar restricciones.
- El campo *policyConstraints*, si está presente, debe especificar el requisito de una indicación explícita de la política de certificado, e incluso no debe contener restricciones de políticas.

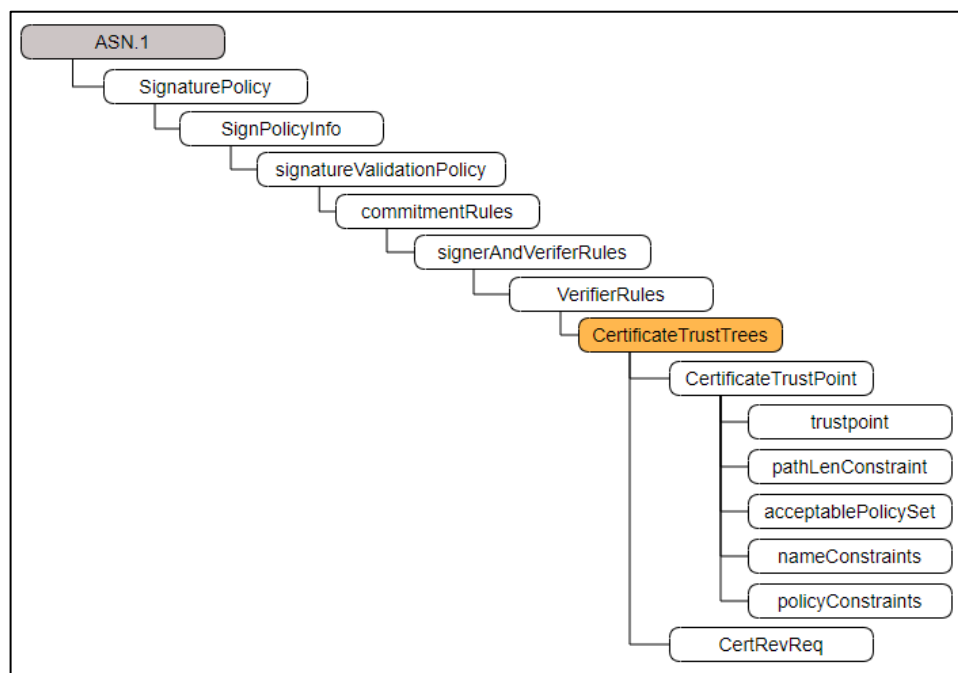


Figura 18. Bloque de los Requerimientos de Certificados.

Referenciado de ETSI TR 102 272, Anexo D

### 6.3.2.2 *Requerimientos de revocación.*

A continuación, se describen los requisitos mínimos para registrar la información de revocación de certificados, obtenidos a través de las CRL o de la ejecución del OCSP, estos se deben usar para verificar el estado de revocación de los certificados.

Los elementos de la estructura ASN.1 del certificado se deben utilizar para definir la política de validación del certificado de firma, el certificado de TSA y los certificados de atributos.

Los requisitos de revocación deben darse en términos como:

- Validación contra las CRLs actuales, sean internas o externas a TigoUne según el caso que aplique para los certificados de firma electrónica.
- El estado de revocación debe verificarse mediante OCSP.

Lo anterior debe estar contenido en el campo *CertRevReq*, como lo muestra la figura 19

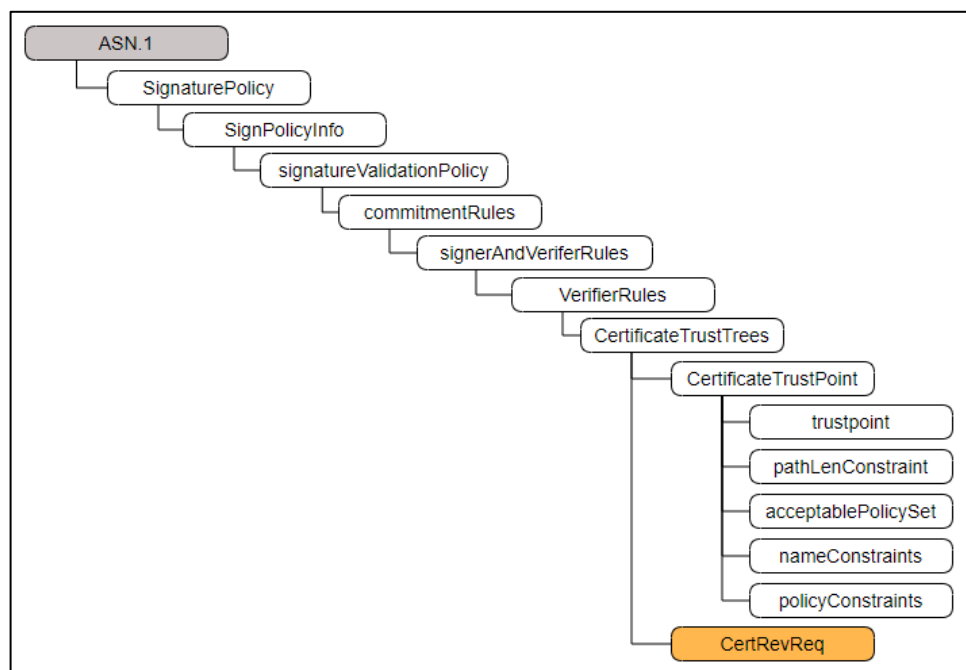


Figura 19. Bloque de Requerimientos de Revocación.

Referenciado de RFC3125, Anexo D

Los requisitos de revocación del certificado se deben especificar en términos de las comprobaciones que para el campo *endCertRevReq* debe ser el certificado del firmante, el certificado de atributo o el certificado de autoridad de sello de tiempo y para *caCerts*. los certificados de la CA.

## **6.4 Resultados de pruebas de software de firma electrónica**

### **6.4.1 PKI actual TigoUne.**

TigoUne Cuenta con una PKI interna implementada la cual consta de los siguientes componentes que podrán ser utilizados para la implementación de un sistema de firma electrónica:

- CA Raíz: con esta CA se generó un certificado auto-firmado para certificar las CAs Subordinadas
- Clúster CA Subordinada: esta CA es la encargada de generar los certificados tanto de servidores como de aplicaciones corporativas y usuarios de dominio.
- DA/RA: esta infraestructura de controladores de dominio está compuesta por dos controladores de dominio principales y 8 secundarios, este DA hace las veces de RA y proporciona las claves privadas a la CA subordinada para la generación de cada certificado de usuario para la firma electrónica.
- Repositorio de certificados: Este componente es el encargado de hacer disponibles las claves públicas de las identidades registradas o usuarios. Cuando se requiere validar un certificado se realiza la consulta en el repositorio, se verifica la firma, el estado del certificado, este componente de la PKI se encuentra en la misma CA subordinada.

- OCSP / AV: Este componente hace las veces de mecanismo alternativo de consulta de validez de los certificados, ya que la entidad certificadora incrementa día a día la CRL y esto hace poco practica su descarga para la verificación del estado de los certificados, este componente también ejerce el rol de autoridad de verificación (AV) en la PKI.

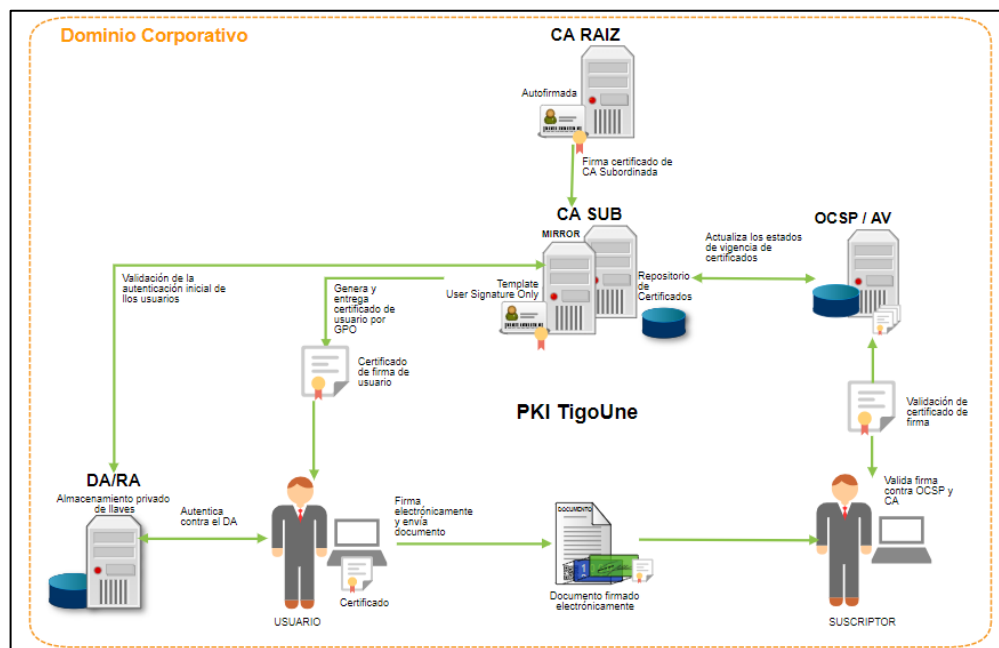


Figura 20. PKI TigoUne

Para el uso de firmas electrónicas de documentos legales contractuales de la compañía, se utiliza la PKI pública de Certicámara para la generación de certificados de usuarios directivos de la compañía con funciones de representación legal, estos certificados se usan para firmar documentos digitales que son válidos tanto al interior de la compañía en la PKI de dominio como fuera de ella.

## 6.4.2 Generación de Certificado en CA de PKI Publica.

Para poder validar el comportamiento de la firma electrónica en documentos digitales y digitalizados, se generó petición y compra de certificado para firma electrónica a través de Certicámara, entidad oficial en Colombia para la emisión de este tipo de certificados que puedan ser reconocidos públicamente.

A través del portal web de Certicámara se hizo el proceso para la obtención del certificado de persona natural aun cuando es posible solicitarlo a través de empresa o persona jurídica, el cual implico diligenciamiento de formato oficial, selección del tipo de certificado según su utilización y periodo de validez, y selección de la opción de token virtual, aun cuando es posible seleccionar la opción de token físico , también los requisitos exigen adjuntar la copia del registro único tributario (RUT) y la copia del documento de identificación para que la solicitud entre a estudio por parte de Certicámara.

En la figura 21 se podrá observar el proceso del trámite ante Certicámara.

**certicámara.**  
Validez y seguridad jurídica electrónica

NOSOTROS PRODUCTOS Y SERVICIOS SOPORTE TÉCNICO SALA DE PRENSA MARCO LEGAL

DETALLE SOLICITUD

SOLICITUD NÚMERO 935570 - JAIME JULIAN RODRIGUEZ ZARATE

Pasos	Descripción	Modificado	Información	Estado
Paso1	Radicación de documentos	21/11/2018	Su solicitud fue radicada con éxito.	Trámite finalizado
Paso2	Verificación de pago	21/11/2018	Su pago fue verificado con éxito. Para realizar la descarga de su factura, haga clic <a href="#">Aquí</a>	Trámite finalizado
Paso3	Aprobación de solicitud	21/11/2018	Su solicitud fue aprobada con éxito.	Trámite finalizado
Paso4	Entrega de certificado	24/11/2018 12:00:00 a.m.	Su certificado de firma digital fue descargado con éxito	Trámite finalizado

NOTA: Para que su trámite finalice exitosamente y pueda recibir su certificado, todos los pasos deben estar finalizados - su trámite tarda entre cinco y ocho días hábiles luego de radicados los documentos y si no se presenta rechazo de los mismos.

[Regresar](#)

Cualquier inquietud adicional comuníquese a nuestro Call Center en Bogotá: 7442727 - Línea Gratuita Nacional: 018000181531.

VERIFICAR  
**Norton**  
SECURED  
powered by **digicert**

Figura 21. Proceso de Solicitud de Certificado CA Pública.

Una vez surtido el proceso de obtención del certificado digital para la firma electrónica, Certicámara envía al usuario las recomendaciones para la asignación de la clave privada de dicho certificado, las cuales comprenden:

- Solo ingresar a la ruta cuando se tenga seguridad de contestar las preguntas de historial crediticio y financiero, se tiene un máximo de cuatro (4) intentos de validación.
- Cada ingreso o apertura del formulario de validación de historial financiero y crediticio, incluyendo los que se generen y no se contesten cuentan como un intento de verificación.
- En el momento que se apruebe el cuestionario de historial financiero y crediticio se debe hacer clic en el botón que aparece en el link "obtenga su certificado".
- No se debe dejar en espera el sistema mientras la ejecución de este proceso, pues ocasiona una indisponibilidad por inactividad de 24 horas.
- El solicitante debe asignar la contraseña del certificado digital, Certicámara S.A. no gestiona o almacena dicha contraseña. Se solicita que se seleccione de forma que sea segura y tenga recordación.
- La contraseña deber ser compleja con características como: tener mínimo 8 caracteres que sean mayúsculas, minúsculas y números.
- El link para la asignación de la contraseña estará habilitado durante 30 días a partir de la recepción del mensaje de aceptación, cumplido este periodo se generará un bloqueo automático del mismo.
- Antes de iniciar la descarga del certificado se debe leer detenidamente el manual de asignación de contraseña Token Virtual.

Este tipo de certificados es utilizado en TigoUne para los directivos que ejercen función de representación legal para firma de contratos o diligencias comerciales a nombre de la compañía.

