# LOS PRESTADORES DE SERVICIOS DE CONFIANZA:

# IDENTIFICACION ELECTRÓNICA Y

# FIRMA ELECTRÓNICA CON CONTROL CENTRALIZADO

**Dra. Esc. María José Viega**

## 1. INTRODUCCIÓN

Por el artículo 28 de la Ley N° 19.535 de 25 de setiembre de 2017, se incorporaron los artículos 31 a 33 a la Ley N° 18.600 de 21 de setiembre de 2009, que regula a los prestadores de servicios de confianza, concretamente los de identificación digital y firma electrónica avanzada con custodia centralizada. El 19 de marzo de 2018 el Poder Ejecutivo aprobó el Decreto N° 70/018 reglamentario de los mencionados artículos.

La Ley N° 18.600 ha permitido el uso generalizado de la firma electrónica en nuestro país, conteniendo nuestro documento de identidad una firma electrónica avanzada. De acuerdo con la normativa, es necesario que la persona cuente con un dispositivo físico que contenga el certificado electrónico (como por ejemplo: token, tarjeta o cédula de identidad electrónica), así como, la utilización de una computadora o lector que pueda leer dicha firma.

Las firmas electrónicas con custodia centralizada (custodia de los certificados en servidores accesibles vía Internet, conocidas como firma electrónica en la nube) supone que los certificados de firma electrónica se alojan en un tercero que tiene su custodia.

Esto permite implementar soluciones de firma electrónica avanzada en dispositivos de uso masivo, como pueden ser smartphones o tablets, lo que permite la flexibilización de su uso, por ejemplo para realizar un trámite completamente en línea o consumir servicios que se brinden a través de Internet, de manera confiable.

Por otra parte, se reconoce legalmente el concepto de Identificación Electrónica y se le otorga respaldo jurídico para su equivalencia frente a la identificación presencial.

Tratándose de un tema tan reciente y práctico, nos ha parecido relevante realizar el presente trabajo, siendo conscientes que aún quedan aspectos por definir, en los cuales se viene trabajando, a los efectos de la aprobación de las respectivas políticas. Estas permitirán que el ecosistema entre en funcionamiento. Pero con este planteo inicial es posible entender cuáles son los presupuestos y requisitos y cómo funcionará el sistema una vez implementado, lo cual se cree que sucederá en los próximos meses.

## 2. ANTECEDENTE: LA LEY N° 18.600

Desde la aprobación de la Ley Nº 16.002 de fecha 25 de noviembre de 1988, en sus artículos 129 y 130 se encuentra regulada la autenticidad y prueba de los documentos trasmitidos a distancia por medios electrónicos entre dependencias oficiales. A partir de ese año existió en nuestro país normativa regulando tanto el documento como la firma electrónica y digital, como se las denominaba en esa etapa.

El 21 de setiembre de 2009 se aprueba la Ley N° 18.600 que establece el régimen jurídico del documento y la firma electrónicos, regulación que reconoce, desde su artículo primero, la admisibilidad, validez y eficacia jurídica del documento y la firma electrónicos.

Desde el punto de vista estructural la Ley cuenta con 30 artículos distribuidos en seis capítulos denominados:

Capítulo I - Disposiciones Generales (arts. 1 – 10)

Capítulo II – Infraestructura Nacional de Certificación Electrónica (arts. 11 a 15)

Capítulo III – Prestadores de Servicios de Certificación Acreditados (arts. 16 a 20)

Capítulo IV - Certificados reconocidos (arts. 21 a 24)

Capítulo V - Firmante o signatario (arts. 25 a 27)

Capítulo VI - Disposiciones finales (arts. 28 a 30)

De acuerdo con la Ley N° 18.600 la firma electrónica puede consistir en usuario y contraseña, datos biométricos o criptografía asimétrica, proporcionando un concepto amplio de ésta.

