Función Pública

Decreto 1413 de 2017

Los datos publicados tienen propósitos exclusivamente informativos. El Departamento Administrativo de la Función Pública no se hace responsable de la vigencia de la presente norma. Nos encontramos en un proceso permanente de actualización de los contenidos.

DECRETO 1413 DE 2017

(Agosto 25)

"*Por el cual se adiciona el tÃtulo 17 a la parte 2 del libro 2 del Decreto Ãnico Reglamentario del sector de TecnologÃas de la InformaciÃ³n y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capÃtulo IV del tÃtulo III de la Ley 1437 de 2011 y el artÃculo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operaciÃ³n de los servicios ciudadanos digitales*"

EL PRESIDENTE DE LA REPÃBLICA DE COLOMBIA

En ejercicio de sus facultades constitucionales y legales, en especial las que le confiere el numeral 11 del artÃculo 189 de la ConstituciÃ³n PolÃtica, el artÃculo 64 de la Ley 1437 de 2011 y el artÃculo 45 de la Ley 1753 de 2015, y

CONSIDERANDO

Que la Ley 527 de 1999 "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrÃ³nico y de las firmas digitales, y se establecen las entidades de certificaciÃ³n y se dictan otras disposiciones", estableciÃ³ el reconocimiento jurÃdico a los mensajes de datos, en las mismas condiciones que se ha otorgado para los soportes que se encuentren en medios fÃsicos.

Que de conformidad con el artÃculo 2 de la Ley 1341 de 2009, las entidades pÃºblicas deberÃ¡n adoptar todas las medidas necesarias para garantizar el mÃ¡ximo aprovechamiento de las TecnologÃas de la InformaciÃ³n y las Comunicaciones en el desarrollo de sus funciones con el fin de lograr la prestaciÃ³n de servicios eficientes a los ciudadanos.

Que el artÃculo 60 de la Ley 1437 de 2011 faculta al Gobierno Nacional para definir los estÃ¡ndares de la Sede ElectrÃ³nica y a su turno el artÃculo 64 lo hace para establecer los estÃ¡ndares y protocolos que deben cumplir las autoridades para incorporar de forma gradual la aplicaciÃ³n de los medios electrÃ³nicos en los procedimientos administrativos.

Que el Decreto Ley 019 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trÃ¡mites innecesarios existentes en la AdministraciÃ³n PÃºblica, establece en el artÃculo 4 que las autoridades deben incentivar el uso de las tecnologÃas de la informaciÃ³n y las comunicaciones para que los procesos administrativos se adelanten con diligencia, dentro de los tÃ©rminos legales y sin dilaciones injustificadas; y que deben adoptar las decisiones administrativas en el menor tiempo posible.

Que a su vez los artÃculos 17 y 18 de la precitada ley, exigen que los trÃ¡mites y actuaciones que se cumplan ante las entidades pÃºblicas y los particulares que ejerzan funciones administrativas donde se exija la obtenciÃ³n de la huella dactilar como medio de identificaciÃ³n inmediata, se harÃ¡ por medios electrÃ³nicos. Para lo cual se deberÃ¡ coordinar en temas de interoperabilidad con la RegistradurÃa Nacional del Estado Civil.

Que de conformidad con el artÃculo 266 de la ConstituciÃ³n PolÃtica modificado por el Acto Legislativo 02 de 1 de julio de 2015 en concordancia con Ã©l Decreto Ley 2241 de 1986 y el Decreto Ley 1010 de 2000, corresponde a la RegistradurÃa Nacional del Estado Civil ejercer, entre otras, la funciÃ³n de organizar el Registro Civil y la IdentificaciÃ³n de los colombianos, asÃ como organizar las elecciones.

Que la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protecciÃ³n de datos personales, desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la informaciÃ³n personal que se haya recogido en las bases de datos o archivos y seÃ±ala, en los artÃculos 10, 11, 12 y 13, las condiciones bajo las cuales las entidades pÃºblicas pueden hacer tratamiento de datos personales y pueden suministrar informaciÃ³n en ejercicio de sus funciones legales.

Que el Decreto 1078 de 2015, "Por medio del cual se expide el Decreto Ãnico Reglamentario del sector de TecnologÃas de la InformaciÃ³n y las Comunicaciones", define los instrumentos, lineamientos y plazos de la estrategia de Gobierno en LÃnea (gobierno electrÃ³nico), desarrollada por el Ministerio de TecnologÃas de la informaciÃ³n y las Comunicaciones. Dicho decreto establece que las entidades estatales deberÃ¡n incluirla de forma transversal en sus planes estratÃ©gicos sectoriales e institucionales, en los que son de especial relevancia la gestiÃ³n documental

electrÃ³nica y el uso de herramientas para optimizar los trÃ¡mites adelantados por medios electrÃ³nicos.

Que el artÃculo 45 de la Ley 1753 de 2015 "Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo paÃs", establece que bajo la plena observancia del derecho fundamental de hÃ¡beas data, el Ministerio de las TecnologÃas de la InformaciÃ³n y las Comunicaciones (MinTIC), en coordinaciÃ³n con las entidades responsables de cada uno de los trÃ¡mites y servicios, definirÃ¡ y expedirÃ¡ los estÃ¡ndares, modelos, lineamientos y normas tÃ©cnicas para la incorporaciÃ³n de las tecnologÃas de la informaciÃ³n y las comunicaciones (TIC), que contribuyan a la mejora de los trÃ¡mites y servicios que el Estado ofrece al ciudadano, los cuales deberÃ¡n ser adoptados por las entidades estatales y aplicarÃ¡n, entre otros, para los siguientes casos: autenticaciÃ³n electrÃ³nica, integraciÃ³n de los sistemas de informaciÃ³n de trÃ¡mites y servicios de las entidades estatales con el Portal del Estado Colombiano, implementaciÃ³n de la estrategia de Gobierno en LÃnea, marco de referencia de arquitectura empresarial para la gestiÃ³n de las tecnologÃas de informaciÃ³n en el Estado.

Que conforme al parÃ¡grafo 1 del artÃculo 45 de la Ley 1753 de 2015, los servicios que allÃ se enuncian pueden ser prestados por el sector privado.

Que el parÃ¡grafo 2 literal a) del artÃculo 45 de la Ley 1753 de 2015 establece que se podrÃ¡ ofrecer a todo ciudadano el acceso a una carpeta ciudadana electrÃ³nica que le permitirÃ¡ contar con un repositorio de informaciÃ³n electrÃ³nica para almacenar y compartir documentos pÃºblicos o privados, recibir comunicados de las entidades pÃºblicas, y facilitar las actividades necesarias para interactuar con el Estado, por lo que se necesita establecer una polÃtica que desarrolle los contenidos mÃnimos necesarios para ello.

Que, en virtud de los anteriores considerandos, es necesario adicionar el tÃtulo 17 a la parte 2 del libro 2 del decreto Ãºnico reglamentario del sector de tecnologÃas de la informaciÃ³n y las comunicaciones, Decreto 1078 de 2015, para reglamentar parcialmente el capÃtulo IV del tÃtulo III de la ley 1437 de 2011 y del artÃculo 45 de la Ley 1753 de 2015, a travÃ©s del establecimiento de lineamientos generales en el uso y operaciÃ³n de los servicios ciudadanos digitales.

En mÃ©rito de lo expuesto,

DECRETA

ARTÃCULO 1. La parte 2 del libro 2 del Decreto Ãnico Reglamentario del sector de TecnologÃas de la InformaciÃ³n y las Comunicaciones, Decreto 1078 de 2015, tendrÃ¡ un nuevo tÃtulo con el siguiente texto:

"TÃTULO 17

REGLAMENTACIÃN PARCIAL DEL CAPÃTULO IV DEL TÃTULO III DE LA LEY 1437 DE 2011 Y DEL ARTÃCULO 45 DE LA LEY 1753 DE 2015, A TRAVÃS DEL ESTABLECIMIENTO DE LINEAMIENTOS GENERALES EN EL USO Y OPERACIÃN DE LOS SERVICIOS CIUDADANOS DIGITALES

CAPÃTULO 1

DISPOSICIONES GENERALES

ARTÃCULO 2.2.17.1.1. *Objeto.* El presente tÃtulo reglamenta parcialmente el CapÃtulo IV del TÃtulo III de la Primera Parte de la Ley 1437 de 2011 y el artÃculo 45 de la Ley 1753 de 2015; estableciendo los lineamientos que se deben cumplir para la prestaciÃ³n de servicios ciudadanos digitales, y para permitir a los usuarios el acceso a la administraciÃ³n pÃºblica a travÃ©s de medios electrÃ³nicos.

ARTÃCULO 2.2.17.1.2. *Ãmbito de aplicaciÃ³n.* SerÃ¡n sujetos obligados de las .disposiciones contenidas en el presente tÃtulo las entidades que conforman la AdministraciÃ³n PÃºblica en los tÃ©rminos del artÃculo 39 de la Ley 489 de 1998 y. los particulares que cumplen funciones pÃºblicas.

PARÃGRAFO. La implementaciÃ³n de los servicios ciudadanos digitales en las Ramas Legislativa y Judicial, en los Ã³rganos de control, los Ã³rganos autÃ³nomos e independientes, y demÃ¡s organismos del Estado no contemplados en este artÃculo, se realizarÃ¡ bajo un esquema de coordinaciÃ³n y colaboraciÃ³n armÃ³nica en aplicaciÃ³n de los principios seÃ±alados en el artÃculo 209 de la ConstituciÃ³n PolÃtica.

ARTÃCULO 2.2.17.1.3. *Definiciones generales.* Para efectos de lo establecido en este tÃtulo, se tendrÃ¡n en cuenta las siguientes definiciones:

1. Aliado tecnolÃ³gico. Es la persona jurÃdica que apoya a la entidad pÃºblica, al particular con funciones pÃºblicas o particulares autorizados por la ley en todos los aspectos relacionados con las tecnologÃas de la informaciÃ³n para el proceso de autenticaciÃ³n biomÃ©trica.

