



**Orden PRE/1551/2003, de 10 junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero de 2003, que regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de certificados por los ciudadanos**

(BOE 13-06-2003)

El Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, dispone en su Disposición final primera que, en el plazo máximo de seis meses desde la entrada en vigor del citado Real Decreto, se establecerán por Orden Ministerial, en el marco de los criterios de seguridad, normalización y conservación a los que se refiere el Real Decreto 263/1996, de 16 de febrero, los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse.

Dichos criterios de seguridad, normalización y conservación han sido objeto de informe favorable del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

Así mismo, en la citada Orden se establecerán las condiciones que ha de reunir el órgano, organismo o entidad habilitada para la prestación del servicio de dirección electrónica única, así como las condiciones para su prestación.

Las condiciones de accesibilidad para las personas discapacitadas y de edad avanzada están sujetas a lo que dispone la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, en su disposición adicional quinta.

La presente Orden Ministerial tiene por objeto dar cumplimiento al mandato señalado en el Real Decreto. A tal fin, se han tenido en consideración las experiencias previas, las implicaciones técnicas de la unicidad de la dirección electrónica, la búsqueda de racionalidad y sencillez de uso para los interesados y el aprovechamiento de las ventajas de las economías de escala.

En su virtud, previo informe favorable del Consejo Superior de Informática y para el Impulso de la Administración Electrónica, a propuesta de los Ministros de Administraciones Públicas, de Ciencia y Tecnología, y de Hacienda, dispongo:

**Primero. Objeto**

De acuerdo con lo establecido en la Disposición final primera del Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados de los ciudadanos, la presente Orden tiene por objeto establecer los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse y, las condiciones que ha de reunir el órgano, organismo o entidad habilitada para la prestación del servicio de dirección electrónica única así como las condiciones de su prestación.

**Segundo. Adopción de las medidas de seguridad, organizativas o técnicas, de los**

## **dispositivos y aplicaciones de registro, notificación y de la prestación del servicio de dirección electrónica única**

1. Con carácter general se aplicarán a los dispositivos y aplicaciones de registro, notificación y de la prestación del servicio de dirección electrónica única las medidas de seguridad, conservación y normalización que se detallan en los «Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades» aprobados por el Consejo Superior de Informática y para el impulso de la Administración Electrónica y accesibles en su sitio web.

Dichas medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la metodología Magerit.

2. Lo dispuesto en esta Orden Ministerial se aplicará en todo caso de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia.

### **Tercero. Requisitos de autenticidad de los dispositivos y aplicaciones de registro y notificación**

1. Los dispositivos y las aplicaciones de registro y notificación sólo admitirán la firma electrónica avanzada basada en un certificado reconocido que cumpla la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997) de acuerdo con lo previsto en la legislación de firma electrónica.

2. La aceptación de una firma electrónica estará condicionada a que la utilización del servicio de consulta sobre la vigencia de los certificados en los que se basen dicha firma electrónica no suponga un coste específico adicional para los órganos, organismos o entidades incluidas en el ámbito de aplicación de la presente Orden.

### **Cuarto. Requisitos de integridad de los dispositivos y aplicaciones de registro y notificación**

Los órganos de la Administración General del Estado y los Organismos Públicos vinculados o dependientes de aquélla que pongan en marcha dispositivos y aplicaciones de registro y notificación, deberán contar con medidas organizativas y técnicas para garantizar la integridad de la información. En cualquier caso establecerán las siguientes medidas:

- a) Aplicación de técnicas de comprobación de la integridad de la información, como firma electrónica (con los requisitos señalados en el apartado tercero), funciones resumen o «hash», y en su caso, de fechado electrónico.
- b) Procedimientos de copias de respaldo de ficheros y bases de datos y de protección y conservación de soportes de información.
- c) Protección de los archivos de información destinados a los interesados mediante atributos de solo lectura.
- d) Instalación de herramientas o procedimientos en las aplicaciones que ejecuten transacciones o procesos donde se produzcan múltiples actualizaciones de datos

que se encuentren relacionados entre sí para prevenir el caso de que se produzca un fallo de proceso y no se pueda completar la transacción.

e) Análisis periódico de los sistemas de información, de los accesos a la información y a las aplicaciones, de los registros de eventos o incidencias, de las operaciones, así como de los recursos utilizados.

f) Adopción de medidas de protección frente a código dañino en los servidores de aplicación y en los soportes circulantes.

g) Establecimiento de procedimientos para evitar la instalación de software no autorizado, el borrado accidental o no autorizado de datos y los accesos no autorizados.

