# III OTRAS RESOLUCIONES

## *PRESIDENCIA DE LA JUNTA*

*RESOLUCIÓN de 6 de octubre de 2010, de la Vicepresidenta Primera y Portavoz, por la que se aprueban las condiciones técnicas de la aplicación informática de gestión electrónica de la actuación administrativa del Consejo de Gobierno y de la Comisión de Secretarios Generales de la Junta de Extremadura.* (2010062363)

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, establece en su artículo 45 que las Administraciones públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias.

A nivel estatal existe un conjunto de normas que desarrollan la utilización de medios informáticos, electrónicos y telemáticos en los procedimientos administrativos, haciendo especial hincapié en la necesidad de garantizar la autenticidad, integridad y conservación de los documentos generados en la tramitación de dichos procedimientos.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, establece la firma electrónica reconocida como una forma de garantizar la autenticidad, integridad y conservación de los documentos, la cual proporciona la adecuada seguridad jurídica, puesto que en un documento firmado electrónicamente interviene una tercera persona, llamada "proveedor de servicios de certificación", que acredita mediante la emisión de un certificado la procedencia del mismo y que garantiza en todo momento:

a) La identificación del órgano competente para tramitar el procedimiento.

b) La autenticidad, integridad y conservación de los documentos.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en su artículo 33 contempla que la gestión electrónica de la actividad administrativa respetará la titularidad y el ejercicio de la competencia por la Administración Pública, órgano o entidad que la tenga atribuida, y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad. A estos efectos, y en todo caso bajo criterios de simplificación administrativa, se impulsará la aplicación de medios electrónicos a los procesos de trabajo y la gestión de los procedimientos de la actuación administrativa.

En el ámbito de la Comunidad Autónoma de Extremadura, el Decreto 2/2006, de 10 de enero, creó el Registro Telemático, y reguló la utilización de técnicas electrónicas, informáticas y telemáticas, así como el empleo de la firma electrónica reconocida por la Administración autonómica.

Con el objetivo de avanzar en el servicio a los administrados alcanzando mayores cotas de eficacia y agilidad en la tramitación, recientemente se ha aprobado el Decreto 188/2010, de 1 de octubre, por el que se aprueban las normas de Organización y Funcionamiento del

Consejo de Gobierno de la Junta de Extremadura y de la Comisión de Secretarios Generales, y se regula la utilización de medios electrónicos en el desarrollo de su actividad. Dicho decreto habilita la utilización de medios electrónicos en el funcionamiento interno de dichos órganos, sustituyendo la tramitación convencional, materializada en la elaboración, firma, notificación y archivo de los actos y trámites procedimentales en soporte papel, por el circuito de tramitación telemática, con la incorporación de la firma electrónica reconocida, notificación telemática, sellado de tiempo y archivo electrónico, lo que repercute en la mejora de los procesos y en la reducción del gasto público, y todo ello con la misma validez jurídica que la tramitación convencional.

Para ello la Presidencia de la Junta de Extremadura ha desarrollado una aplicación informática que gestiona de forma electrónica el circuito de tramitación de los asuntos sometidos a la deliberación, y en su caso, acuerdo de la Comisión de Secretarios Generales y del Consejo de Gobierno de la Junta de Extremadura, cuyas características técnicas se regulan a través de la presente resolución.

El aplicativo desarrollado utiliza los servicios de validación de certificados y sellado de tiempo de la plataforma @firma, gestionada por el Ministerio de la Presidencia, lo que garantiza la autenticidad y validez de la firma electrónica incorporada a los documentos, así como la acreditación del sellado de tiempo a cargo de un tercero de confianza.

En virtud de lo anterior, en el ejercicio de las competencias atribuidas en materia de administración electrónica, y de conformidad con lo establecido en el artículo 15.1 del Decreto 188/2010, de 1 de octubre,

R E S U E L V O :

Primero. Objeto.

Aprobar las características técnicas del sistema informático Tabul@rium, responsable de la generación, firma, custodia y archivo de los documentos electrónicos asociados a la tramitación de los asuntos que hayan de someterse a la deliberación y, en su caso, acuerdo de la Comisión de Secretarios Generales y del Consejo de Gobierno de la Junta de Extremadura, cuyo detalle, requerimientos y condiciones de uso se recogen en la presente resolución.

Segundo. Funcionalidades de la aplicación.

Tabul@rium es la aplicación informática que gestiona de modo electrónico el circuito completo de tramitación de los asuntos que han de someterse a la deliberación y, en su caso, acuerdo de la Comisión de Secretarios Generales y del Consejo de Gobierno de la Junta de Extremadura. Para ello, la aplicación despliega las siguientes funcionalidades:

1. Alta de asuntos por los usuarios, con la identificación del detalle, clase, subclase y tipo de asunto, y gestión del calendario de sesiones propuestas para su tramitación.