2. Articulador. Es la entidad encargada de adelantar las interacciones con los distintos actores involucrados en la prestaciÃ³n de los servicios ciudadanos digitales para lograr una prestaciÃ³n coordinada y adecuada de tales servicios.

3. Autenticidad. Es el atributo generado en un mensaje de datos, cuando existe certeza sobre la persona que lo ha elaborado, emitido, firmado, o cuando exista certeza respecto de la persona a quien se atribuya el mensaje de datos.

4. Cadenas de trÃ¡mites. Es la relaciÃ³n de dos o mÃ¡s trÃ¡mites que implica la interacciÃ³n entre dos o mÃ¡s entidades o particulares que ejerzan funciones administrativas, con el propÃ³sito de cumplir los requisitos de un determinado trÃ¡mite.

5. CÃ©dula de ciudadanÃa digital. Es el equivalente funcional de la cÃ©dula de ciudadanÃa, expedida por la RegistradurÃa Nacional del Estado Civil.

6. Credenciales de autenticaciÃ³n. Son las firmas digitales o electrÃ³nicas que utilizadas por su titular permiten atribuirle la autorÃa de un mensaje de datos. Sin perjuicio de la autenticaciÃ³n notarial.

7. Documento electrÃ³nico. Es la informaciÃ³n generada, enviada, recibida, almacenada o comunicada a travÃ©s de medios electrÃ³nicos.

8. Documento electrÃ³nico de archivo. Es el registro de la informaciÃ³n generada, recibida, almacenada, y comunicada por medios electrÃ³nicos, que permanece en estos medios durante su ciclo de vida; es producida por una persona o entidad en razÃ³n de sus actividades y debe ser tratada conforme con los principios y procesos digitales archivÃsticos.

9. Escritura PÃºblica electrÃ³nica. Es el equivalente funcional de la escritura pÃºblica, la cual debe cumplir las normas sustanciales relativas a las diferentes actuaciones notariales que ella contiene y de los preceptos de derecho notarial, conforme al Decreto-ley 960 de 1970 y demÃ¡s normas concordantes.

10. Formato o formulario. Es la plantilla estandarizada por las entidades pÃºblicas para la creaciÃ³n de documentos electrÃ³nicos de archivo.

11. Integridad. Es la condiciÃ³n que garantiza que la informaciÃ³n consignada en un mensaje de datos ha permanecido completa e inalterada, salvo la adiciÃ³n de algÃºn endoso o de algÃºn cambio que sea inherente al proceso de comunicaciÃ³n, archivo o presentaciÃ³n.

12. Manual de Condiciones. Es el documento aprobado y adoptado por el Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones mediante acto administrativo,-en el cual se definen los requisitos especÃficos para adelantar los procesos de selecciÃ³n objetiva mediante los cuales se escogerÃ¡n a los operadores de los servicios ciudadanos digitales, asÃ como los lineamientos, estÃ¡ndares y normas tÃ©cnicas necesarios para la prestaciÃ³n del servicio que deben observar los actores involucrados en la prestaciÃ³n de servicios ciudadanos digitales.

13. Marco de interoperabilidad. Es el conjunto de principios, polÃticas y recomendaciones que busca facilitar y optimizar la colaboraciÃ³n entre organizaciones privadas y entidades del Estado para intercambiar informaciÃ³n y conocimiento, en el marco de los procesos de negocio, con el propÃ³sito de facilitar la entrega de servicios a ciudadanos, empresas y a otras entidades para intercambiar informaciÃ³n, aporte de documentos y datos en lÃnea.

14. Nivel de garantÃa. Es el grado de confianza en los procesos que conducen a la autenticaciÃ³n electrÃ³nica.

15. No repudio. Es el atributo que brinda protecciÃ³n contra la denegaciÃ³n por parte de una de las partes que interviene en un trÃ¡mite ante el estado a travÃ©s de los servicios ciudadanos digitales.

16. Operador. Es la persona jurÃdica que presta los servicios ciudadanos digitales en el marco de la ley y del presente tÃtulo.

17. Privacidad por diseÃ±o: Es la protecciÃ³n de la informaciÃ³n que exige la incorporaciÃ³n en las especificaciones de diseÃ±o de tecnologÃas, procesos, prÃ¡cticas de negocio e infraestructuras fÃsicas que aseguren la protecciÃ³n de la privacidad de la informaciÃ³n.

18. Registro de usuario. Es el proceso mediante el cual las personas naturales o jurÃdicas se incorporan a los servicios ciudadanos digitales como usuarios.

19. Servicios ciudadanos digitales. Es el conjunto de servicios que brindan capacidades y eficiencias para optimizar y facilitar el adecuado acceso de los usuarios a la administraciÃ³n pÃºblica a travÃ©s de medios electrÃ³nicos. Estos servicios se clasifican en bÃ¡sicos y especiales.

20. Sistema de informaciÃ³n de monitoreo. Es el mecanismo que permite verificar el correcto funcionamiento, la calidad del servicio y capturar informaciÃ³n estadÃstica general de los operadores.

21. Usuario. Es la persona natural, nacional o extranjera titular de cÃ©dula de extranjerÃa, o la persona jurÃdica, de naturaleza pÃºblica o privada, que haga uso de los servicios ciudadanos digitales.

ARTÃCULO 2.2.17.1.4. *Actores involucrados.* La prestaciÃ³n de los servicios ciudadanos digitales involucra la participaciÃ³n de los siguientes actores:

1. Los usuarios.

2. Los organismos y entidades establecidos en el artÃculo 2.2.17.1.2 de este Decreto.

3. Los operadores de servicios ciudadanos digitales.

4. El articulador.

5. Las autoridades que tienen a su cargo las funciones de polÃtica, regulaciÃ³n, vigilancia y control sobre las actividades que involucran la prestaciÃ³n de los servicios ciudadanos digitales.

6. La RegistradurÃa Nacional del Estado Civil, como autoridad facultada por la ConstituciÃ³n PolÃtica y las leyes para la identificaciÃ³n de las personas.

ARTÃCULO 2.2.17.1.5. *Principios.* AdemÃ¡s de los previstos en el artÃculo 209 de la ConstituciÃ³n PolÃtica, 2 de la Ley 1341 de 2009, 3 de la Ley 1437 de 2011 y los atinentes a la estrategia de Gobierno en LÃnea contenida en el presente decreto, la prestaciÃ³n de los servicios ciudadanos digitales se orientarÃ¡ por los siguientes principios:

1. Accesibilidad inclusiva. Se busca que los servicios ciudadanos digitales cuenten con las caracterÃsticas necesarias para que toda la poblaciÃ³n pueda acceder a ellos, y en especial las personas que se encuentran en situaciÃ³n de discapacidad.

2. Escalabilidad. La prestaciÃ³n de los servicios ciudadanos digitales debe asegurar que, ante el incremento de la demanda por parte de nuevos usuarios, sea posible mantener los mismos niveles de servicio.

3. Gratuidad. En la prestaciÃ³n de los servicios ciudadanos digitales bÃ¡sicos no se podrÃ¡ cobrar valor alguno a los usuarios, correspondiÃ©ndoles a las entidades pÃºblicas y/o particulares que desempeÃ±en funciones pÃºblicas asumir los costos asociados a su prestaciÃ³n.

4. Libertad de entrada al mercado. En el proceso de vinculaciÃ³n de los operadores de servicios ciudadanos digitales se observarÃ¡ la libre concurrencia de interesados.

5. Libre elecciÃ³n y portabilidad. Los usuarios tendrÃ¡n el derecho a escoger el operador de su preferencia y a trasladarse entre operadores, en cualquier momento y sin restricciÃ³n alguna, conservando los mismos derechos y las caracterÃsticas mÃnimas de los servicios ciudadanos digitales bÃ¡sicos.

6. Privacidad por diseÃ±o y por defecto. Desde antes que se recolecte informaciÃ³n y durante todo el ciclo de vida de la misma, se deben adoptar medidas preventivas de diversa naturaleza (tecnolÃ³gica, organizacional, humana, procedimental) para evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la informaciÃ³n, asÃ como fallas de seguridad o indebidos tratamientos de datos personales. La privacidad y la seguridad deben hacer parte del diseÃ±o, arquitectura y configuraciÃ³n predeterminada del proceso de gestiÃ³n de informaciÃ³n y de las infraestructuras que lo soportan.

7. Seguridad, privacidad y circulaciÃ³n restringida de la informaciÃ³n. Toda la informaciÃ³n de los usuarios que se genere, almacene o transmita en el marco de los servicios ciudadanos digitales, debe ser protegida y custodiada bajo los mÃ¡s estrictos esquemas de seguridad y privacidad con miras a garantizar la confidencialidad, el acceso y circulaciÃ³n restringida de la informaciÃ³n, de conformidad con lo estipulado en el componente de seguridad y privacidad de la Estrategia de Gobierno en LÃnea.

8. Usabilidad. En el diseÃ±o y configuraciÃ³n de los servicios ciudadanos digitales se propenderÃ¡ porque su uso resulte de fÃ¡cil manejo para los usuarios.

CAPÃTULO 2

CARACTERÃSTICAS DE LOS SERVICIOS CIUDADANOS DIGITALES

SECCIÃN 1

GENERALIDADES DE LOS SERVICIOS CIUDADANOS DIGITALES

ARTÃCULO 2.2.17.2.1.1. *DescripciÃ³n de los servicios ciudadanos digitales.* Los servicios ciudadanos digitales se clasifican en bÃ¡sicos y especiales.

