RESOLUCIÓN DE 4 DE JUNIO DE 2013, DE LA SUBSECRETARÍA DEL MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, SOBRE ESTABLECIMIENTO DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA CORPORATIVA Y UN DIRECTORIO INTEGRADO DE DATOS DE PERSONAL EN EL ÁMBITO DEL MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), contiene la regulación básica de la identificación y autenticación por medios electrónicos y, por lo que hace a las Administraciones Públicas, prevé la utilización de sistemas de firma electrónica basados en certificados para la identificación de las sedes electrónicas, para el ejercicio de la actuación administrativa automatizada mediante sellos electrónicos, y para la firma electrónica del personal al servicio de las Administraciones Públicas.

En esta resolución se establecen las condiciones necesarias para el cumplimiento de la identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia conforme a lo dispuesto en los artículos 13.3 y 17 al 19 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en el ámbito del Ministerio de Hacienda y Administraciones Públicas, no siendo óbice para el posible uso adicional de otras formas de identificación y autenticación distintas de las previstas en la Resolución.

El 6 de julio de 2009 se dictó una Resolución por parte de la Subsecretaría del Ministerio de Economía y Hacienda sobre establecimiento de una infraestructura de clave pública corporativa y un directorio integrado de datos de personal en el ámbito del Ministerio.

La implantación de una Infraestructura de Clave Pública (PKI) se contemplaba como una herramienta fundamental para la implementación de servicios de seguridad en los sistemas de información y en las aplicaciones. Mediante la gestión de claves y certificados a través de una PKI en una

organización se facilita la posibilidad de utilización de los servicios de firma electrónica y cifrado en una amplia variedad de aplicaciones, estableciendo y manteniendo un entorno de red seguro.

El uso generalizado, en el Ministerio de Hacienda y Administraciones Públicas, de Sistemas de Información y Telecomunicaciones a través de los cuales se procesa, almacena o transmite información, exige la necesidad de dotarlo de la necesaria protección en los sistemas. La implantación de una PKI corporativa o departamental permite la utilización de servicios de seguridad en los sistemas y aplicaciones empleando certificados digitales sobre un soporte seguro. Con ello se ofrece a los responsables de la gestión ministerial un amplio abanico de opciones para desarrollar sus políticas de seguridad de acuerdo con los riesgos asociados en cada caso a la naturaleza de la información que ha de ser gestionada.

La implantación de la PKI, por otra parte, hace imprescindible contar con una herramienta integrada en la que el directorio de personal se mantenga permanentemente actualizado, con el fin de permitir una correcta gestión de las emisiones y revocaciones de certificados. Para ello, la presente resolución determina que la gestión de los certificados se realicen sobre la aplicación denominada MEDUSA (Modelo Estructurado de Datos Unificados para Servicios de Acceso), sobre la cual los distintos Centros Directivos asuman, junto con el Servicio de Información Administrativa, la responsabilidad de verificar la adecuación de los datos aportados por la aplicación y suministrar aquellos otros que requiera el sistema para su correcto funcionamiento.

La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda ejercerá las funciones de autoridad de certificación en relación con la PKI a que se refiere la presente resolución de conformidad con las disposiciones de su estatuto, modificado por el Real Decreto 199/2009, de 23 de febrero.

Como consecuencia de la nueva estructura organizativa derivada del Real Decreto 1823/2011, de 21 de diciembre, por el que se reestructuran los departamentos ministeriales, es necesario dictar la presente resolución para

asegurar el establecimiento de la infraestructura de clave pública corporativa y el directorio integrado de datos de personal en el ámbito de todo el Ministerio.

La operativa de despliegue de la PKI del Ministerio implica la realización de un conjunto de actividades que han de correr a cargo de diferentes órganos o unidades que precisan, por esa misma variedad, de la indispensable coordinación la cual, a su vez, reclama la oportuna cobertura jurídica de carácter interno, necesaria por otra parte para la delimitación de responsabilidades en los sistemas de seguridad de la información del Departamento. A ello responde la elaboración de la presente Resolución, que se dicta en ejercicio de las funciones de dirección, impulso y coordinación de la administración electrónica que la Subsecretaría tiene atribuidas por el artículo 18.3.e) del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas.

En su virtud resuelvo lo siguiente:

Primero.- Uso de la Infraestructura de Clave Pública en el Ministerio de Hacienda y Administraciones Públicas.

1. Para dar cumplimiento a lo establecido respecto a la identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia en los artículos 13.3 y 17 al 19 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, se utilizará en el ámbito del Ministerio de Hacienda y Administraciones Públicas la Infraestructura de Clave Pública (PKI) Departamental actualmente existente.

