

ORGANIZACIÓN LATINOAMERICANA Y DEL CARIBE DE ENTIDADES FISCALIZADORAS SUPERIORES (OLACEFS)

XXIX Asamblea General Ordinaria

Tema técnico 1: Aplicación y validez jurídica de firmas electrónicas y documentos electrónicos en el proceso de auditoría.

PROPUESTA INICIAL

EFS Coordinadora: Contraloría General del Estado de Ecuador

I. PRESENTACIÓN

El crecimiento exponencial del uso del internet, ha modificado las estructuras políticas, sociales, económicas, laborales y comunicacionales tradicionales; este fenómeno, hace imprescindible que las diversas actividades humanas armonicen y adecuen sus estructuras al compás de este vertiginoso desarrollo.

Este panorama no ha sido ajeno al ámbito de control de las Entidades Fiscalizadoras Superiores (EFS), debiendo asumir el reto de actualizarse tecnológicamente acorde a estos tiempos. Para ello, se ha vuelto imprescindible incorporar en sus labores el uso de las denominadas nuevas tecnologías o TIC (Tecnologías de la Información y la Comunicación), a fin de obtener eficiencia y calidad en armonía con el tiempo actual. En este contexto, la implementación de las TIC en las labores de revisión del uso de los recursos públicos; así como del patrimonio de los servidores públicos -como en el caso de Ecuador-, requiere un replanteamiento de legislación, de políticas y programas, que abandonen las viejas prácticas sustentadas en procedimientos que incluyen formalidades no indispensables, que a la óptica de la nueva conciencia digital, ocasionan la pérdida de tiempo y recursos tanto al sector gubernamental como a los propios administrados.

De igual manera, la aplicación de herramientas tecnológicas efectivas y dinámicas por parte de las EFS, conllevará al cumplimiento de sus objetivos en un lapso menor; así como también, el ahorro de recursos, a la vez que les permitirá estar preparadas para enfrentar los riesgos que suponen los avances tecnológicos.

Se debe resaltar el hecho de que el uso y empleo de las TIC, facilitará el acceso de los ciudadanos a las labores que desempeñan las entidades fiscalizadoras y le permitirán conocer con transparencia, cómo se realiza el cumplimiento de los objetivos en el control de los recursos públicos.

De esta manera, como resultado de la aplicación de las tecnologías de la información han surgido importantes herramientas como la firma electrónica y los documentos electrónicos, las cuales se vuelven de uso imprescindible para agilizar los procesos administrativos, de auditoría, comerciales etc.

No obstante, se puntualiza que, si bien la implementación de las Tecnologías de la Información y la Comunicación han tenido un innegable avance normativo, su aplicación aún se encuentra limitada en temas de infraestructura. Entonces, aunque existe ya un importante avance en la aplicación y validez jurídica de las firmas y documentos

electrónicas en los procesos de auditoría; queda aún mucho más por desarrollar en este campo; esto, constituye un reto para las Entidades Fiscalizadoras Superiores, que debe ser asumido con el fin de obtener la eficiencia y eficacia necesarias a fin de mejorar los procesos de control de los recursos públicos.

1.2 ANTECEDENTES

El 22 de octubre de 2009, en el marco de la XIX Asamblea General de la OLACEFS, se realizó la Declaración de Asunción sobre Principios de Rendición de Cuentas; los asistentes debido al reclamo de la sociedad civil por el escaso acceso a la información pública sobre la rendición de cuentas de las entidades gubernamentales; convinieron en incentivar el desarrollo de instrumentos y sistemas de información para facilitar el acceso a información pública al periodismo y la población en general a fin de obtener una efectiva política de rendición de cuentas.

Con este objetivo, entre el 31 de mayo y el 2 de julio de 2017, en la ciudad de Viena se desarrolló el 24º Simposio NU/INTOSAI *“sobre digitalización, datos abiertos y extracción de datos: relevancia e implicaciones para las auditorías de las EFS y para aumentar su contribución al seguimiento y la revisión de los ODS”*. Los participantes analizaron la relevancia y las implicaciones que tendrían el uso de la digitalización, los datos abiertos y la extracción de datos, en las auditorías efectuadas por Entidades Fiscalizadoras Superiores, y entre otras conclusiones y recomendaciones en las que convinieron, se pueden destacar la necesidad de que las Entidades Fiscalizadoras Superiores desarrollen de acuerdo con sus capacidades *“...nuevos métodos, herramientas y técnicas de auditoría e incorporarlos en su metodología de auditoría para aprovechar los análisis de datos para fines de auditoría y garantizar la calidad en el uso de datos abiertos...”*; así mismo, se las alentó a *“...desarrollar **estrategias externas** en el ámbito de la digitalización, los datos abiertos y la extracción de datos en materia de:*

- a. aspectos legales y especificaciones sobre la seguridad de datos;*
- b. cuestiones relativas a la evaluación y la garantía de la calidad de datos y el acceso a estos, en particular, por parte de los auditados, que puede ser permanente o solo en relación con casos concretos;*
- c. datos abiertos, en lo que atañe a
 - i. la cuestión de su uso como insumo para auditorías y*
 - ii. la medida en la que los datos de auditoría podrán ser publicados como datos abiertos a efectos de generar un beneficio adicional para la ciudadanía;**

También se alentó a las *“...EFS a que velen por que sus auditados implementen los “datos abiertos” y la digitalización y adopten medidas que garanticen su acceso a este tipo de datos, tanto para su análisis como para la elaboración de informes”*; recomendando a la *“...INTOSAI trabajar con las EFS y las Organizaciones Regionales de la INTOSAI en la medida en que sus mandatos se lo permitan, para alinear los esfuerzos de las EFS a efectos del mejor uso posible de la digitalización, los datos abiertos y la extracción de datos en sus auditorías”*.

Posteriormente; como respuesta al creciente desarrollo de las nuevas tecnologías; y su innegable presencia en todos los ámbitos y actividades actuales, en el marco de la XXVIII Asamblea General Ordinaria de la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS), realizada entre el 9 y 12 de octubre de 2018 en Buenos Aires, República Argentina, se suscribió la Declaración de Buenos Aires cuyo tema de discusión fue *“El Rol de las Entidades de Fiscalización Superior ante las Nuevas Tecnologías de la Información del Siglo XXI”*, que definió a las nuevas tecnologías *“...como aquellas técnicas de la informatización que permiten la adquisición,*

producción, almacenamiento, tratamiento, comunicación, registro y/o presentación de información en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética que en lo principal estableció:

- **Primero.** Que las nuevas tecnologías del siglo XXI constituyen una verdadera oportunidad para mejorar de manera efectiva la calidad del control público en cumplimiento de nuestros mandatos constitucionales y legales. Las EFS deben erigirse como instituciones modelo, lo que implica que deben estar inmersas en un proceso de mejora continua.

