

**MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS  
COMUNICACIONES**

**SERVICIOS DIGITALES BÁSICOS**  
*Documento de trabajo*

**DIRECCIÓN DE GOBIERNO EN LÍNEA  
DIRECCIÓN DE ESTÁNDARES Y ARQUITECTURA TI  
2016**

## TABLA DE CONTENIDO

1. CONTEXTO .....	3
2. OBJETIVO DE LOS SERVICIOS DIGITALES BASICOS .....	7
3. ACTORES INVOLUCRADOS EN LOS SERVICIOS DIGITALES BASICOS .....	7
4. DESCRIPCIÓN GENERAL DE LOS SERVICIOS BASICOS DIGITALES Y SU AMBITO DE APLICACIÓN .....	7
5. USUARIOS POTENCIALES DE LOS SERVICIOS DIGITALES BÁSICOS .....	9
6. BENEFICIOS DE LOS SERVICIOS DIGITALES BÁSICOS .....	13
7. PRINCIPIOS BÁSICOS Y FUNDAMENTOS DE LOS SERVICIOS DIGITALES BÁSICOS .....	14
8. ALINEACIÓN ESTRATÉGICA DE LOS SERVICIOS DIGITALES BÁSICOS .....	15
9. MODELO DE IMPLEMENTACIÓN DE LOS SERVICIOS DIGITALES BÁSICOS	17
9.1 Modelo Operativo .....	18
9.2 Modelo Técnico.....	24
9.3 Modelo de Seguridad y Privacidad.....	32
9.4 Modelo Financiero.....	42
9.5 Modelo de Gobernabilidad.....	44

# SERVICIOS DIGITALES BÁSICOS

## 1. CONTEXTO

De acuerdo con la información publicada por la Dirección de Gobierno en línea<sup>1</sup> del Ministerio de Tecnologías de la Información y las Comunicaciones, en el año 2012 el 50% de los ciudadanos y el 78% de las empresas usaban medios digitales para relacionarse con entidades públicas, esta cifra aumentó al 82% y 79% respectivamente en el año 2015<sup>2</sup> (MINTIC, 2015) señalando un incremento importante y una clara tendencia a mayor crecimiento en los próximos años dada la cobertura cada vez mayor del internet y la telefonía móvil. Igualmente, tomando cifras del Sistema Único de Información de Trámites SUIT<sup>3</sup> entre el año 2013 y el 2015 hubo un incremento del 24% en los trámites y servicios en línea a nivel nacional y territorial y se espera que esta cifra siga en aumento dado el impulso de la estrategia de Gobierno en línea, las políticas y la normatividad que ha expedido el gobierno para promover los servicios digitales. En este escenario se generan los siguientes retos:

### **Dificultad de identificar plenamente a las personas beneficiarias de los servicios del Estado y suplantación de identidad.**

La dificultad de identificar plenamente a los beneficiarios de los servicios del Estado o la suplantación de identidad conllevan a una asignación errada de derechos o de obligaciones, y así mismo impactan negativamente la asignación de recursos públicos. Algunos ejemplos de este impacto se pueden ver en casos como los siguientes: En el año 2012 se hicieron giros a las Entidades territoriales por valor de 132.000 millones de pesos por concepto de matrículas de niños que no existen, dejando de beneficiar, por tanto, aquellos que realmente lo necesitaban<sup>4</sup>; en el año 2015 se detectaron 656.143 casos de registros adulterados en el SISBEN lo cual involucra recursos públicos por un monto cercano a los 364.000 millones de pesos<sup>5</sup>; en el 2015, la solicitud de pensiones ante Colpensiones se presentó un fraude cercano a los 4.500 millones de pesos<sup>6</sup> ocasionados por suplantación de identidad; la Unidad de Víctimas reportó que entre el 30% y el 50% de los subsidios girados a las víctimas del conflicto tuvieron problemas de suplantación<sup>7</sup>.

