ECIJA | Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa

Madrid, 06 de abril de 2020

Identificación y firma electrónica: soluciones del presente con garantías a futuro

En el estado de alarma derivado de la pandemia del COVID-19, las tecnologías de identificación y firma electrónica adquieren una especial relevancia y valor, surgiendo nuevas soluciones válidas, tanto en el sector público como privado, cuyo objetivo principal es permitir la continuidad del negocio y la gestión de trámites administrativos.

La contratación electrónica de productos y servicios, así como la tramitación electrónica de trámites administrativo, juega un papel fundamental que debe ponerse en valor, no solo ante la situación excepcional que vivimos, sino como parte de los procesos elementales en el seno de toda actividad, ya sea ésta pública o privada.

(I) Novedades derivadas de la disposición adicional undécima del Real Decreto-ley 11/2020 – videoconferencia para la renovación de certificados cualificados

Debido a la situación con la que se encuentra la sociedad actualmente, la implantación del teletrabajo y la tramitación de las gestiones electrónicamente se ha convertido en un proceso prioritario y clave para todas organizaciones. La realidad es que la mayoría de las organizaciones no tenían previsto o implantado hasta el momento modelos de teletrabajo, no contando con una política interna que regulara el trabajo a distancia de sus trabajadores, ni con procesos digitalizados que permitan la gestión de toda su actividad por medios electrónicos.

La implantación de una correcta digitalización en los procesos se hace imprescindible para la tramitación de documentación generada en el seno de la actividad empresarial o administrativa y especialmente, para garantizar la continuidad de negocio en muchas actividades consideradas esenciales para nuestra económica y sociedad.

De ello se deriva que, a pesar de su reconocimiento durante los últimos tiempos, los servicios de confianza, fundamentalmente de identificación y firma electrónica y de entrega electrónica certificada, regulados por el Reglamento Europeo 910/2014 de 23 de Julio (eIDAS), estén adquiriendo un protagonismo indiscutible en estos momentos.

Entre las medidas urgentes publicadas como consecuencia del estado de alarma, se encuentra la publicación, en el marco del Real Decreto-ley11/2020, de 31 de marzo por el que se adoptan medidas urgentes en el ámbito social y económico para hacer frente al COVID-19, de **medidas provisionales para la expedición de certificados electrónicos cualificados.**

Estas medidas provisionales se regulan en la **Disposición Adicional Undécima** del citado Real Decreto-ley, que dice así:

"Durante la vigencia del estado de alarma, decretado por el Real Decreto 463/2020, de 14 de marzo, ***se permitirá la expedición de certificados electrónicos cualificados*** *de acuerdo con lo previsto en el artículo 24.1.d) del Reglamento (UE) 910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior".*

"A tal efecto, ***el organismo supervisor aceptará aquellos métodos de identificación por videoconferencia basados en los procedimientos autorizados por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias*** *o reconocidos para la expedición de certificados cualificados por otro Estado miembro de la Unión Europea. La equivalencia en el nivel de seguridad será* ***certificada por un organismo de evaluación de la conformidad. Los certificados así emitidos serán revocados por el prestador de servicios al finalizar el estado de alarma, y su uso se limitará exclusivamente a las relaciones entre el titular y las Administraciones públicas".***

Según lo anterior, durante el presente estado de alarma, se va a permitir emitir certificados electrónicos de forma remota (sin presencialidad) pudiendo, para ello, utilizar sistemas de videoconferencia, siempre que se éstos cumplan con las especificaciones técnicas de seguridad publicadas por el SEPBLAC (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias) que autorizó dentro del ámbito de las transacciones del sector financiero.

Estas especificaciones se encuentran descritas en la Autorización de 12 de febrero de 2016 relativa a los procedimientos de identificación no presencial mediante videoconferencia (sistema de identificación asistida).

Algunas de las medidas de seguridad que se exponen para utilizar este tipo de métodos de videoconferencia son: la realización de un análisis de riesgos, establecer mecanismos de seguridad que garanticen la autenticidad, vigencia e integridad de los documentos de identificación que se vayan a utilizar durante el proceso o la obtención del consentimiento expreso por parte del sujeto firmante. Este consentimiento deberá ser por un lado de la realización del procedimiento de identificación no presencial mediante videoconferencia y, por otro, de la grabación y conservación del proceso con carácter previo al proceso o en el curso de este.

No obstante, para ser admitido como medio de identificación para la emisión de certificados cualificados, este sistema **tiene que contar con un informe de evaluación de la conformidad emitido por un organismo de evaluación de conformidad**. Por ello, dado el escaso plazo con el que se cuenta, parece que los sistemas a utilizar se reducen a aquellos sistemas de videoconferencia que ya estén siendo utilizados por un Prestador de Servicios de Confianza Cualificado en la Unión Europea.

(II) DNIe Remote para el acceso a Administración electrónica.

Otra solución que cobra relevancia en la situación actual del estado de alarma en el que se han paralizado los procesos presenciales en las Administraciones Públicas, es la aplicación **DNIeRemote** gestionada por la Policía Nacional que utiliza la tecnología NFC.

Esta tecnología hacer referencia al chip NFC insertado en el DNI electrónico, donde se incluyen los datos relativos a la identificación del sujeto que puede ser leído por un dispositivo móvil con sistema operativo Android. El dispositivo se convertiría en un lector del DNIe conectado al ordenador, a través de una aplicación para Android llamada "*Lector de DNIe para PC*".

De esta manera, se permite acceder a los servicios de la administración electrónica que solicitan la autenticación con certificado digital, y realizar firmas digitales en documentos a través de las aplicaciones de que dispone.