2. Determinación por la aplicación de la documentación preceptiva para su tramitación asociada a la clase, subclase y tipo de asunto.

3. Incorporación por los usuarios de la documentación en soporte electrónico, identificando en la ficha de alta del documento si requiere o no firma y, de precisarse, la autoridad u

órgano competente para ello; o, en su caso, necesidad o no de compulsa, que necesariamente deberá ser firmada electrónicamente por el usuario validado en el sistema.

4. Validación de certificados y firma electrónica de los documentos, con incorporación de sellado de tiempo.

5. Generación de la imagen electrónica del documento firmado con la adición de metadatos en forma de una huella de firma indicativa de la identificación de la persona y cargo que ha firmado el documento, lugar y fecha, así como el código de verificación y la dirección electrónica de acceso.

6. Archivo y custodia de los documentos electrónicos generados e incorporados al sistema.

7. Portal de consulta y verificación de la autenticidad e integridad de los documentos electrónicos mediante el acceso a los archivos electrónicos de la Administración pública, órgano o entidad emisora.

Tercero. Medidas de seguridad.

1. Para la tramitación de los asuntos, los usuarios se deberán validar en el sistema mediante un "código de usuario" y una "clave de acceso personal".

   El código de usuario es el código alfanumérico personal proporcionado a cada usuario por el responsable de diseño, desarrollo, producción y mantenimiento del sistema.

   La clave de acceso personal completará el código de usuario para acceso al sistema y será registrada en el sistema informático mediante una función de transformación hash, de tal manera que no sea posible su lectura. La actualización y renovación de la palabra de control se realizará con arreglo a lo establecido en el documento de seguridad de la aplicación.

2. El código de usuario y la palabra de control personal deberán mantenerse bajo exclusivo control de su titular y no deberán ser facilitados por el mismo a otras personas. La responsabilidad que se pueda derivar del uso indebido de los códigos de usuarios, incluso mediando consentimiento de su titular, corresponderá a los usuarios y titulares de los mismos.

3. En el momento de la firma el usuario, además, será autenticado y habilitado para la misma mediante su certificado electrónico reconocido, almacenado en tarjeta criptográfica u otro dispositivo de características análogas. El tipo de certificado validado por la aplicación cumplirá las características que se detallan en el Anexo de esta resolución.

   Para la autenticación se utilizará el parámetro NIF que aparece en el certificado. Esta forma de autenticación se considera más segura que el esquema descrito anteriormente, ya que la clave privada del usuario permanece en todo momento en el dispositivo, impidiendo éste su utilización directa por parte de otros programas o sistemas informáticos.

4. Las comunicaciones cliente-servidor se llevarán a cabo a través de una conexión segura SSL que garantizará el intercambio encriptado de los datos.

Cuarto. Protocolo de firma.

1. La firma de documentos electrónicos tendrá lugar única y exclusivamente mediante los mecanismos establecidos al efecto en la aplicación Tabul@rium, de acuerdo con las prescripciones definidas en el Anexo.

2. Todo documento firmado electrónicamente deberá ajustarse a los formatos preestablecidos en la aplicación de referencia.

   El usuario autorizado deberá acceder a dicha aplicación, mediante la utilización de su "código de usuario" y "clave de acceso personal".

3. Para la firma electrónica, el usuario deberá proceder de acuerdo con el siguiente protocolo:

   a. En el espacio "Documentos pendientes de firma" la aplicación le mostrará la lista de documentos a firmar por el usuario validado, que podrá estar compuesta por uno o varios elementos, con la posibilidad de abrir cada uno de ellos para verificar si su contenido es, o no, correcto.

   b. Pulsará la opción Firmar documentos, y la aplicación mostrará los certificados disponibles en el equipo, debiendo el usuario seleccionar el certificado de personal al servicio de las Administraciones públicas (APE).

   c. Seleccionado el certificado, la aplicación procederá a autentificar y validar dicho certificado electrónico contra la Plataforma @firma mostrando el resultado de la operación con la expresión "Documento Firmado", en caso de éxito.

   d. En aquellos casos en que se detecten anomalías de tipo técnico en la firma electrónica del documento, dicha circunstancia se pondrá en conocimiento del firmante por la propia aplicación, mediante los correspondientes mensajes de error, para que proceda a la subsanación.

Quinto. Conservación e integridad de los documentos electrónicos generados.

1. La aplicación informática Tabul@rium garantizará la conservación de los documentos electrónicos, identificando cada uno de ellos con el código de asunto en el que se genera, y almacenando de forma segura los mismos en el archivo electrónico.

2. El uso de la firma electrónica reconocida garantiza la integridad del contenido, ya que el documento electrónico firmado no puede ser alterado sin que quede constancia de ello.