Los certificados públicos de directivos son gestionados a través del área legal y jurídica de TigoUne.

Certicámara específica con la entrega del certificado digital en términos legales y jurídicos que el certificado de firma es un servicio acreditado ante el ONAC, Y que es considerado un mecanismo equivalente a la firma manuscrita con lo que ello implica.

### 6.4.3 Generación de certificados CA privada.

Para las pruebas de firma electrónica con algunas aplicaciones reconocidas en el mercado, se solicitó la habilitación de la plantilla predeterminada de certificados *User Signature Only* que contienen la CA local de TigoUne.

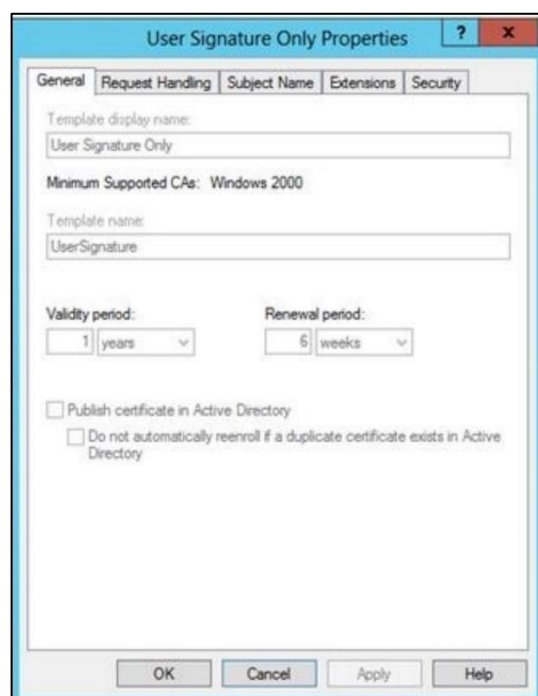
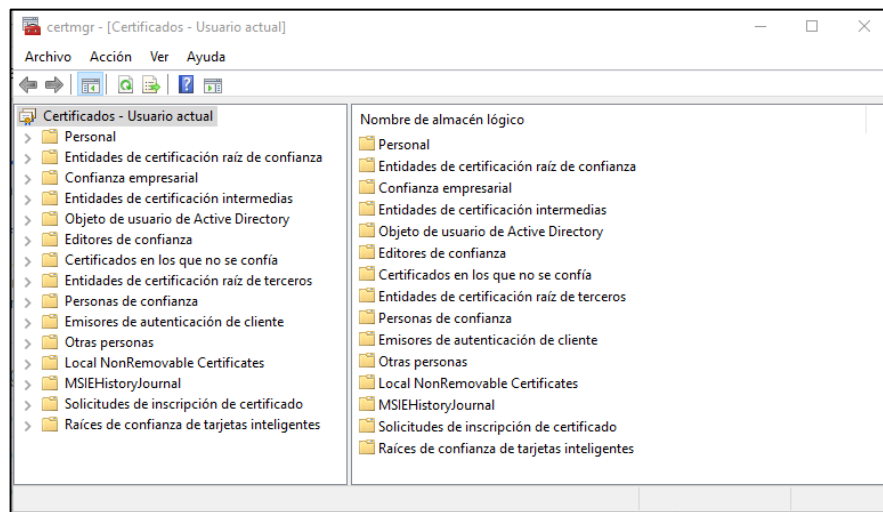


Figura 22. Plantilla de User Signature Only.

Una vez fue ejecutada la habilitación de la plantilla se procedió a solicitar el certificado de usuario a la CA, para efectos de las pruebas el certificado de usuario se solicitó de forma manual, para ello se siguieron los pasos desde una estación de trabajo.

Desde el administrador de certificados de usuario se solicitó la generación del certificado con las credenciales del usuario autenticado en el DA.



*Figura 23.* Administrador de Certificados de Usuario

A través de la opción de solicitud de nuevo certificado se ejecutó el gestor de generación de certificado



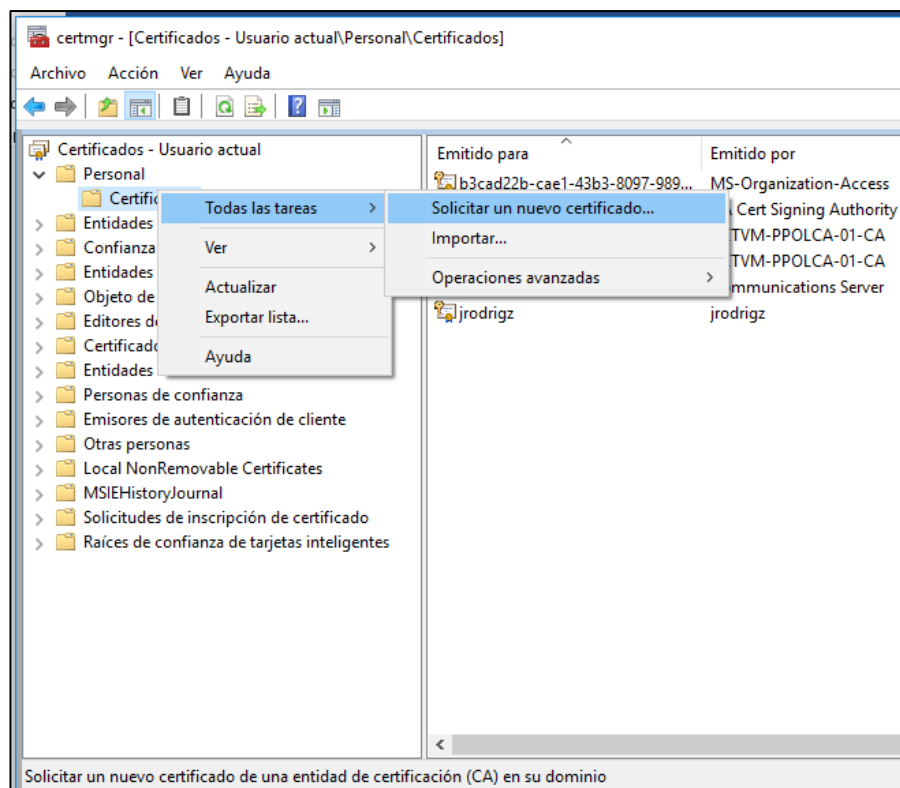
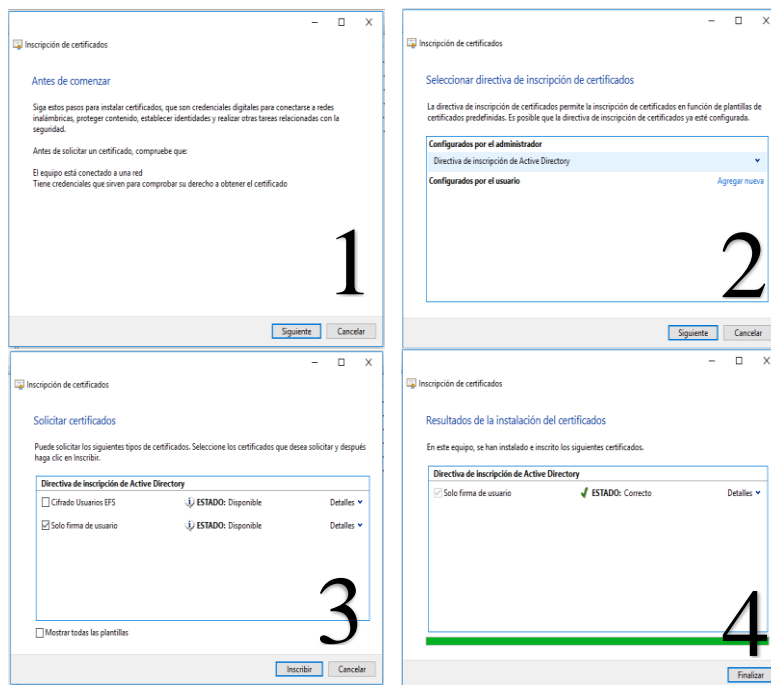


Figura 24. Gestor de Generación de Certificados.

A continuación, se siguieron los cuatro pasos del gestor en la generación del certificado como se muestra en la figura 25



*Figura 25.* Pasos del Gestor de Generación de Certificado.

Como resultado se obtiene un certificado de usuario habilitado para firmar digitalmente y que puede ser utilizado para firma electrónica a través de diversos sistemas para tal fin, dicho certificado se puede observar en la siguiente figura.

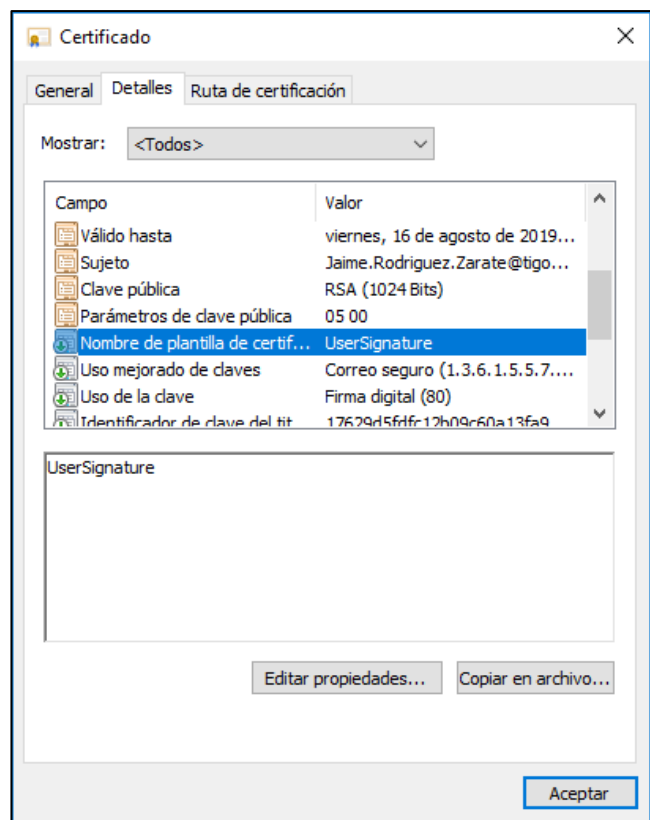


Figura 26. Certificado de Usuario.

En el anexo F podrá observarse el detalle de la sintaxis del certificado de pruebas emitido por la CA local de TigoUne.

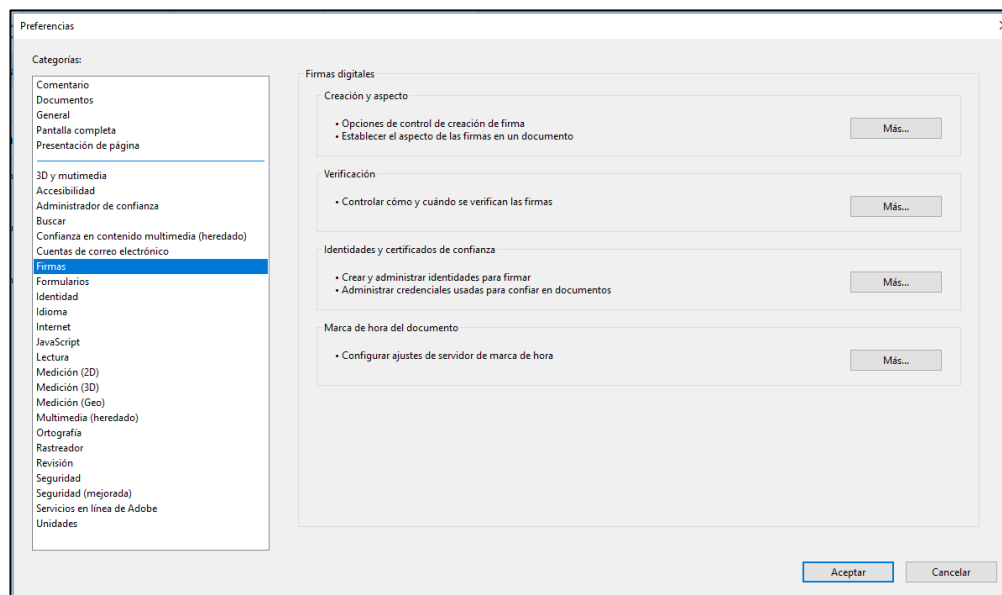
Una vez seleccionado e implementado el sistema de firma electrónica en TigoUne, el proceso de emisión de certificados debe hacerse a través de GPO desde el DA para dar cumplimiento al numeral 8 del apartado 6.2.1 de este documento.