#### **Quinto. Requisitos de disponibilidad de los dispositivos y aplicaciones de registro y notificación**

1. En la página web de cada órgano u organismo notificador, y en su caso en el Portal del ciudadano, se encontrarán a disposición del interesado los programas necesarios que debe instalar en su ordenador personal para el correcto funcionamiento de los sistemas de registro y notificación en especial para la lectura de las notificaciones, para verificar la autenticidad del órgano notificador y para descifrar los escritos a él dirigidos.

Dichos programas habrán de ser compatibles con los medios técnicos de que dispongan las Administraciones Públicas.

2. Los órganos de la Administración General del Estado y los Organismos Públicos vinculados o dependientes de aquella que pongan en marcha dispositivos y aplicaciones de registro o de notificación telemáticos establecerán las medidas organizativas y técnicas para que la disponibilidad del servicio sea de 7 días a la semana y 24 horas al día. En cualquier caso establecerán las siguientes medidas:

a) Mantenimiento actualizado del software de base y específico sobre el que está soportado el sistema de registro y notificaciones telemáticas, siguiendo las recomendaciones indicadas en las listas de vulnerabilidades correspondientes.

b) Actualización periódica o cuando sea necesario del software de base y corrección, en su caso, de las debilidades observadas en éste.

c) Adopción de medidas de seguridad física en el entorno donde se encuentren los equipos que den soporte a las aplicaciones.

d) Protección de los sistemas y las aplicaciones contra el código dañino y contra ataques de denegación del servicio y establecimiento en cualquier caso de las medidas oportunas.

e) Se deberá preparar y mantener operativo un plan de contingencias.

#### **Sexto. Requisitos de confidencialidad de los dispositivos y aplicaciones de registro y de notificación**

Los órganos de la Administración General del Estado y los Organismos Públicos vinculados o dependientes de aquella que pongan en marcha dispositivos y aplicaciones

de registro y notificación deben adoptar medidas de seguridad para la salvaguarda de la confidencialidad. En cualquier caso establecerán las siguientes medidas:

- a) Medidas de seguridad física.
- b) Control de los accesos a los dispositivos y aplicaciones de registro y notificación, en especial los que lleguen a través de las redes de comunicaciones.
- c) Protección de los soportes de información y copias de respaldo.
- d) Cifrado de las notificaciones, cuando así se establezca por la legislación sobre protección de los datos de carácter personal o lo estime necesario el órgano u organismo notificador.

### **Séptimo. Protocolos y criterios técnicos de los dispositivos y aplicaciones de registro y notificaciones**

1. La sincronización de la fecha y la hora de los servicios de registro telemático y de notificación telemática se realizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio del Real Instituto y Observatorio de la Armada como laboratorio depositario del patrón Nacional de Tiempo y laboratorio asociado al Centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

2. El registro telemático y el servicio de notificación telemática deberán cumplir los requerimientos en materia de accesibilidad establecidos por la Iniciativa para una Web Accesible (WAI) del Consorcio World Wide Web y en particular las especificaciones de la Recomendación de 5 de mayo de 1999 sobre Pautas de Accesibilidad del Contenido en la Web, versión 1.0, en su nivel AA.

3. El acceso del ciudadano a través de Internet a las notificaciones telemáticas y a los registros telemáticos se realizará mediante un navegador web que cumpla la especificación W3C HTML.4.01 o superior.

4. El protocolo para la comunicación entre el navegador web del interesado y el servidor de la Administración será http 1.0, o superior.

5. Los servicios de registro y de notificación telemática deberán poder utilizar en su canal de comunicaciones con los interesados cifrado simétrico de, al menos, 128 bits.

### **Octavo. Condiciones que ha de reunir el órgano, organismo, o entidad habilitada para la prestación del servicio de dirección electrónica única**

1. El órgano, organismo o entidad habilitada para la prestación del servicio de dirección electrónica única deberá poner los medios técnicos para desarrollar las siguientes funciones:

- a) Crear y mantener el directorio de direcciones electrónicas únicas.
- b) Almacenar y custodiar las notificaciones en la dirección electrónica única.

c) Gestionar los acuses de recibo de los interesados y de los órganos u organismos notificadores.

d) Mantener el registro de eventos de las notificaciones, el cual contendrá, al menos la dirección electrónica, la traza de la fecha y la hora de la recepción de la notificación en la dirección electrónica única y del acceso del interesado a la notificación y la descripción del contenido de la notificación.

e) Establecer las medidas organizativas y técnicas para que la disponibilidad del servicio sea de 7 días a la semana y 24 horas al día.