- **Segundo.** Que este entorno tecnológico avasallador, cambiante y universal, podría resultar altamente beneficioso para expandir las fronteras de los enfoques tradicionales de nuestras auditorías incorporando las TIC de una manera eficiente en todo el proceso (planificación, ejecución, informe y seguimiento).

- **Sexto.** Que entendemos de alto interés incorporar estos objetivos en la Estrategia de la OLACEFS (2017-2022) reforzando las Metas 4 y 5, impulsando tácticas que promuevan el uso de nuevas tecnologías en el control gubernamental, al mismo tiempo que se desarrollan nuevos medios educativos de la Región, especialmente tomando en cuenta las estrategias:

4.2 Promoción de buenas prácticas y herramientas para la mejora del desempeño de las EFS.

4.4 Promoción de los ODS a nivel regional y del papel de las EFS para la consecución de la Agenda 2030

5.3 Promoción de la Innovación Tecnológica y Pedagógica de las Acciones de Capacitación

Séptimo. Que nos comprometemos de manera indeclinable e irreversible a avanzar en el uso de las herramientas y las innovaciones que ellas nos proveen, convencidos de que es un camino que aportará confianza a la ciudadanía sobre la calidad, transparencia y oportunidad de nuestro trabajo. Ayudando a los destinatarios de nuestros informes en la toma de decisiones, cumpliendo con el principio 3 de la ISSAI 12, al proporcionar información relevante, objetiva y puntual a las partes interesadas.

Octavo. De forma paralela, asumimos el compromiso de fortalecer la infraestructura informática en materia de seguridad para hacer frente a las amenazas cibernéticas que enfrentan los sistemas externos e internos de las EFS lo que permitirá garantizar el principio básico de velar por la calidad de la información que se recibe y se produce como parte de las funciones del control.

1.3. Desarrollo del Tema

Una de las bases fundamentales para efectuar un proceso de modernización administrativa, con el fin de optimizar la gestión en labores gubernamentales del Estado consiste en la implementación de las denominadas TIC. Ciertamente, a través de su uso, se puede generar la apertura, transformación y transparencia de las actividades que realizan los organismos de control, para un acercamiento con la ciudadanía; además, de implantar la optimización de recursos, la despapelización y la digitalización de los procesos de trabajo.

El empleo de nuevas tecnologías puede aplicarse en la publicidad de las actividades desarrolladas por las EFS, poniendo al alcance de la mano de los ciudadanos los resultados de sus trabajos de fiscalización, transparentando sus acciones; las mismas que, serían percibidas como dignas de confianza, creíbles, competentes e

independientes; al contrario de la actualidad en la que este tipo de actividades se limitan al conocimiento exclusivo de los involucrados; además, información dotada de estas características facilita que se cualquier persona o colectivo, pueda exigir la rendición de cuentas a los responsables del mal manejo del erario público, marcándose así la modernidad.

La aplicación de nuevas tecnologías en el proceso de auditoría, hará del Control Interno un procedimiento integral y dinámico, que se adapte constantemente a los cambios que ocurran; y, en algunos casos, que incluso anticipe los conflictos involucrando a la Alta Dirección con el personal de todos los niveles jerárquicos comprometiéndolos en el proceso para enfrentarse a los posibles riesgos garantizando el logro de la misión de la institución y el cumplimiento de sus objetivos generales.

El crecimiento de la conectividad digital motiva a la ciudadanía a reclamar que los adelantos que la tecnología ofrece se incluyan también en los servicios de las Entidades Fiscalizadoras Superiores, que no son ajenos a la vertiginosa revolución tecnológica y sus aplicaciones. En consecuencia, las EFS ante su responsabilidad para con la ciudadanía se encuentran impelidas a incorporar las herramientas que las nuevas tecnologías ofrecen en su trabajo fiscalizador, esto es empleando herramientas como bases de datos, uso de imágenes de satélite, análisis de las evidencias en tiempo real, etc.

Así, el proceso de implementación de las nuevas tecnologías del siglo XXI en el trabajo auditor, constituye para las Entidades Fiscalizadoras Superiores una oportunidad que les permita armonizar con la modernidad y agilizar de manera efectiva la calidad del control público, cumpliendo sus mandatos constitucionales y legales, de acuerdo con los requerimientos de los nuevos tiempos; sin embargo, también se convierte en un reto que involucra contar con recursos económicos y talento humano capacitado.

1.3.1 LA FIRMA ELECTRÓNICA Y EL USO DE LA MISMA POR PARTE DE LA ADMINISTRACIÓN PÚBLICA.

1.3.1.1 Presentación.

Cabe puntualizar que la idea de la Firma Electrónica corresponde a un ámbito limitado, que tiene como referencia al más avanzado concepto denominado firma digital; que incluye a la criptografía, rama de las matemáticas, que utilizando fórmulas o algoritmos transforma mensajes ininteligibles a su forma original, siendo la criptografía asimétrica la empleada para crear firmas digitales a través de la utilización de claves.

Sin embargo; para continuar con el desarrollo del tema diremos que para su funcionamiento la Firma Electrónica necesita la utilización de certificados de Firma Electrónica y la intervención de una tercera parte de confianza, conocida como entidad de certificación.

1.3.1.2 Firma Electrónica

“Es un mecanismo electrónico mediante el cual se añaden ciertos códigos a un archivo electrónico para asegurarlo, de aquí, que las transacciones electrónicas deben garantizar a los usuarios principalmente seguridad y confianza, características que son propias de las firmas manuscritas y a las que deben responder las Firmas Electrónicas”.

Sobre éstas no hay un criterio único de denominación, es así como en ciertas normativas existentes sobre el tema como en el caso de Ecuador se habla de Firma Electrónica; en tanto que para la legislación argentina el término es Firma Digital. Por tanto, Firma

Electrónica sería una denominación genérica y tecnológicamente neutra que hace referencia al universo de métodos por los que se podría “firmar” un documento electrónico. Estas firmas podrían tomar diversas formas y ser creadas por medio de diferentes tecnologías. Serían entonces firmas electrónicas, por ejemplo, el nombre de una persona colocada al final de un correo electrónico, la imagen digitalizada de una firma manuscrita agregada a un documento electrónico, un código secreto o PIN, un identificador basado en un mecanismo biométrico.

En la legislación ecuatoriana, el artículo 13 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos señala que la Firma Electrónica *“Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos”*(subrayado fuera del texto).