#### 6.4.4 Acrobat Reader.

Una vez obtenido el certificado de usuario de la CA Raíz de TigoUne, se debe ejecutar Instalación de dicho certificado y confiar en los certificados emitidos por esta entidad, esto último se debe hacer con la aplicación Adobe Acrobat Reader ya que esta contiene una lista

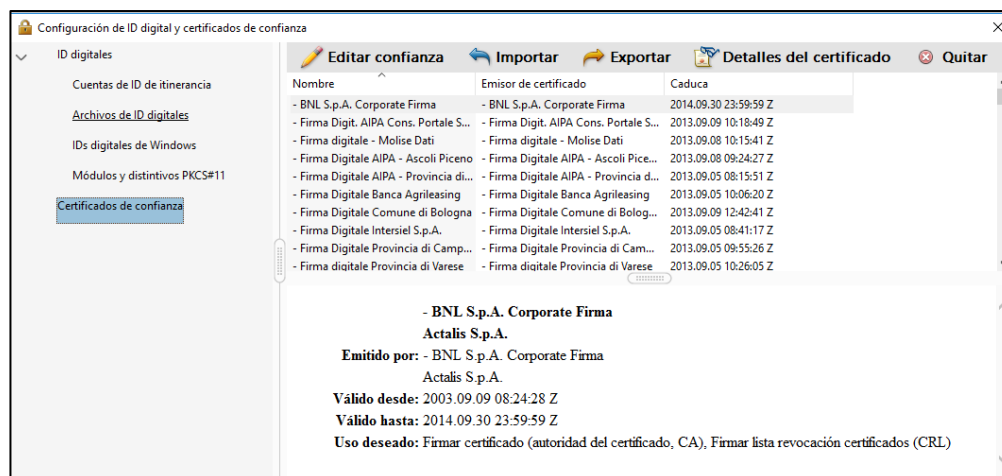
predeterminada de entidades de confianza reconocidas públicamente y no contiene entidades de certificación local de dominio.

Lo primero que se hizo fue Importar certificado desde la aplicación, desde el panel de preferencias y en la opción de firmas como se muestra en la figura 27.



*Figura 27.* Preferencias de Adobe Reader.

Desde la opción identidades y certificados de confianza, se ingresó al gestor de certificados de confianza, figura 28.



*Figura 28.* Certificados de Confianza Adobe Reader.

Desde la opción de importar, se desplegó el asistente para importar certificados, allí se debió buscar la ruta de almacenamiento del certificado de la entidad de certificación de TigoUne obtenido como se mostró en el apartado 6.4.2 de este documento.

A continuación, se muestran los cuatro pasos que se siguieron para importar el certificado.

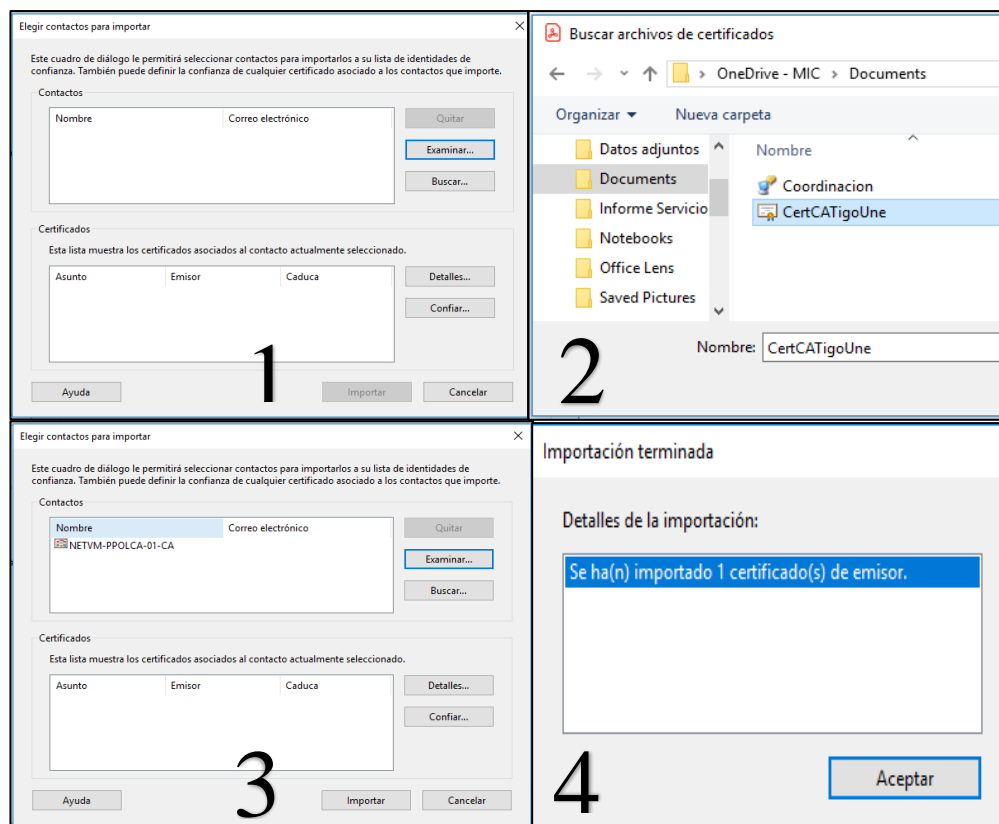


Figura 29. 4 pasos Para Importar Certificado de CA TigoUne.

Una vez importado el certificado de la CA, aparecerá como entidad de confianza para Adobe Reader y podrá consultar la validez de los certificados al momento de la validación de las firmas.

En la figura 30 se muestra la forma en que debe aparecer importado el certificado con el nombre del certificado, el nombre de la entidad certificadora vigencia.

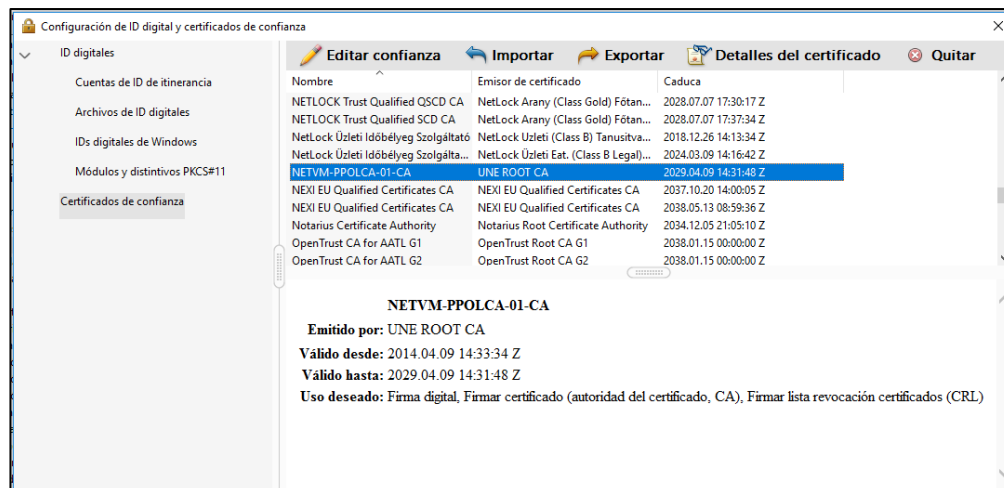


Figura 30. Certificado Importado de CA Interna.

Una vez importado el certificado, y desde la pestaña de *confianza* en la opción de *Agregar a certificados de confianza* se debió habilitar la opción de *utilizar este certificado como raíz de confianza* como aparece en la figura 31, esto con el fin de que cuando se reciba un documento firmado por un usuario autenticado en el dominio, pueda validar la firma contra la entidad certificadora local.

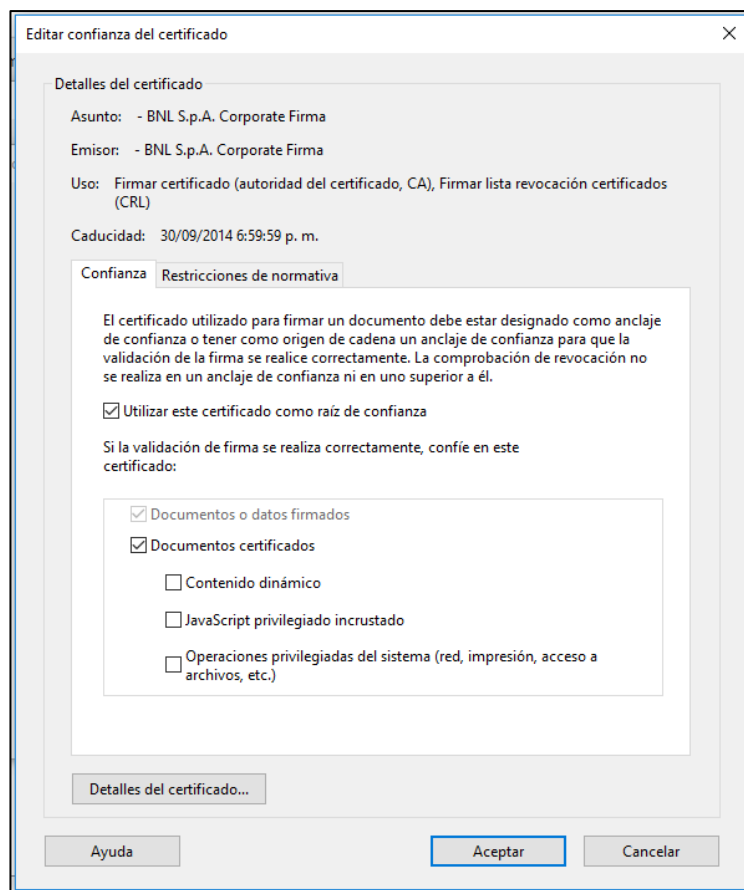


Figura 31. Configuración de Raíz de Confianza.

Ya contando con la configuración previa del certificado de usuario y habiendo configurado la entidad certificadora como de confianza, se generó el ID para firmar electrónicamente un documento, esto se hizo a través de la opción *Creación y aspecto* del menú firmas de las preferencias de Adobe Reader seleccionando las opciones de formato de firma como tipo equivalente a CAdES para formatos PDF o PAdES, seleccionando la opción *incluir estado de revocación de la firma*, activando la opción de *revisión de advertencia de documento e impedir firmar hasta que se hayan revisado las advertencias* así también se activó la opción de *utilizar la interfaz de usuario moderna para la configuración de la firma e ID digital* para facilitar la disposición de la firma electrónica en el documento como se muestra en la figura 32.



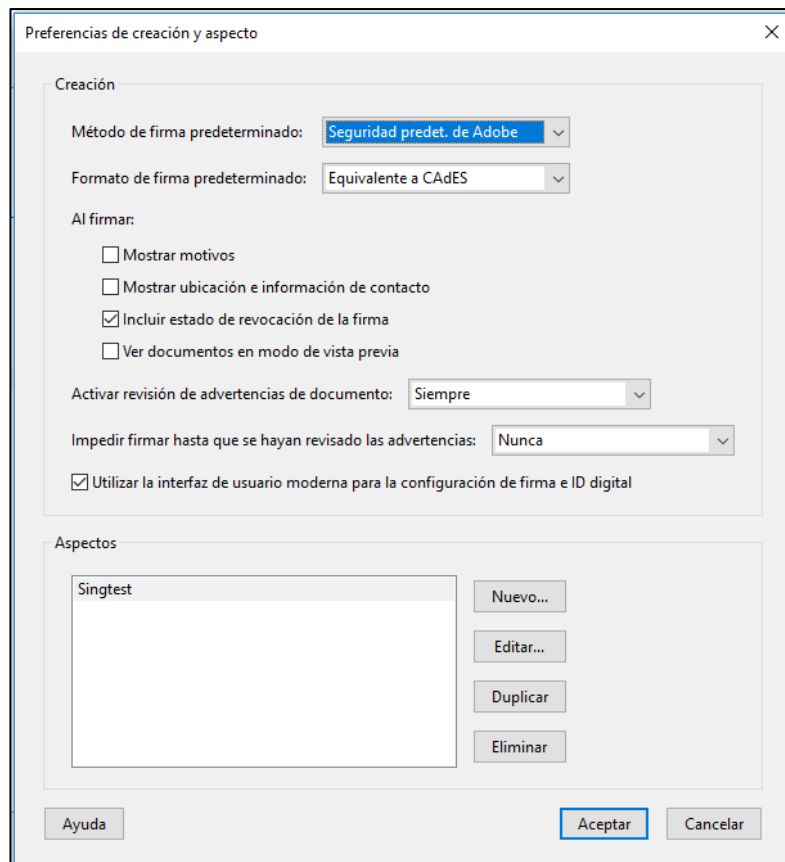


Figura 32. Creación y Aspecto de Firma Electrónica.

Desde la opción de *nuevo* en la sección de aspecto se personaliza la firma electrónica, aquí se le debe dar un nombre a la firma, se observa una previsualización se configura un gráfico asociado a la firma que puede ser la misma firma manuscrita del usuario, se configura para que visualmente la firma muestre datos como *Nombre, fecha, ubicación, motivo, logotipo y etiquetas*, como se muestra en la figura 33.