Y consagra la firma electrónica avanzada, definiéndola como: "*la firma electrónica que cumple los siguientes requisitos:*

*1) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;*

*2) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;*

*3) ser susceptible de verificación por terceros;*

*4) estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detestable; y*

*5) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma"*.

La firma electrónica avanzada refiere a criptografía asimétrica, específicamente cuando el certificado electrónico es reconocido, por lo tanto es expedido por un prestador de servicios

de certificación acreditado. Cuando el prestador no se encuentra acreditado, el certificado electrónico constituye una firma electrónica común.

## 3. PRESTADORES DE SERVICIOS DE CONFIANZA

Como antecedente en nuestro país podemos mencionar el Proyecto de ley remitido al Parlamento por el Poder Ejecutivo con fecha 3 de agosto de 2017, regulando la firma electrónica avanzada con control centralizado, o también llamada firma en nube y a los prestadores de servicios de confianza. Este proyecto perdió interés con la aprobación del artículo 28 de la Ley N° 19.535, al que ya hemos hecho referencia.

De acuerdo al Decreto reglamentario N° 70/018, artículo 3 literal f), son servicios de confianza: "*los servicios electrónicos que permiten brindar seguridad jurídica a los hechos, actos y negocios realizados por medios electrónicos, entre ellos:*

a) *servicios de firma electrónica avanzada con custodia centralizada;*

b) *servicios de identificación digital;*

c) *servicios de sellado de tiempo;*

d) *otros servicios establecidos por la Unidad de Certificación Electrónica*".

Como surge del título del presente trabajo, el análisis corresponde a los dos primeros, en virtud a que los servicios de sellado de tiempo ya se encontraban regulados en la Ley N° 18.600 y en su decreto reglamentario, pudiendo acreditarse en este servicio los prestadores de servicios de certificación que se encuentran acreditados, lo cual no ha sucedido hasta el momento.

En base a la nueva normativa, quienes tengan interés en brindar servicios de sellado de tiempo podrían también acreditarse como prestadores de servicios de confianza, para ello será necesario el dictado de una política que establezca las condiciones de esa acreditación, en virtud a que el Decreto solamente establece la posibilidad pero no los regula.

El literal d) es residual, dejando la norma abierta a servicios que puedan surgir en el futuro y que se deseen acreditar o controlar.

### 3.1 El Reglamento UE 910/014 de 23 de julio de 2014

Los prestadores de servicios electrónicos de confianza se encuentran regulados en la Unión Europea en el Reglamento UE 910/014 de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS), que derogó la Directiva 1999/93/CE y entró en vigencia el 1 de julio de 2016.

Pedro Canut plantea que: "…la gran novedad de este Reglamento es el reconocimiento de los Servicios de Confianza y los Servicios Cualificados de Confianza, además de la regulación de la firma electrónica (para personas físicas) y el sello electrónico (para personas jurídicas).

Efectivamente, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica se ocupaba exclusivamente de la regulación de la firma electrónica y los prestadores de servicios de certificación basados en certificados reconocidos, en tanto que el Reglamento eIDAS contempla y regula asimismo los servicios de confianza consistentes en la entrega electrónica certificada, la certificación de sitios web, los servicios de sellado de tiempo y los servicios relativos a los documentos electrónicos; servicios éstos que, sin sustento en la Directiva 1999/93/CE, de 13 de diciembre, ni en la legislación nacional (Ley 59/2003, de 19 de diciembre, de firma electrónica) ya contaban, en España, con la cobertura del órgano de supervisión que, con una interpretación amplia de la Ley 59/2003, de 19 de diciembre, venía admitiendo las comunicaciones realizadas por prestadores de servicios que se dedicaban a otros servicios relacionados con la firma electrónica pero distintos a la generación de certificados de firma electrónica reconocida". (CANUT, Pedro J. "El Prestador Cualificado de Servicios de Confianza – Seguridad Jurídica en Internet").