Sobre el cuerpo legal precedente, es necesario precisar que fue promulgado el 17 de abril de 2002, teniendo como referencia la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico, aprobada mediante Resolución 51/162 de la Asamblea General el 16 de diciembre de 1996. Instrumento que se hizo necesario en respuesta al creciente número de operaciones comerciales por vías electrónicas, como lo explica Horacio Fernández Delpech: *“...fue una respuesta frente a las aplicaciones de las nuevas tecnologías a las relaciones comerciales, ofreciendo a los diferentes Estados un texto armónico y completo para la regulación de este tipo de actividades comerciales”* (2011, p. 277).

El artículo 7 Firma -nótese que no lleva la palabra electrónica- expresa:

“1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos...” (Subrayado fuera del texto).

Nótese que en los artículos citados se repiten dos elementos constitutivos de la firma electrónica, a) la identificación de la persona titular de la firma; y, b) la aprobación y reconocimiento de la información contenida en el mensaje de datos.

Ahora bien, el artículo 7, inciso segundo, determina que *“Se considera que un mensaje de datos permanece íntegro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación...”*; circunstancia concordante con lo establecido el artículo 6 del Reglamento *“Integridad de un mensaje de datos.- La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del artículo 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente (subrayado fuera del texto). [...] Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación...”*; como se observa la integridad del mensaje de datos se ve supeditada al requisito de que tal mensaje de datos se haya firmado electrónicamente, situación que sustenta que no ha sido adulterado y que permanece intacto.

Es conveniente también referirnos al principio de la *“equivalencia funcional”* que se refiere a que el contenido de un documento electrónico surte los mismos efectos que el contenido de un documento en soporte papel. En tal sentido, la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre

Comercio Electrónico en su artículo 5 Reconocimiento jurídico de los mensajes de datos manifiesta *“No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos”*. Cuando lo que se procura es lograr la optimización de recursos mediante la incorporación de herramientas tecnológicas, se considera indispensable dejar atrás el criterio de que solo la información que consta en un documento escrito agregado a un archivo manejado por un funcionario dotado de fe pública, puede sustentar una obligación legal o contractual. Este cambio de esquema ya se encuentra analizado en los párrafos 16 y 17 de la página 21 de la Guía de la Ley Modelo de la CNUMDI; así, se realiza la siguiente equivalencia entre el documento que consta por escrito y aquel que se encuentra contenido en un mensaje de datos *“...ese documento de papel cumple funciones como las siguientes: proporcionar un documento legible para todos; asegurar la inalterabilidad de un documento a lo largo del tiempo; permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito; permitir la autenticación de los datos consignados suscribiéndolos con una firma; y proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales”*.

Se observa que la costumbre, hace que el documento escrito por tradición sea el más aceptado; sin embargo, el desarrollo de nuevas tecnologías en todos los aspectos y actividades humanas abren espacios que tienden a facilitar los trámites y actualmente el documento electrónico cuenta con todos los elementos que podía brindar un documento escrito; y, brindar aún más beneficios que éste, como se explica en la Guía Ibídem *“...la documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente al del papel y, en la mayoría de los casos, mucha mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos, con tal que se observen ciertos requisitos técnicos y jurídicos”*.

El principio de neutralidad tecnológica según Cristina Cullel March supone *“...que la legislación debe definir los objetivos a conseguir sin imponer ni discriminar el uso de cualquier otro tipo de tecnología para conseguir los objetivos fijados”*, en el artículo 43 de la Ley Modelo CNUMDI, podemos encontrar menciones que se relacionan a este principio número 2) validar las operaciones efectuadas por medio de las nuevas tecnologías de la información; número 3) fomentar y estimular la aplicación de nuevas tecnologías de la información; y, número 5) apoyar las nuevas prácticas comerciales.

En el mismo sentido se expresa Héctor R. Peñaranda Quintero cuando manifiesta *“Utilizar el concepto electrónico para referirse a cualquier situación relacionada con las tecnologías de la información es impreciso, porque cuando se utiliza la expresión digital no se limita con ninguna tecnología específica, sino que es la manera convencional que se ha adoptado para tratar la información, independientemente de la tecnología de turno. Porque si los datos que viajan por redes de fibra óptica (tecnología de luz y no electrónica), se hace representar como 0 y 1, lo que sería digitalmente hablando un sistema binario, entonces no sería preciso denominar a dicha transmisión como una comunicación electrónica, sino digital. Lo digital puede ser introducido en cualquier tecnología, en el caso antes planteado podría ser una firma fibra óptica digital. De lo anterior se puede concluir que para generalizar y no ubicar y limitar a la firma digital en alguna tecnología, es preferible hablar de firma digital, y si se requiere más detalle con el nacimiento de nuevas tecnologías dentro de otras ciencias se podría hablar de firma electrónica digital, firma eléctrica digital, y así sucesivamente”*¹.

¹ La Firma Digital en Venezuela, Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas http://dx.doi.org/10.5209/rev_NOMA.2011.v29.n1.26828.

Entonces, parece más acertada la funcionalidad otorgada en la Unión Europea para la firma electrónica, su Reglamento (UE) N o 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 Relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, cuyos considerandos “(26) *En razón de la rápida evolución de la tecnología, el presente Reglamento debe adoptar un planteamiento abierto a innovaciones*”; y, “(27) *El presente Reglamento debe ser neutral en lo que se refiere a la tecnología. Los efectos jurídicos que otorga deben poder lograrse por cualquier medio técnico, siempre que se cumplan los requisitos que en él se estipulan*”, aclaran que la normativa debe ser abierta a fin de acoger innovaciones; circunstancias que obedecen al principio de neutralidad tecnológica.

La Unión Europea tiene tres tipos de Firmas Electrónicas.