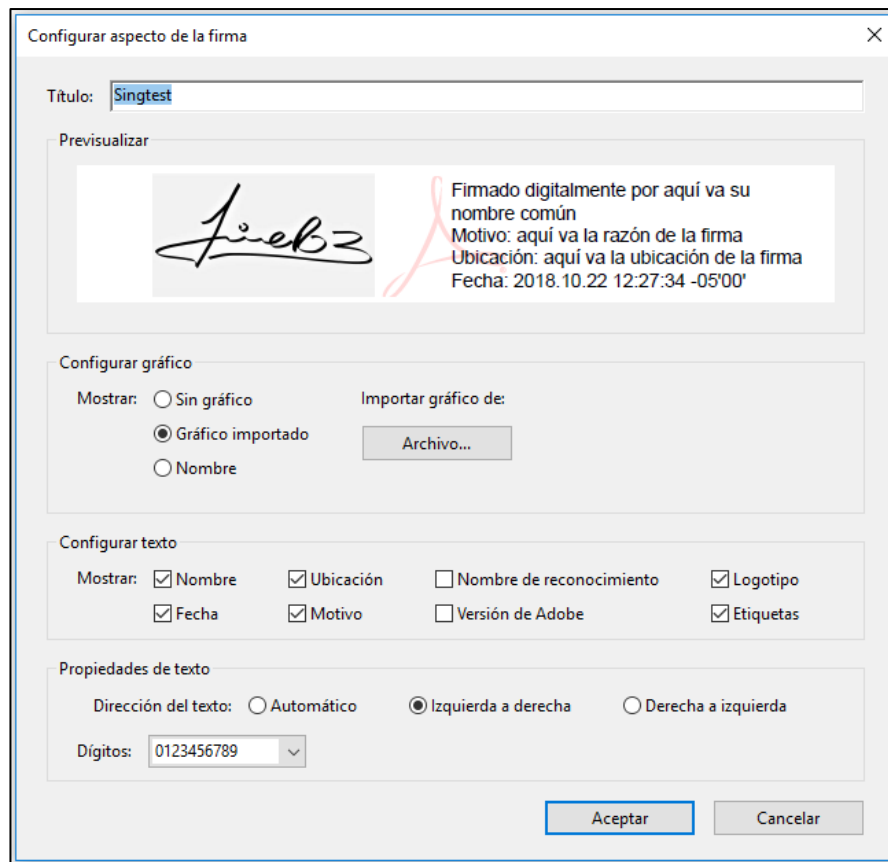


Figura 33. Configuración del ID de Firma Adobe Reader.

Habiendo ya configurado la firma electrónica en la aplicación Adobe Reader, ya se puede utilizar para firmar documentos en formato PDF, y de la misma forma se validan documentos firmados por usuarios autenticados en el dominio como se muestra en la figura 34 donde se podrá observar en el panel de validación de firmas todos los componentes de estas y sus correspondientes certificados emitidos por la CA de TigoUne.

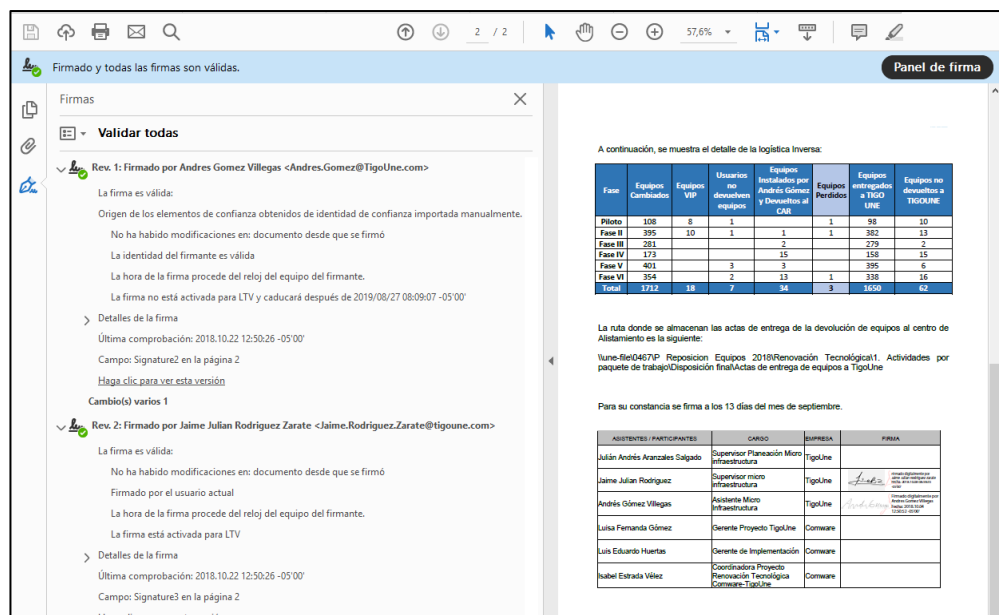


Figura 34. Validación de Firmas Electrónicas Adobe Reader.

De igual forma en la figura 34 se identifica un archivo de prueba el cual fue firmado por dos usuarios con su respectivo certificado de TigoUne, esto demuestra el cumplimiento del numeral 7 del apartado 6.2.1 del presente documento.

#### 6.4.5 Office 365.

Habiendo solicitado e instalado el certificado de usuario como se explicó en el apartado 6.4.1, y haciendo uso de Office 365 de Microsoft, se hicieron pruebas de firmado de documentos.

En primera medida se dispuso de un archivo en Word 2016 con extensión .docx, el cual en su base es un archivo comprimido del que hacen parte tanto el documento en sí y la firma en formato XML, en dicho formato se pudo extraer la sintaxis de la firma adjunta al documento firmado que puede detallarse en el anexo E de este documento.

Para firmar los documentos en Office365, lo primero que se debe hacer es agregar la línea de firma en el lugar que se designe para las firmas, como se muestra en la figura 35

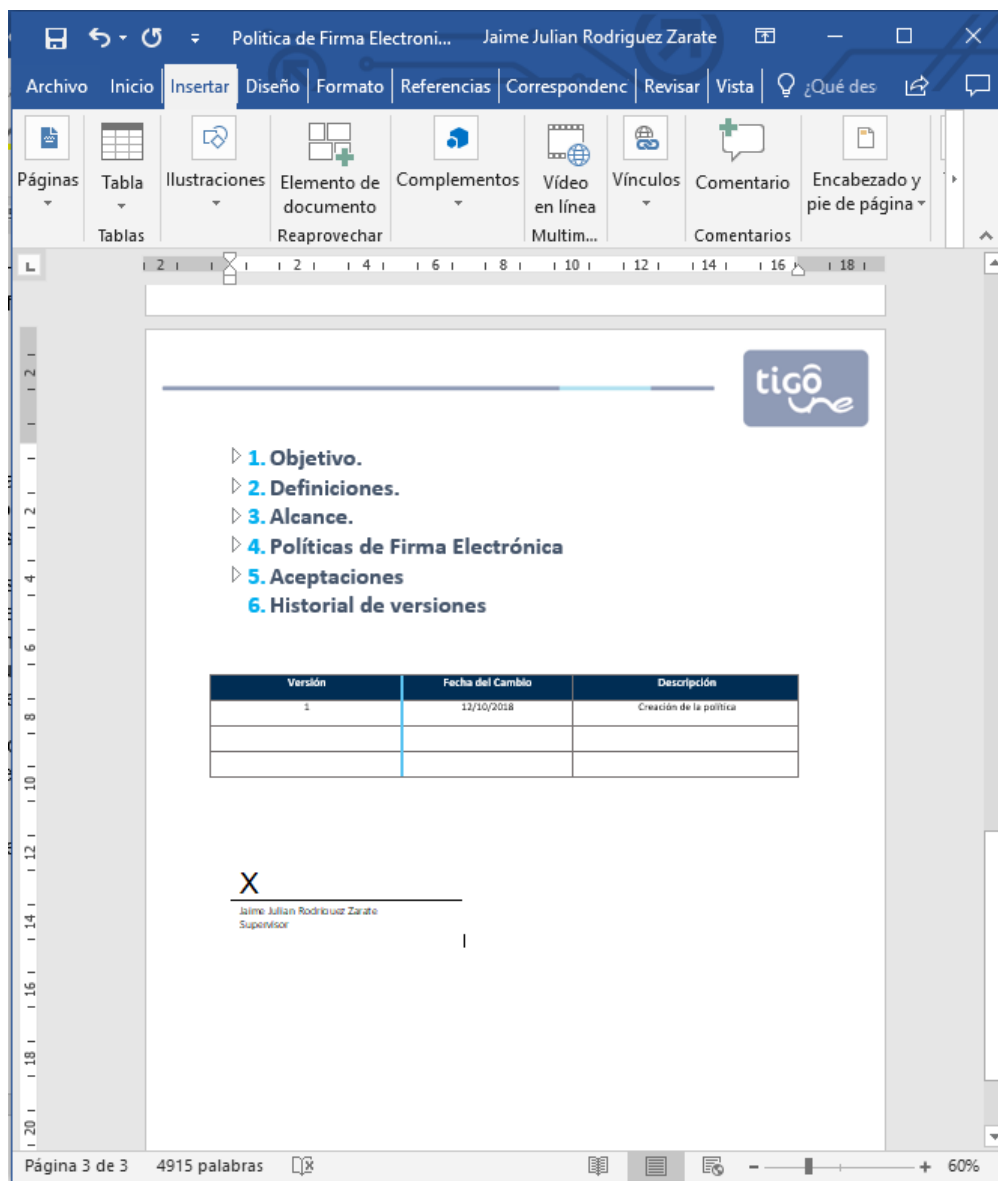


Figura 35. Insertar Línea de Firma Office 365

El paso siguiente fue agregar la firma a través del certificado ya instalado en el equipo de cómputo, desde el menú que se despliega al hacer clic derecho sobre la línea de firma insertada y seleccionando la opción de *Firmar* se despliega el asistente de firma, donde se seleccionó la imagen de la firma manuscrita, se agregaron detalles de la firma como cargo del firmante, dirección, ciudad, municipio y país, se selecciona el certificado desde el campo *Firmar como* y se

selecciona el certificado emitido por la CA con el nombre del firmante como se muestra en la figura 36

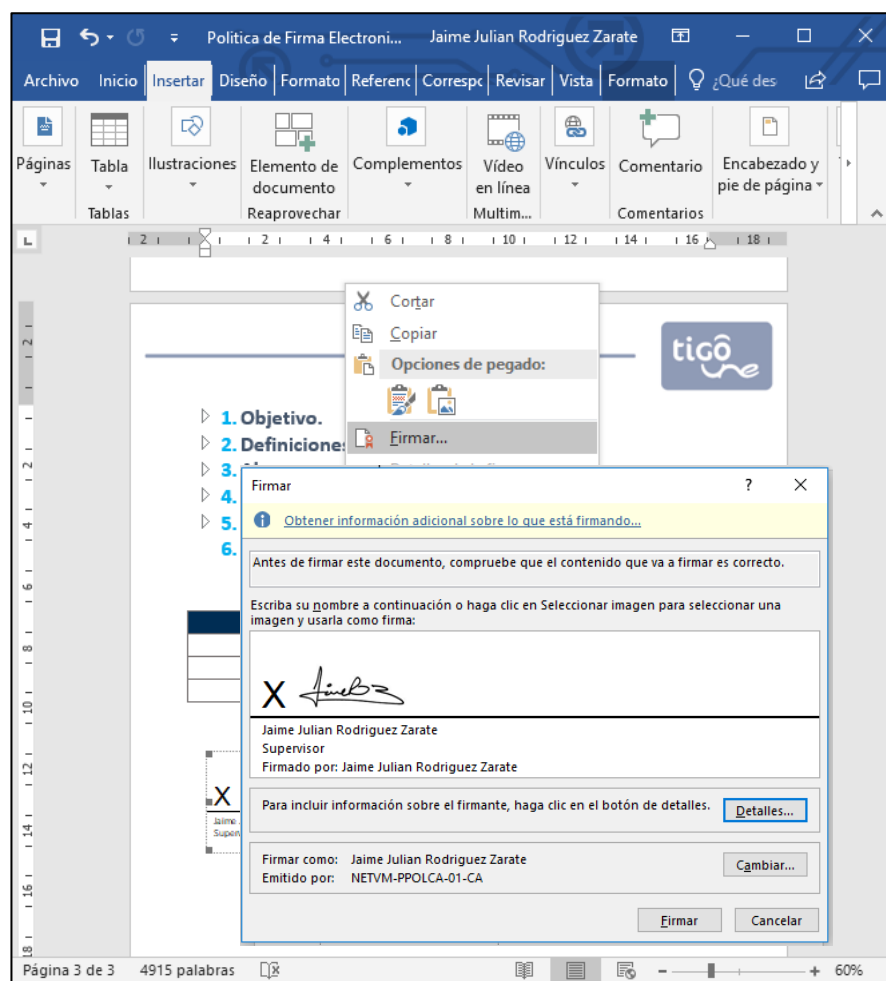


Figura 36. Configuración de Firma Electrónica Office 365.

Una vez firmado el documento se hizo la prueba de validación de dicha firma, seleccionando la opción *Detalles de la firma* del menú que se despliega al hacer clic derecho sobre la firma, pudiendo así obtener información si la firma es válida, el certificado utilizado y sus correspondientes características como se muestran en la figura 37.

También se puede obtener información del formato empleado para la firma que para este caso es XAdES-EPES y podrá verse la los atributos del certificado de usuario.