1. Servicios ciudadanos digitales bÃ¡sicos. Son servicios ciudadanos digitales bÃ¡sicos los siguientes:

1.1. Servicio de autenticaciÃ³n biomÃ©trica. Es aquel que permite verificar y validar la identidad de un ciudadano colombiano por medio de huellas dactilares contra la base de datos biomÃ©trica y biogrÃ¡fica de la RegistradurÃa Nacional del Estado Civil, dando pleno cumplimiento a la ResoluciÃ³n 5633 de 2016 emitida por la RegistradurÃa Nacional del Estado Civil o cualquier otra norma que la adicione, modifique, aclare, sustituye o derogue.

1.2. Servicio de autenticaciÃ³n con cÃ©dula digital. Es aquel que permite la validaciÃ³n de la identidad de los ciudadanos colombianos por medios electrÃ³nicos, a travÃ©s de la cÃ©dula de ciudadanÃa digital que para tal efecto expida la RegistradurÃa Nacional del Estado Civil.

1.3. Servicio de autenticaciÃ³n electrÃ³nica. Es aquel que permite validar a los usuarios por medios electrÃ³nicos, en relaciÃ³n con un mensaje de datos y provee los mecanismos necesarios para firmarlos electrÃ³nicamente, en los tÃ©rminos de la Ley 527 de 1999 y sus normas reglamentarias sin perjuicio de la autenticaciÃ³n notarial.

1.4. Servicio de carpeta ciudadana. Es aquel que permite el almacenamiento y conservaciÃ³n electrÃ³nica de mensajes de datos en la nube para las personas naturales o jurÃdicas, en donde Ã©stas pueden recibir, custodiar y compartir de manera segura y confiable la informaciÃ³n

generada en su relaciÃ³n con el Estado a nivel de trÃ¡mites y servicios. En ningÃºn caso la carpeta ciudadana harÃ¡ las veces de sistema de gestiÃ³n de documentos electrÃ³nicos de archivo.

1.5. Servicio de interoperabilidad. Es aquel que brinda las capacidades necesarias para garantizar el adecuado flujo de informaciÃ³n y de interacciÃ³n entre los sistemas de informaciÃ³n de las entidades del Estado, permitiendo el intercambio, la integraciÃ³n y la comparticiÃ³n de la informaciÃ³n, con el propÃ³sito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad.

2. Servicios ciudadanos digitales especiales. Se consideran servicios ciudadanos digitales especiales aquellos adicionales a los servicios ciudadanos digitales bÃ¡sicos, tales como el desarrollo de aplicaciones o soluciones informÃ¡ticas que puedan ser de interÃ©s para la administraciÃ³n o cualquier interesado en el marco de la prestaciÃ³n de los servicios ciudadanos digitales bÃ¡sicos, que aplicarÃ¡n, entre otros, para los casos descritos en el artÃculo 45 de la Ley 1753 de 2015 o aquellas normas que la sustituyan, modifiquen o deroguen, para cuyo efecto, el Ministerio de las TecnologÃas de la InformaciÃ³n y las Comunicaciones definirÃ¡ y reglamentarÃ¡ en coordinaciÃ³n con las entidades responsables de cada uno de los trÃ¡mites y servicios los estÃ¡ndares, protocolos y modelos que aplicarÃ¡n en cada caso.

Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberÃ¡ hacer uso de o estar soportado en los servicios ciudadanos digitales bÃ¡sicos cuando lo requieran.

SECCIÃ N 2

ARTICULADOR, CONDICIONES PARA LOS OPERADORES Y ACUERDOS ENTRE LOS ACTORES

ARTÃCULO 2.2.17.2.2.1. *Articulador de los servicios ciudadanos digitales.* Los servicios ciudadanos digitales serÃ¡n articulados a travÃ©s del mecanismo que determine el Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones. Para tal fin, se podrÃ¡ acudir a la creaciÃ³n de una asociaciÃ³n entre entidades pÃºblicas con o sin participaciÃ³n de particulares; a la designaciÃ³n de una entidad descentralizada que pueda cumplir tales funciones a partir de su objeto y experiencia; o a la asunciÃ³n de dicho rol directamente por el Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones.

ARTÃCULO 2.2.17.2.2.2. *Operadores de servicios ciudadanos digitales.* De conformidad con el parÃ¡grafo 1 del artÃculo 45 de la Ley 1753 de 2015, los servicios ciudadanos digitales podrÃ¡n ser ofrecidos por personas jurÃdicas pÃºblicas o privadas.

ARTÃCULO 2.2.17.2.2.3. *Condiciones mÃnimas.* AdemÃ¡s de cumplir con los requisitos exigidos en el Manual de Condiciones, cada interesado en prestar a tÃtulo de operador cualquiera de los servicios ciudadanos digitales bÃ¡sicos, deberÃ¡ acreditar ante el articulador las siguientes condiciones:

1. En relaciÃ³n con el servicio de autenticaciÃ³n con cÃ©dula digital: Las que para tal efecto establezca la RegistradurÃa Nacional del Estado Civil.

2. En relaciÃ³n con el servicio de autenticaciÃ³n electrÃ³nica: Contar con la acreditaciÃ³n del Organismo Nacional de AcreditaciÃ³n de Colombia (ONAC), en las siguientes actividades.

2.1. Emitir certificados en relaciÃ³n con las firmas electrÃ³nicas o digitales de personas naturales o jurÃdicas.

2.2. Ofrecer o facilitar los servicios de generaciÃ³n de datos de creaciÃ³n de las firmas digitales certificadas u ofrecer o facilitar los servicios de generaciÃ³n de los datos de creaciÃ³n de las firmas electrÃ³nicas.

3. En relaciÃ³n con el servicio de carpeta ciudadana. Contar con la acreditaciÃ³n del Organismo Nacional de AcreditaciÃ³n de Colombia (ONAC), en las siguientes actividades:

3.1. Emitir certificados sobre la verificaciÃ³n respecto de la alteraciÃ³n entre el envÃo y recepciÃ³n del mensaje de datos y de documentos electrÃ³nicos transferibles.

3.2. Ofrecer o facilitar servicios de registro y estampado cronolÃ³gico en la generaciÃ³n, transmisiÃ³n y recepciÃ³n de mensajes de datos.

3.3. Ofrecer los servicios de registro, custodia y anotaciÃ³n de los documentos electrÃ³nicos transferibles o transmisibles.

3.4. Ofrecer los servicios de archivo y conservaciÃ³n de mensajes de datos y documentos electrÃ³nicos transferibles o transmisibles.

4. En relaciÃ³n con el servicio de autenticaciÃ³n biomÃ©trica. Haber sido autorizado por la RegistradurÃa Nacional del Estado Civil, en las siguientes actividades:

4.1. Ofrecer el servicio de validaciÃ³n de identidad biomÃ©trica bajo los preceptos de la ResoluciÃ³n 5633 de 2016 expedida por la RegistradurÃa Nacional del Estado Civil, o cualquier otra norma que la adicione, modifique, aclare, sustituya o derogue.

4.2. Ofrecer servicio de soporte y de mecanismos de validaciÃ³n alternos para quienes no puedan identificarse a travÃ©s del sistema biomÃ©trico de huella.

4.3. Contar con presencia a nivel nacional para el registro de los usuarios en el sistema.

PARÃGRAFO. Un operador puede prestar mÃ¡s de un servicio ciudadano digital.

ARTÃCULO 2.2.17.2.2.4. *VinculaciÃ³n de las entidades pÃºblicas y particulares que ejercen funciones pÃºblicas.* CorresponderÃ¡ al articulador suscribir con los organismos y entidades pÃºblicas, asÃ como los particulares que ejercen funciones pÃºblicas, los convenios y/o contratos para que Ã©stos accedan a la prestaciÃ³n de los servicios ciudadanos digitales ofrecidos por los operadores.

ARTÃCULO 2.2.17.2.2.5. *VinculaciÃ³n de los operadores.* CorresponderÃ¡ al articulador definir el procedimiento bajo el cual los interesados en prestar los servicios ciudadanos digitales deben acreditar el cumplimiento de los requisitos y condiciones que, adicionales a los mÃnimos fijados en este tÃtulo, se establecen a nivel tÃ©cnico, de experiencia, administrativo y financiero, en el Manual de Condiciones. Para ello acudirÃ¡ a los procesos de selecciÃ³n objetiva necesarios.

ARTÃCULO 2.2.17.2.2.6. *Causales de desvinculaciÃ³n de los operadores.* El articulador podrÃ¡ desvincular a un operador de la posibilidad de prestar servicios ciudadanos digitales en cualquiera de los siguientes casos:

1. A solicitud del Operador, sin perjuicio de que este deba cumplir las obligaciones emanadas de los acuerdos o contratos que tenga vigentes para la fecha de la solicitud de retiro.

2. Cuando el operador entre voluntaria o forzosamente en causal de liquidaciÃ³n.

3. Cuando el operador no haya realizado las adecuaciones que se deriven de la actualizaciÃ³n de los requisitos mÃnimos para operar dispuestas por el Manual de Condiciones dentro del plazo estipulado por el Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones al adoptarlas.

4. Ante el incumplimiento reiterado de las obligaciones e indicadores emanados de los contratos o convenios suscritos por el articulador con las entidades para la prestaciÃ³n de los servicios ciudadanos digitales.

CAPÃTULO 3

CONDICIONES DE USO Y VIGENCIA DE LOS SERVICIOS CIUDADANOS DIGITALES

ARTÃCULO 2.2.17.3.1. *Uso de los servicios ciudadanos digitales.* SerÃ¡ obligatorio para los organismos y entidades pÃºblicas, asÃ como para los particulares que desempeÃ±en funciones pÃºblicas utilizar los servicios ciudadanos digitales, de conformidad con el artÃculo 2.2.17.1.2. de este Decreto. Su implementaciÃ³n se harÃ¡ de conformidad con la gradualidad definida en el artÃculo 2.2.17.8.1 del presente decreto.