La firma electrónica generalizada que consiste en “...*los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar*;

La firma electrónica avanzada, que es la firma electrónica que cumple los siguientes requisitos;

- a) *estar vinculada al firmante de manera única;*
- b) *permitir la identificación del firmante;*
- c) *haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y*
- d) *estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.*

La firma electrónica cualificada, que corresponde a la “...*firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica*”;

Los certificados cualificados de firma electrónica contendrán:

- a) *una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de firma electrónica;*
- b) *un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y -para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales, - para personas físicas, el nombre de la persona;*
- c) *al menos el nombre del firmante o un seudónimo; si se usara un seudónimo, se indicará claramente;*
- d) *datos de validación de la firma electrónica que correspondan a los datos de creación de la firma electrónica;*
- e) *los datos relativos al inicio y final del período de validez del certificado;*
- f) *el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;*
- g) *la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;*
- h) *el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);*
- i) *la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;*

j) cuando los datos de creación de firma electrónica relacionados con los datos de validación de firma electrónica se encuentren en un dispositivo cualificado de creación de firma electrónica, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

Podría ser recomendable desarrollar equivalentes funcionales para los distintos tipos y niveles de firmas requeridas existentes. Ese enfoque aumentaría el nivel de certidumbre en cuanto al grado de reconocimiento legal que podría esperarse del uso de los distintos tipos de autenticación utilizados en la práctica del comercio electrónico como sustitutos de la "firma". Sin embargo, la noción de firma está íntimamente vinculada con el empleo del papel. Además, cualquier esfuerzo por elaborar reglas sobre las normas y procedimientos que deberían utilizarse como sustitutos en casos específicos de "firmas" podría crear el riesgo de vincular irremisiblemente el régimen de la Ley Modelo a una determinada etapa del desarrollo técnico.

Entonces, se vuelve necesario que los miembros de la OLACEFS, previo a implementar la firma digital consideren aplicar el principio de equivalencia funcional, para evitar que en el futuro se configure necesidad constante de reformar sus cuerpos legales.

Es pertinente en este punto, observar el caso de la Ley 25.506 o Ley de Firma Digital promulgada por la República Argentina, en diciembre de 2001, cuyo artículo 1 señala:

"Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley".

De lo anterior se desprende que, la Ley de Firma Digital reconoce la eficacia jurídica y el empleo de la firma electrónica y de la firma digital; sin embargo, para sus efectos no las considera equivalentes; así, el artículo 5 Firma electrónica manifiesta:

"Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital (subrayado fuera del texto). En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez".

Consecuentemente, la naturaleza de la firma digital tiene un sentido más amplio, el artículo 2 Firma Digital sostiene:

"Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma".

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

Ahora bien, como quedó señalado anteriormente, la XXVIII Asamblea General Ordinaria de la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS) sobre "El Rol de las Entidades de Fiscalización Superior ante las Nuevas Tecnologías de la Información del Siglo XXI", se realizó en el mes de octubre de 2018, es lógico pensar que desde la primera definición de firma electrónica hasta la actualidad, al ritmo vertiginoso en el que se desarrolla la tecnología, hayan surgido

nuevos elementos que busquen prevenir la vulneración o el ataque a los datos; así como también, el desarrollo de nuevas tecnologías

1.4 Firma Electrónica, Documentos Electrónicos, aplicación en procesos de auditoría, caso ecuatoriano.

Las Constituciones de la República del Ecuador de 1998 y 2008, contemplaron la obligatoriedad de que los servidores públicos presenten declaraciones juradas, respecto al desempeño de sus gestiones; además, en las dos cartas magnas, se estableció la facultad auditora de la Entidad Fiscalizadora Superior.

La Constitución Política del Ecuador de 1998 en su artículo 122 disponía que *“Los funcionarios de libre nombramiento y remoción, los designados para período fijo, los que manejan recursos o bienes públicos y los ciudadanos elegidos por votación popular, deberán presentar, al inicio de su gestión, una declaración patrimonial jurada, que incluya activos y pasivos, y la autorización para que, de ser necesario, se levante el sigilo de sus cuentas bancarias. [...] Al terminar sus funciones presentarán también una declaración patrimonial jurada, que incluya igualmente activos y pasivos. La Contraloría General del Estado examinará las dos declaraciones e investigará los casos en que se presuma enriquecimiento ilícito. La falta de presentación de la declaración al término de las funciones hará presumir enriquecimiento ilícito. Cuando existan graves indicios de utilización de un testaferro, la Contraloría podrá solicitar declaraciones similares, a terceras personas vinculadas con quien ejerza o haya ejercido una función pública”*. Para la aplicación de esta disposición constitucional, se promulgó la Ley que Regula las Declaraciones Patrimoniales Juradas publicada en el Registro Oficial 83 el 16 de mayo de 2003, cuyo artículo 3 Contenido de la declaración establecía que *“La declaración patrimonial jurada se hará a través de escritura pública (subrayado fuera del texto) y contendrá información completa sobre el patrimonio, los activos y pasivos del declarante, en el país como el extranjero”*. De su lado el artículo 164 del Código de Procedimiento Civil definía al Instrumento público o auténtico *“...como el autorizado con las solemnidades legales por el competente empleado. Si fuere otorgado ante notario e incorporado en un protocolo o registro público, se llamará escritura pública (el subrayado fuera del texto)”. Se colige que, anteriormente, la declaración jurada que los servidores públicos presentaban ante la Entidad Fiscalizadora Superior, requería para su validez la formalidad de ser otorgada ante un Notario quien posteriormente la incorporaba a su protocolo.*

Posteriormente, según el artículo 4 ibídem, los servidores debían entregar Copias certificadas de las declaraciones patrimoniales juradas a la institución nominadora, a la matriz de la Contraloría General del Estado, o las direcciones regionales, o delegaciones provinciales, ocasionando que se triplique la documentación física Notaría-Entidad Fiscalizadora-Entidad Nominadora, llegando según datos de la nota periodística del diario El Universo <https://www.eluniverso.com/noticias/2017/01/01/nota/5976166/hoy-servidores-publicos-declararan-sus-bienes-linea>, a acumular 3 146 128 Declaraciones Juradas a nivel nacional al 1 de enero de 2017; sin mencionar el costo en que debían incurrir debido a que las declaraciones juradas tenían un valor económico.

La Constitución de la República del Ecuador promulgada en el Registro Oficial 449 de 20 de octubre de 2008 ratificó la obligación para los servidores públicos de presentar la declaración jurada de bienes; además, se establece la facultad de la Entidad Fiscalizadora Superior de auditar estas declaraciones como lo dispone el artículo 231.

Las servidoras y servidores públicos sin excepción presentarán, al iniciar y al finalizar su gestión y con la periodicidad que determine la ley, una declaración patrimonial jurada

que incluirá activos y pasivos, así como la autorización para que, de ser necesario, se levante el sigilo de sus cuentas bancarias; quienes incumplan este deber no podrán posesionarse en sus cargos. [...] La Contraloría General del Estado examinará y confrontará las declaraciones e investigará los casos en que se presuma enriquecimiento ilícito. La falta de presentación de la declaración al término de las funciones o la inconsistencia no justificada entre las declaraciones hará presumir enriquecimiento ilícito. Cuando existan graves indicios de testaferrismo, la Contraloría podrá solicitar declaraciones similares a terceras personas vinculadas con quien ejerza o haya ejercido una función pública”.