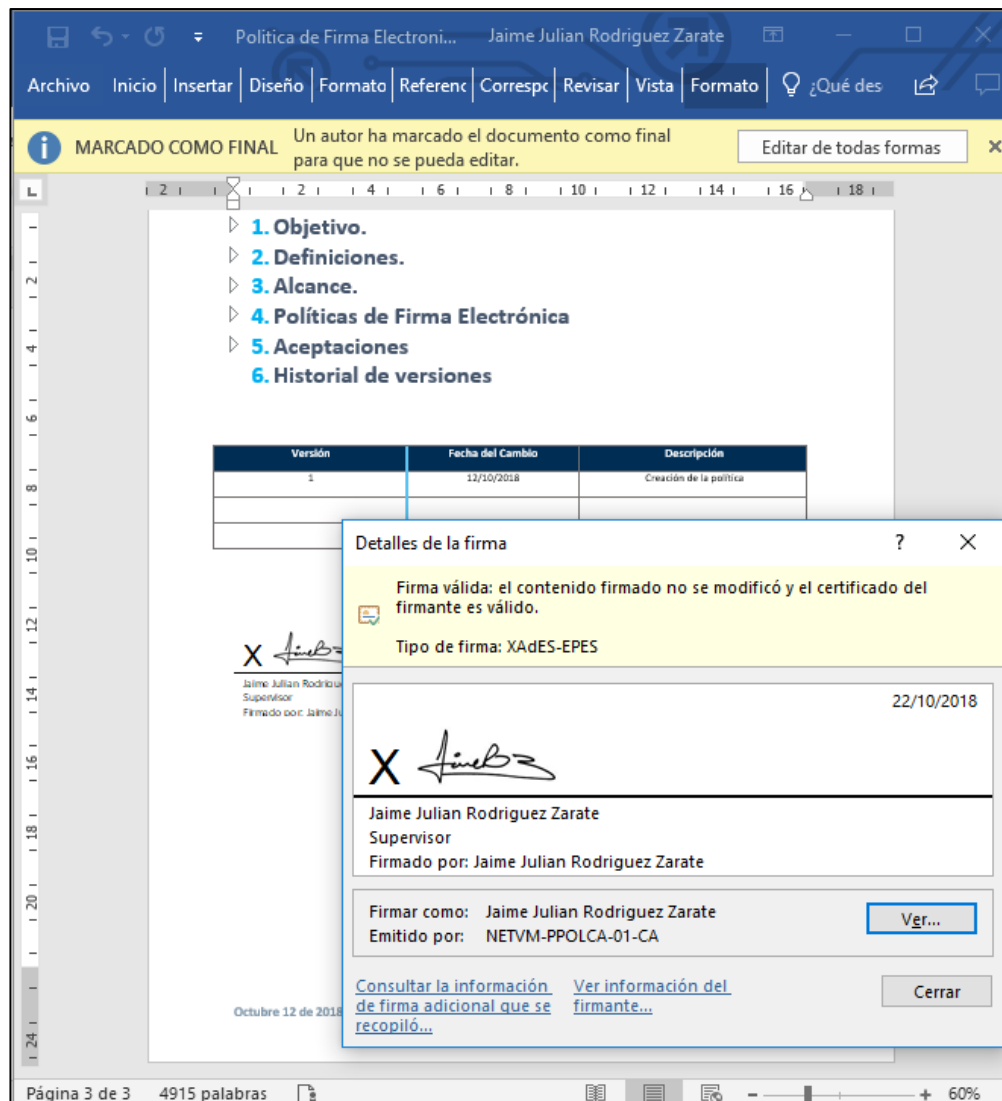


Figura 37. Validación de Firma en Office 365.

## 7 Conclusiones

1. Para implementar sistemas de firma electrónica adecuados a través de herramientas tecnológicas, primero se debieron analizar y entender dichos sistemas, basándose en buenas prácticas y estándares internacionales reconocidos, alineándolos a las necesidades de la organización, de cada área de esta o persona, e incluso del negocio en sí y a las normativas legales que aplican en esta materia. Esto permitió generar un marco de gobierno, definido a partir de políticas y reglas para la adecuada implementación y permitió conservar las principales propiedades de la seguridad de la información en documentos digitales y digitalizados.
2. Se logro determinar que al Igual que en cualquier implementación de tecnología, el eslabón más débil es el usuario, por lo tanto, es importante mantenerlo educado, informado y sensibilizado, de tal forma que interiorice que es el principal responsable en el proceso, a través del buen uso de sus claves y de los sistemas de información utilizados para firma electrónica.
3. La eficiencia en cuanto a la mitigación de riesgos que afecten la confidencialidad, integridad y disponibilidad de la información relevante para una compañía como TigoUne, en cuanto a los documentos digitales y digitalizados aptos para firma electrónica, está basada en la robustez de los algoritmos de cifrado, adecuada selección e implementación de los tipos de formatos de certificados y tipos de formatos de firmas electrónicas, así como los procesos de gestión y operación de la PKI interna de TigoUne y de las externas que se hagan uso.

4. Existen diferentes alternativas de sistemas de firma electrónica que cumplen con las especificaciones legales y técnicas de firmas electrónicas que se adaptan a las necesidades de cada negocio y de los cuales se pueden seleccionar de la clasificación del cuadrante mágico de Gartner.



## 8 Trabajos Futuros

Concluido este trabajo de grado, se abre la puerta a proyectos de:

1. Implementación de sistemas de firma electrónica avanzados.
2. Definición e implementación de plantillas de CA para firmado electrónico.
3. Implementación y mejora de arquitecturas de cifrado de información.
4. Diseño de arquitecturas base para sistemas de firma electrónica “*On Premises*”
5. Diseño de arquitecturas base para sistemas de firma electrónica “*As a services*”.
6. Actualización de formatos de cifrado de CAs locales o de Dominio privado.
7. Firmas electrónicas corporativas reconocidas públicamente por entidades de confianza externas.

## 9 Referencias

1. AENOR. UNE 166006 Norma Española. Gestión de la I+D+i: Sistema de Vigilancia Tecnológica e Inteligencia Competitiva, Pub. L. No. UNE 166006:2011 (2011). España: AENOR. Obtenido de [http://www.imre.uh.cu/wordpress/wpcontent/uploads/2015/06/UNE\\_1660062011.pdf](http://www.imre.uh.cu/wordpress/wpcontent/uploads/2015/06/UNE_1660062011.pdf)
2. Angelozzi, S. M., & Martín, S. G. (2011). Vigilancia Tecnológica e Inteligencia Competitiva: aportes desde las bibliotecas y centros de documentación. 9° Simposio Sobre La Sociedad de La Información Dentro de Las 40 Jornadas de Informática E Investigación Operativa Organizadas Por La SADIO, 1–17. Obtenido de [http://eprints.rclis.org/16752/1/2011\\_Vigilancia\\_Tecnologica\\_e\\_Inteligencia\\_Competitiva\\_aportes\\_desde\\_las\\_bibliotecas\\_y\\_centros\\_de\\_documentacion.pdf](http://eprints.rclis.org/16752/1/2011_Vigilancia_Tecnologica_e_Inteligencia_Competitiva_aportes_desde_las_bibliotecas_y_centros_de_documentacion.pdf)
3. Barker, E. B. (2006). NIST.SP.800-89, Recommendation for obtaining assurances for digital signature applications, (November). Obtenido de <http://doi.org/10.6028/NIST.SP.800-89>
4. Barker, E. B. (2009). NIST.SP.800-102, Recommendation for digital signature timeliness, (September). Obtenido de <http://doi.org/10.6028/NIST.SP.800-102>
5. Barker, E. B., Barker, W.C. & Lee, A (2005). NIST Special Publication 800-21 2nd edition, Guideline for Implementing Cryptography in the Federal Government, (December). Obtenido de <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-21e2.pdf>
6. Barker, E. B.,(2016). NIST Special Publication 800-175B, Guideline for Implementing Cryptography in the Federal Government, (March). Obtenido de <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-21e2.pdf>

7. Baker, E., Smid, M., Branstad, D., Chokhani, S., (2013). NIST Special Publication 800-130, A Framework for Designing Cryptographic Key Management Systems (August).  
Obtenido de <http://dx.doi.org/10.6028/NIST.SP.800-130>
8. Barreto, L.A., (2011). Evolución de la firma autógrafa a la firma electrónica avanzada. *Revista Digital Universitaria - UNAM*. Volumen 12 (3), 1-9
9. Certicámara. (s.f). Firmas Digitales, Certificado Digital. Obtenido de <https://web.Certicámara.com/productos-y-servicios/certificados-de-firma-digital/>
10. Certicámara. (s.f). Casos de éxito, certificados de firma digital. Obtenido de <https://web.Certicámara.com/casos-de-exito/certificados-de-firma-digital/>
11. Congreso de Colombia. (1999). Ley 527 de 1999. Diario Oficial, 1–7. Obtenido de <http://goo.gl/kYtP9D>
12. Daft, R.L (2010). *Organization Theory and Design*, Tenth Edition, Mason, USA: South-Western, Cengage Learning. pp 510
13. Diffie, W. and Hellman, M. E. (1976), *New Directions in Cryptography*. IEEE Transactions on Information Theory, pp. 644-654.
14. Dirección de impuestos y aduanas nacionales. ANEXO TÉCNICO – Política de firma para los documentos electrónicos de la Facturación Electrónica en Colombia. V 1.0 (2016).
15. Empresas Públicas de Medellín. (2017). *Tips para el uso inteligente: Mis consumos en el hogar*. Medellín, Colombia.: EPM. Obtenido de [http://www.epm.com.co/site/clientes\\_usuarios/Clientesyusuarios/Empresas/Energía/Gran desempresas/Tipsparaelusointeligente.aspx](http://www.epm.com.co/site/clientes_usuarios/Clientesyusuarios/Empresas/Energía/Gran desempresas/Tipsparaelusointeligente.aspx)
16. Federal Agencies Digital Guidelines Initiative, (2017). *Technical Guidelines for Digitizing*, obtenido de [www.digitizationguidelines.gov/](http://www.digitizationguidelines.gov/)

17. Gartner peer insights, (2018). Reviews for Electronic Signature market obtenido de <https://www.gartner.com/reviews/market/electronic-signature>
18. Hunt, R., (2002). PKI and Digital Certification Infrastructure. New Zealand. Obtenido de <http://www.au-kbc.org/bpmain1/PKI/PKIieee.pdf>
19. Lucena, M. Criptografía y Seguridad en Computadores. (2010). Obtenido de [https://www.u-  
cursos.cl/ingenieria/2010/2/EL65C/1/material\\_docente/bajar?id\\_material=311979](https://www.ucursos.cl/ingenieria/2010/2/EL65C/1/material_docente/bajar?id_material=311979)
20. Ministerio de Cultura. (2016). Archivo de la Nacion, Política Publica de Archivos. Colombia. Obtenido de [http://www.archivogeneral.gov.co/sites/default/files/Estructura\\_Web/2\\_Politica\\_archivistica/PoliticasyPublicasdeArchivo\\_V2.pdf](http://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/2_Politica_archivistica/PoliticasyPublicasdeArchivo_V2.pdf)
21. Ministerio de Tecnologías de la Información y la Comunicaciones. (s.f). Guía No 5, Digitalización Certificada de Documentos. Colombia. Obtenido de [http://programa.gobiernoenlinea.gov.co/apc-aa-files/Cero\\_papel/guia-5-digitalizacion-de-documentos-v1.pdf](http://programa.gobiernoenlinea.gov.co/apc-aa-files/Cero_papel/guia-5-digitalizacion-de-documentos-v1.pdf).
22. National Institute of Standards and Technology. (2001). Advanced Encryption Standard (AES). Fips Pub 197, (November), Obtenido de <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>
23. National Institute of Standards and Technology. (2013). Digital Signature Standard (DSS). Fips Pub 186-4, (July), Obtenido de <http://doi.org/10.6028/NIST.FIPS.186-4>
24. Pinkas, D., Pope, N., Ross, J. (2001).RFC 3125, Electronic Signature Policies (September). obtenido de <https://tools.ietf.org/pdf/rfc3125.pdf>
25. Pinkas, D., Pope, N., Ross, J. (2008).RFC 5126, CMS Advanced Electronic Signatures (CADES) (February). obtenido de <https://tools.ietf.org/pdf/rfc5126.pdf>

26. Presidencia de la república de Colombia. (2000). Decreto número 1747 de 2000, 2000(septiembre 11), 10. Obtenido de [http://www.alcaldiabogota.gov.co/sisjur/m/m\\_norma.jsp?i=4277](http://www.alcaldiabogota.gov.co/sisjur/m/m_norma.jsp?i=4277)
27. Quiroz Gutiérrez, Marcos. Papel de la Entidades de Certificación y la seguridad de la información y Los Derechos Personales en el Comercio Electrónico. Bogotá. Librería Ediciones del Profesional Ltda. 2009.
28. Rivest, R., Shamir, A. and Adleman, L., A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Communications of the ACM, 21(1978), pp. 120-126.
29. Sefelayer Secure Communications S.A (2010). Secity Target TrustedX. obtenido de <https://www.commoncriteriaportal.org/files/epfiles/2009-03-DS.pdf>.
30. Signinhub. (s.f) Firmas Electronicas, obtenido de <https://www.signinghub.com/electronic-signatures/>
31. Superintendente de Industria y Comercio. (2000). Resolución 26930 de octubre 26 de 2000. Obtenido de <http://www.si3ea.gov.co/Portals/0/Conoce/res26930.pdf>
32. Telvent (2004). Manual de Arquitectura @firma Versión 4.0. Obtenido de <https://ws024.juntadeandalucia.es/ae/descargar/3020>
33. Universidad Europea de Madrid. (2012). Política de firma electrónica. Obtenido de [http://universidadeuropea.es/myfiles/pageposts/Politica\\_Firma\\_Electronica\\_v1.0.pdf](http://universidadeuropea.es/myfiles/pageposts/Politica_Firma_Electronica_v1.0.pdf)
34. World Wide Web Consortium (W3C) (2003). XML Advanced Electronic Signatures (XAdES) Obtenido de <https://www.w3.org/TR/XAdES/#XMLDSIG>
35. Zubite, H. (2002) “Los Mensajes de Datos y las Entidades de Certificación”. Internet, Comercio Electrónico y Telecomunicaciones. Primera Edición. Bogotá. Universidad de los Andes, Legis Editores S.A.