El ámbito de la misma se extenderá a la totalidad de los órganos superiores y directivos del Ministerio de Hacienda y Administraciones Públicas, incluidos los órganos y unidades territoriales que dependan de los mismos. Quedan excluidos los organismos vinculados o dependientes o cualquier otra entidad de distinta naturaleza adscritos al Ministerio que se atendrán a lo dispuesto en el Resuelvo Octavo.2"

2. La PKI Departamental del Ministerio incluye los siguientes sistemas de identificación y autenticación electrónica previstos en el artículo 13.3 de la ley más arriba citada:

a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.
b) Sistemas de firma electrónica para la actuación administrativa automatizada basados en la utilización de certificados de sello electrónico de órgano.
c) Firma electrónica del personal a su servicio basada en la utilización de certificados de dispositivo seguro, a los efectos de su identificación o autenticación, firma y cifrado.

3. Como soporte físico de los certificados de firma electrónica del personal se utilizarán, en su caso, tarjetas chip/criptográficas individuales y personalizadas para cada usuario del Ministerio.

Segundo.- Gestión de la infraestructura de clave pública del Ministerio de Hacienda y Administraciones Públicas y del directorio integrado de datos de personal.

1. La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, en el marco de los convenios o encomiendas establecidos, proporciona los servicios de certificación y de emisión de certificados electrónicos propios de la PKI del Ministerio de Hacienda y Administraciones Públicas. Las especificaciones referentes a las obligaciones y procedimientos que la citada entidad, en cuanto Autoridad de Certificación-Prestadora de Servicios de Certificación, asume en relación con la emisión y gestión de los certificados integrados en la PKI Departamental, son las contenidas en la correspondiente Declaración de Prácticas de Certificación (DPC).

2. Se constituye la Autoridad de Registro del Ministerio de Hacienda y Administraciones Públicas, que será ejercida por la persona titular de la Oficialía

Mayor, bajo la coordinación del Departamento de Servicios y Coordinación Territorial de la Subsecretaría del Departamento. La Autoridad de Registro, actuando directamente o por medio de las Oficinas de Registro Delegadas a que se refiere el apartado 3 siguiente, ejerce las siguientes funciones:

a) Tramitar ante la Autoridad de Certificación la emisión de los certificados a que se refiere la presente resolución, así como la revocación de los mismos.
b) Solicitar de la Autoridad de Certificación la renovación de dichos certificados cuando tenga lugar su caducidad y no hayan variado las circunstancias del titular que motivaron su emisión, así como tramitar los acuerdos de suspensión de los mismos y de cancelación de la suspensión adoptados por los órganos a que se refiere el apartado 3.
c) Intervenir en la descarga de los certificados (generación de claves privadas) y comprobar presencial y fehacientemente los datos de los titulares referidos a su identidad, haciendo entrega en su caso de las tarjetas criptográficas y recabando la firma de aquellos en la documentación de respaldo pertinente.
d) El impulso de la implementación y la supervisión del mantenimiento de las aplicaciones de soporte de la PKI del Departamento.
e) Las de relación con la Autoridad de Certificación no asignadas a otros órganos.
f) Las restantes que, por aplicación de la normativa aplicable a la PKI, puedan corresponderle en su condición de Autoridad de Registro del Ministerio.

Atendida la dimensión del Ministerio y la distribución territorial de sus órganos y unidades, existirán Oficinas de Registro a cargo de Registradores Delegados de la Autoridad de Registro en el número que se considere oportuno. Corresponde a dicha Autoridad autorizar la creación de las oficinas, así como el nombramiento de los responsables de las mismas y las acciones conducentes a su formación.

Las Oficinas de Registro delegadas desarrollarán las funciones que la Autoridad de Registro les asigne, dependiendo funcionalmente de ésta a los citados efectos.

3. Corresponde a los titulares de los órganos incluidos en el ámbito de la PKI del Ministerio de Hacienda y Administraciones Públicas las siguientes funciones en relación con la misma, así como con el mantenimiento y gestión del directorio de personal necesario a tales efectos y para la integración de los datos básicos de empleados del Departamento en la aplicación MEDUSA:

a) Designar unidades gestoras en los ámbitos que sea preciso, las cuales, conforme determine el Departamento de Servicios y Coordinación Territorial, aportarán en el entorno MEDUSA los datos necesarios para la gestión del directorio de personal y para la emisión y revocación de certificado. Dado que este sistema automatizado verifica que el personal que figura en MEDUSA tiene la condición de empleado público del Ministerio, no se requerirá un acto expreso de los titulares de los órganos del Ministerio para autorizar la emisión del certificado. Cuando los centros directivos tengan sus propias aplicaciones de directorio, los datos podrán ser aportados directamente desde dichas aplicaciones, para lo cual la aplicación MEDUSA proporcionará un servicio web, En todo caso, las unidades gestoras serán quienes coordinen estos procesos, resuelvan las incidencias que se originen en su ámbito y comuniquen al citado Departamento aquellas otras que se deban resolver centralizadamente.
b) Proponer a la Autoridad de Registro, en su caso, los titulares de las Oficinas de Registro delegadas, que podrán coincidir con los de las unidades gestoras indicadas en el apartado anterior.
c) Acordar la suspensión de certificados y la cancelación de la suspensión en los supuestos que proceda y comunicarlo a la Autoridad de Registro.
d) Acordar la emisión de los certificados de aquellas personas correspondientes a su ámbito que, sin tener la condición de empleados públicos del Ministerio, deban disponer de este sistema de autenticación conforme a lo establecido en el apartado quinto 2 de esta

Resolución. Este supuesto deberá aplicarse de forma excepcional, cuando la utilización del certificado sea imprescindible para el ejercicio de las funciones encomendadas a estas personas o, en el caso de personal contratado por empresas, cuando se derive claramente de las prestaciones requeridas por la Administración en los pliegos de condiciones que rijan el contrato. Asimismo, corresponderá a los titulares de dichos órganos, acordar la revocación cuando desaparezcan las circunstancias que justifiquen la utilización del certificado.

Tercero.- Identificación de sedes electrónicas del Ministerio de Hacienda y Administraciones Públicas.

1. Los órganos y unidades incluidos en el ámbito de la PKI del Ministerio de Hacienda y Administraciones Públicas podrán disponer de certificados de identificación de sede electrónica. Las solicitudes de emisión de dichos certificados habrán de dirigirse a la Autoridad de Registro, una vez creada la sede electrónica conforme a las normas legales y reglamentarias aplicables, con indicación de los datos recogidos en el artículo 18.1 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos.

2. Son obligaciones de los titulares de las plataformas tecnológicas que sirvan de soporte a los procedimientos y servicios contenidos en una sede electrónica:

a) Solicitar, a través de la Autoridad de Registro, la revocación del certificado cuando cambie cualquiera de los datos contenidos en el mismo.
b) Abstenerse de utilizar el certificado cuando se produzca el supuesto indicado en el apartado anterior.
c) Las restantes contenidas en las normas de desarrollo de la LAECSP.

Cuarto.- Sello electrónico para la actuación administrativa automatizada.

1. Los órganos y unidades incluidos en el ámbito de la PKI del Ministerio de Hacienda y Administraciones Públicas podrán disponer de certificados de sello electrónico para la actuación administrativa automatizada. La creación de sellos electrónicos se realizará mediante resolución de la Subsecretaría y se ajustará a lo especificado en la normativa de desarrollo de la Ley 11/2007 y en la legislación sobre firma electrónica. La resolución se publicará en la sede electrónica correspondiente, junto con una relación completa de los utilizados en su ámbito.

2. La emisión de dichos certificados estará sujeta a los siguientes requisitos:

a) Cursar la correspondiente solicitud, firmada por el titular del órgano, que habrá de dirigirse a la Autoridad de Registro.
b) Contar con la previa autorización de creación del sello electrónico.
c) Los restantes que procedan en virtud de las normas de desarrollo de la LAECSP.

3. Son obligaciones del titular del órgano a quien corresponda un certificado para la actuación administrativa automatizada:

a) Instar la revocación del certificado cuando cambie cualquiera de los datos contenidos en el mismo.
b) Abstenerse de utilizar el certificado cuando se produzca alguno de los supuestos indicados en el apartado anterior.
c) Las restantes contenidas en la DPC o en las normas de desarrollo de la Ley 11/2007.

Quinto.- Firma electrónica del personal al servicio del Ministerio de Hacienda y Administraciones Públicas basada en certificado de empleado público.

1. De conformidad con lo previsto en el artículo 19.2 de la LAECSP, el Ministerio de Hacienda *y* Administraciones Públicas proveerá a su personal de sistemas de firma electrónica basados en certificados de empleado público.

2. La inclusión en la PKI del Ministerio de Hacienda y Administraciones Públicas mediante distribución de la correspondiente tarjeta criptográfica y expedición de certificado de firma electrónica es obligatoria para la totalidad del personal que preste sus servicios en los órganos y unidades a los que se extienda el ámbito de la misma, determinado conforme al apartado siguiente, que deberá hacer uso de ella en todos los supuestos y aplicaciones en que le sea requerido, sin perjuicio de su derecho a utilizar, alternativamente, el DNI electrónico.