ARTÃCULO 2.2.17.3.2. *Vigencia de los servicios de autenticaciÃ³n electrÃ³nica y carpeta ciudadana.* Los servicios de autenticaciÃ³n electrÃ³nica y carpeta ciudadana tendrÃ¡n vigencia indefinida, y terminarÃ¡n por las siguientes causas:

1. Por solicitud expresa del usuario ante el operador del servicio.

2. Por muerte de la persona natural o liquidaciÃ³n de la persona jurÃdica.

3. Por decisiÃ³n judicial.

4. La no utilizaciÃ³n por un periodo consecutivo de tres (3) aÃ±os.

5. Las demÃ¡s que establezca el Manual de Condiciones.

CAPÃTULO 4

MODELO DE GOBERNABILIDAD

ARTÃCULO 2.2.17.4.1. *PolÃtica de uso y aprovechamiento de los servicios ciudadanos digitales.* Corresponde al Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones fijar la polÃtica de uso y aprovechamiento de los servicios ciudadanos digitales en el marco del desarrollo de los componentes de la Estrategia de Gobierno en LÃnea.

ARTÃCULO 2.2.17.4.2. *SupervisiÃ³n.* El articulador adelantarÃ¡ la supervisiÃ³n de las obligaciones derivadas de los contratos suscritos por los distintos operadores de servicios ciudadanos digitales, sin perjuicio que pueda apoyarse en un tercero para adelantar tal funciÃ³n.

ARTÃCULO 2.2.17.4.3. *Vigilancia y control de las actividades involucradas en la prestaciÃ³n de los servicios ciudadanos digitales.* La vigilancia y control de las actividades involucradas en la prestaciÃ³n de los servicios ciudadanos digitales se realizarÃ¡ por cada uno de los organismos del Estado que en el marco de sus competencias tengan que conocer de una o varias de las actividades involucradas en la prestaciÃ³n de tales servicios.

CAPÃTULO 5

DERECHOS Y OBLIGACIONES DE LOS ACTORES

ARTÃCULO 2.2.17.5.1. *Obligaciones del articulador.* El articulador tendrÃ¡ a su cargo las siguientes funciones:

1. Elaborar y actualizar el Manual de Condiciones para su aprobaciÃ³n por parte del Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones.

2. Verificar el cumplimiento de los requisitos por parte de los interesados en prestar los servicios ciudadanos digitales.

3. Verificar que los operadores de autenticaciÃ³n electrÃ³nica entreguen las credenciales de autenticaciÃ³n a los usuarios que se registren ante el sistema.

4. Celebrar los acuerdos necesarios con las entidades pÃºblicas y particulares que desempeÃ±en funciones pÃºblicas para que estas puedan implementar los servicios ciudadanos digitales y cumplir con las exigencias del presente tÃtulo.

5. Adelantar los procesos de selecciÃ³n objetiva necesarios para proveer los servicios a las entidades pÃºblicas y particulares que desempeÃ±en funciones pÃºblicas con quienes haya suscrito acuerdos para la prestaciÃ³n de los servicios ciudadanos digitales.

6. Administrar los servicios de informaciÃ³n necesarios para la integraciÃ³n y unificaciÃ³n de la entrada a los servicios ciudadanos digitales.

7. Administrar el directorio de servicios de intercambio de informaciÃ³n.

8. Monitorear los indicadores de calidad del .servicio de los operadores.

9. Tramitar y responder las peticiones, quejas, reclamos y solicitudes de informaciÃ³n que le presenten los actores del sistema.

10. Verificar que los operadores cumplan con las condiciones establecidas en el Manual de Condiciones, las cuales deberÃ¡n mantenerse durante el plazo que dure su calidad de operador, para garantizar los estÃ¡ndares mÃnimos de seguridad, privacidad, acceso y neutralidad tecnolÃ³gica.

11. En caso de que el articulador sea un tercero diferente al Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones, se obliga a asistir a todas las reuniones a las que sea convocado por Ã©ste para hacer seguimiento a sus labores.

12. Informar a los operadores sobre cualquier cambio en los requisitos tÃ©cnicos para la prestaciÃ³n del servicio y definir un tiempo prudencial para su adecuaciÃ³n.

13. Generar reportes de prestaciÃ³n del servicio, conforme lo disponga el Manual de Condiciones.

14. DiseÃ±ar y desarrollar estrategias de comunicaciÃ³n y difusiÃ³n que permitan dar a conocer los beneficios, condiciones, derechos, obligaciones y deberes y demÃ¡s informaciÃ³n 1 relacionada con el uso de los servicios ciudadanos digitales.

15. AcompaÃ±ar a las entidades pÃºblicas en el anÃ¡lisis de los riesgos asociados a la implementaciÃ³n de los servicios ciudadanos digitales y definir conjuntamente con ellas los niveles de garantÃa requeridos para cada trÃ¡mite.

16. Verificar que las entidades pÃºblicas cumplan con los lineamientos de la sede electrÃ³nica, definidos en el presente tÃtulo, para efectos de su integraciÃ³n con los servicios ciudadanos digitales.

En caso de que, por cualquier causa, se haga necesaria la migraciÃ³n de usuarios de un operador a otro, el articulador deberÃ¡ adoptar las medidas necesarias para garantizar la continuidad en la prestaciÃ³n del servicio. Tales medidas deberÃ¡n contemplar, como mÃnimo, el traslado oportuno de las bases de datos, el registro de eventos, la documentaciÃ³n tÃ©cnica actualizada y la informaciÃ³n de los usuarios a otro operador con miras a que los servicios se presten sin interrupciÃ³n.

Una vez hecho lo anterior, deberÃ¡ verificar que el operador elimine de manera fÃsica y definitiva la informaciÃ³n que administrÃ³ o tratÃ³ con ocasiÃ³n de la prestaciÃ³n de sus servicios, garantizando al usuario la supresiÃ³n de la informaciÃ³n.

ARTÃCULO 2.2.17.5.2. *Obligaciones comunes de los operadores que presten servicios ciudadanos digitales.* Los operadores que presten servicios ciudadanos digitales deberÃ¡n cumplir las siguientes obligaciones:

1. Suscribir los acuerdos necesarios con el articulador conforme con el rÃ©gimen de contrataciÃ³n que sea aplicable.

2. Mantener durante toda la vigencia de la operaciÃ³n las condiciones tÃ©cnicas, organizacionales, financieras y jurÃdicas exigidas por el articulador, asÃ como los estÃ¡ndares de seguridad, privacidad, acceso, neutralidad tecnolÃ³gica y continuidad en el servicio y las condiciones acordadas con sus usuarios y entidades pÃºblicas vinculadas, sin imponer o cobrar servicios que no hayan sido aceptados expresamente por el usuario.

3. Coordinar con los otros operadores de servicios ciudadanos digitales el intercambio y la circulaciÃ³n oportuna, segura y eficiente de la informaciÃ³n de los servicios y usuarios.

4. Atender las peticiones, quejas, reclamos y solicitudes de informaciÃ³n, por parte de los usuarios y de las entidades que hacen uso de los servicios ciudadanos digitales, asÃ como los requerimientos que efectÃºen autoridades administrativas o judiciales en el marco de sus competencias.

5. Reportar al articulador y a las autoridades del caso, las anomalÃas que se registren en la prestaciÃ³n del servicio.

6. DiseÃ±ar y ejecutar estrategias de apropiaciÃ³n del modelo entre los ciudadanos, empresas y entidades pÃºblicas, buscando su participaciÃ³n activa como proveedor o consumidor de servicios ciudadanos digitales, proceso que realizarÃ¡n conjuntamente con el articulador y el Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones.

7. Suministrar servicios de soporte a los usuarios.

8. Implementar sistemas de gestiÃ³n de seguridad y controles que permitan disminuir el riesgo asociado a la integridad, confidencialidad y disponibilidad de la informaciÃ³n para lo cual adoptarÃ¡n prÃ¡cticas de amplio reconocimiento internacional.

9. Adoptar medidas para garantizar, cuando sea pertinente, el traslado oportuno de la informaciÃ³n de los usuarios a otro operador de servicios ciudadanos digitales con miras a que los servicios se presten sin interrupciÃ³n.

10. Suministrar acceso a la informaciÃ³n que sea necesaria para adelantar las acciones de monitoreo y control permanente. Para ello, de manera conjunta, los operadores deberÃ¡n contratar y asumir los costos de implementaciÃ³n, administraciÃ³n, operaciÃ³n y mantenimiento de un sistema centralizado para monitorear todos los servicios. Dicha herramienta serÃ¡ administrada por el articulador.

11. Las demÃ¡s que establezca el Manual de Condiciones.

ARTÃCULO 2.2.17.5.3. *Obligaciones especiales de los operadores que presten servicios de autenticaciÃ³n biomÃ©trica.* Los operadores que presten servicios de autenticaciÃ³n biomÃ©trica deberÃ¡n cumplir las siguientes obligaciones especiales:

1. Validar la identidad de las personas de manera presencial en los puntos acordados con los operadores de autenticaciÃ³n electrÃ³nica.

2. Guardar la evidencia del resultado de los cotejos realizados por el tiempo y bajo las condiciones que determine la RegistradurÃa Nacional del Estado Civil.

3. Informar de cualquier forma fiable a los operadores de autenticaciÃ³n electrÃ³nica acerca del resultado de la validaciÃ³n de la identidad de la persona para que estos, en caso de ser satisfactoria, procedan a la entrega de las credenciales de autenticaciÃ³n electrÃ³nica.

4. Informar a las entidades pÃºblicas, los particulares que ejerzan funciones pÃºblicas, y los particulares autorizados por la Ley, acerca del resultado de la validaciÃ³n de la identidad de las personas en los trÃ¡mites y actuaciones en los que se exija la obtenciÃ³n de la huella dactilar como medio de identificaciÃ³n.