36. Zayas, F., & Milagro, Y. (2013). La firma electrónica, su recepción legal. *Revista del instituto de ciencias jurídicas de Puebla*, MÉXICO, Año 7 (31), 104-120 Obtenido de <http://www.redalyc.org/pdf/2932/293227561007.pdf>

## ANEXO A

## SINTAXIS BASICA DEL CERTIFICADO DE X.509

```

Certificate ::= SEQUENCE {
    tbsCertificate    TBSCertificate,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue    BIT STRING }

TBSCertificate ::= SEQUENCE {
    version          [0] EXPLICIT Version DEFAULT v1,
    serialNumber     CertificateSerialNumber,
    signature        AlgorithmIdentifier,
    issuer           Name,
    validity         Validity,
    subject          Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID  [1] IMPLICIT UniqueIdentifier OPTIONAL,
                    -- If present, version MUST be v2 or v3
    subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,
                    -- If present, version MUST be v2 or v3
    extensions      [3] EXPLICIT Extensions OPTIONAL
                    -- If present, version MUST be v3
}

Version ::= INTEGER { v1(0), v2(1), v3(2) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
    notBefore    Time,
    notAfter     Time }

Time ::= CHOICE {
    utcTime      UTCTime,
    generalTime GeneralizedTime }

UniqueIdentifier ::= BIT STRING

SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm      AlgorithmIdentifier,
    subjectPublicKey BIT STRING }

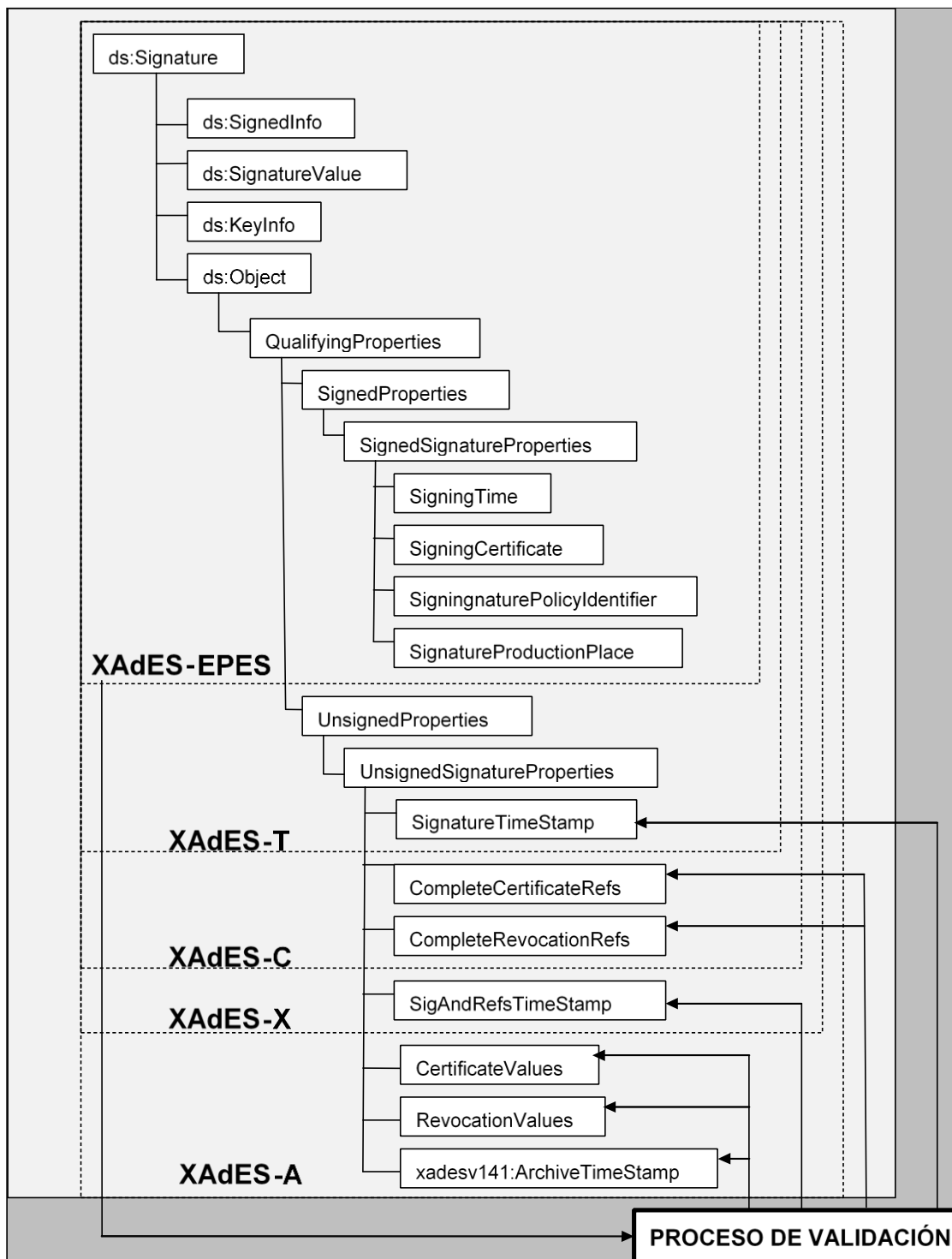
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
    extnID    OBJECT IDENTIFIER,
    critical  BOOLEAN DEFAULT FALSE,
    extnValue OCTET STRING
            -- contains the DER encoding of an ASN.1 value
            -- corresponding to the extension type identified
            -- by extnID
}

```

**ANEXO B**

**ESTRUCTURA DE LA FIRMA ELECTRONICA EN FORMATO XAdES Y  
VARIANTES**

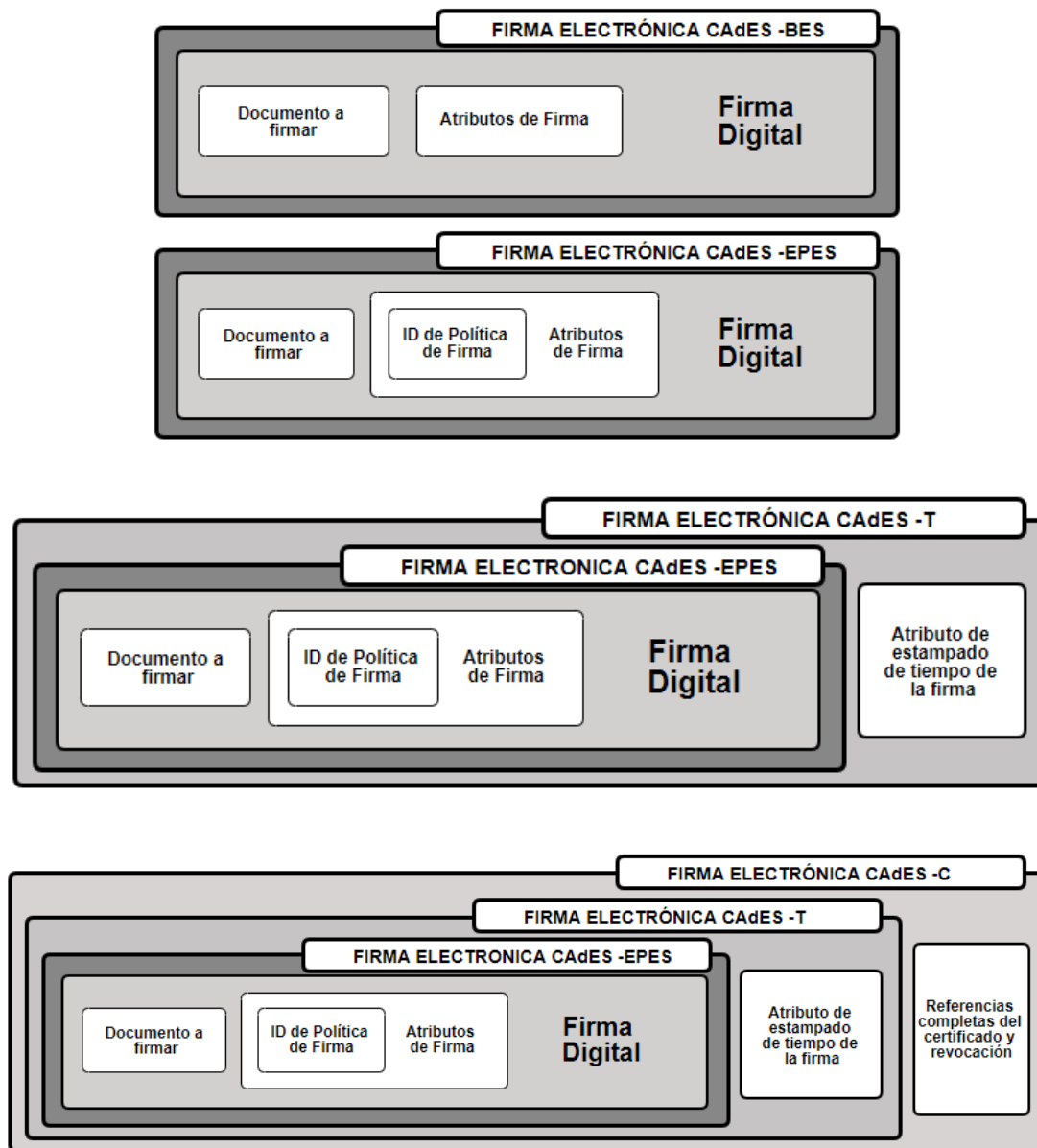


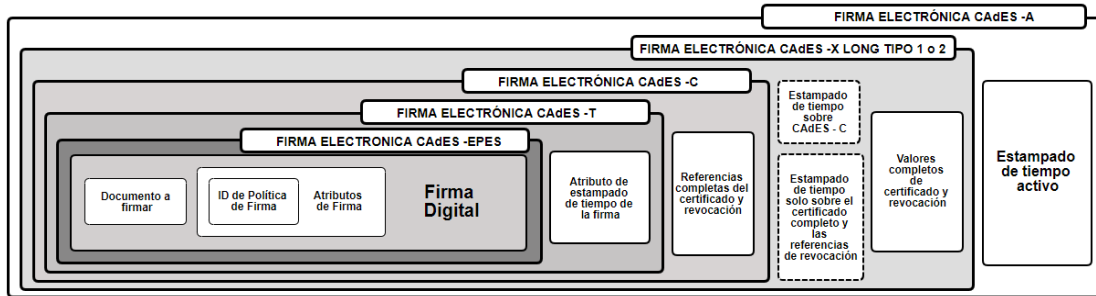
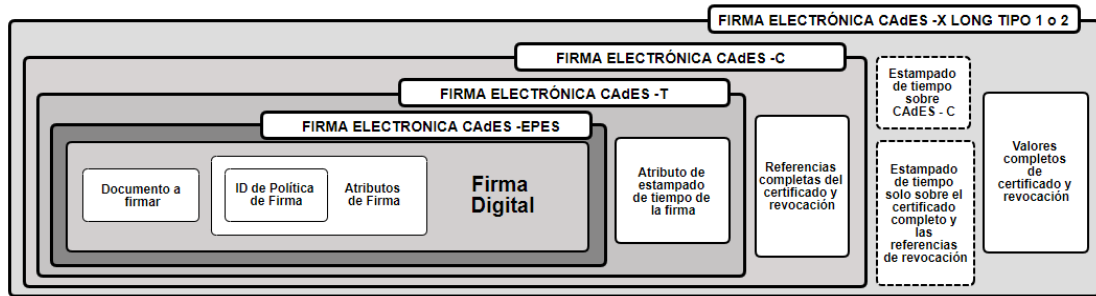
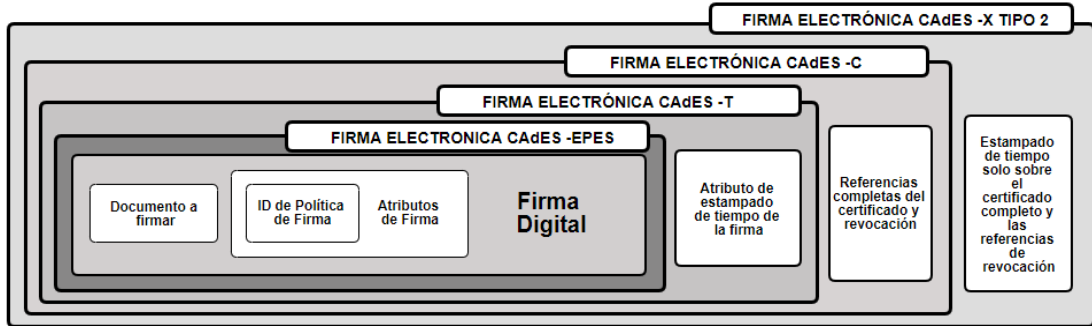
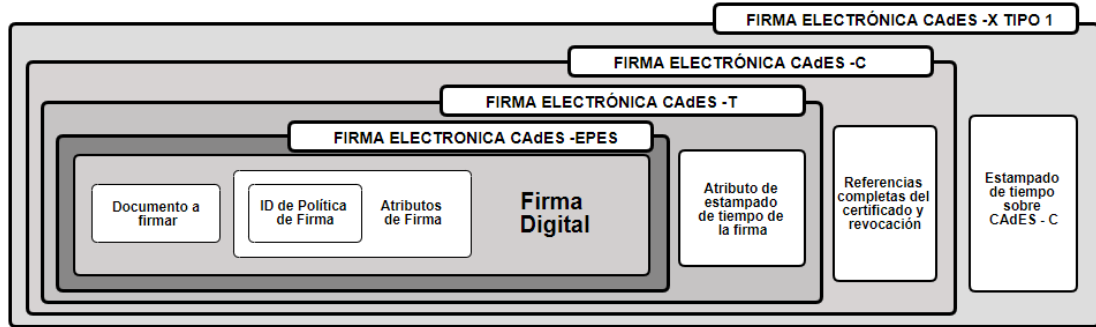