Esta problemática se presenta en situaciones presenciales pero también cuando se hace uso de los medios tecnológicos. De acuerdo con las cifras de la DIJIN<sup>8</sup>, en el año 2015 el 64% de las denuncias por delitos informáticos en el país estuvieron relacionadas con hurtos o prácticas que incorporan la suplantación y robo de identidad, siendo estas las causas más relevantes de denuncias. De igual manera, de acuerdo con las cifras de la Policía Nacional, alrededor del 16% de ciberincidentes reportados en el año 2015 estuvieron asociados con la misma situación de suplantación de identidad siendo esta la segunda causa más importante de incidentes cibernéticos<sup>9</sup>.

<sup>1</sup> MINTIC, Ministerio de Tecnologías de la Información y las Comunicaciones 2014, “Conocimiento y uso – Ciudadanos”, visto el 5 de Febrero de 2016, <http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7654.html>

<sup>2</sup> MINTIC Ministerio de Tecnologías de la Información y las Comunicaciones 2015, “Estudio de cultura de uso de TIC en los colombianos para relacionarse con el Estado”

<sup>3</sup> SUIT- Sistema Único de Información de Trámites, administrado por el Departamento Administrativo de la Función Pública. <http://www.suit.gov.co>

<sup>4</sup> El Espectador, 2012, “Denuncian corrupción en sector educativo por \$132.000 millones”, visto el 22 de Febrero de 2016, <http://www.elespectador.com/noticias/educacion/denuncian-corrupcion-sector-educativo-132000-millones-articulo-327449>

<sup>5</sup> Revista Dinero 2015, “Gobierno alista reforma al SISBEN por trampas que cuestan unos \$364.000 millones al año”, 11 de Marzo, visto el 22 de Febrero de 2016, <http://www.dinero.com/economia/articulo/colombia-alista-reforma-sisben-trampas-cuestan-unos-364000-millones-ano/215527>

<sup>6</sup> La República. 2015, “Colpensiones frena más de \$15.000 millones por fraudes”, 26 de Agosto, visto el 22 de Febrero de 2016, [http://www.larepublica.co/colpensiones-frena-m%C3%A1s-de-15000-millones-por-fraudes\\_293141](http://www.larepublica.co/colpensiones-frena-m%C3%A1s-de-15000-millones-por-fraudes_293141)

<sup>7</sup> El Tiempo, 2015, “Ya son 55 los capturados señalados de estafar y suplantar a víctimas”, 14 de Octubre, visto 22 de Febrero de 2016, <http://www.eltiempo.com/politica/justicia/red-estafaba-y-suplantaba-a-victimas-del-conflicto/16402746>

<sup>8</sup> Medina, E. 2016, “En 2015, cibercrimen generó pérdidas por US\$ 600 millones en Colombia”, El Tiempo, 28 de Enero 2016, visto el 22 de Febrero de 2016, <http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604>

<sup>9</sup> Centro Cibernético Policial 2015, Ciberincidentes, Policía Nacional, Gobierno de Colombia, visto el 29 de Enero de 2016, <http://www.ccp.gov.co/ciberincidentes/tiempo-real>

Por esta razón, las entidades públicas han venido dedicando importantes esfuerzos y recursos para el diseño de sus plataformas, sistemas de información y mecanismos que permitan interactuar con las personas y validar la identificación de estas cuando acceden a sus servicios. En el año 2015, por ejemplo, la inversión en tecnología por parte del sector público nacional fue de 1,44 billones de pesos y el 25.1% de dicha inversión se dio en software o sistemas de información<sup>10</sup>, la mayoría de ellos involucrando esquemas o componentes de autenticación electrónica.

Un análisis preliminar para determinar el nivel de validación requerido por estos trámites muestra que el 29% requiere mecanismos simples de verificación de identificación, lo cual incluye el uso de claves, por ejemplo; el 67% requiere mecanismos más robustos de verificación de identificación como tokens, One Time Password- OTP o firmas digitales o electrónicas.

De otra parte, la Registraduría Nacional del Estado Civil ha desarrollado un esquema para verificar información biográfica y biométrica de las personas a través de canales digitales al cual pueden acceder instituciones públicas y privadas, lo cual representa una oportunidad para que la validación de la identidad de las personas pueda ser realizada de la más precisa posible<sup>11</sup>.