ARTÃCULO 2.2.17.5.4. *Obligaciones especiales de los operadores que presten servicios de AutenticaciÃ³n con cÃ©dula Digital.* Los operadores que presten servicios de autenticaciÃ³n con cÃ©dula digital deberÃ¡n cumplir con todas las obligaciones y exigencias que para dicho propÃ³sito establezca la RegistradurÃa Nacional del Estado Civil, una vez se expida la cÃ©dula de ciudadanÃa digital.

ARTÃCULO 2.2.17.5.5. *Obligaciones especiales de los operadores que presten servicios de AutenticaciÃ³n ElectrÃ³nica.* Los operadores que presten servicios de autenticaciÃ³n electrÃ³nica deberÃ¡n cumplir las siguientes obligaciones especiales:

1. Registrar a los usuarios y entregar las credenciales de autenticaciÃ³n electrÃ³nica.

2. Verificar las credenciales presentadas por los usuarios de servicios ciudadanos digitales en el momento que acceden a un trÃ¡mite o servicio del Estado o cuando requieren firmar un documento electrÃ³nico.

3. Proveer los mecanismos de firma electrÃ³nica o digital en la carpeta ciudadana para que las personas naturales y jurÃdicas y las entidades pÃºblicas puedan garantizar la integridad y autenticidad de los documentos.

4. Crear y mantener una base de datos de sus usuarios, que deberÃ¡ ser actualizada, compartida y sincronizada con el articulador.

5. Gestionar las autorizaciones de los usuarios para tratar y suministrar datos personales.

6. Gestionar y comunicar oportunamente las autorizaciones de los usuarios para tratar y suministrar datos personales y la informaciÃ³n con entidades pÃºblicas en el marco de sus trÃ¡mites y servicios dando cumplimiento a los requerimientos probatorios en esta materia.

ARTÃCULO 2.2.17.5.6. *Obligaciones especiales de los operadores que presten servicios de carpeta ciudadana.* Los operadores que presten servicios de carpeta ciudadana deberÃ¡n cumplir las siguientes obligaciones especiales:

1. Disponer de una plataforma que permita al menos las siguientes funcionalidades:

1.1. Recibir documentos, comunicaciones y notificaciones electrÃ³nicas generadas por las entidades pÃºblicas o los particulares que ejercen funciones pÃºblicas.

1.2. Aportar documentos electrÃ³nicos a los trÃ¡mites que se adelanten ante entidades pÃºblicas o ante particulares que ejercen funciones pÃºblicas.

1.3. Compartir documentos electrÃ³nicos con usuarios de servicios ciudadanos digitales.

1.4. Gestionar notificaciones y comunicaciones electrÃ³nicas de las entidades pÃºblicas o de los particulares que ejercen funciones pÃºblicas.

1.5. Almacenar, conservar, gestionar y firmar electrÃ³nicamente documentos de forma segura.

2. Permitir, previa aceptaciÃ³n de tÃ©rminos y condiciones de uso y una vez otorgada la autorizaciÃ³n para el tratamiento de datos personales, el ingreso al servicio de carpeta ciudadana por parte de los usuarios mediante las credenciales de autenticaciÃ³n entregadas por el operador de autenticaciÃ³n con cÃ©dula digital y/o de autenticaciÃ³n electrÃ³nica.

3. Emitir certificaciones electrÃ³nicas a las entidades sobre el envÃo y recepciÃ³n de comunicaciones y sobre las notificaciones electrÃ³nicas enviadas a la carpeta ciudadana.

4. Crear y mantener una base de datos con la informaciÃ³n proporcionada por sus usuarios la cual deberÃ¡ ser actualizada, compartida y sincronizada con el articulador.

5. Almacenar y custodiar los avisos de puesta a disposiciÃ³n de notificaciones en la carpeta ciudadana.

6. Gestionar los acuses de recibo de los usuarios y de entidades que notifican.

7. Mantener el registro de eventos de las notificaciones.

ARTÃCULO 2.2.17.5.7. *Obligaciones especiales de los operadores que presten servicios de interoperabilidad.* Los operadores que presten servicios de interoperabilidad deberÃ¡n cumplir las siguientes obligaciones especiales:

1. AcompaÃ±ar a las entidades pÃºblicas en la creaciÃ³n, diseÃ±o, implementaciÃ³n o adecuaciones tÃ©cnicas de los trÃ¡mites y servicios que sus sistemas de informaciÃ³n expondrÃ¡n a partir de los servicios ciudadanos digitales y que estÃ©n vinculados para intercambio de informaciÃ³n en el marco de interoperabilidad.

2. Disponer en su plataforma los servicios de interoperabilidad que las entidades pÃºblicas tengan actualmente implementados o que fueron publicados en la plataforma de interoperabilidad del Estado colombiano y que han logrado el cumplimiento del requisito del nivel tres (3) de madurez "optimizado" de conformidad con lo dispuesto en el Marco de Interoperabilidad.

3. Registrar en el directorio de servicios de intercambio de informaciÃ³n que administra el articulador, los servicios de interoperabilidad que implemente o despliegue en su plataforma.

4. Configurar, habilitar y exponer servicios de intercambio de informaciÃ³n que podrÃ¡n ser consumidos por una entidad, empresa o ciudadano u otro operador de servicios ciudadanos digitales.

5. Mediar y coordinar el intercambio de informaciÃ³n de las entidades pÃºblicas y particulares que desempeÃ±en funciones pÃºblicas, los operadores de servicios ciudadanos, integrando los servicios habilitados o expuestos de conformidad con las reglas y polÃticas predeterminadas el marco de interoperabilidad.

ARTÃCULO 2.2.17.5.8. *Obligaciones de las entidades pÃºblicas y particulares que desempeÃ±en funciones pÃºblicas.* Las entidades pÃºblicas y los particulares que desempeÃ±en funciones pÃºblicas, en la implementaciÃ³n de los servicios ciudadanos digitales tendrÃ¡n las siguientes obligaciones:

1. Actualizar ante el Departamento Administrativo de la FunciÃ³n PÃºblica -DAFP- los trÃ¡mites u otros procedimientos administrativos en los cuales se haga uso de los servicios ciudadanos digitales, donde se informe claramente a los ciudadanos, usuarios o grupos de interÃ©s los pasos que deben adelantar para acceder a travÃ©s de estos servicios.

2. Analizar con el articulador los riesgos de cada trÃ¡mite con el fin de determinar los niveles de garantÃa requeridos para cada uno de ellos.

3. Definir las reglas y polÃticas que deben ser consideradas por el operador en el intercambio y composiciÃ³n de la informaciÃ³n de un servicio o trÃ¡mite determinado, lo anterior, atendiendo tos lineamientos del Marco de Referencia de Arquitectura Empresarial para la GestiÃ³n de TI en el Estado, asÃ como del Marco de Interoperabilidad para que las entidades que requieran esta informaciÃ³n en sus procesos puedan exponer o consumir servicios segÃºn corresponda.

4. Delegar formalmente los procesos de autenticaciÃ³n con cÃ©dula digital y/o autenticaciÃ³n electrÃ³nica al operador seleccionado a travÃ©s del articulador para prestarles este servicio. En este caso a la entidad se le garantizarÃ¡ tÃ©cnica y jurÃdicamente la validaciÃ³n de identidad de las personas en medio digital, de acuerdo a los niveles de garantÃa seleccionados. Â·

5. Recibir o acceder a documentos e informaciÃ³n que comparte el usuario desde su carpeta ciudadana, previo consentimiento del mismo, e integrarlos dentro de un trÃ¡mite o actuaciÃ³n sin exigir que sean presentados en medios fÃsicos.

6. Hacer uso de los servicios de intercambio de informaciÃ³n publicados con el objeto de optimizar sus procesos, automatizar los trÃ¡mites y servicios y recibir o acceder a documentos que comparte el usuario desde su carpeta ciudadana para integrarlos dentro de un trÃ¡mite o actuaciÃ³n.

7. Firmar electrÃ³nicamente los documentos que asÃ lo requieran, haciendo uso de las credenciales de autenticaciÃ³n otorgadas para tal efecto al funcionario respectivo.

8. Enviar comunicaciones, documentos y gestionar notificaciones electrÃ³nicas dirigidas a los usuarios del servicio de la carpeta ciudadana garantizando su veracidad, legalidad y exactitud, asÃ como su recepciÃ³n por el usuario.

9. No utilizar el servicio de carpeta ciudadana para el envÃo de documentaciÃ³n que tenga fines exclusivamente publicitarios o comerciales, salvo autorizaciÃ³n previa por parte del usuario.

10. Concertar con el articulador los esquemas de soporte al usuario de tal manera que los casos que competan a la prestaciÃ³n de servicios ciudadanos digitales sean escalados adecuadamente, sin perjuicio de los niveles de servicios y soporte que le competen a la entidad pÃºblica en el marco de la administraciÃ³n de sus sistemas de informaciÃ³n.

11. Presentar las peticiones, quejas, reclamos y solicitudes de informaciÃ³n ante el articulador cuando se presenten desviaciones en la calidad o anomalÃas en los servicios recibidos.

12. Inscribir y asignar roles y autorizaciones a los funcionarios pÃºblicos que intervienen en los procedimientos y trÃ¡mites que se prestarÃ¡n a travÃ©s de los servicios ciudadanos digitales y que deban ser firmados electrÃ³nicamente.

13. En los eventos de cambio de operador, deben haberse dado por terminadas las delegaciones y acuerdos de confianza, sin perjuicio de los servicios recibidos y de la integridad de la informaciÃ³n que administra la entidad a travÃ©s de los servicios ciudadanos digitales, adoptando las medidas para garantizar el traslado oportuno de la informaciÃ³n al otro operador evitando la interrupciÃ³n del servicio.