## ANEXO C

## ESTRUCTURA EN BLOQUES DE LA FIRMA ELECTRONICA EN FORMATO

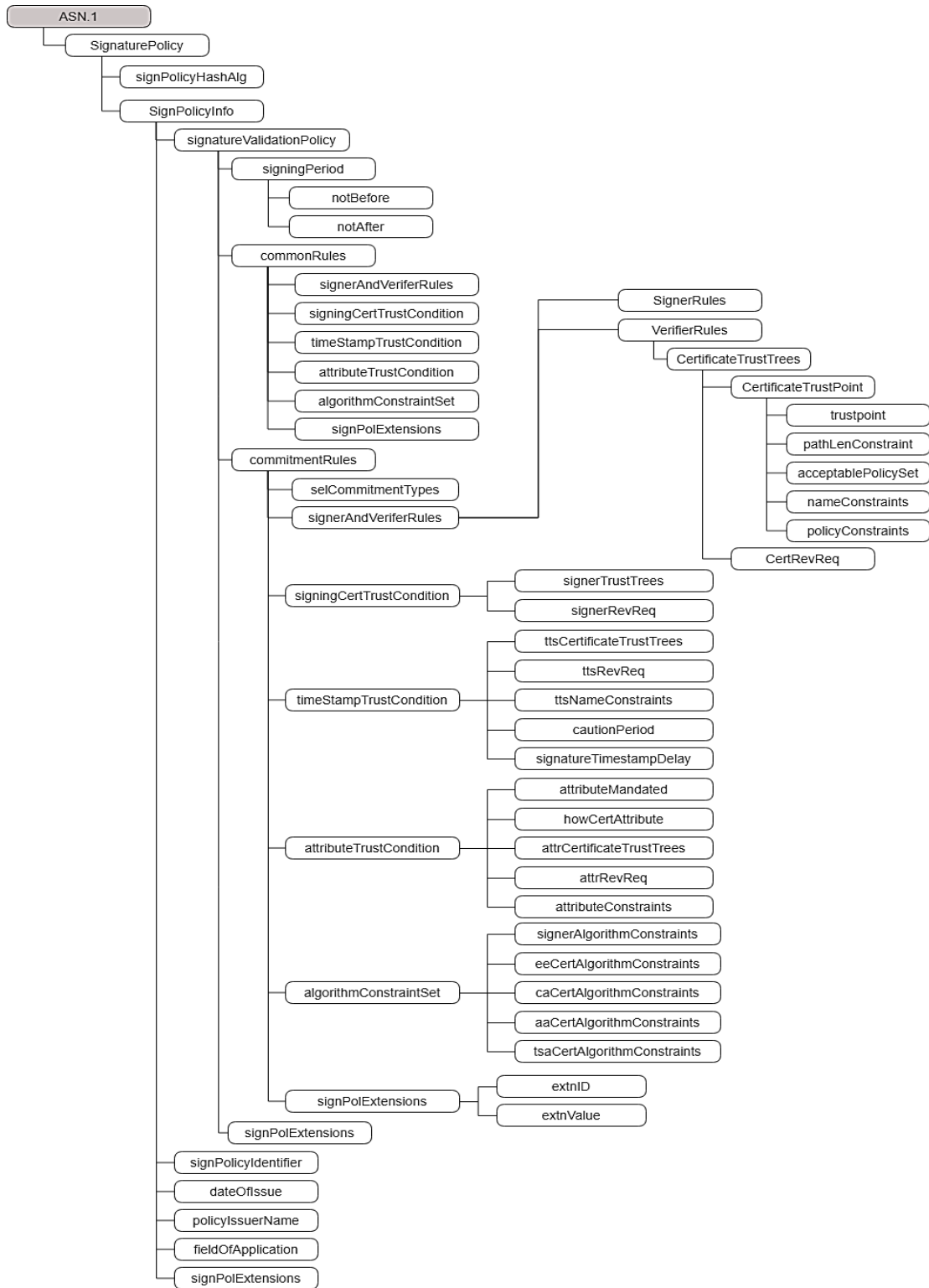
## CADES Y VARIANTES ETSI TS 101 733





ANEXO D

INFRAESTRUCTURA DE FIRMA ELETRÓNICA ASN.1 ETSI TR 102 272



## ANEXO E

**EJEMPLO DE CODIGO XML DE FIRMA ELECTRONICA TIGOUNE PARA  
DOCUMENTOS EN OFFICE 365**

```

<?xml version="1.0" encoding="UTF-8"?>
<Signature Id="idPackageSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
  - <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    - <Reference URI="#idPackageObject" Type="http://www.w3.org/2000/09/xmldsig#Object">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>VKENmHRVJOrMYW45Bcid
q+tSKYI=</DigestValue> </Reference>
    - <Reference URI="#idOfficeObject" Type="http://www.w3.org/2000/09/xmldsig#Object">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>3r/vvQ6/Fji226FTO65XoXH13I
o=</DigestValue> </Reference>
    - <Reference URI="#idSignedProperties" Type="http://uri.etsi.org/01903#SignedProperties">
    - <Transforms>
      <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>GW8f421Za4LO2kScLMizctjy
Gko=</DigestValue> </Reference>
    - <Reference URI="#idValidSigLnImg" Type="http://www.w3.org/2000/09/xmldsig#Object">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>kYksBKFGiJPYcwb3wsIzSHK
p/v0=</DigestValue> </Reference>
    - <Reference URI="#idInvalidSigLnImg" Type="http://www.w3.org/2000/09/xmldsig#Object">
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>Fxf0pTtLvXm/Cz716hY
3WXxJUkg=</DigestValue> </Reference>
    </SignedInfo>
    <Signature Value>rmrxaG+eE+tWd1n+hIIzohom26T6exREdHb+a+MhoG0rS8htOWkvH9DYTqGI2
eb8IJtxCsXHsxHU
opPH28kjGvyXc5ba+tLKpGsZMRcIdDaIqi8tkD9vNltf0/U9nGL6mw2Ii47XMVUQEuhLZT007fXy
ZrgW8d+0qGQWDD2Z0Ls=</SignatureValue> - <KeyInfo>
    - <X509Data>
      <X509Certificate>MIIFsjCCBJqgAwIBAgITEQALbsmLITi8uDmOfwABAAAtuyTANBgkqhkiG9w0BA
QUFADBgMRIwEAYK CZImiZPYLGQBGRYCY28x </X509Data>
    </KeyInfo>
    - <Object Id="idPackageObject"> - <Manifest>
    - <Reference URI="/_rels/.rels?ContentType=application/vnd.openxmlformats-
package.relationships+xml">
    - <Transforms>
    - <Transform Algorithm="http://schemas.openxmlformats.org/package/2006/RelationshipTransform">
      <mdssi:RelationshipReference SourceId="rId1"
xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature"/>
    </Transform>
      <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>

```

```

    <DigestValue>1vWU/YTF/7t6ZjnE44gAF
    TbZvvA=
    </DigestValue> </Reference>
- <Reference URI="/word/_rels/document.xml.rels?ContentType=application/vnd.openxmlformats-
package.relationships+xml">
- <Transforms>
- <Transform Algorithm="http://schemas.openxmlformats.org/package/2006/RelationshipTransform">
    <mdssi:RelationshipReference SourceId="rId3"
    xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature"/>
    <mdssi:RelationshipReference SourceId="rId2"
    xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature"/>
    <mdssi:RelationshipReference SourceId="rId1"
    xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature"/>
    <mdssi:RelationshipReference SourceId="rId6"
    xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature"/>
    <mdssi:RelationshipReference SourceId="rId5"
    xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature"/>
    <mdssi:RelationshipReference SourceId="rId4"
    xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature"/>
    </Transform>
    <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
  </Transforms>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>kVYcPjZZG3SU5+sOsB1PRnQSCzk=</DigestValue>
</Reference>
- <Reference URI="/word/document.xml?ContentType=application/vnd.openxmlformats-
officedocument.wordprocessingml.document.main+xml"> <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>HHutKVTzrmuHskq42bLX
d7AUcqQ=</DigestValue> </Reference>
- <Reference URI="/word/fontTable.xml?ContentType=application/vnd.openxmlformats-
officedocument.wordprocessingml.fontTable+xml"> <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>ghDCixtfmmRXlaloirsODn
2nhY4=</DigestValue> </Reference>
- <Reference URI="/word/media/image1.emf?ContentType=image/x-emf">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>807sulBU6wRSxbGpd/kng
nX6RQ=</DigestValue> </Reference>
- <Reference URI="/word/settings.xml?ContentType=application/vnd.openxmlformats-
officedocument.wordprocessingml.settings+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>fiYoAiVE21AdmArq1cIkj/2
6cRc=</DigestValue> </Reference>
- <Reference URI="/word/styles.xml?ContentType=application/vnd.openxmlformats-
officedocument.wordprocessingml.styles+xml"> <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>e7ogjsC4GRjdTIHAWbcXA9QPgyI=</DigestValue>
</Reference>
- <Reference URI="/word/theme/theme1.xml?ContentType=application/vnd.openxmlformats-
officedocument.theme+xml">
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>sArrX1Xba4pLosqeADdAu
PRNEe4=</DigestValue> </Reference>

```

```

- <Reference URI="/word/webSettings.xml?ContentType=application/vnd.openxmlformats-officedocument.wordprocessingml.webSettings+xml"> <DigestMethod Algorithm="http://www.w3.org/2000/09/xmlsig#sha1"/>
  <DigestValue>YMmN0SJEtM8fTLc+PdnqE2ISGRM=</DigestValue> </Reference>
</Manifest>
- <SignatureProperties>
- <SignatureProperty Id="idSignatureTime" Target="#idPackageSignature">
- <mdssi:SignatureTime xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature">
  <mdssi:Format>YYYY-MM-DDThh:mm:ssTZD</mdssi:Format>
  <mdssi:Value>2018-10-05T19:20:47Z</mdssi:Value>
</mdssi:SignatureTime>
</SignatureProperty>
</SignatureProperties>
</Object>
- <Object Id="idOfficeObject"> - <SignatureProperties>
- <SignatureProperty Id="idOfficeV1Details" Target="#idPackageSignature">
- <SignatureInfoV1 xmlns="http://schemas.microsoft.com/office/2006/digsig"> <SetupID>{06437414-EF4F-4404-BF75-B20CE41C1B12}</SetupID>
  <SignatureText/>
  <SignatureImage>AQAAAGwAAAAAAAAAAAAAAAAAHoAAAA0AAAAAAAAAAAAAAAAADdCgAAqQQAACBFTUYAAAEAzIQAAAwAAAAABA
  <SignatureComments/>
  <WindowsVersion>10.0</WindowsVersion>
  <OfficeVersion>16.0.9126/12
  </OfficeVersion>
  <ApplicationVersion>16.0.9126
  </ApplicationVersion>
  <Monitors>2
  </Monitors>
  <HorizontalResolution>1366
  </HorizontalResolution>
  <VerticalResolution>768
  </VerticalResolution>
  <ColorDepth>32</ColorDepth>
  <SignatureProviderId>{00000000-0000-0000-0000-000000000000}</SignatureProviderId>
  <SignatureProviderUrl/>
  <SignatureProviderDetails>9</SignatureProviderDetails>
  <SignatureType>2</SignatureType>
</SignatureInfoV1>
- <SignatureInfoV2
  xmlns="http://schemas.microsoft.com/office/2006/digsig">
  <Address1/>
  <Address2/>
</SignatureInfoV2>
</SignatureProperty>
</SignatureProperties>
</Object>