Sexto. Sistema de firma, validez y efectos de los documentos electrónicos generados.

1. La identificación y autenticación del ejercicio de la competencia en los documentos electrónicos generados a través del sistema, y cuya firma corresponda a las autoridades y órganos de la Junta de Extremadura, se realizará mediante firma electrónica del personal a su servicio basada en un certificado electrónico reconocido, expedido por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

2. La firma electrónica generada de esta forma tendrá respecto de los datos consignados en forma electrónica el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel, de acuerdo con lo previsto en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

3. En los términos y condiciones de los artículos 5, 6 y 7 del Decreto 188/2010, de 1 de octubre, las compulsas electrónicas, las copias en soporte papel, así como las copias electrónicas de documentos electrónicos generados por el sistema tendrán el carácter de copia auténtica y, por lo tanto, la misma eficacia jurídica que el documento electrónico original.

4. A partir del documento electrónico original generado, firmado y custodiado electrónicamente, el sistema genera una imagen electrónica del mismo que tendrá el carácter de copia auténtica, de acuerdo con el artículo 30.5 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, siempre que dicha imagen incorpore una huella de firma con los siguientes metadatos:

   — Dirección electrónica de verificación del documento.
   — Código de verificación del documento.
   — Identificación de la persona que firma el documento.
   — Identificación del cargo de la persona que firma el documento.
   — Lugar y fecha.

Séptimo. Portal de consulta de documentos electrónicos.

1. La verificación de la validez y autenticidad de las imágenes electrónicas y de las copias en soporte papel de documentos electrónicos se podrá efectuar a través del portal de consulta de documentos electrónicos alojado en la dirección https://cerbero.juntaex.es

2. El acceso a dicho portal requerirá la utilización de alguno de los siguientes certificados electrónicos:

   a) El que incorpora el Documento Nacional de Identidad electrónico.

   b) El certificado de personal al servicio de la Administración pública expedido por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

   c) Certificado de la clase 2 CA, expedido por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

3. Una vez autenticado en el portal será necesario introducir el Código de Verificación, que aparece en la huella de firma del documento, para tener acceso al documento electrónico original, que incorpora, junto con la firma electrónica, el sellado de tiempo. Podrá verificar además la vigencia del certificado electrónico con el que se firmó, mediante la respuesta facilitada por la plataforma de validación de certificados.

Octavo. Disponibilidad y mantenimiento del sistema.

El sistema dispone de un servicio de soporte de 24 x 7 para atender las posibles incidencias o anomalías que pudieran ocurrir. Este servicio está disponible de lunes a viernes, de 8 a 15 horas, para resolver las dudas o consultas de los usuarios del sistema.

Se realizará monitorización del sistema, de forma que se tenga un control continuado del correcto funcionamiento del mismo, que permita detectar anomalías para la generación de alertas.

Por otra parte, se lleva a cabo un exhaustivo análisis de las incidencias sucedidas en el entorno de producción originadas en el código a medida. Este análisis da como resultado la ejecución de procedimientos adecuados a cada situación.

Este servicio incluye el soporte a la puesta en producción de nuevos módulos de código, así como su test previo a la puesta en producción.

Se incluye soporte correctivo del sistema, con tareas orientadas a resolver bugs del código y optimizar su rendimiento.

Tan sólo de forma excepcional, cuando por dificultades técnicas el sistema no se encuentre disponible, se llevará a cabo la tramitación convencional en soporte papel.

Noveno. Eficacia.

La presente resolución será de aplicación a partir del día siguiente al de su publicación en el Diario Oficial de Extremadura.

Mérida, a 6 de octubre de 2010.

La Vicepresidenta Primera y Portavoz,
MARÍA DOLORES PALLERO ESPADERO

## ANEXO TÉCNICO

Los programas y aplicaciones para la firma electrónica reconocida de documentos de Presidencia de la Junta de Extremadura, para la gestión electrónica de la actuación administrativa del Consejo de Gobierno y de la Comisión de Secretarios Generales de la Junta de Extremadura, son soportados por los servidores de aplicaciones propiedad de la Presidencia, bajo sistema operativo Microsoft Windows.

Los programas de presentación de documentos electrónicos y los ficheros generados a partir de los mismos han sido desarrollados en entorno Java e interactúan con un sistema gestor documental (Alfresco), quedando garantizado por el Servicio de Régimen Interior y Tecnologías de la Información y las Comunicaciones de la Presidencia de la Junta de Extremadura su conservación e integridad.

Características del certificado y sistema:

1. Requisitos mínimos del sistema.

— Procesador Pentium II - AMD Athlon.

— 128 MB RAM.

— Sistemas operativos:

• Microsoft Windows (XP, Vista, 7).
• Linux (acceso sólo a certificados de navegador Mozilla).