De acuerdo a lo establecido en el Reglamento podemos decir que el servicio de confianza, es el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o

b) la creación, verificación y validación de certificados para la autenticación de sitios web, o

c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

Una distinción relevante en orden a los efectos jurídicos de un servicio de confianza y un servicio de confianza cualificado es que sólo una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita. La firma electrónica no cualificada de acuerdo a lo dispuesto en el párrafo 1 del artículo 25, no se le denegará efectos jurídicos ni admisibilidad como prueba en juicio.

Y el artículo 35 del Reglamento dispone que a los sellos electrónicos (para persona jurídica) no se les negará efectos jurídicos ni admisibilidad de prueba en juicio, aunque solo los sellos electrónicos cualificados disfrutarán de la presunción de integridad y corrección del origen de los datos a los que el sello esté vinculado.

A partir de julio de 2016, es obligatoria la exigencia de una cualificación administrativa a quienes deseen prestar servicios de confianza cualificados, según lo establece el artículo 21.1 del Reglamento. (…) Corresponde al organismo de supervisión verificar el

cumplimiento de los requisitos y decidir, sobre la base de esta verificación, si otorga o no la cualificación al prestador de servicios de confianza y a los servicios que éste prestará. (RICO CARRILLO, Mariliana. "La entrada en vigencia de la regulación europea sobre servicios de confianza y su impacto en el comercio electrónico". Actas del XX Congreso iberoamericano de Derecho e Informática. Salamanca – España, 2016. Página 421).

En el Capítulo II del Reglamento se regula la identificación electrónica y la define en el artículo 3° numeral 1) como el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.

Se conceptualizan los datos de identificación de la persona como el conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica.

También se define autenticación como el proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.

El objetivo del Reglamento con carácter general es la confianza en las transacciones electrónicas. Si bien se han realizado esfuerzos proteccionistas, las estafas a través de Internet son una realidad.

### 3.2 La normativa uruguaya

En nuestro país la Ley N° 18.600 establece en el artículo 2° lit. k) como uno de los requisitos de la Firma Electrónica Avanzada: "*haber sido creada utilizando un dispositivo de creación de firma técnicamente segura y confiable*…" y en el artículo 6° lit. C) garanticen que ha sido creada usando medios que el signatario mantiene bajo su exclusivo control.

La firma en nube o firma con control centralizado es cuando los dispositivos de creación de firma se alojan en un tercero denominado proveedor de servicios de confianza, su acceso se produce mediante factores de autenticación y el proveedor custodia el par de claves en instalaciones accesibles (la nube) y controla su acceso.

La firma en la nube no cumple con los dos requisitos establecidos en la ley. Por lo tanto, fue necesaria la ampliación de la norma, para facilitar la apropiación y el uso de la firma electrónica avanzada, pudiendo en esta nueva modalidad firmar desde cualquier dispositivo móvil, no siendo necesario portar e instalar un dispositivo físico que aloje el certificado y las claves.

Con tal finalidad se aprobó el artículo 28 de la Ley N° 19.535, reglamentado por el Decreto N° 70/018 del Poder Ejecutivo, normas que analizaremos en los apartados siguientes.

## 4. LA FIRMA ELECTRÓNICA AVANZADA CON CUSTODIA CENTRALIZADA

El artículo 31 de la Ley N° 18.600 en la redacción dada por la Ley N° 19.535 establece la creación en la Unidad de Certificación Electrónica (UCE) el Registro de Prestadores de Servicios de Confianza. Estos prestadores podrán prestar servicios de confianza *"que brinden seguridad jurídica a los hechos, actos y negocios realizados o registrados por medios electrónicos, entre ellos, la creación, verificación y validación de firmas electrónicas avanzadas con custodia centralizada, la identificación digital y el sellado de tiempo…".*

Para ello deben cumplir con las siguientes obligaciones:

*"A. Custodiar diligentemente la clave del firmante o signatario y asegurar los medios para su generación, protección y destrucción.*

*B. Establecer mecanismos seguros para realizar firmas electrónicas por orden del firmante o signatario de acuerdo con lo que determine la Unidad de Certificación Electrónica.*

*C. Disponer de mecanismos seguros para el registro y autenticación de personas para su identificación digital".*

El inciso final del artículo establece que los prestadores de servicios de confianza deberán acreditarse ante la UCE.