Posteriormente, con la figura de *vacatio legis*, en el Registro Oficial Suplemento 729 de 8 de abril de 2016 se publica la Ley Para la Presentación y Control de las Declaraciones Patrimoniales Juradas, que entró en vigencia el 1 de enero de 2017, este cuerpo normativo supone un adelanto sobre el uso de las tecnologías de la información, y el concepto de los mensajes de datos incorporados al control auditor.

En los siguientes artículos, se incluye la documentación electrónica al uso del trabajo de auditoría primero mediante el uso de la plataforma que facilita el Registro en línea señala el mecanismo por el cual *“El declarante ingresará la información de sus activos y pasivos mediante un formulario electrónico de declaración patrimonial jurada a través del sitio web de la Contraloría General del Estado”.*

Luego se ha dotado a las declaraciones juradas de valor y efectos jurídicos como se describe en el artículo 14:

“Valor y efectos jurídicos de las declaraciones electrónicas. Para todos los efectos jurídicos, las declaraciones patrimoniales juradas electrónicamente en línea otorgadas ante el Contralor General del Estado, como autoridad pública competente a través del sitio web de la Contraloría, son documentos públicos. Una vez efectuada la declaración en línea, se notificará al declarante con la constancia de la recepción de la declaración al domicilio electrónico por él señalado. Cuando el declarante requiera presentar ante terceros, o cuando una autoridad competente solicite”.

El artículo 205 del Código Orgánico General de Procesos refuerza la calidad de documento público de la declaración jurada *“Documento público. Es el autorizado con las solemnidades legales. Si es otorgado ante notario e incorporado en un protocolo o registro público, se llamará escritura pública”.*

Se resalta que la falsedad en los datos presentados en la declaración jurada acarrearía un quebrantamiento de tipo penal en los términos del artículo 270 del Código Orgánico Integral Penal que señala:

“Perjurio y falso testimonio. - La persona que, al declarar, confesar, informar o traducir ante o a (sic) autoridad competente, falte a la verdad bajo juramento, cometa perjurio, será sancionada con pena privativa de libertad de tres a cinco años; cuando lo hace sin juramento, cometa falso testimonio, será sancionada con pena privativa de libertad de uno a tres años”.

A este momento, mediante ACUERDO No. 14-CG-2019 se distribuye el control de las declaraciones juradas en todas las direcciones de auditoría a fin de auditar de una mejor manera la documentación electrónica *“Establézcanse funciones y atribuciones para que las Direcciones Nacionales de Auditoría, DNA1 a DNA8, planifiquen y ejecuten acciones de control a las declaraciones patrimoniales juradas, en el ámbito de su competencia.*

Sin embargo, es pertinente señalar que, si bien existe una sanción por el delito de perjurio, este no constituye el objeto principal del control de las declaraciones juradas, este lo constituye los Delitos contra la eficiencia de la administración pública, entre ellos:

Artículo 278 Peculado “*Las o los servidores públicos y las personas que actúen en virtud de una potestad estatal en alguna de las instituciones del Estado, determinadas en la Constitución de la República, en beneficio propio o de terceros; abusen, se apropien, distraigan o dispongan arbitrariamente de bienes muebles o inmuebles, dineros públicos o privados, efectos que los representen, piezas, títulos o documentos que estén en su poder en virtud o razón de su cargo, serán sancionados con pena privativa de libertad de diez a trece años. Si los sujetos descritos en el primer inciso utilizan, en beneficio propio o de terceras personas, trabajadores remunerados por el Estado o por las entidades del sector público o bienes del sector público, cuando esto signifique lucro o incremento patrimonial, serán sancionados con pena privativa de libertad de cinco a siete años. La misma pena se aplicará cuando los sujetos descritos en el primer inciso se aprovechen económicamente, en beneficio propio o de terceras personas, de estudios, proyectos, informes, resoluciones y más documentos, calificados de secretos, reservados o de circulación restringida, que estén o hayan estado en su conocimiento o bajo su dependencia en razón o con ocasión del cargo que ejercen o han ejercido. Son responsables de peculado las o los funcionarios o servidores públicos, las o los funcionarios, administradores, ejecutivos o empleados de las instituciones del Sistema Financiero Nacional que realicen actividades de intermediación financiera, así como los miembros o vocales de los directorios y de los consejos de administración y vigilancia de estas entidades, que con abuso de las funciones propias de su cargo: a) dispongan fraudulentamente, se apropien o distraigan los fondos, bienes, dineros o efectos privados que los representen; b) hubiesen ejecutado dolosamente operaciones que disminuyan el activo o incrementen el pasivo de la entidad; o, c) dispongan de cualquier manera el congelamiento o la retención arbitraria o generalizada de los fondos o depósitos en las instituciones del Sistema Financiero Nacional, causando directamente un perjuicio económico a sus socios, depositarios, cuenta partícipes o titulares de los bienes, fondos o dinero. En todos estos casos serán sancionados con pena privativa de libertad de diez a trece años. Si los sujetos descritos en el inciso precedente causan la quiebra fraudulenta de entidades del Sistema Financiero Nacional, serán sancionados con pena privativa de libertad de diez a trece años. La persona que obtenga o conceda créditos vinculados, relacionados o intercompañías, violando expresas disposiciones legales respecto de esta clase de operaciones, en perjuicio de la Institución Financiera, será sancionada con pena privativa de libertad de siete a diez años. La misma pena se aplicará a los beneficiarios que intervengan en el cometimiento de este ilícito y a la persona que preste su nombre para beneficio propio o de un tercero, aunque no posea las calidades previstas en el inciso anterior. Las o los sentenciados por las conductas previstas en este artículo quedarán incapacitadas o incapacitados de por vida, para el desempeño de todo cargo público, todo cargo en entidad financiera o en entidades de la economía popular y solidaria que realicen intermediación financiera”.*

Artículo 279 Enriquecimiento ilícito “*Las o los servidores públicos y las personas que actúen en virtud de una potestad estatal en alguna de las instituciones del Estado, determinadas en la Constitución de la República, que hayan obtenido para sí o para terceros un incremento patrimonial injustificado a su nombre o mediante persona interpuesta, producto de su cargo o función, superior a cuatrocientos salarios básicos unificados del trabajador en general, serán sancionados con pena privativa de libertad de siete a diez años. Se entenderá que hubo enriquecimiento ilícito no solo cuando el patrimonio se ha incrementado con dinero, cosas o bienes, sino también cuando se han cancelado deudas o extinguido obligaciones. Si el incremento del patrimonio es superior a doscientos y menor a cuatrocientos salarios básicos unificados del trabajador en general, la pena privativa de libertad será de cinco a siete años. Si el incremento del*

patrimonio es hasta doscientos salarios básicos unificados del trabajador en general, la pena privativa de libertad será de tres a cinco años”.