### **Alta complejidad para que las personas evidencien su identidad**

La dinámica de inversiones y crecimiento en materia de sistemas de información y de mecanismos de autenticación, conlleva una nueva dificultad, esta vez para las personas usuarias de servicios del Estado. Debido a que no existe un esquema unificado de autenticación electrónica y las personas se ven enfrentadas a numerosas plataformas tecnológicas, claves, usuarios, y demás mecanismos de autenticación, resultando en una tarea desgastante.

Si a esto se suman los mecanismos digitales que un ciudadano tiene para acceder a servicios privados con bancos, empresas de salud, redes sociales, entre otros, su situación puede ser caótica en cuanto la administración y custodia de claves, usuarios, tokens y otros mecanismos de autenticación.

Desde otro punto de vista, según estudios adelantados por la Dirección de Gobierno en línea, el 84% de los ciudadanos y empresarios estaría dispuesto a usar un mecanismo de autenticación electrónica<sup>12</sup>. Adicionalmente, la gran mayoría de ciudadanos esperarían que dicho mecanismo fuese gratuito en cuanto a que hace parte del proceso de trámites con el Estado. En este mismo estudio, el 40% los servidores públicos consultados consideran que la seguridad y confiabilidad serían los factores claves que motivarían la implementación de un esquema unificado de Autenticación Electrónica para su relacionamiento con los usuarios<sup>13</sup>.

### **Generación y envío de altos volúmenes de información y documentos de las entidades estatales a sus usuarios**

El proceso de interacción que se da entre las entidades públicas y las personas usuarias de sus servicios está mediado por una serie de requisitos y procedimientos que se deben cumplir a través de documentos de diversa índole que permiten demostrar estados, hechos o circunstancias.

En Colombia, actualmente existen cerca de 2.280 trámites de entidades nacionales y entre 93 y 150 trámites en cada entidad del orden territorial (alcaldías y gobernaciones)<sup>14</sup>. De estos trámites, el 100% produce documentos e información que debe ser entregada de vuelta a las personas como resultado. De acuerdo a un análisis interno realizado por la Dirección de Gobierno en línea del Ministerio de Tecnologías de la Información, un ciudadano

---

<sup>10</sup> Cifras extractadas por el MINTIC a partir de los reportes de las entidades públicas al Departamento Nacional de Planeación. DNP-SPI (Seguimiento a proyectos de Inversión) Visto en <http://estrategiaticolombia.co/estadisticas/stats.php?&pres=content&jer=4&cod=&id=134#TTC>

<sup>11</sup> Resolución 5633 de 2016, por la cual se reglamentan las condiciones y el procedimiento para el acceso a las bases de datos de la información que produce y administra la registraduría nacional del Estado Civil

<sup>12</sup> Dirección de Gobierno en línea, MINTIC, 2015- Evaluación de conceptos y levantamiento de la línea base de cuatro proyectos estratégicos para el Gobierno en línea - Ciudadanos, empresas y funcionarios.

<sup>13</sup> *Ibid.*

<sup>14</sup> Departamento Administrativo de la Función Pública DAFP, 2016, Sistema Único de Información de Trámites SUIT, 2016, “Trámites y otros procedimientos administrativos en el estado colombiano” 1 de Agosto, visto el 12 de agosto de 2016, [http://www.suit.gov.co/documents/10179/460149/2016-08-01-Total\\_tramites\\_medios.pdf/bd39c38f-54f4-4d02-a83b-23c79b022fe6](http://www.suit.gov.co/documents/10179/460149/2016-08-01-Total_tramites_medios.pdf/bd39c38f-54f4-4d02-a83b-23c79b022fe6)

realiza 62 trámites a lo largo de su vida<sup>15</sup>, algunos de ellos se realizan periódicamente, pero todos ellos generan la gestión de más de 1500 documentos por persona (incluyendo requisitos y resultados).

Cuando se analiza otro tipo de actuaciones administrativas como las peticiones, quejas y reclamos, la situación es similar. De acuerdo con la información reportada por 168 entidades del orden nacional, el total de peticiones, quejas y reclamos recibidos en el año 2014 ascendió a cerca de 13.884.000<sup>16</sup>, en donde la respuesta a estas solicitudes generó por lo menos igual número de documentos para los respectivos peticionarios.