El artículo 32 regula específicamente la firma electrónica avanzada con custodia centralizada, estableciendo que*: "La firma electrónica avanzada con custodia centralizada, realizada a través de un Prestador de Servicios de Confianza, si cumple con todos los requisitos legales tendrá la misma validez y eficacia jurídica que la firma electrónica avanzada".*

El uso de la firma electrónica avanzada implica que no se depende más de un dispositivo físico, tampoco es necesario un lector para la cédula. En lugar de comprar el token, se va realizar un contrato con el proveedor de confianza para que aloje el certificado, del cual van a surgir todas las obligaciones para el prestador en cuanto a la custodia y el uso que se va a hacer del certificado. El proveedor puede coincidir con el prestador de servicios de certificación, tener las dos acreditaciones, de certificación y de confianza.

A los efectos de regular este nuevo escenario se aprueba el Decreto N° 70/018 que regula únicamente a los prestadores de firma electrónica avanzada con custodia centralizada y a los de identificación electrónica o digital, tal cual lo establece el artículo 1° al referirse al ámbito de aplicación objetivo de la norma.

El artículo 3° define en el literal b) a la primera de ellas como: "*la firma electrónica avanzada en la cual la clave privada del firmante se encuentra en custodia de un prestador de servicios de confianza acreditado, que realiza la firma bajo orden expresa del firmante*".

El artículo 4° establece las competencias de la UCE: acreditar y controlar los servicios prestados por los prestadores de servicios de confianza, establecer las especificaciones técnicas, normas y procedimientos respecto a los servicios de confianza y definir nuevos servicios de confianza.

Actualmente la UCE ya aprobó la política que deben cumplir los prestadores de servicios de confianza de firma electrónica avanzada con custodia centralizada de personas físicas y se encuentra en proceso de estudio la política que regula a los prestadores de identificación electrónica.

Los servicios de confianza de firma electrónica avanzada con custodia centralizada podrán consistir en la generación, almacenamiento y firma con certificados de firma electrónica avanzada de personas físicas y jurídicas.

Por tanto, es posible distinguir las siguientes situaciones:

a) El prestador que genera el certificado, almacena y firma, para los casos de personas físicas y jurídicas.

b) El prestador que solo almacena y firma, esta hipótesis aplica solo a personas jurídicas, como por ejemplo en los casos de certificados de personas jurídicas para facturación electrónica.

El artículo 9° del decreto establece la prohibición de migrar la clave privada para la firma avanzada de persona física, entre los diferentes prestadores de servicios de confianza, ni modificar el medio de almacenamiento dentro del mismo prestador de servicios de certificación. Por tanto, aquella firmas que se hayan emitido en dispositivos seguros de almacenamiento deben permanecer en ellos y el usuario deberá adquirir una nueva firma electrónica avanzada para utilizarla desde la nube.

## 5. IDENTIFICACIÓN ELECTRÓNICA

La identidad digital es el conjunto de informaciones publicadas en Internet sobre una persona y que componen la imagen que los demás tienen de ésta: datos personales, imágenes, noticias, comentarios, gustos, amistades, aficiones, etc. Todos estos datos nos describen en Internet ante los demás y determinan la reputación digital, es decir, la opinión que los demás tienen en la red. Esta identidad puede construirse sin que se corresponda exactamente con la realidad. Sin embargo lo que se hace bajo esa identidad digital tiene sus consecuencias en el mundo real y viceversa.