3. Se entenderá a estos efectos por personal a quienes prestan sus servicios en el Ministerio de Hacienda y Administraciones Públicas, aunque no sea de forma permanente y que acceden o pueden acceder a los sistemas informáticos existentes en el mismo, incluyendo básicamente al siguiente:

a) Personal funcionario y laboral en situación de activo en la nómina del Ministerio, con excepción del que, por cualquier circunstancia, no preste materialmente servicios en el mismo.
b) Altos cargos y personal eventual que ocupe puestos en el ámbito de la PKI ministerial.
c) Personal de las Administraciones públicas no incluido en la nómina del Ministerio, siempre que se estime que va a prestar servicios continuados en el mismo.
d) Personal externo, si ha de tener acceso a entornos informáticos para los que sea preciso contar con el certificado.

4. Son obligaciones del personal titular de un certificado de firma electrónica:

a) Realizar un uso adecuado del certificado en relación con las competencias y facultades propias del cargo, puesto de trabajo o empleo como personal al servicio de la Administración Pública.
b) Comunicar al responsable del órgano de quién dependa, el deterioro o destrucción, pérdida, extravío o conciencia de sustracción de la tarjeta o soporte del certificado del que es titular, así como la existencia, en su caso, de indicios de riesgo de vulneración de la seguridad que pueda derivarse del uso del mismo.

c) Las restantes que establezcan las normas de desarrollo de la Ley 11/2007.

Sexto.- Alcance de la PKI Departamental en el marco de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

La utilización de los sistemas de firma electrónica a que se refiere esta resolución por parte del personal y los órganos o unidades incluidos en el ámbito de la PKI del Ministerio de Hacienda y Administraciones Públicas, siempre que se lleve a cabo cumpliendo la totalidad de los requisitos y especificaciones legales aplicables, tendrá la validez y efectos que le atribuyen la LAECSP y sus normas de desarrollo.

Séptimo.- Implementación y mantenimiento de la PKI Departamental.

1. El Departamento de Servicios y Coordinación Territorial dependiente de la Subsecretaría es el encargado de las tareas de despliegue y gestión de la PKI Departamental, salvo que las funciones a ejercer estén asignadas expresamente a otro órgano.

2. Las actuaciones indicadas en el apartado anterior se ajustarán, en todo caso, a lo dispuesto en la Ley 11/2007, sus normas de desarrollo, la Declaración de Prácticas de Certificación aplicable a la PKI y la presente resolución.

3. La información de base de la PKI deberá ser objeto de permanente actualización. La incorporación de las altas, bajas o modificaciones reflejará con la mayor inmediatez posible los cambios producidos en el personal incluido o que deba figurar en la PKI. El mantenimiento incluirá también acciones extraordinarias, como la realización de cruces, con la periodicidad que se defina, con otros sistemas en los que figure información relevante para la PKI. Se prestará en todo caso especial atención al mantenimiento derivado de los supuestos de revocación o caducidad de certificados que en su caso procedan de acuerdo con las normas aplicables. El sistema de gestión informática asegurará la trazabilidad de las operaciones realizadas.

Octavo.- Disposiciones finales.

1. Todos los órganos y unidades del Ministerio de Hacienda y Administraciones Públicas afectados habrán de prestar su colaboración en las actuaciones de implementación y mantenimiento de la infraestructura de clave pública del Departamento descritas en la presente resolución.

2. Los organismos vinculados o dependientes o cualquier otra entidad de distinta naturaleza adscritos al Ministerio adoptarán las medidas oportunas para implementar en su caso, en sus respectivos ámbitos, los sistemas de identificación electrónica regulados en los artículos 13.3 y 17 al 19 de la Ley 11/2007, pudiendo contar a estos efectos con el apoyo de los servicios de esta Subsecretaría.

3. Los certificados de empleado público, sede electrónica y sello electrónico emitidos en el ámbito del Ministerio de Hacienda y Administraciones Públicas con anterioridad a la aprobación de esta Resolución mantendrán su validez.

4. La presente Resolución no implica un incremento en los costes de personal de este Ministerio.

5. Queda sin efecto la Resolución de 6 de julio de 2009 de la Subsecretaría del Ministerio de Economía y Hacienda sobre establecimiento de una infraestructura de clave pública corporativa y un directorio integrado de datos de personal en el ámbito del Ministerio

Madrid, 4 de JUNIO de 2013
LA SUBSECRETARIA,

Pilar Platero Sanz