Desde el punto de vista de las entidades públicas, lo anterior significa un gran volumen de documentos que deben gestionar y enviar a sus usuarios y para las personas implica la recepción, custodia y organización de información y documentos que posteriormente serán usados para otras actuaciones ante el mismo Estado o ante privados.

El envío de toda esta información y comunicaciones desde las entidades públicas a las personas genera costos al Estado, es así como en el segundo semestre del año 2015, con cargo al presupuesto del Ministerio de Tecnologías de la Información se hicieron cerca de 4.200.000 envíos de correspondencia a nivel nacional por un valor de 27.900 millones de pesos<sup>17</sup>, lo cual representa un costo promedio por envío de \$6.643 pesos por envío. Así mismo, 4-72, realizó en el año 2014 107 millones de envío y la composición del portafolio de la empresa muestra que el 56% corresponde documentos, de estos, el 24%, es decir cerca de 14.3 millones corresponde a comunicaciones desde el sector gobierno<sup>18</sup>.

### **Alta demanda y dificultad de los procesos de notificación personal**

La notificación personal es el proceso que busca informar de manera inequívoca el resultado de una actuación administrativa a la persona solicitante<sup>19</sup>. La dificultad en este proceso radica en encontrar a las personas a las cuales se debe notificar<sup>20</sup>.

El Ministerio de Educación Nacional por ejemplo, realizó 822 notificaciones mediante aviso en su página web entre 2013 y 2014<sup>21</sup>. De igual manera, la Dirección de Impuestos y Aduanas Nacional realiza en promedio 380 notificaciones quincenales por aviso correspondientes a obligaciones tributarias<sup>22</sup>. En el caso de Colpensiones, en el año 2015 se realizaron 51.329 notificaciones por aviso, asociadas a solicitudes de reconocimiento de pensión; de estas, 38.644 se hicieron a través del sitio web de la entidad y 12.685 por correspondencia.

### **Dificultad de acceso, conservación y protección de los documentos e información generados en trámites y servicios con el Estado, por parte de las personas.**

La conservación y gestión de la información y documentos que reciben las personas de las entidades públicas o que requieren para relacionarse con las mismas en formatos físicos conlleva a la pérdida de documentos, deterioro de los mismos, incapacidad de tenerlos a tiempo y la necesidad de copiarlos o solicitarlos cada vez que los necesita.

<sup>15</sup> De acuerdo con un análisis realizado por el MINTIC, un ciudadano promedio hace 62 trámites con el Estado diferentes a lo largo de toda su vida. Algunos se hacen una vez como el registro civil de nacimiento pero otros se pueden hacer varias veces en año como el pago de impuestos.

<sup>16</sup> Esta cifra se obtuvo a partir de la información reportada por las entidades del orden nacional a través del Formulario Único de Reporte de Avance de la Gestión que hace parte del Modelo Integrado de Planeación y Gestión establecido en el título 22 del Decreto 1083 de 2015. Más información se encuentra disponible en: <http://modelointegrado.funcionpublica.gov.co/inicio>.

<sup>17</sup> Esta información fue suministrada por la Dirección de Vigilancia y Control del MINTIC, en cumplimiento de lo establecido en la Resolución 1121 de 2014.

<sup>18</sup> 4-72 Servicios Postales Nacionales 2015, *Audiencia pública de rendición de cuentas vigencia 2014*, Servicios Postales Nacionales, Gobierno de Colombia, Bogotá, pp. 9-36, visto el 5 de Febrero de 2016, <http://www.4-72.com.co/sites/default/files/TextoImagenArchivo/Presentacion%20APRC%20Vig%202014%20V10.pdf>

<sup>19</sup> La Ley 1437 de 2011, Código de Procedimiento Administrativo y de lo Contencioso Administrativo, establece en el Artículo 67 que “Las decisiones que pongan término a una actuación administrativa se notificarán personalmente al interesado, a su representante o apoderado, o a la persona debidamente autorizada por el interesado para notificarse”.

<sup>20</sup> El artículo 69 de la Ley 1437 de 2011 establece que “Cuando se desconozca la información sobre el destinatario, el aviso, con copia íntegra del acto administrativo, se publicará en la página electrónica y en todo caso en un lugar de acceso al público de la respectiva entidad por el término de cinco (5) días, con la advertencia de que la notificación se considerará surtida al finalizar el día siguiente al retiro del aviso”.