Como se puede observar el uso de Internet cada día va en aumento, por lo que la sociedad ha evolucionado considerablemente para formar comunidades en medios intangibles que se manifiestan día con día.

En este contexto es importante la identificación de la identidad ya que la información vertida directa e indirectamente por sí o por tercera persona puede producir efectos positivos y negativos en el mundo real. Un ejemplo de esta tendencia es cuando personas y empresas navegan por las redes sociales para investigar la identidad digital de un candidato y tomar decisiones sobre él/ella. (MOLINA MARTÍNEZ. Laura. "El Reconocimiento de la identidad digital a través de la firma electrónica avanzada". Hacia una Justicia 2.0. Actas del XX Congreso Iberoamericano de Derecho e Informática. Volumen II. Página106).

Como las contraseñas son incómodas y difíciles de recordar, para su eliminación la FIDO Alliance y W3C, los consorcios que regulan los estándares en el uso de la web están trabajando en WebAuthn, el nuevo estándar que regulará la autenticación de los usuarios y eliminará las contraseñas.

Este nuevo estándar cuenta con el respaldo de Google, Mozilla y Microsoft y, en lugar de la contraseña, apuesta por sistemas de identificación biométricos a los que los usuarios de móviles de última generación están más habituados. El nuevo estándar va a permitir que un usuario pueda identificarse de forma inequívoca en un sistema o navegador empleando la huella digital o su propio rostro, o bien confiar su identidad a un segundo dispositivo (un móvil, tableta o pendrive USB).

En materia de identificación electrónica el Reglamento de la UE parte de la importancia de asegurar la interoperabilidad transfronteriza en el seno de la UE, de las identificaciones nacionales, así como el reconocimiento y aceptación mutuos entre los Estados Miembros de los medios de identificación electrónica. Objetivo básico del Reglamento es garantizar la identificación y la autenticación electrónicas seguras para el acceso a los servicios transfronterizos en línea ofrecidos por los Estados miembros, pero preservando la libertad de los Estados respecto a la gestión de la identificación electrónica y las infraestructuras conexas. (DE MIGUEL ASENCIO, Pedro. "Unificación en la UE del régimen de los servicios de confianza para las transacciones electrónicas").

El artículo 33 de la Ley N° 18.600 en la redacción dada por la Ley N° 19.535 establece la equivalencia funcional de la identificación digital. *"La Unidad de Certificación Electrónica definirá los niveles de seguridad que proporcionen a la identificación digital el mismo valor y efecto jurídicos que la identificación presencial*."

Por su parte, el Decreto N° 70/018 define en el artículo 3°, en el literal A) la autenticación electrónica como el proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital. En el literal C) establece los medios de identificación electrónica o digital como: "*la unidad material o inmaterial, procesable por un sistema informático, con una parte en control del sistema y otra en exclusivo control de la persona, ya sea mediante: su conocimiento; un dispositivo físico o lógico; algún rasgo físico o comportalmental*".

Define además en el literal E) el Registro de identificación digital y en G) los servicios de identificación digital, como aquellos que realizan registros de autenticación electrónica de personas para su verificación por terceros.

En el Capítulo III del Decreto se encuentran regulados los servicios de identificación digital. Estableciendo el artículo 5° que éstos pueden contar con diversos niveles de seguridad, otorgándole competencias a la UCE para definir las condiciones para determinarlos, debiendo considerar el procedimiento de registro de identificación, los medios de identificación digital y el proceso de autenticación. Y siendo este organismo quien definirá los niveles de seguridad que proporcionen a la identificación digital el mismo valor y efectos jurídicos que la identificación presencial. Para que exista esta equivalencia, los prestadores de servicios de confianza que brinden este servicio deberán estar acreditados.

El artículo 7° establece que es responsabilidad de quien utiliza el servicio de identificación digital definir cuál es el nivel de seguridad que necesita, obviamente en virtud del servicio que se está brindando.