```

```

- </Object>
- <xd:QualifyingProperties
  Target="#idPackageSignature"
  xmlns:xd="http://uri.etsi.org/01903/v1.3
  .2#"> - <xd:SignedProperties
  Id="idSignedProperties">
- <xd:SignedSignatureProperties>
  <xd:SigningTime>2018-10-
  05T19:20:47Z
  </xd:SigningTime>
- <xd:SigningCertificate>
- <xd:Cert>
- <xd:CertDigest>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <DigestValue>+XgQmStHNuswx/hTTOuJg+0E8jU
  =</DigestValue> </xd:CertDigest>
- <xd:IssuerSerial>
  <X509IssuerName>CN=NETVM-PPOLCA-01-CA, DC=epmtelco,
  DC=com, DC=co</X509IssuerName>
  <X509SerialNumber>379116558742609815659030814669239572262252233<
  /X509SerialNumber> </xd:IssuerSerial>
  </xd:Cert>
</xd:SigningCertificate>
- <xd:SignaturePolicyIdentifier>
  <xd:SignaturePolicyImplied/>
</xd:SignaturePolicyIdentifier>
- <xd:SignatureProductionPlace>
  <xd:City/>
  <xd:StateOrProvince/>
  <xd:PostalCode/>
  <xd:CountryName/>
</xd:SignatureProductionPlace>
</xd:SignedSignatureProperties>
</xd:SignedProperties>
- <xd:UnsignedProperties>
- <xd:UnsignedSignatureProperties> -
  <xd:CertificateValues>
  <xd:EncapsulatedX509Certificate>MIIH5zCCBc+gAwIBAgITMwAAAahraRxc1tm/wABA
  AAACDANBgkqhkiG9w0BAQUFADBZMRIwE
  <xd:EncapsulatedX509Certificate>MIIGiTCCBHGgAwIBAgIQebU317mW/ppE3gjnXR+JFD
  ANBgkqhkiG9w0BAQUFADBZMRIwEAYKcz
  </xd:CertificateValues>
</xd:UnsignedSignatureProperties>
</xd:UnsignedProperties>
</xd:QualifyingProperties>
</Object>
<Object
  Id="idValidSigLnImg">AQAAAGwAAAAAAAAAAAAAAAAAP8AAAB/AAAAAAAAAAAAAAAAACfFgAARAsAAC
  BFTUYAAAEA+I4AAMsAAAAFAAAAAAAAA
  <Object
  Id="idInvalidSigLnImg">AQAAAGwAAAAAAAAAAAAAAAAAP8AAAB/AAAAAAAA
  AAAAAACfFgAARAsAACBFTUYAAAEA+I4AAMsAAAAFAAAAAAAAA
</Signature>

```

## ANEXO F

### EJEMPLO DE ESTRUCTURA DE CERTIFICADO DIGITAL TIGOUNE PARA FIRMAS ELECTRONICAS

```

OpenSSL> x509 -in dumpcertfile -inform der -in CertExchangeJaimeJulianRodriguezZarate.cer -
text -noout
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
11:00:0b:6e:c9:8b:21:38:bc:b8:39:8e:7f:00:01:00:0b:6e:c9
Signature Algorithm: sha1WithRSAEncryption
Issuer: DC = co, DC = com, DC = epmtelco, CN = NETVM-PPOLCA-01-CA
Validity
Not Before: Aug 16 21:25:36 2018 GMT
Not After : Aug 16 21:25:36 2019 GMT
Subject: DC = co, DC = com, DC = epmtelco, OU = Usuarios, OU = Office365, OU = E3, CN =
Jaime Julian Rodriguez Zarate, emailAddress = Jaime.Rodriguez.Zarate@tigoune.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (1024 bit)
Modulus:
00:c9:05:b8:ea:87:4d:78:9c:a4:14:dc:b6:7c:f2:
ec:83:3f:1b:4e:67:76:7c:72:0b:eb:2f:6d:13:5a:
fc:d4:6d:7d:72:ea:13:e1:93:01:4e:1e:91:44:e2:
2c:f7:e6:74:8e:80:a3:aa:19:5e:6e:32:bf:7b:40:
fc:3e:65:52:b9:3e:11:eb:01:0e:7b:63:3b:5d:a6:
d2:2b:b1:53:b7:4c:6b:57:1c:98:7a:13:33:8e:95:
24:f8:8a:4f:b9:63:1d:39:66:56:25:62:74:ed:4a:
f0:c1:cf:a2:3a:89:48:0f:07:b4:c1:d8:5f:0e:ba:
24:7e:2d:20:f4:6c:28:6a:fd
Exponent: 65537 (0x10001)
X509v3 extensions:
1.3.6.1.4.1.311.20.2:
...U.s.e.r.S.i.g.n.a.t.u.r.e
X509v3 Extended Key Usage:

E-mail Protection, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature
X509v3 Subject Key Identifier:
17:62:9D:5F:DF:C1:2B:09:C6:0A:13:FA:94:06:DD:8A:22:49:63:35
X509v3 Authority Key Identifier:
keyid:B2:CC:D4:D9:37:AA:AE:62:D9:0B:31:5C:A4:D1:2F:D4:41:EB:EA:8F

X509v3 CRL Distribution Points:

```



## Full Name:

URI:<http://revocacion.une.com.co/pki/NETVM-PPOLCA-01-CA.crl>URI:<http://mirror-revocacion.une.com.co/pki/NETVM-PPOLCA-01-CA.crl>

## Authority Information Access:

CA Issuers - URI:[http://revocacion.une.com.co/pki/netvm-ppolca-01.epmtelco.com.co\\_NETVM-PPOLCA-01-CA\(1\).crl](http://revocacion.une.com.co/pki/netvm-ppolca-01.epmtelco.com.co_NETVM-PPOLCA-01-CA(1).crl)CA Issuers - URI:[http://mirror-revocacion.une.com.co/pki/netvm-ppolca-01.epmtelco.com.co\\_NETVM-PPOLCA-01-CA\(1\).crl](http://mirror-revocacion.une.com.co/pki/netvm-ppolca-01.epmtelco.com.co_NETVM-PPOLCA-01-CA(1).crl)

## X509v3 Subject Alternative Name:

othername:&amp;lt;unsupported&amp;gt;, email:Jaime.Rodriguez.Zarate@tigoune.com

Signature Algorithm: sha1WithRSAEncryption

55:43:09:43:e9:fd:82:61:6e:0e:43:ce:26:d4:b6:6c:90:86:  
7a:36:64:b3:cb:41:d4:4a:38:ec:8f:49:70:d1:62:0c:44:00:  
42:a2:db:b0:a9:09:37:41:fb:d6:5e:55:53:17:e6:32:ae:cc:  
f4:47:e8:54:69:24:21:a2:8a:6c:7c:e4:b7:f7:03:b7:d7:63:  
28:ff:28:54:1f:b5:cb:59:03:ef:f4:81:4d:2a:8d:55:9b:31:  
a7:04:26:d8:7b:36:e2:cd:3c:d9:57:bb:72:e4:b2:19:3c:ba:  
fd:24:36:1b:a2:3e:aa:cb:ad:21:59:a5:51:42:ae:cf:25:b6:  
ef:61:ef:47:cd:39:03:ab:44:20:bd:a1:5f:26:74:ac:c1:a1:  
c0:6a:59:48:f8:52:4e:c9:b5:81:6c:d6:df:a6:26:5d:c3:f4:

80:e3:6d:4f:2f:f6:71:89:f8:2d:1a:b8:02:c9:c3:c7:5f:c0:  
42:23:09:12:3b:2e:f1:13:02:84:66:35:80:1a:3c:3c:21:7d:  
86:90:85:41:58:61:ba:5c:5e:60:ff:59:28:88:4e:a8:3e:82:  
41:91:6a:1a:80:61:44:e5:ea:12:ab:08:7b:df:57:f8:98:01:  
fb:9d:46:6f:29:d7:20:f2:d8:d3:36:6c:76:7f:0e:ee:93:26:  
42:cd:4f:ae

OpenSSL&amp;gt;

## ANEXO G

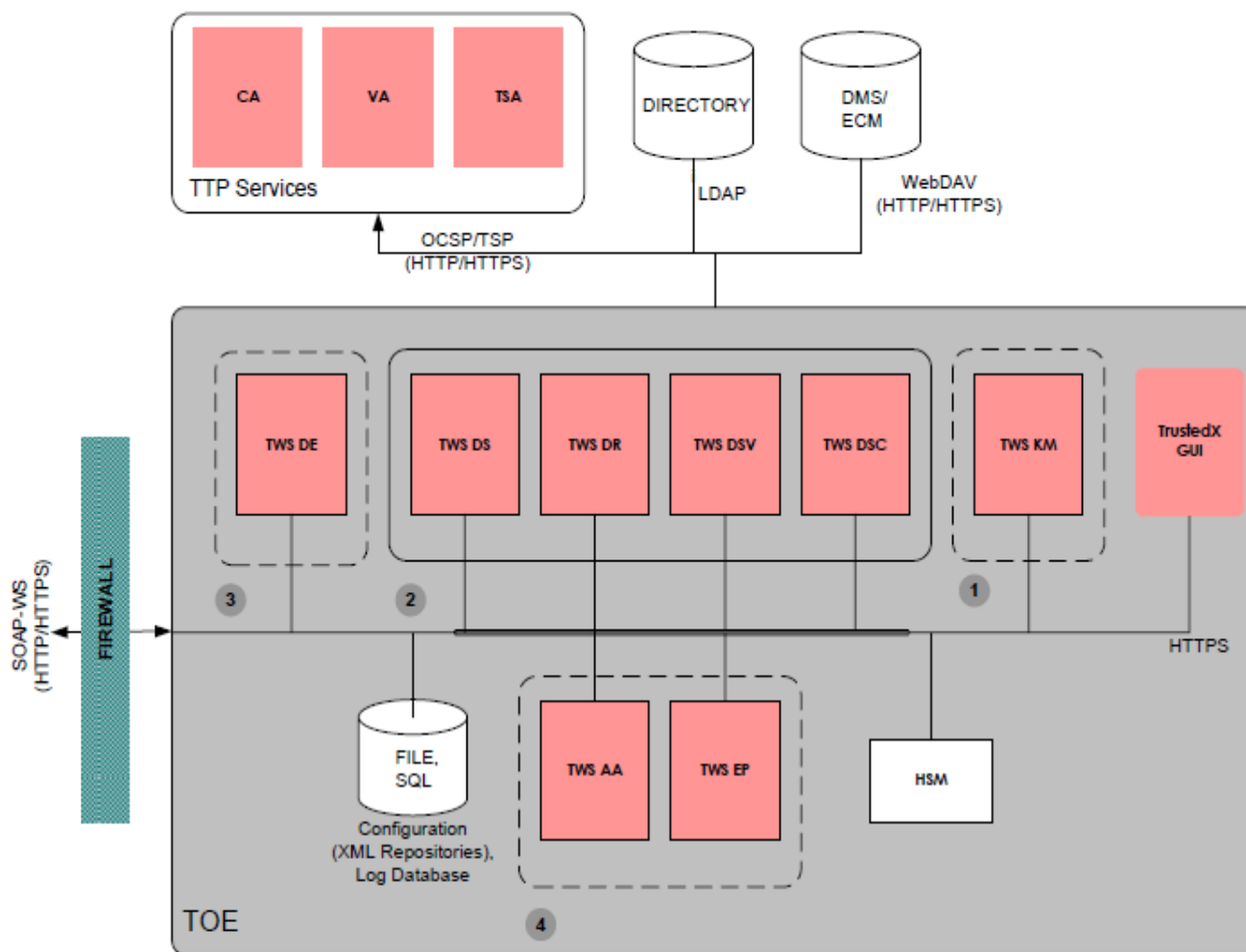
## TABLA DE NORMAS SEGÚN EL FORMATO DE FIRMA ELECTRONICA

<u>Formato</u>	<u>Versión</u>	<u>Estándar</u>	<u>Operaciones Soportadas</u>	
			<u>Generación</u>	<u>Validación</u>
PKCS#7	1.5	IETF RFC 2315	×	✓
	1 (06-1999)	IETF RFC 2630	×	✓
CMS	2 (08-2002)	IETF RFC 3369	×	✓
	3 (07-2004)	IETF RFC 3852	✓	✓
	1.6.3 (09-2005)	ETSI TS 101 733	×	✓
	1.7.3 (01- 2007)	ETSI TS 101 733	×	✓
CAdES	1.7.4 (07- 2008)	ETSI TS 101 733	×	✓
	1.8.1 (11-2009)	ETSI TS 101 733	×	✓
	1.8.3 (01-2001)	ETSI TS 101 733	✓	✓
XMLDSig	-	IETF RFC 3275	×	✓
	1.1.1 (02-2002)	ETSI TS 101 903	×	✓
	1.2.2 (04-2004)	ETSI TS 101 903	×	✓
XAdES	1.3.2 (03-2006)	ETSI TS 101 903	×	✓
	1.4.1 (06-2009)	ETSI TS 101 903	✓	✓
	1.4.2 (12-2010)	ETSI TS 101 903	✓	✓
PDF	1.4 o Superior	PDF, PDF/A(ISO19001)	✓	✓
	1.2.1 (07-2009)	ETSI TS 102 778-2	✓	✓
PAdES	1.1.2 (12-2009)	ETSI TS 102 778-3	✓	✓
	1.1.2 (12-2009)	ETSI TS 102 778-4	✓	✓
ODF	1.2 (draft)	OpenDocument 1.2	✓	✓

<u>Formato</u>	<u>Versión</u>	<u>Estándar</u>	<u>Generación</u>	<u>Validación</u>
OOXML	2 (2008)	ISO/IEC 29500:2008	✘	✓
CAdES Baseline	2.2.1 (04-2013)	ETSI TS 103 173	✓	✓
XAdES Baseline	2.1.1 (03-2012)	ETSI TS 103 171	✓	✓
PAdES Baseline	2.1.1 (03-2012)	ETSI TS 103 172	✓	✓
ASiC Baseline	2.1.1 (03-2012)	ETSI TS 103 174	✘	✓

## ANEXO H

**ARQUITECTURA GENERAL DE LA APLICACIÓN TRUSTEDX TOMADA DEL  
DOCUMENTO ORIGINAL DEL FABRICANTE**



1. Key Management
2. Digital certificate validation, advanced signature generation and verification and signature custody
3. Encryption and decryption
4. Entity Management, authentication and authorization

## ANEXO I

ARQUITECTURA GENERAL DE LA APLICACIÓN @FIRMA, TOMADA DEL  
DOCUMENTO ORIGINAL DEL DESARROLLADOR.