14. Garantizar una adecuada gestiÃ³n documental de la informaciÃ³n recibida de la carpeta ciudadana, respaldada en su sistema de gestiÃ³n de documentos electrÃ³nicos de archivo, aplicando las directrices que en esta materia han expedido o expidan el Archivo General de la NaciÃ³n y el Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones. En todo caso deberÃ¡n garantizar la preservaciÃ³n documental a largo plazo.

15. Incluir los mecanismos de interoperabilidad necesarios que permitan hacer mÃ¡s Ã¡giles y eficientes los trÃ¡mites y servicios evitando solicitar informaciÃ³n a ciudadanos y empresas que puedan acceder, consultar o solicitar a otra entidad. De igual forma deben usarse mecanismos de interoperabilidad para el intercambio de informaciÃ³n con otras entidades.

ARTÃCULO 2.2.17.5.9. *Deberes de los usuarios de los servicios ciudadanos digitales.* Los usuarios de los servicios ciudadanos digitales tendrÃ¡n, como mÃnimo, los siguientes deberes:

1. Informarse acerca de condiciones del servicio a travÃ©s de los tÃ©rminos y condiciones de los mismos y realizar el correspondiente registro.

2. Registrarse presencialmente ante un operador de autenticaciÃ³n electrÃ³nica, o en lÃnea cuando cuente con la cÃ©dula de ciudadanÃa digital que expida la RegistradurÃa Nacional del Estado Civil.

3. Custodiar sus credenciales de autenticaciÃ³n y hacer un buen uso de los servicios ciudadanos digitales.

4. Aceptar los tÃ©rminos y condiciones para hacer uso de los servicios ciudadanos digitales.

5. No ceder o transferir los derechos y/o obligaciones derivados de los tÃ©rminos y condiciones aprobados.

6. Velar por el buen uso que de la informaciÃ³n a la que tenga acceso a travÃ©s de los Servicios ciudadanos digitales.

7. No cometer o ser partÃcipe directa o indirectamente de actividades fraudulentas a travÃ©s de los servicios ciudadanos digitales ni hacer uso de los servicios ofrecidos para:

7.1. Difundir contenidos delictivos, violentos, pornogrÃ¡ficos, racistas, xenÃ³fobos, ofensivos, de apologÃa al terrorismo o, en general, contrarios a la ley o al orden pÃºblico.

7.2. Introducir en la red virus informÃ¡ticos o realizar actuaciones susceptibles de alterar, estropear, interrumpir o generar errores o daÃ±os en

los documentos e informaciÃ³n digital, datos o sistemas fÃsicos y lÃ³gicos, asÃ como obstaculizar el acceso de otros usuarios mediante el consumo masivo de los recursos informÃ¡ticos.

7.3. Intentar acceder a las cuentas de otros usuarios o a servicios no permitidos, o extraer informaciÃ³n.

7.4. Vulnerar los derechos de propiedad intelectual o industrial.

7.5. Violar la confidencialidad de la informaciÃ³n o de terceros.

7.6. Suplantar la identidad de otro usuario o de un tercero.

ARTÃCULO 2.2.17.5.10. *Derechos de los usuarios de los servicios ciudadanos digitales.* Los usuarios de los servicios ciudadanos digitales tendrÃ¡n derecho a:

1. Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estÃ©n vinculados por el articulador.

2. Aceptar, actualizar y revocar las autorizaciones para recibir informaciÃ³n, comunicaciones y notificaciones electrÃ³nicas desde las entidades pÃºblicas a su elecciÃ³n a travÃ©s de los servicios ciudadanos digitales.

3. Hacer uso responsable de los servicios ciudadanos digitales a los cuÃ¡les se registre.

4. Interponer peticiones, quejas, reclamos y solicitudes de informaciÃ³n en relaciÃ³n con la prestaciÃ³n a los servicios ciudadanos digitales.

5. Elegir y cambiar libremente el operador de servicios ciudadanos digitales.

6. Solicitar en cualquier momento, y a travÃ©s de cualquiera de los medios de atenciÃ³n al usuario, su retiro de la plataforma de servicios enÂ· cuyo caso podrÃ¡ descargar su informaciÃ³n a un medio de almacenamiento propio.

CAPÃTULO 6

TRATAMIENTO DE DATOS PERSONALES, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÃN

ARTÃCULO 2.2.17.6.1. *Responsable y encargado del tratamiento.* Los operadores de servicios ciudadanos digitales serÃ¡n responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen.

En cada caso, los operadores de servicios ciudadanos digitales deberÃ¡n cumplir los deberes legales que les corresponden como responsables o encargados y sin perjuicio de las obligaciones que se establecen en el presente tÃtulo.

ARTÃCULO 2.2.17.6.2. *EvaluaciÃ³n del impacto de tratamiento de datos personales.* Antes de dar inicio a la prestaciÃ³n del servicio, los operadores de servicios ciudadanos digitales deberÃ¡n evaluar el impacto de las operaciones de dichos servicios en el tratamiento de datos personales, la cual deberÃ¡ incluir como mÃnimo lo siguiente:

1. Una descripciÃ³n detallada de las operaciones de tratamiento de datos personales que involucra la prestaciÃ³n de los servicios ciudadanos digitales y de los fines del tratamiento;

2. Una evaluaciÃ³n de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

3. Una evaluaciÃ³n de los riesgos especÃficos para los derechos y libertades de los titulares de los datos personales, y

4. Las medidas previstas para afrontar los riesgos, incluidas garantÃas, medidas de seguridad, diseÃ±o de software, tecnologÃas y mecanismos que garanticen la protecciÃ³n de datos personales, teniendo en cuenta los derechos e intereses legÃtimos de los titulares de los datos y de otras personas eventualmente afectadas.

Los resultados de esta evaluaciÃ³n junto con las medidas para mitigar los riesgos serÃ¡n tenidas en cuenta e implementadas como parte de la aplicaciÃ³n del fundamento de privacidad por diseÃ±o y por defecto.

ARTÃCULO 2.2.17.6.3. *Responsabilidad demostrada y programa integral de gestiÃ³n de datos.* Los operadores de servicios ciudadanos digitales deberÃ¡n adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de GestiÃ³n de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.

El PIGD debe cumplir las instrucciones de la Superintendencia de Industria y Comercio, en particular, la guÃa para la implementaciÃ³n del principio de responsabilidad demostrada (accountability) de dicha entidad.

ARTÃCULO 2.2.17.6.4. *Delegado de protecciÃ³n de datos.* Cada operador designarÃ¡ un encargado de protecciÃ³n de datos que acredite conocimientos especializados en la materia, que actuarÃ¡ de manera autÃ³noma, imparcial e independiente y que tendrÃ¡, como mÃnimo, las siguientes funciones:

1. Velar por el respeto de los derechos de los titulares de los datos personales respecto del tratamiento de datos que realice el operador.

2. Informar y asesorar al operador en relaciÃ³n con las obligaciones que les competen en virtud de la regulaciÃ³n colombiana sobre privacidad y tratamiento de datos personales.

3. Supervisar el cumplimiento de lo dispuesto en la citada regulaciÃ³n y en las polÃticas de tratamiento de informaciÃ³n del operador y del principio de responsabilidad demostrada.

4. Prestar el asesoramiento que se le solicite acerca de la evaluaciÃ³n de impacto relativa a la protecciÃ³n de datos.

5. Atender los lineamientos y requerimientos que le haga la Delegatura de ProtecciÃ³n de Datos Personales de la Superintendencia de Industria y Comercio o quien haga sus veces.

ARTÃCULO 2.2.17.6.5. *Privacidad por diseÃ±o y por defecto.* Los operadores de servicios ciudadanos digitales deberÃ¡n atender las buenas prÃ¡cticas y principios desarrollados en el Ã¡mbito internacional en relaciÃ³n con la protecciÃ³n y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protecciÃ³n de la privacidad y de los datos no puede ser asegurada Ãºnicamente a travÃ©s del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de informaciÃ³n, modelos, prÃ¡cticas de negocio, diseÃ±o fÃsico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relaciÃ³n con la recolecciÃ³n, uso, almacenamiento, divulgaciÃ³n y disposiciÃ³n de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador. Para ello los operadores deberÃ¡n tener en cuenta los siguientes lineamientos:

1. Realizar y actualizar las evaluaciones del impacto de tratamiento de los datos personales y el Programa Integral de GestiÃ³n de Datos Personales ante cambios que generen riesgos de privacidad.

2. Incorporar prÃ¡cticas y procesos de desarrollo necesarios destinados a salvaguardar la informaciÃ³n personal de los individuos a lo largo del ciclo de vida de un sistema, programa o servicio.

3. Mantener las prÃ¡cticas y procesos de gestiÃ³n adecuados durante el ciclo de vida de los datos que son diseÃ±ados para asegurar que sistemas de informaciÃ³n cumplen con los requisitos, polÃticas y preferencias de privacidad de los ciudadanos.

4. Uso de los mÃ¡ximos medios posibles necesarios para garantizar la seguridad, confidencialidad e integridad de informaciÃ³n personal durante el ciclo de vida de los datos, desde su recolecciÃ³n original, a travÃ©s de su uso, almacenamiento, difusiÃ³n y seguro destrucciÃ³n al final del ciclo de vida.

5. Asegurar la infraestructura, sistemas TI, y prÃ¡cticas de negocios que interactÃºan o implican el uso de cualquier informaciÃ³n o dato personal siendo sujeta a verificaciÃ³n independiente por parte de todas las partes interesadas, incluyendo clientes, usuarios y organizaciones afiliadas.