La UCE se encuentra trabajando en la política de Identificación digital para la cual se han tomado como referencia los lineamientos de identidad digital establecidos por el NIST y el marco que establece el eIDAS.

En el proceso de identificación digital tenemos que tener en cuenta el nivel de registro de la identificación digital, los medios de identificación digital y el nivel de autenticación electrónica.

Para el caso del Registro, podemos encontrar la existencia de 3 o 4 niveles, que van desde niveles muy bajos de seguridad hasta el nivel equivalente al presencial. Sin lugar a dudas, en nuestro país un alto nivel de identificación y por tanto equivalente al presencial requerirá al momento del registro la instancia presencial, pudiendo el proceso comenzar en línea, pero siendo necesaria la presencia física de la persona que solicita la acreditación de su identidad física a los efectos de vincularla con medios digitales y será necesaria la captura de datos biométricos del suscriptor y el tipo de medio digital asociado al solicitante es un certificado de firma electrónica avanzada otorgado dentro de la infraestructura de certificación electrónica de Uruguay.

Los medios de identificación electrónica digital que pueden ser considerados durante la etapa de autenticación son los siguientes:

a) Nombre de usuario y contraseña.

b) Lista de contraseñas, en soporte papel que posee el reclamante. Consiste en una lista de códigos a menudo en combinación con una contraseña estática o PIN dentro del sistema de autenticación.

c) Dispositivo de contraseña de un solo uso: es un dispositivo de hardware personal que genera una contraseña de "una sola vez", el cual es válido para una sola sesión de autenticación.

d) Certificado en software: es una clave criptográfica que normalmente se almacena en un disco, dispositivo USB u otro medio de dispositivo de comunicación. La autenticación se realiza probando la posesión y el control de la clave.

e) Certificado en hardware: es una tarjeta inteligente o medio similar que contiene una clave criptográfica protegida. La autenticación se realiza probando la posesión del dispositivo y el control de la clave.
d) Certificado electrónico reconocido de persona física: certificado de firma electrónica avanzada emitido por un prestador de servicios de certificación acreditado ante la UCE.

El tercer paso del proceso, la autenticación electrónica, como ya hicimos referencia, se encuentra definida en el artículo 3° literal A) del Decreto como "*el proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital"*.

El nivel de confianza que se puede plantear en un mecanismo de autenticación remota depende del nivel de seguridad que posea, los cuales están muy relacionados con los tipos de ataques y el medio de identificación digital utilizado durante el proceso de autenticación.

Las amenazas dentro de los procesos de autenticación pueden ser:

a) Fuerza bruta: es un ataque donde se intenta adivinar el secreto de la comunicación, por ejemplo una clave.

b) Eavesdropping: consiste en una escucha secreta o sigilosa. En la red, consiste en observar los mensajes que pasan por un canal de comunicación. Esos mensajes se almacenan para realizar un análisis fuera de línea de la información, obteniendo por ejemplo metadatos, que son utilizados para lanzar ataques sucesivos.

c) El secuestro: es un ataque que consiste en hacerse cargo de una sesión ya autenticada por un atacante y para aprender información sensible.

d) Retransmisión**:** es una forma de ataque donde una entidad maliciosa repite o retrasa previamente mensajes interceptados para obtener acceso a información confidencial.

e) *Man-in-the-middle*: es una forma de espionaje activo consiste en introducirse en la comunicación entre dos equipos para que todo el tráfico pase por él y poder así desencriptar sus datos, contraseñas, etc.

El nivel de seguridad del protocolo de autenticación lo hace o no susceptible de determinados ataques, por tanto el nivel de seguridad dependerá de a qué tipo de riesgos se encuentra expuesto.

De acuerdo a los niveles definidos durante el procedimiento es que se definen los niveles de seguridad de la identificación digital.