<sup>21</sup> MEN, Ministerio de Educación Nacional 2014, “Notificaciones por aviso”, visto el 5 de Febrero de 2016, <http://www.mineducacion.gov.co/1759/w3-propertyvalue-56746.html>

<sup>22</sup> Información consultada con funcionarios de la DIAN, 2016.

A lo anterior se suma el hecho de que las personas no tienen toda su información en su poder. Hoy en día es difícil que un ciudadano tenga acceso directo a la información de su historia clínica, en dónde para acceder a ella debe hacer una solicitud a cada entidad de salud. Lo mismo ocurre con otro tipo de documentos como la historia laboral, las certificaciones de estudios, licencias, permisos y similares.

Así mismo, la dispersión de la misma información de las personas, servicios, trámites y documentos en diferentes entidades y bases de datos, con criterios y estándares diversos, genera riesgos en el tratamiento de la información, dificulta su administración y custodia.

Según estudios adelantados por la Dirección de Gobierno en línea del MINTIC, los ciudadanos como las empresas valoran la posibilidad de acceder a su información desde cualquier lugar o medio y resaltan la posibilidad de poder compartirla con las entidades públicas. El 59% de los ciudadanos y el 65% de las empresas, consideran que compartirían información en la interacción con las entidades públicas para adelantar trámites y servicios que requieran de dichos documentos<sup>23</sup>.

### **Dificultad en el intercambio de información, datos y conocimiento entre las entidades públicas**

Los sistemas de información de las diferentes entidades del Estado Colombiano cumplen con la misión específica para la cual fueron desarrollados, pero estos sistemas de información no siempre son compatibles entre sí, dificultando el intercambio de información y, por lo tanto, haciendo menos eficiente la administración pública. Para garantizar el adecuado flujo de información y de interacción entre los sistemas de información de las entidades del Estado, se hace necesario implementar modelos de integración e interoperabilidad que permitan que sistemas de información incompatibles puedan comunicarse adecuadamente.

Hoy en día un total de 2280 trámites de orden nacional tan solo 219 y otros procedimientos administrativos han logrado alcanzar un nivel de cumplimiento 2 o 3 de interoperabilidad, niveles que representan un avance inicial en materia de estandarización para el intercambio de información.

Lo anterior se traduce en que aún existen ineficiencias, poca oportunidad y descoordinación de datos e información entre entidades dando lugar a que cada entidad diseñe, desarrolle y ofrezca sus propios trámites y servicios, digitales de manera individual y aislada, solicitando a los ciudadanos que aporten una y otra vez los mismos documentos, duplicando esfuerzos y generando información heterogénea y generalmente inconsistente sin tener en cuenta las necesidades de integración e interacción con servicios, plataformas y sistemas de información de otras entidades, lo que a su vez ha generado en los ciudadanos una sensación de insatisfacción, por la pérdida de tiempo y los recursos usados para trasladarse a las distintas entidades para recolectar la información necesaria y poder realizar sus trámites y servicios.

No menos importante resulta la incongruencia de estadísticas y resultados obtenidos de la gestión de las entidades del Estado cuando este no actúa de manera integrada y se desconoce qué datos se producen y dónde.

*Como conclusión final, la dificultad de las personas para validar su identidad y acceder a los servicios del Estado, el riesgo de ser suplantados, el gran volumen de documentos e información que debe manejar y la dificultad para custodiarlos, así como la dispersión de esfuerzos e inversiones en sistemas de información por parte de las entidades, los costos asociados al envío físico de documentos y notificaciones, los riesgos y dificultades en el intercambio de la información y el creciente aumento de los servicios con diversas plataformas digitales no interconectadas dan lugar a la necesidad y la oportunidad para transformar y masificar el acceso a la información y servicios del Estado mediante un esquema integrado de servicios digitales básicos que permita hacer mucho más fácil, transparente, eficiente y seguro el relacionamiento de las personas con un Estado colombiano que funcione como una sola institución.*

---

<sup>23</sup> Dirección de Gobierno en línea, MINTIC, 2015- Evaluación de conceptos y levantamiento de la línea base de cuatro proyectos estratégicos para el Gobierno en línea - Ciudadanos, empresas y funcionarios.