— Navegadores:

• Internet Explorer 5.5 o superior.
• Mozilla Firefox 2.0 o superior.

— Lector de tarjetas.

— Acceso a red SARA.

— Java Runtime Environment versión 1.5 o superior.

2. Certificados reconocidos.

La firma electrónica de documentos queda sujeta al uso de Certificado Digital Reconocido, conforme el estándar ITU-T X.509 v3, válido para la realización de firma electrónica por parte del personal al servicio de las Administraciones públicas (APE), en los términos contemplados en el artículo 13.3 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, emitido por la FNMT-RCM, que vincula a su titular con unos datos de verificación de firma y confirma, de forma conjunta:

— La identidad de su titular, número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado.

— El órgano, organismo o entidad de la Administración pública, bien sea ésta General, Autonómica, Local o Institucional, donde ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

El ámbito de uso de este tipo de certificados lo componen las diferentes competencias y funciones propias de los titulares de acuerdo con su cargo, empleo y, en su caso, condiciones de autorización.

Estos certificados pertenecen a AC APE, que está subordinada a la AC Raíz FNMT-RCM. Se generan en tarjeta criptográfica y tienen una longitud de clave de 2.048 bits, siendo su caducidad de 48 meses.

Las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de dichos certificados se encuentran recogidas en la Declaración de Prácticas de Certificación de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

3. Validación de certificados.

La validación de autenticación de dichos certificados se llevará a cabo haciendo uso de los servicios de validación proporcionados por la Plataforma @firma gestionada por el Ministerio de la Presidencia, a través de la Red SARA.

La Red SARA (Sistema de Aplicaciones y Redes para la Administraciones) es una infraestructura tecnológica que permite y garantiza la comunicación entre las distintas Administraciones (local, autonómica y estatal) además de servir de plataforma de intercambio de operaciones.

Está formada por la Intranet Administrativa, que hoy ofrece un amplio número de servicios que se prestan en cooperación en el ámbito de la Administración General del Estado, sus elementos de incardinación en TESTA II, y los elementos de enlace con las Redes Corporativas de las Comunidades Autónomas, conocido como Extranet de las Administraciones públicas. TESTA II es la Red transeuropea que enlaza la Red Corporativa de la Comisión de la Unión Europea, con las de los Estados Miembros, para el soporte de intercambio de datos y cooperación en la prestación de servicios.

La interconexión a la Extranet se realiza a través de lo que se denomina Área de Conexión (AC). Este AC responde básicamente al esquema de una zona desmilitarizada (DMZ) formada por un cortafuegos externo (que, en este caso, conecta con el resto de la red), un servidor donde residen los servicios básicos que se mencionan más adelante y un cortafuegos interno.

El sistema que actúa como cortafuegos externo será también el encargado, siempre que sea posible, de cerrar una VPN con el Centro de Acceso Remoto (CAR) de la Intranet Administrativa de la Administración General del Estado o con el AC de otro Organismo conectado directamente a la Red SARA. Este cortafuegos puede realizar igualmente funciones de NAT dinámico para las conexiones entrantes desde el resto de la Extranet hacia el Organismo.

4. Formato de firma electrónica.

El formato de firma electrónica utilizado por el sistema es el PDF, cuya principal ventaja es la capacidad de gestionar firmas. Se trata de una implementación de PKCS#7, estándar de criptografía de clave pública, usado para firmar y/o cifrar mensajes en PKI (Infraestructura de Clave Pública).

Con PDF es posible realizar las denominadas firmas longevas, de gran importancia. La firma longeva incluye información acerca del momento en que se produjo la firma, todos los certificados que conforman la cadena de confianza y la información fiable del estado de los certificados en dicho instante, es decir, incluye todo el material que puede demostrar la autenticidad, la validez y el no-repudio de la existencia de un documento en un determinado instante, más allá del periodo de validez del material de confianza que se utilizó en su momento.

Principales características de la firma PDF:

— Firma y validación con Acrobat Reader.
— Personalización de la razón de la firma.
— Incorporación de CRL/OCSP, timestamp y cadena de certificados.
— Creación de políticas de firma.
— Integración con el repositorio de confianza de Windows.

5. Formato de documentos.

Los tipos de documentos aceptados por el sistema, susceptibles de firma electrónica, sin perjuicio de futura integración de nuevas versiones de los mismos o de la aparición de nuevos formatos debido a la evolución tecnológica, son los siguientes:

— .doc: formato de Microsoft Word 97-2003.
— .docx: formato de Microsoft Word 2007.
— .odt: formato de OpenOffice.org.
— .rtf: Rich Text Format, propiedad de Microsoft.
— .pdf: Portable Document Format, propiedad de Adobe.