ARTÃCULO 2.2.17.6.6. *Seguridad de la informaciÃ³n.* Los actores que traten informaciÃ³n, en el marco del presente tÃtulo, deberÃ¡n adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prÃ¡cticas consignadas en el modelo de seguridad y privacidad de la informaciÃ³n emitido por el Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones, o un sistema de gestiÃ³n de seguridad de la informaciÃ³n certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de informaciÃ³n.

ARTÃCULO 2.2.17.6.7. *LimitaciÃ³n al uso de la informaciÃ³n.* Los datos personales, la informaciÃ³n contenida en la carpeta ciudadana y los datos enviados a travÃ©s de los servicios de interoperabilidad de los usuarios y en general la informaciÃ³n generada, producida, almacenada, enviada o compartida en la prestaciÃ³n de los servicios ciudadanos digitales, no podrÃ¡n ser objeto de comercializaciÃ³n ni de explotaciÃ³n econÃ³mica de ningÃºn tipo, salvo autorizaciÃ³n expresa del titular de los datos.

CAPÃTULO 7

REGLAMENTACIÃN PARCIAL DEL CAPÃTULO IV DEL TÃTULO III DE LA LEY 1437 DE 2011

ARTÃCULO 2.2.17.7.1. *Sedes electrÃ³nicas.* La sede electrÃ³nica es una direcciÃ³n electrÃ³nica que permite identificar la entidad y la informaciÃ³n o servicios que provee en la web, a travÃ©s de la cual se puede acceder de forma segura y realizar con todas las garantÃas legales, los procedimientos, servicios y trÃ¡mites electrÃ³nicos que requieran autenticaciÃ³n de sus usuarios.

La sede electrÃ³nica deberÃ¡ garantizar la igualdad en el acceso a la administraciÃ³n pÃºblica y el respeto a los lineamientos de calidad, usabilidad, accesibilidad, neutralidad, interoperabilidad, confidencialidad, disponibilidad, estÃ¡ndares abiertos, seguridad y privacidad en la informaciÃ³n, servicios y trÃ¡mites provistos de conformidad con los lineamientos del Manual de Gobierno en lÃnea, el Marco de Referencia y Arquitectura TI.

Corresponde a cada entidad pÃºblica adoptar su respectiva sede electrÃ³nica mediante acto administrativo, el cual deberÃ¡ contener, como mÃnimo, la siguiente informaciÃ³n: direcciÃ³n electrÃ³nica, identificaciÃ³n de la entidad o entidades encargadas de la gestiÃ³n de la misma y de los procedimientos, servicios y trÃ¡mites puestos en ella a disposiciÃ³n de los ciudadanos e identificaciÃ³n de los canales de acceso.

ARTÃCULO 2.2.17.7.2. *CaracterÃsticas mÃnimas de la sede electrÃ³nica:* La sede electrÃ³nica deberÃ¡ tener como mÃnimo las siguientes caracterÃsticas:

1. Aplicaciones mÃ³viles: Como componente opcional de la sede electrÃ³nica se podrÃ¡ integrar el uso de aplicaciones mÃ³viles para garantizar un contacto permanente con el usuario.

2. IdentificaciÃ³n: La direcciÃ³n electrÃ³nica de referencia a la sede debe incorporar de forma visible e inequÃvoca el nombre que la identifique como tal, pudiendo utilizarse la denominaciÃ³n actual del sitio web de la entidad para identificarla siempre y cuando cumpla con las caracterÃsticas de una sede electrÃ³nica. La sede electrÃ³nica utilizarÃ¡, para identificarse y garantizar una comunicaciÃ³n segura con la misma, sistemas de firma electrÃ³nica basados en certificados de servidor web .seguro o medio equivalente.

3. PolÃticas de seguridad y tratamiento de informaciÃ³n: En la sede electrÃ³nica deberÃ¡n publicarse las polÃticas y procedimientos que rijan el tratamiento adecuado de la informaciÃ³n de la entidad, en la cual se deberÃ¡ informar a los usuarios sobre el tratamiento que se le darÃ¡ a sus datos personales, el propÃ³sito de su recolecciÃ³n y los derechos que tienen a accederlos, actualizarlos, corregirlos y revocar las autorizaciones que hayan otorgado. AsÃ mismo, se informarÃ¡ sobre las condiciones, el procedimiento y los mecanismos puestos a disposiciÃ³n para ejercerlos.

4. Procedimientos y trÃ¡mites electrÃ³nicos: A travÃ©s de la sede electrÃ³nica se realizarÃ¡n todos los procedimientos, servicios y trÃ¡mites electrÃ³nicos que requieran autenticaciÃ³n electrÃ³nica de sus usuarios. La sede deberÃ¡ admitir el uso de las credenciales de autenticaciÃ³n otorgadas por los operadores de Servicios de AutenticaciÃ³n ElectrÃ³nica y/o AutenticaciÃ³n de cÃ©dula digital a los usuarios.

5. Servicios de la sede: La sede electrÃ³nica deberÃ¡ contar con los siguientes servicios mÃnimos: relaciÃ³n de los servicios disponibles en la sede electrÃ³nica, informaciÃ³n a los usuarios sobre los servicios que tienen encomendados, los derechos que les asisten en relaciÃ³n con aquellos y sobre los compromisos de calidad en su prestaciÃ³n, formulaciÃ³n de peticiones, quejas y reclamos, acceso al estado del procedimiento o trÃ¡mite, comprobaciÃ³n de la autenticidad e integridad de los documentos emitidos por la entidad o entidades que abarca la sede, calendario de dÃas hÃ¡biles, fecha y hora oficial.

6. TÃ©rminos y condiciones de uso: En la sede electrÃ³nica deberÃ¡n publicarse los tÃ©rminos y condiciones de su uso que seÃ±alarÃ¡n como mÃnimo la identificaciÃ³n de la sede, entidad titular, naturaleza jurÃdica de la entidad o entidades responsables, el objeto de la sede, los derechos y obligaciones de la entidad y de sus usuarios respecto de su navegaciÃ³n y el uso de la informaciÃ³n publicada, informaciÃ³n necesaria para su correcto uso, propiedad intelectual, servicios electrÃ³nicos de informaciÃ³n al usuario, niveles de garantÃa requeridos o utilizadas en la sede.

ARTÃCULO 2.2.17.7.3. *Procedimiento para el registro de usuarios por medios electrÃ³nicos.* Los ciudadanos colombianos, los extranjeros con cÃ©dula de extranjerÃa vigente y las personas jurÃdicas, podrÃ¡n registrarse ante el operador de autenticaciÃ³n electrÃ³nica de su elecciÃ³n. En dicho proceso se les solicitarÃ¡ por parte del operador de autenticaciÃ³n electrÃ³nica la informaciÃ³n mÃnima necesaria para adelantar el proceso de registro y la aceptaciÃ³n expresa de los tÃ©rminos y condiciones de uso y operaciÃ³n del servicio.

El registro se harÃ¡ bajo las siguientes pautas:

1. Registro de las personas naturales. El registro de las personas naturales se efectuarÃ¡ a travÃ©s del procedimiento adelantado por los operadores de autenticaciÃ³n electrÃ³nica, en donde estos, en alianza con los operadores de autenticaciÃ³n biomÃ©trica, validarÃ¡n la identidad de las personas consultando la base de datos biomÃ©trica y biogrÃ¡fica de la RegistradurÃa Nacional del Estado Civil de acuerdo con los lineamientos definidos por dicha entidad. El registro se podrÃ¡ hacer en lÃnea cuando la persona cuente con la cÃ©dula de ciudadanÃa digital expedida por la RegistradurÃa Nacional del Estado Civil.

2. Registro de extranjeros titulares de cÃ©dula de extranjerÃa. El registro de extranjeros titulares de cÃ©dula de extranjerÃa se efectuarÃ¡ a travÃ©s del procedimiento adelantado por los operadores de autenticaciÃ³n electrÃ³nica para validar su identidad contra las bases de datos de MigraciÃ³n Colombia. Si el resultado de la validaciÃ³n de la identidad es satisfactorio, MigraciÃ³n Colombia enviarÃ¡ al operador de autenticaciÃ³n electrÃ³nica los atributos bÃ¡sicos de las personas a partir de la informaciÃ³n biogrÃ¡fica que tenga la entidad.

3. Registro de personas jurÃdicas. El registro de las personas jurÃdicas se podrÃ¡ hacer presencialmente en las CÃ¡maras de Comercio, o realizarse en lÃnea ante el operador de autenticaciÃ³n electrÃ³nica si su representante legal se ha registrado previamente como persona natural. El operador de autenticaciÃ³n elegido por el usuario, deberÃ¡ validar que dicha persona natural cuenta con la autorizaciÃ³n para representar a la persona jurÃdica, verificando la informaciÃ³n contra las bases de datos que produzca y administre la entidad facultada para ello.

4. Registro de funcionarios pÃºblicos y particulares que desempeÃ±en funciones pÃºblicas. Los funcionarios pÃºblicos y los particulares que desempeÃ±en funciones pÃºblicas deberÃ¡n registrarse ante el operador de autenticaciÃ³n electrÃ³nica de su preferencia para adquirir la calidad de usuario. En relaciÃ³n con los atributos que relacionen a un usuario con el rol de funcionario pÃºblico o particular que desempeÃ±e funciÃ³n pÃºblica, el operador deberÃ¡ complementar los datos de sus usuarios, verificando la informaciÃ³n contra las bases de datos que produzca y administre la entidad facultada para ello o en su defecto el usuario deberÃ¡ aportar actas o documentos que permitan verificar la informaciÃ³n y competencias para firmar electrÃ³nicamente actos administrativos, expedientes y documentos en general, en el marco propio de sus funciones.

ARTÃCULO 2.2.17.7.4. *ExpediciÃ³n de credenciales de autenticaciÃ³n electrÃ³nica a usuarios.* Como resultado del proceso de registro se otorgarÃ¡ al usuario un conjunto de credenciales las cuales deberÃ¡n ser usadas en los procesos de autenticaciÃ³n electrÃ³nica, para la firma de documentos en los procedimientos y trÃ¡mites que adelanten ante las entidades pÃºblicas a travÃ©s de medios electrÃ³nicos.