## 2. OBJETIVO DE LOS SERVICIOS DIGITALES BASICOS

Tomando en consideración las problemáticas anteriormente enunciadas, los objetivos de los servicios digitales básicos son los siguientes:

- Que todas las personas<sup>24</sup> puedan ser reconocidas, mitigando el riesgo de suplantación de su identidad cuando adelanten trámites y servicios provistos por el Estado a través de medios digitales.
- Que todas las personas puedan tener acceso, recibir, custodiar y compartir documentos<sup>25</sup> que se producen cuando adelante trámites o acceda a servicios con el Estado.
- Que las entidades trabajen de manera coordinada e intercambien información para prestar servicios de calidad a sus usuarios.

## 3. ACTORES INVOLUCRADOS EN LOS SERVICIOS DIGITALES BASICOS

Para que los servicios digitales básicos sean implementados se requiere la participación de los siguientes actores:

- Los **ciudadanos y empresas colombianas** en sus actuaciones y relacionamiento (trámites y servicios) con las Entidades Públicas.
- Las **entidades públicas** que integran el Estado colombiano, así como las entidades privadas que ejercen funciones públicas, tanto de manera individual como en el relacionamiento entre ellas para el suministro de servicios a los ciudadanos y empresas colombianas.
- Los **operadores** que son las personas jurídicas públicas o privadas que proveerán los servicios digitales básicos una vez sean habilitados tras cumplir con la totalidad de los requisitos técnicos, financieros y jurídicos que se señalen por el Ministerio de Tecnología y Comunicaciones.
- Los **entes reguladores** que corresponden a las entidades del Estado que coordinarán los procesos de habilitación, implementación, inspección, vigilancia, control y fomento de los servicios digitales básicos garantizando el cumplimiento de los requisitos y el respeto de los derechos y garantías de todos los actores, en especial de los Ciudadanos y Empresas colombianas en su relación con el Estado. Lo anterior sin perjuicio de las competencias atribuidas a otros órganos o entidades de derecho público. Integrarán al ente regulador las siguientes entidades principalmente: MinTIC, la Superintendencia de Industria y Comercio, la Registraduría Nacional del Estado Civil, el Archivo General de la Nación y el Ministerio Público.

## 4. DESCRIPCIÓN GENERAL DE LOS SERVICIOS BASICOS DIGITALES Y SU AMBITO DE APLICACIÓN

Los servicios digitales básicos contemplan:

- La **autenticación electrónica** unificada como servicio que permita reconocer y validar la identidad de las personas cuando adelanten trámites o servicios con el Estado por medios digitales.

---

<sup>24</sup> Ciudadanos y empresas colombianas.

<sup>25</sup> Para efectos de los Servicios Digitales Básicos se entiende por documento toda aquella información generada, enviada, recibida, almacenada o comunicada a través de medios electrónicos que tenga carácter representativo o declarativo de tales, tales como mensajes de datos, archivos, URLs, registros.

- La **carpeta ciudadana** como servicio en donde las personas puedan recibir, custodiar y compartir de manera segura y confiable la información generada en su relación (trámites y servicios) con el Estado.
- La **interoperabilidad** como servicio que brinde las capacidades necesarias a las Entidades del Estado para intercambiar, integrar, compartir información con otras entidades públicas en el marco de sus procesos.

Los servicios digitales básicos se enmarcan en lo definido en el Plan Nacional de Desarrollo<sup>26</sup>, en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo<sup>27</sup> y en el cumplimiento de la normatividad aplicable. En tal sentido, su uso se dará en el **ámbito de lo público**, es decir, para aquellos procesos y actuaciones que deben surtir las personas naturales y jurídicas ante las entidades públicas o **ante los privados que desarrollen funciones públicas** y como desarrollo del derecho de toda persona de actuar ante las autoridades utilizando medios digitales, e incluso ante los privados que desarrollen funciones públicas.