## 6. PRESTADORES DE SERVICIOS DE CONFIANZA

El capítulo V del Decreto N° 70/018 regula a los prestadores de servicios de confianza, estableciendo en el artículo 10 los requisitos para ser considerados tales, en el artículo 11 sus obligaciones, el artículo 12 establece los requerimientos técnicos y de gestión y el

artículo 13 remite, en cuanto a la responsabilidad, a lo previsto en el artículo 20 de la Ley N° 18.600 respecto a los prestadores de servicios de certificación.
En el capítulo VI se establece cual es el procedimiento de acreditación de los prestadores de servicios de confianza. El artículo 14 establece los tres tipos de servicios de confianza que pueden brindarse, ellos son:

a) Generación, almacenamiento de certificados y firma de personas físicas y jurídicas.

b) Almacenamiento de certificados de personas físicas o jurídicas.

c) Identificación digital de personas físicas con niveles de seguridad equivalentes a la identificación presencial.

En el segundo caso de almacenamiento y firma será necesaria la existencia de un contrato que vincule al prestador de servicios de certificación con el prestador de servicios de confianza que proporcionará el servicio de almacenamiento.

Los requisitos para cada uno de ellos se encuentran regulados en los artículos 15 y 16 respectivamente.

El artículo 15, para los casos de prestadores de generación, almacenamiento y firma, remite a lo establecido en la Ley N° 18.600 y su Decreto reglamentario N° 436/011.

Para el caso de los prestadores que solo den servicio de almacenamiento y firma, el artículo 16 establece que no será necesario que se acrediten, teniendo la UCE facultades para controlar en cualquier momento la regularidad de los servicios prestados. Sí establece la obligación de que cuenten con procedimientos de acceso y resguardo de certificados, cláusulas contractuales y todo lo que establezca la UCE en las políticas específicas.

Al igual que para los prestadores de servicios de certificación se exige una garantía de solvencia económica, mediante la constitución de un seguro de responsabilidad por daños y perjuicios que pudiera ocasionar la prestación del servicio.

La resolución de acreditación tiene los siguientes efectos: la incorporar del prestador en el Registro de prestadores de servicios de confianza acreditados y la habilitación para prestar el servicio en el cual se acredite.

Los artículos 23 al 27 regulan la suspensión y revocación de la acreditación de los prestadores de servicios de confianza, tanto de los prestadores de firma electrónica avanzada con custodia centralizada como para los prestadores de identificación digital, así como el cese de las actividades de éstos.

En el capítulo VII se regula el control y supervisión de los prestadores de servicios de confianza acreditados, remitiendo al artículo 14 numeral 5° de la Ley N° 18.600 referente a las potestades sancionatorias de la UCE.

El artículo 30 establece el deber de colaboración en los siguientes términos: "*Los prestadores de servicios de confianza tienen la obligación de facilitar a la UCE toda la información y elementos necesarios para el ejercicio de sus funciones, así como la de permitir al personal inspector el acceso a sus instalaciones y la consulta de toda la documentación relevante*".

En forma complementaria a lo establecido en el artículo 30, el artículo 31 prevé el relacionamiento entre prestadores de servicios de certificación y prestadores de servicios de confianza, estableciendo que los primeros deberán informar a la UCE la existencia de acuerdos y convenios que suscriban con prestadores de servicios de confianza para la prestación de los servicios que se regulan.

Finaliza el artículo haciendo la referencia a que "*Dicha obligación se considerará cumplida mediante la entrega a la UCE del listado de los prestadores participantes. La UCE garantizará la confidencialidad de la información entregada*".

El artículo 31 le permite a la UCE conocer quiénes son los prestadores que brindan servicios de almacenamiento y firma, que si bien no están acreditados, posee el cometido de controlarlos.

## 7. CONCLUSIONES

La aprobación de las normas analizadas ha proporcionado a Uruguay un marco jurídico completo y garantista a los efectos de la utilización de la firma electrónica avanzada con custodia centralizada y la identificación digital.