2. Podrán añadirse otras funciones de mejora del servicio y complementarias de las expresadas, como es el caso de aviso de puesta a disposición de los interesados de las notificaciones.

### **Noveno. Condiciones de la prestación del servicio de dirección electrónica única**

1. La titularidad de la dirección electrónica a partir de la cual se construyan las direcciones electrónicas únicas de los interesados, corresponde al Ministerio de Administraciones Públicas.

2. El prestador del servicio de dirección electrónica única estará sujeto a las medidas de seguridad, los requisitos de autenticidad, integridad, confidencialidad, disponibilidad y a la utilización de los protocolos y criterios técnicos establecidos en esta Orden Ministerial.

3. El directorio del servicio de dirección electrónica única deberá recoger el nombre y apellidos o la razón o denominación social del interesado, el número del documento nacional de identidad o el código de identificación fiscal o cualquier otro equivalente y la dirección electrónica única.

4. El prestador del servicio de dirección electrónica única designará a un administrador de la seguridad, responsable de la realización y actualización del análisis y gestión de riesgos, del registro de incidencias de seguridad, de la correcta implementación de las salvaguardas de seguridad técnicas, organizativas, y de cuantas otras actuaciones en materia de seguridad sean necesarias para la protección de los sistemas a su cargo.

5. El prestador del servicio de dirección electrónica única deberá remitir al órgano u organismo notificador por cada notificación telemática:

a) Certificación electrónica de la fecha y hora en la que recibe la notificación enviada por el órgano u organismo notificador.

b) Certificación electrónica de la fecha y hora en la que se produce la recepción de la notificación en la dirección electrónica única asignada al interesado.

c) Certificación electrónica en el que conste la fecha y hora en la que se produce el acceso del interesado al contenido de la notificación en la dirección electrónica.

d) Certificación electrónica de cualquier incidencia que se produzca en la práctica de lo dispuesto en los apartados anteriores.

6. El prestador del servicio de dirección electrónica única deberá adoptar las medidas organizativas y técnicas, que garanticen la calidad de dicho servicio.

7. En el caso de cese de actividad o cambio del prestador del servicio de dirección electrónica única, las bases de datos, los programas informáticos asociados, el registro de eventos y el dominio de direcciones electrónicas con las notificaciones que existan en ese momento y la documentación técnica, deberán entregarse al Ministerio de Administraciones Públicas, o a la entidad que ésta designe debidamente actualizadas.

8. Los programas necesarios para el correcto funcionamiento del sistema de notificación a los que se refiere el apartado quinto.1, serán suministrados a los órganos y organismos notificadores por el prestador del servicio de dirección electrónica única.

#### **Décimo. Competencia del Ministerio de Administraciones Públicas para el establecimiento de parámetros de calidad y vigilancia de su cumplimiento**

1. Corresponde al Ministerio de Administraciones Públicas, previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica establecer los parámetros de calidad de la prestación del servicio de dirección electrónica única y de cumplimiento de los requisitos y condiciones establecidas en la presente Orden Ministerial, así como las penalizaciones y demás medidas correctoras que sean de aplicación.

2. Corresponde al Ministerio de Administraciones Públicas validar y vigilar el cumplimiento de lo establecido en el párrafo anterior.

#### **Undécimo. Competencia del Ministerio de Administraciones Públicas para la actualización de requisitos y criterios técnicos**

La actualización de los requisitos y los criterios técnicos de esta Orden Ministerial, corresponde al Ministerio de Administraciones Públicas, previo informe favorable del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

#### **Disposición transitoria única. Validez de las notificaciones telemáticas previstas en la normativa vigente**

Serán válidas las notificaciones telemáticas de los Departamentos Ministeriales y Organismos Públicos previstas en los procedimientos telemáticos publicados en el Boletín Oficial del Estado al amparo de la Ley 30/1992 y normativa de desarrollo que a la entrada en vigor de la presente Orden se encuentren vigentes.

No obstante, deberán adaptarse a lo previsto en la presente Orden Ministerial en el plazo de un año desde su entrada en vigor.

#### **Disposición final única. Entrada en vigor**

La presente Orden Ministerial entrará en vigor el día siguiente a su publicación en el Boletín Oficial del Estado, a excepción de las disposiciones relativas a la prestación del servicio de notificación en la dirección electrónica única que entrarán en vigor a partir del inicio de actividad del prestador del servicio de dirección electrónica única previsto en la disposición final primera del Real Decreto 209/2003.