1.4.1 Declaraciones Patrimoniales Juradas

Reglamento Sustitutivo para la Declaración, Presentación y Registro de las Declaraciones Patrimoniales Juradas, otorgadas Electrónicamente a Través de la página web de la Contraloría General del Estado (Acuerdo No. 005-CG-2019).

Como se explicó ut supra la facultad constitucional para realizar la auditoría a las declaraciones juradas de los servidores públicos por parte de la Entidad Fiscalizadora Superior, se encuentra prevista en el artículo 231.

Cabe aclarar que el proceso de auditoría consta de dos fases plenamente determinadas como lo establece en su dictamen vinculante la Procuraduría General del Estado, como consta a continuación:

“Es decir que, se trata de un procedimiento que la reforma introducida por el Código Orgánico Integral Penal ha dividido en dos fases claramente diferenciadas, la de sustanciación y la de aprobación, que se deben desarrollar una después de la otra, estableciendo un período de tiempo específico e improrrogable para cada una de ellas. Por lo expuesto en atención a los términos de su segunda consulta se concluye que, el término de treinta días que establece la parte final del artículo 26 reformado de la Ley Orgánica de la Contraloría General del Estado, para que el informe de auditoría sea aprobado por parte del Contralor General del Estado o su Delegado, se debe contar desde que el informe de auditoría, suscrito por el director de la unidad administrativa respectiva, haya sido puesto en conocimiento del Contralor General del Estado o su delegado.”:

El hecho de que las declaraciones juradas sean objeto de revisión por cualquier ciudadano o incluso por las entidades de control facilita que puedan denunciar un supuesto incremento de patrimonio, al observar movimientos inusuales respecto a la adquisición de bienes, vehículos, maquinaria.

La Ley para la Presentación y Control de las Declaraciones Patrimoniales Juradas promulgada en el Registro Oficial Suplemento 729 de 8 de abril de 2016, tomo un giro innovador al aprovechar la coyuntura para implementar el uso de documentos electrónicos, en detrimento de la documentación tradicional que exigía una declaración jurada rendida por el servidor público ante un Notario; es decir, una escritura pública suscrita en papel incorporada posteriormente a un protocolo.

Este cuerpo legal supuso para la Entidad Fiscalizadora Superior un reto y a la vez una oportunidad, el desafío de desarrollar una plataforma que soporte las declaraciones juradas de todos los servidores públicos a nivel nacional; la puesta en línea de una página institucional que además de brindar un servicio, asegure la integridad e invulnerabilidad y sigilo de los datos consignados; a la par que contribuya a mejorar la comunicación e interacción entre la sociedad y el organismo de control para la salvaguardia y control de los recursos públicos con transparencia.

En tal virtud, mediante Acuerdo 040-CGE-2016 publicado en el Registro Oficial Suplemento 913 de 30 de diciembre de 2016 la Entidad Fiscalizadora Superior expidió el Instructivo de Registro y Uso de Medios o Servicios Electrónicos que Brinda la Contraloría General del Estado, cuyo artículo 2 manifiesta:

De los "Servicios en Línea" de la Contraloría General del Estado.- La Contraloría General del Estado a través de su página web institucional y conforme sus facultades constitucionales y legales, brinda "Servicios en Línea", que consisten en aplicativos informáticos regulados mediante normativa expedida por la entidad de control, para el desarrollo de trámites tanto de personas naturales: ingreso de declaraciones patrimoniales juradas, obtención del reporte de la información personal que consta registrada en la base de datos institucional, generación del informativo de caución; así como, para personas jurídicas: emisión de órdenes de movilización y aplicativos de validación. En la opción "Servicios en Línea" de la página web de la Contraloría General del Estado, constarán los medios o servicios electrónicos de uso público, emitidos mediante acto normativo emitido por la entidad de control".

Como se observa, la entidad de control impulsó el desarrollo de su plataforma tecnológica armonizada con el requerimiento legal derivado de la Ley de Declaración Patrimonial.

Como norma adjetiva, mediante Acuerdo 005-CG-2019, publicado en el Registro Oficial Suplemento 423 de 07 de febrero de 2019, el Contralor General del Estado, expide el Reglamento Sustitutivo para la Declaración, Presentación y Registro de las Declaraciones Patrimoniales Juradas, Otorgadas Electrónicamente a Través de la Pagina Web de la Contraloría General del Estado cuyo ámbito de aplicación abarca según lo señala el artículo 2:

"Ámbito de aplicación.- El presente Reglamento rige para todos los servidores/as públicos/as a los que se refieren los artículos 229 y 231 de la Constitución de la República, y los artículos 2 y 3 de la Ley para la Presentación y Control de las Declaraciones Patrimoniales Juradas, que en cualquier forma o a cualquier título, trabajen, presten servicios o ejerzan un cargo, función o dignidad dentro del sector público y ex servidores/as, que deben realizar su declaración de fin de gestión dentro de los veinte días siguientes al cese".

De su lado, los artículos 3 y 4 detallan que las declaraciones patrimoniales juradas de inicio de gestión, periódicas y/o declaración de fin de la gestión se formularan por el declarante a través link "Servicios en Línea " opción "persona natural" dentro de la página web de la Contraloría General del Estado www.contraloria.gob.ec, con su respectivo usuario y contraseña.

El Registro de la declaración patrimonial jurada electrónica se hará utilizando el formulario electrónico diseñado para el efecto, el mismo que hace plena referencia a lo dispuesto en el artículo 14 de la Ley para la Presentación y Control de las Declaraciones Patrimoniales Juradas que otorga la solemnidad de documento público *"Valor y efectos jurídicos de las declaraciones electrónicas. Para todos los efectos jurídicos, las declaraciones patrimoniales juradas electrónicamente en línea otorgadas ante el Contralor General del Estado, como autoridad pública competente a través del sitio web de la Contraloría, son documentos públicos"*; el formato de la declaración jurada cita esta disposición legal al expresar *:El declarante se responsabiliza por toda la información registrada en el sistema de manera irregular y responderá con todos los efectos jurídicos que de ella se desprenda, por tratarse de un documento público otorgado electrónicamente, ante la autoridad pública competente, esto es, el Contralor General del Estado.*

Como se colige, se ha tenido la prolijidad de resaltar el concepto y la cualidad de documento público de la declaración jurada para otorgar su validez procesal.