El objetivo de la normativa es asegurar que el dispositivo de creación y almacenamiento de firmas electrónicas sea confiable y que el firmante tenga el acceso exclusivo a su clave de firma electrónica avanzada de persona física con una custodia centralizada, con un alto grado de confianza.

Como se mencionó en la introducción, los servicios permitirán firmar documentos evitando utilizar dispositivos adicionales para la firma como los token o los lectores de cédula de identidad, facilitando el proceso a los usuarios.

El otorgar la equivalencia de la firma en nube con la firma electrónica avanzada y de la identidad digital con la identidad electrónica constituye, sin lugar a dudas, dos herramientas poderosísimas para el avance de los proyectos de gobierno electrónico, especialmente el proyecto de trámites 100% en línea.

## BIBLIOGRAFIA

MOLINA MARTÍNEZ. Laura. "El Reconocimiento de la identidad digital a través de la firma electrónica avanzada". Hacia una Justicia 2.0. Actas del XX Congreso Iberoamericano de Derecho e Informática. Volumen II.

RICO CARRILLO, Mariliana. "La entrada en vigencia de la regulación europea sobre servicios de confianza y su impacto en el comercio electrónico". Actas del XX Congreso iberoamericano de Derecho e Informática. Salamanca – España, 2016.

VIEGA RODRIGUEZ, María José y HERNANDEZ VARELA María Jimena. "Derecho Informático e Informática Jurídica II". Fundación de Cultura Universitaria". Montevideo, marzo, 2018.

VIEGA RODRIGUEZ, María José. "Derecho Informático e Informática Jurídica I". Fundación de Cultura Universitaria". Montevideo, octubre, 2017.
VIEGA RODRIGUEZ, María José y RODRIGUEZ, Beatriz. "Documento y firma. Equivalentes funcionales en el mundo electrónico. Ley N° 18.600 – Decreto N° 436/2011". Editorial CADE, junio 2012.

**Formato electrónico**

Canal TIC. Educación. Tecnologías de la información y comunicación. http://canaltic.com/internetseguro/manual/3_mi_identidad_digital.html Página visitada el 17 de abril de 2018.

CANUT, Pedro J. "El Prestador Cualificado de Servicios de Confianza – Seguridad Jurídica en Internet". https://www.blogespierre.com/2015/11/27/el-prestador-cualificado-de-servicios-de-confianza-seguridad-juridica-en-internet/ Página visitada el 25 de agosto de 2017.

[1]https://www.cromo.com.uy/el-fin-las-contrasenas-esta-aqui-llega-webauthn-n1223243?utm_source=planisys&utm_medium=Cromo-Titularesdelasemana&utm_campaign=Cromo-Titularesdelasemana2018&utm_content=27&ns_campaign=Cromo-Titularesdelasemana2018&ns_source=planisys&ns_linkname=27&ns_mchannel=Cromo-Titularesdelasemana Página visitada el 16 de abril de 2018.

SHELDON, Robert. "Qué buscar en un proveedor de almacenamiento en nube". http://searchdatacenter.techtarget.com/es/consejo/Que-buscar-en-un-proveedor-de-almacenamiento-en-nube Página visitada el 25 de agosto de 2017.

VIEGA RODRIGUEZ, María José y RODRIGUEZ, Beatriz. "Documento electrónico y firma digital. Cuestiones de seguridad en las nuevas formas documentales". Libro electrónico: www.viegasociados.com Montevideo, 2005.

WINKLER, Vic (J.R.). "Informática en nube: problemas legales y reglamentarios". https://technet.microsoft.com/es-es/library/hh994647.aspx Página visitada el 25 de agosto de 2017.

"Prestadores de servicios electrónicos de confianza". http://www.minetad.gob.es/telecomunicaciones/es-

es/servicios/firmaelectronica/paginas/prestadores.aspx Página visitada el 25 de agosto de 2017.