Cabe destacar que, de acuerdo con las medidas dirigidas a facilitar la tramitación de los ciudadanos en sus gestiones con la Agencia Estatal de Administración Tributaria (AEAT), esta Agencia durante el periodo de alarma, permite la utilización de aquellos certificados que se

encuentren caducados, situación que deberá resolverse, y proceder a la renovación del certificado, una vez haya vuelto la situación a la normalidad.

(III) Implantación de soluciones de identificación y firma electrónica

Desde el punto de vista empresarial, existen en el mercado distintas plataformas que integran distintos sistemas de identificación y firma, de forma que se ofrece a las organizaciones flexibilidad para la implantación de distintos sistemas en el seno de diversidad de procesos, sin que ello suponga grandes esfuerzos de desarrollo, integración y recursos, permitiendo que con una inversión limitada, y en un plazo de tiempo escaso, sea posible implantar y desplegar este tipo de sistemas tecnológicos.

A la hora de valorar la implantación de procesos electrónicos presenciales o a distancia, debe tenerse en cuenta que cada proceso exigirá unas garantías distintas de acuerdo con el riesgo que suponga cada uno de ellos de tal manera que garantice la identificación del sujeto, su consentimiento y la integridad y confidencialidad de la propia transacción

Por lo que, en un primer momento, la organización debe evaluar los riesgos que supondrían la tramitación de un servicio electrónico de esta índole y, en base a los posibles riesgos identificados, se determinará el nivel de seguridad y garantías que se le requerirán al servicio de confianza que se desee implantar, pudiendo ser:

- Servicios de firma electrónica
- Sellados de tiempo
- Servicios de entrega electrónica certificada
- Servicios de custodia electrónica
- Servicios de identificación mediante videoconferencia
- o inclusive, nuevos servicios que utilicen certificados electrónicos o sellados de tiempo en diferentes partes del proceso

Lo relevante a la hora de implantar un servicio de confianza es que aporte las garantías necesarias de acuerdo con los procesos de identificación elegidos y obtener el consentimiento del sujeto por vía electrónica, conocer el riesgo que el trámite o proceso a digitalizar supone para la compañía, y en base a ese riesgo, se adopten e implanten las medidas y sistemas que permitan minorar y/o evitar dicho riesgo.

El Reglamento eIDAS distingue entre servicios de confianza cualificados y no cualificados, siendo los primeros aquellos que han sido homologados de forma previa por el organismo de supervisión y establece distintos niveles de seguridad y, en consecuencia, de garantías, que pueden dar lugar a distintos prestadores de servicios de confianza. Estos niveles son:

- **Nivel de Seguridad Bajo**: aquellos medios de identificación electrónica que establecen un grado limitado de confianza en la identidad de una persona. Las especificaciones técnicas, normas y procesos incluidos tienen por objetivo reducir el riesgo de uso indebido o alteración de la identidad.

- **Nivel de Seguridad Sustancial**: aquellos medios de identificación electrónica que establecen un grado de confianza sustancial en la identidad de una persona. Las especificaciones técnicas, normas y procesos incluidos tienen por objetivo reducir sustancialmente el riesgo de uso indebido o alteración de la identidad.

- **Nivel de Seguridad Alto**: aquellos medios de identificación electrónica que establecen un grado de confianza superior al sustancial en la identidad de una persona. Las especificaciones técnicas, normas y procesos incluidos tienen por objetivo evitar el riesgo de uso indebido o alteración de la identidad.

Centrándonos solo en los servicios de firma electrónica, es interesante saber que los tipos de firma electrónica que existen y se reconocen en la normativa, serían la firma electrónica simple o básica, la avanzada y la cualificada, presentando cualquiera de las tres, eficacia jurídica y siendo legalmente vinculantes y admisibles como pruebas válidas ante cualquier tribunal dependiendo, según el tipo de firma, de las evidencias que se presenten para acreditar su validez.

(IV) Conclusiones. La actividad debe continuar

Desde el momento en que las empresas son conscientes de la necesidad de estar conectados electrónicamente por la situación de alarma que vive el mundo entero, se plantea la necesidad de hacer las cosas bien, de evitar ser víctima de posibles fraudes y de ofrecer fiabilidad y garantías suficientes en los procesos electrónicos en el momento de comunicarse con proveedores, clientes o empleados de forma segura y efectiva.

En todos los ámbitos de cualquier entidad, sea pública o privada la firma electrónica a distancia resulta de gran utilidad, no solo porque agiliza los procesos de gestión, se ha demostrado su aportación ecológica y sostenible y supone un ahorro en costes administrativos a largo plazo, sino también porque en estos momentos **supone la alternativa idónea para continuar con la actividad normal** de cualquier entidad con plenas garantías.

Además, no suponen una novedad en el mercado, son numerosos los proveedores que llevan años ofreciendo soluciones a las entidades, lo que permite la rápida implantación en las entidades plataformas que permitan, con las máximas garantías legales y de seguridad, seguir actuando en el tráfico mercantil, relacionándose con las administraciones públicas, etc.

Es por eso que, en momentos excepcionales como el presente, la decisión temporal de implantar servicios de identificación y firma electrónica no solo debe resultar una vía de escape ante situaciones no previstas como el COVID -19, sino que, por sus demostrables resultados, se convierte en un proceso a largo plazo clave, legal y eficaz en una organización, ofreciendo numerosas ventajas respecto a posibles competidores y mejoras en la efectividad y productividad del negocio.

Quedamos a su disposición para cualquier cuestión que pudieran necesitar.

Área IT, Privacidad y Seguridad de ECIJA
+ 34 91 781 61 60
info@ecija.com