1.4.2 Proceso de Auditoría

Reglamento para las Notificaciones que la Contraloría General del Estado efectúa a través de Medios Electrónicos de sus Actuaciones y Actos Administrativos

Así también, se tienen normado las notificaciones por medios electrónicos, a través de Acuerdo 009-CG-2019 Registro Oficial Suplemento 456 de 28 de marzo de 2019, donde consta:

“ Regular el procedimiento para las notificaciones que la Contraloría General del Estado efectúa por medios electrónicos, a través de sus diferentes unidades administrativas dentro de los procedimientos de auditoría y control de recursos públicos, predeterminación de responsabilidades, determinación de responsabilidades, recursos de revisión y procesos de ejecución coactiva; así como establecer las condiciones y requisitos que, para estos efectos, deberán reunir las direcciones de correo electrónico proporcionadas al Organismo Técnico de Control y/o las casillas electrónicas correspondientes a los administrados, sujetos de control, sujetos de responsabilidad, coactivados y abogados patrocinadores.”.

Se define la Notificación electrónica como: *“el procedimiento mediante el cual se comunica a la o las personas relacionadas, el contenido de las actuaciones y actos administrativos que les conciernen, por medios y mecanismos electrónicos y digitales, a efectos de que estén en condiciones de ejercer los derechos y garantías de las que se consideren asistidas”*

Además, en su artículo 5.- Determinación del lugar de notificación electrónica indica:

“Toda persona que actúe o comparezca dentro de cualquier procedimiento administrativo cuya ejecución sea competencia de la Contraloría General del Estado, determinará el lugar en la que será notificada, debiendo consignar:

- 1. Una dirección de correo electrónico habilitada; y/o,*
- 2. Una casilla electrónica habilitada.*

Si la persona interesada no compareciere, ni hubiere fijado su lugar de notificación de conformidad con este artículo, se dejará constancia del particular y se continuará regularmente con el procedimiento administrativo, practicando las notificaciones en la casilla electrónica o en las direcciones de correo electrónico que consten registradas en la base de datos de las declaraciones patrimoniales juradas, o en otros documentos y archivos institucionales.”

Estas disposiciones podrían ser aplicable en diferentes etapas de la auditoría como:

1. Etapa de planificación cuando se notifica el inicio de la acción de control.
2. Etapa de comunicación de resultados cuando se comunican resultados provisionales, y se convoca a la lectura de borrador de informe.
3. En la etapa posterior a la del borrador de informe cuando solicitan los administrados el borrador de informe.

1.5 Terminología y conceptos técnicos

1.5.1 La criptografía

Se define la criptografía como “*la ciencia que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlos a su forma original*”². De otra parte, la etimología del término *cripto* en griego significa *oculto*. Por lo expuesto, se puede concluir: que la criptografía en un significado amplio es aquella que, utilizando fórmulas o algoritmos, transforma mensajes en forma aparentemente ininteligibles a su forma original.

Es necesario indicar que la firma digital viene a constituirse en una especie de Firma Electrónica, al respecto, al respecto Oliver Hance expresa: “*la criptografía también puede emplearse para crear firmas digitales, para autenticar mensajes electrónicos y para verificar su integridad (esto es: los mensajes se recibieron en la misma forma en que se enviaron y provienen de la fuente indicada), lo que en el contexto de los negocios electrónicos resulta de vital importancia.*”³

Para este trabajo se debe considerar los siguientes tipos de criptografía, la simétrica de una sola clave, y la asimétrica o de clave pública, que se maneja con dos claves diferentes pero matemáticamente relacionadas entre sí, lo anterior en base a grandes números producidos utilizando una serie de fórmulas matemáticas aplicadas a números primos, sin embargo, la criptografía de clave pública no necesariamente podría utilizar algoritmos, en la actualidad se están utilizando o desarrollando otras técnicas matemáticas, que se suelen describir como sistemas que ofrecen un alto grado de seguridad mediante el empleo de longitudes de clave notablemente reducidas, es así, como estas nuevas técnicas ofrecen más seguridad a las claves y por ende a la firma digital.

La criptografía simétrica como explica Miguel Dávora es aquella en la que: “*se utiliza la misma clave para cifrar y para descifrar los datos, con lo que ambas partes, emisor y receptor, deben conocer la clave (uno para cifrar y otro para descifrar), teniendo que basar sus relaciones en cuestiones de total y absoluta confianza, ya que, para que exista seguridad, la clave debe permanecer secreta y uno debe confiar en que el otro no la da a conocer a nadie y viceversa*”⁴, como se explica, las dos partes u operadores comparten una clave secreta por medio de la cual es posible cifrar y descifrar el mensaje.

La criptografía asimétrica en cambio, se basa en que cada uno de los operadores tiene dos claves; una privada que sólo él conoce, y una pública que conocen o pueden conocer todos los que intervienen en el tráfico electrónico, clave que incluso puede constar en un directorio público, para comprender mejor lo anotado, citemos a Rafael Mateu De Ros que explica: “*Cuando el operador A quiere enviar un mensaje electrónico aplica al mismo su clave privada y el mensaje así cifrado se envía a B, que al recibir el mensaje le aplica la clave pública de A para obtener el mensaje descifrado.*”⁵. Este último sistema tiene la ventaja de generar confidencialidad en el envío de mensajes a través de canales inseguros como son las redes abiertas Internet, así como también, permite crear las firmas digitales, dotando a los mensajes de datos de autenticidad, integridad y no rechazo de origen, que son las condiciones básicas de las firmas digitales.

De acuerdo a como se concibe a la Firma Electrónica en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, debemos tener presente a la criptografía asimétrica, la cual cumple un papel importante en nuestra normativa, sin embargo,

² Apol L. Martínez, *Comercio Electrónico, Firma digital y Autoridades de Certificación*, Madrid, p. 45.

³ Oliver Hance, *Leyes y Negocios en Internet*, México, Mc Graw - Hill., 1997, p. 180.

⁴ Miguel Dávora A., *Firma Electrónica y Autoridades de Certificación: El Notario Electrónico*, en: *Problemática Jurídica en Torno al Fenómeno de Internet*, Madrid – España, Lerko Print S.A., p. 421.

⁵ Rafael Mateu de Ros, *Derecho de Internet, Comercio Electrónico y Firma Digital*, Navarra, Editorial Arazandi, S.A., 1ra ed., 2000, p. 182.

podrían presentarse a futuro nuevas especies de Firma Electrónica para lo cual el artículo 10 del Reglamento a la Ley contempla la neutralidad tecnológica.