En caso que el usuario quiera contar con credenciales de autenticaciÃ³n electrÃ³nica adicionales a las bÃ¡sicas ofrecidos por el operador de autenticaciÃ³n electrÃ³nica, deberÃ¡ asumir el costo.

El Manual de Condiciones definirÃ¡ las credenciales bÃ¡sicas que deberÃ¡n ofrecer los operadores de autenticaciÃ³n electrÃ³nica.

ARTÃCULO 2.2.17.7.5. *Registro de documentos electrÃ³nicos.* Las entidades pÃºblicas y particulares que desempeÃ±en funciones pÃºblicas, deberÃ¡n disponer los servicios de registro electrÃ³nico, accedidos a travÃ©s de la sede electrÃ³nica, para la recepciÃ³n y remisiÃ³n de peticiones, escritos y documentos.

La sede electrÃ³nica debe integrar aplicaciones especÃficas para el tratamiento de los formatos normalizados de los procedimientos y trÃ¡mites que administra dotado de medios de control de tiempo y plazos y servicios de comunicaciones y notificaciones electrÃ³nicas. Los sistemas de informaciÃ³n que soportan la sede deben garantizar la disponibilidad e integridad de la informaciÃ³n y la correcta gestiÃ³n documental en los distintos procedimientos y trÃ¡mites electrÃ³nicos y permitir:

1. Admitir documentos electrÃ³nicos correspondientes a los servicios, procedimientos y trÃ¡mites que se especifiquen, los cuales podrÃ¡n ser aportados por el ciudadano utilizando el servicio de carpeta ciudadana u otros medios electrÃ³nicos. Los documentos se podrÃ¡n presentar todos los dÃas del aÃ±o durante las veinticuatro horas.

2. Disponer en la sede electrÃ³nica la relaciÃ³n actualizada de las peticiones, escritos y documentos recibidos incluyendo la fecha y hora de recepciÃ³n.

3. Asignar un nÃºmero consecutivo, a las comunicaciones recibidas o producidas, dejando constancia de la fecha y hora de recibo o de envÃo, con el propÃ³sito de oficializar el trÃ¡mite y cumplir con los tÃ©rminos de vencimiento que establezca la ley y hacer seguimiento a todas las actuaciones recibidas y enviadas.

4. Enviar automÃ¡ticamente por el mismo medio un mensaje acusando el recibo y registro de la peticiones, escritos o documentos de que se trate, en el que constarÃ¡n los datos proporcionados por los ciudadanos, la fecha y hora de presentaciÃ³n y el nÃºmero consecutivo de radicaciÃ³n asignado.

5. Recibir los documentos anexos a la correspondiente solicitud, mensaje o comunicaciÃ³n.

El registro electrÃ³nico generarÃ¡ mensajes que acrediten la entrega de estos documentos.

6. Distribuir electrÃ³nicamente en los tÃ©rminos que establezca la entidad para cada trÃ¡mite, los documentos registrados al destinatario o destinatarios o entidad responsable de atender el trÃ¡mite correspondiente.

7. Utilizar formatos o formularios preestablecidos para la presentaciÃ³n de documentos electrÃ³nicos normalizados correspondientes a los servicios y trÃ¡mites que se especifiquen en el sistema.

8. Adoptar en la sede electrÃ³nica el calendario oficial de la entidad con fecha y hora, los dÃas hÃ¡biles y los declarados inhÃ¡biles.

9. Posibilitar la interconexiÃ³n de todas las dependencias de la entidad para el acceso por medios electrÃ³nicos a la informaciÃ³n.

10. Adecuar un nivel de interoperabilidad entre los registros electrÃ³nicos y otros sistemas diferentes establecidos por las entidades pÃºblicas para atender otros trÃ¡mites o requerimientos especiales.

ARTÃCULO 2.2.17.7.6. *NotificaciÃ³n electrÃ³nica.* Para la notificaciÃ³n de actos administrativos las autoridades podrÃ¡n usar soluciones de notificaciÃ³n por medios electrÃ³nicos, de acuerdo a lo dispuesto en el presente artÃculo.

Las entidades podrÃ¡n notificar sus actos mediante los servicios de gestiÃ³n de notificaciones del operador de carpeta ciudadana siempre que el administrado haya autorizado expresamente tal posibilidad. Las notificaciones enviadas por las entidades pÃºblicas serÃ¡n recibidas y registradas de forma segura en la carpeta ciudadana.

La notificaciÃ³n electrÃ³nica deberÃ¡ evidenciar la fecha y hora del envÃo y acuse de recibo del acto objeto de notificaciÃ³n. La notificaciÃ³n personal se entenderÃ¡ surtida con la certificaciÃ³n de la fecha y hora de apertura del mensaje de datos que la contiene, remitida por el operador de carpeta ciudadana a la entidad que profiriÃ³ el acto administrativo.

De no poderse surtir la notificaciÃ³n en los anteriores tÃ©rminos, se darÃ¡ aplicaciÃ³n al artÃculo 69 y siguientes de la Ley 1437 de 2011.

CAPÃTULO 8

DISPOSICIONES FINALES

ARTÃCULO 2.2.17.8.1. *Gradualidad.* Las entidades a que se refiere el artÃculo 2.2.17.1.2 deberÃ¡n implementar los servicios ciudadanos digitales y la sede electrÃ³nica conforme a los lineamientos dados en este tÃtulo, dentro de los siguientes plazos:

1. Las entidades pÃºblicas priorizadas por la Ruta de la Excelencia de Gobierno en LÃnea en la categorÃa de proyectos de trÃ¡mites y servicios, tendrÃ¡n un plazo de dieciocho (18) meses contados a partir de la publicaciÃ³n, por parte del Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones, del acto administrativo a travÃ©s del cual apruebe y adopte el Manual de Condiciones.

2. Las entidades pÃºblicas del orden nacional tendrÃ¡n un plazo de veinticuatro (24) meses contados a partir de la publicaciÃ³n, por parte del Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones, del acto administrativo a travÃ©s del cual apruebe y adopte el Manual de Condiciones.

3. Las entidades pÃºblicas del orden territorial implementaran el modelo en funciÃ³n de su disponibilidad presupuestal.

4. Los particulares que desempeÃ±en funciones pÃºblicas tendrÃ¡n un plazo de veinticuatro (24) meses, contados a partir de la publicaciÃ³n, por parte del Ministerio de TecnologÃas de la InformaciÃ³n y las Comunicaciones, del acto administrativo a travÃ©s del cual apruebe y adopte el Manual de Condiciones.

5. El plazo de registro de los funcionarios pÃºblicos serÃ¡ el mismo que se definiÃ³ para la implementaciÃ³n de los servicios ciudadanos digitales y la sede segÃºn el orden nacional o territorial de la entidad a la que presta sus servicios.

6. En caso que los sujetos obligados por este decreto cuenten con implementaciones cuyas funcionalidades sean similares a las de los servicios ciudadanos digitales, estas deberÃ¡n elaborar un plan de migraciÃ³n, dentro del plazo de implementaciÃ³n que a cada una le corresponde.

PARÃGRAFO 1. Las entidades pÃºblicas del orden nacional y/o territorial requerirÃ¡n de la aprobaciÃ³n del MinTIC para realizar inversiones o proyectos de tecnologÃas de la informaciÃ³n relacionados con la prestaciÃ³n de servicios ciudadanos digitales.

ParÃ¡grafo 2. Los servicios de autenticaciÃ³n con cÃ©dula digital entrarÃ¡n en operaciÃ³n una vez sean habilitados legalmente y sean implementados por la RegistradurÃa Nacional del Estado Civil. Las entidades pÃºblicas y los particulares que ejercen funciones pÃºblicas podrÃ¡n exigir la autenticaciÃ³n con cÃ©dula digital para la realizaciÃ³n de sus trÃ¡mites en funciÃ³n de la complejidad de los mismos.

ARTÃCULO 2.2.17.8.2. *Recursos.* Los recursos necesarios para la implementaciÃ³n y operaciÃ³n de los servicios ciudadanos digitales bÃ¡sicos de las entidades que hagan parte del Presupuesto General de la NaciÃ³n y cuya financiaciÃ³n corresponda a recursos de la NaciÃ³n, serÃ¡n asumidos por el Fondo de TecnologÃas de la InformaciÃ³n y las Comunicaciones.

PARÃGRAFO. Las entidades pÃºblicas del orden nacional y/o territorial atenderÃ¡n con sus propios recursos la integraciÃ³n y operaciÃ³n al modelo de nuevos servicios ciudadanos digitales, y su implementaciÃ³n.

ARTÃCULO 2. *Vigencia y modificaciones.* El presente decreto rige a partir de su publicaciÃ³n en el Diario Oficial, y adiciona el tÃtulo 17 a la parte 2 del libro 2 del Decreto Ãnico Reglamentario del sector de TecnologÃas de la InformaciÃ³n y las Comunicaciones, Decreto 1078 de 2015.

PUBLÃQUESE Y CÃMPLASE

Dado en BogotÃ¡ D.C., a los 25 dÃas del mes de agosto de 2017

MAURICIO CÃRDENAS SANTAMARÃA

EL MINISTRO DE HACIENDA Y CRÃDITO PÃBLICO,

DAVID LUNA SÃNCHEZ

EL MINISTRO DE TECNOLOGÃAS DE LA INFORMACIÃN Y LAS COMUNICACIONES,

LILIANA CABALLERO DURÃN

LA DIRECTORA DEL DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÃN PÃBLICA

Nota: Publicado en el Diario Oficial No.

Fecha y hora de creación: 2024-06-02 21:32:26