1.5.2 Claves públicas y claves privadas

Habiendo hecho alusión a la criptografía, queda claro que para su función de cifrado y descifrado hace uso de claves, y que estas pueden ser públicas y privadas, particularmente en la criptografía asimétrica que es con la que se construye la firma digital. En relación a las claves Mauricio Devotolas describe como: *“Las claves complementarias utilizadas para las firmas digitales se denominan “claves privadas”, que se utiliza para firmar digitalmente, mediante un dispositivo de creación de firma digital en un criptosistema asimétrico seguro, y la “clave pública”, que de ordinario conocen más personas y se utiliza para que el tercero que actúa confiando en el certificado pueda verificar la firma digital”*. La clave pública es aquella que es conocida tanto por el emisor como por el receptor, es decir, por las dos partes implicadas en la transacción, lo cual no es garantía para la integridad y autenticidad del mensaje. Mientras que la clave privada es exclusivamente conocida por el emisor, lo cual sí garantiza su integridad y autenticidad, tanto como la identidad de su autor.

Es importante mencionar, que las claves públicas son una combinación de letras, números o combinaciones de estos, es decir, que una clave puede ser incluso nuestro nombre, para que sea fácil de identificar y ser conocido por los usuarios; mientras que la clave privada es una extensa combinación de símbolos gráficos de difícil memorización, este tipo de clave puede estar plasmada en un soporte magnético, al que se le puede agregar un PIN o un número de identificación personal esta clave puede incluirse en una tarjeta magnética como la de los cajeros de los bancos, al respecto se presenta el siguiente comentario: *“Las claves no son otra cosa que una combinación de letras y números, es decir, un conjunto de bits, que a su vez constituyen un conjunto de ceros y unos. La creación de una firma digital implica combinar los caracteres que conforman la clave privada del usuario con los caracteres del documento o información al que se desea firmar.”*⁶

Para concluir el presente tema, debemos subrayar que las claves públicas y privadas son técnicas utilizadas en la criptografía asimétrica, que es con la que se crea la firma digital o también llamada de clave pública, mecanismo de autenticación que en la actualidad se constituye como el más seguro dentro de lo que es la Firma Electrónica, siendo también contemplado en las normativas existentes en el tema, incluida la Ley de Comercio Electrónico del Ecuador.

1.5.3 Diferencias entre la Firma Electrónica y la firma digital

1.5.3.1 Firma Electrónica

Por Firma Electrónica se entiende: *“Es un mecanismo electrónico mediante el cual se añaden ciertos códigos a un archivo electrónico para asegurarlo”*⁷, de aquí, que las transacciones electrónicas deben garantizar a los usuarios principalmente seguridad y confianza, características que son propias de las firmas manuscritas y a las que deben responder las Firmas Electrónicas.

Sobre éstas no hay un criterio único de denominación, es así como en las normativas existentes sobre el tema se habla de Firma Electrónica, firma digital y firma electrónica

⁶ Rafael Mateu de Ros, *Derecho de Internet, Comercio Electrónico y Firma Digital*, Navarra, Editorial Arazandi, S.A., 1ra ed., 2000, p. 205.

⁷ *El ABZ de las Firmas Electrónicas*, www.corpece.org.ec/informante

avanzada; *El término Firma Electrónica sería un término genérico y tecnológicamente neutro, y haría referencia al universo de métodos por los que se podría “firmar” un documento electrónico. Estas firmas podrían tomar diversas formas y ser creadas por medio de diferentes tecnologías. Serían firmas electrónicas, por ejemplo, el nombre de una persona colocada al final de un correo electrónico, la imagen digitalizada de una firma manuscrita agregada a un documento electrónico, un código secreto o PIN, un identificador basado en un mecanismo biométrico, y, finalmente, una firma digital creada por medio del uso de criptografía de clave pública.*⁸

La Firma Electrónica como se encuentra definida en la mayor parte de las normativas del mundo es un término genérico, por lo cual también se contempla dentro de éstas a la firma digital, así cuando se define la Firma Electrónica se hace en un sentido de neutralidad tecnológica, que permite anticiparse al avance de la tecnología donde podrían presentarse otro tipo de firmas que no sean la firma digital o de clave pública.

1.5.3.2 Firma digital

La firma digital es aquella que se basa en el uso de la criptografía asimétrica que es una especie de Firma Electrónica caracterizada por agregar elementos de seguridad que la Firma Electrónica no posee, esto lo corrobora José Manuel Villar al expresar: *“ello es así porque la firma digital cumple, en relación con los documentos electrónicos, las principales funciones que se atribuyen a la firma manuscrita sobre un documento en papel; a saber, permite identificar al autor del escrito autenticación y constatar que el mensaje no ha sido alterado después de su firma integridad”.*⁹

Otra característica de la firma digital es que da lugar al no rechazo o no repudio, es decir, que las partes que intervienen no pueden negar su actuación y, finalmente es garantía de confidencialidad; esto se traduce en ciertos servicios que están contemplados en las normativas sobre el tema y que protegen los datos al acceso de terceros no autorizados, pero desde ya podemos decir que específicamente se refiere al certificado de Firma Electrónica y entidades de certificación que se encuentran regulados en la Ley de Comercio Electrónico ecuatoriana.

Además, se debe indicar que en normativas como de la Unión Europea y de los Estados Unidos de Norteamérica, las Firmas Electrónicas tienen otra concepción en cuanto a su clasificación, concibiéndolas como Firmas Electrónicas y firmas electrónicas avanzadas; en relación a las Firmas Electrónicas avanzadas, consideramos que éstas son equiparables a la firma digital, además se puede decir que a pesar de que ciertas normativas la conciben así, indirectamente mantienen vigentes a las firmas electrónicas, aduciendo una neutralidad tecnológica, y argumentando que con el avance de la tecnología podrían presentarse otro tipo de Firmas Electrónicas que garanticen más seguridad que la firma digital.

La distinción que entre los dos tipos de firma hace Ricardo Lorenzetti: *“La gran diferencia estriba en que cuando se utilice la firma digital, se aplican presunciones juris tantum sobre la identidad del firmante y la identidad del documento que suscriba.”*¹⁰ Para concluir, podemos decir que la firma digital basada en la criptografía asimétrica, por el momento constituye el sistema más seguro y un paso fundamental para el comercio electrónico.

⁸ Mauricio Devoto, *op. cit* p. 166.

⁹ José Manuel Villar, *Una aproximación a la Firma Electrónica*, en Rafael Mateu De Ros, *Derecho de Internet, Contratación Electrónica y Firma Digital*, Navarra, Editorial Aranzadi, S.A., p.170.

¹⁰ Ricardo L. Lorenzetti, *Comercio Electrónico*, Buenos Aires, Ediciones Abeledo - Perrot, p. 8.