Los servicios digitales comprenden funciones básicas y de valor agregado que se pueden ofrecer, de acuerdo con lo se describe a continuación:

**Funciones básicas:** Son las actividades mínimas a las que podrán acceder los ciudadanos, empresas y las entidades públicas y que deben ser desarrolladas y provistas por cualquier proveedor u operador de los Servicios Digitales Básicos, respetando siempre la seguridad de la información, la privacidad de las personas y el debido tratamiento de los datos personales:

**Tabla 1. Funciones básicas de los Servicios Digitales Básicos**

<b>Autenticación electrónica</b>	<b>Carpeta Ciudadana</b>	<b>Interoperabilidad</b>
<p><b>Reconocer y validar la identidad de las personas</b> de la manera más fiel posible, ante los sistemas de información del Estado, usando mecanismos adecuados para los diferentes niveles de garantía, mitigando el riesgo de suplantación de identidad.</p> <p><b>Firmar electrónicamente documentos</b><sup>28</sup> garantizando así la validez jurídica de las actuaciones con el Estado y de las transacciones adelantadas por medios digitales en el marco de los principios de autenticidad, integridad y disponibilidad.</p>	<p><b>Recibir documentos, comunicaciones y notificaciones.</b> Una persona natural o jurídica una vez validada su identidad podrá recibir a través del servicio de Carpeta Ciudadana todos los documentos y comunicaciones que generen desde las entidades públicas y que requieran ser entregados. Por tanto, este servicio también servirá como medio de notificación oficial, teniendo por tanto validez jurídica. Todo lo anterior, únicamente con el consentimiento pleno del titular.</p> <p><b>Compartir documentos.</b> Los ciudadanos y empresas podrán aportar documentos desde la Carpeta Ciudadana, dentro de una actuación administrativa ante entidades públicas, los cuales tendrán plena validez jurídica. En tal sentido, la Carpeta Ciudadana</p>	<p><b>Habilitar y consumir servicios:</b> Las entidades públicas podrán, a través de los operadores, exponer y registrar sus servicios en el directorio de servicios de intercambio de información habilitado por MINTIC<sup>29</sup>, de forma que puedan ser compartidos o consumidos por otras entidades para construir cadenas de trámites<sup>30</sup> y servicios de interés para los usuarios. Los servicios abarcan desde el intercambio de grandes volúmenes de datos, tipo archivos o expedientes, pasando por el intercambio de documentos sencillos e intercambio de datos e información.</p> <p><b>Virtualizar datos.</b> Las entidades públicas podrán, a través de los operadores, recopilar grandes volúmenes de datos provenientes de diversas fuentes al interior de</p>

<sup>26</sup> Ley 1753 de 2015, Artículo 45.

<sup>27</sup> Ley 1437 de 2011, Artículo 53 y siguientes

<sup>28</sup> La expresión “firmar electrónicamente” comprende cualquier alternativa de identificación digital como, entre otras, la firma electrónica o la firma digital.

<sup>29</sup> Para mayor información consultar el Portal de Lenguaje común de intercambio de información de la Dirección de Gobierno en Línea del MINTIC que se encuentra disponible en <http://lenguaje.intranet.gov.co/web/gelxml/inicio>

<sup>30</sup> La relación que se establece entre los trámites en función de los requisitos exigidos para su realización, los cuales se cumplen a través de otros trámites o servicios prestados por otras entidades, genera las cadenas de trámites. Visto en : <http://www.MINTIC.gov.co/portal/604/w3-article-5496.html>.



	<p>podrá integrarse con las sedes electrónicas, ventanillas únicas y demás plataformas transaccionales en donde se realizan trámites y servicios. De igual forma, las personas naturales y jurídicas podrán compartir documentos entre ellos mismos o con privados. Todo lo anterior, únicamente bajo la autorización del propietario/titular de la Carpeta.</p> <p><b>Custodiar documentos:</b> Los ciudadanos y empresas podrán almacenar y administrar sus documentos dentro de su Carpeta, de forma segura. Dicha administración incluye como mínimo cargar, almacenar, descargar, imprimir, organizar, borrar y recuperar documentos, al igual que el monitoreo y estadísticas de tales tareas.</p> <p>En lo que respecta al intercambio de información o interoperabilidad, se proveerán los siguientes servicios mínimos o básicos para las entidades.</p>	<p>sus áreas funcionales y mostrarlos de forma centralizada y saneada para su posterior uso, facilitando y agilizando la provisión de información a los trámites y servicios que ofrecen a los usuarios, con el fin de mejorar el rendimiento y hacer más oportuna la respuesta.</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Funciones de valor agregado.** Podrán desarrollarse funcionalidades adicionales de acuerdo con las necesidades de los usuarios y las posibilidades que vayan surgiendo una vez se consoliden las funcionalidades básicas. Esta expansión quedará a discreción de los operadores de servicios quienes los podrán desarrollar de manera autónoma y bajo los lineamientos de operación y prestación del servicio que defina el gobierno nacional. Lo anterior siempre y cuando cumplan las siguientes reglas:

- Deben respetar los principios y fundamentos definidos para los Servicios Digitales Básicos con excepción del principio de gratuidad pues podrán los usuarios previo consentimiento adherirse a funcionalidades agregadas de los operadores asumiendo un costo.
- Deben cumplir con el régimen legal colombiano.
- Deben respetar siempre los derechos de las personas y la privacidad de su información.
- Su uso debe ser aprobado previamente y con claro conocimiento por los usuarios a quienes van dirigidos.
- No deben menoscabar la calidad y disponibilidad de los servicios básicos.
- Deben ser aprobados previamente por la instancia que realice la vigilancia y control.

## 5. USUARIOS POTENCIALES DE LOS SERVICIOS DIGITALES BÁSICOS

Los siguientes son los usuarios que podrán acceder y beneficiarse con los servicios digitales básicos:

- **Personas naturales entre 7 y 18 años:** Podrán acceder al servicio de autenticación electrónica las personas naturales mayores de 7 años, edad desde la cual se cuenta con su información biométrica y cuando es posible la emisión de su tarjeta de identidad. Estas personas podrán alojar sus documentos en la Carpeta Ciudadana de uno de los padres, es decir que los procesos de recibir, custodiar y de compartir, estarán mediados por uno de los padres o tutor.

- **Personas naturales mayores de 18 años:** Podrán acceder a los servicios digitales de autenticación electrónica y carpeta ciudadana sin restricción alguna.
- **Extranjeros que cuenten con cédula de extranjería:** Podrán acceder a los servicios digitales de autenticación electrónica y carpeta ciudadana sin restricción alguna.
- **Personas Jurídicas establecidas legalmente en Colombia:** Podrán acceder a los servicios digitales de autenticación electrónica y carpeta ciudadana sin restricción alguna y al servicio de interoperabilidad, esto incluye a entidades públicas y privadas.

Frente a la población que realiza transacciones con el Estado, las cifras señalan que en 2015 el 64% de las personas entre 16 y 70<sup>31</sup> realizaron gestiones con el Estado haciendo uso de medios digitales<sup>32</sup>. En este caso, para efectuar la proyección en los próximos años se asume que habrá un incremento de 4 puntos porcentuales anuales hasta el año 2018 y a partir de allí se mantiene<sup>33</sup>.

En cuanto a las personas dispuestas a usar servicios de Carpeta Ciudadana, las cifras actuales señalan que el 15% sí la utilizaría y el 44% posiblemente, dependiendo sus beneficios. Esto significa que la población dispuesta a usar la carpeta oscila entre el 15% y el 59%. En lo que respecta a las personas dispuestas a usar el servicio de Autenticación Electrónica, las cifras actuales señalan que el 26,3% definitivamente utilizarían el servicio y el 58,5% lo utilizaría solo en caso de algunos beneficios<sup>34</sup>. Esto significa que la población dispuesta a usar el servicio de Autenticación Electrónica oscila entre el 26% y el 84%. Para realizar la proyección hasta el año 2020 se asume que este porcentaje se mantiene en los próximos años.

A partir de los anteriores escenarios se calcula la población potencial a beneficiar con los servicios digitales básicos, la cual aparece en la siguiente tabla:

**Tabla 2. Estimación de la población potencial a beneficiar con Servicios Digitales Básicos (Carpeta Ciudadana y Autenticación Electrónica)**

Criterio	2016	2017	2018	2019	2020
A. Población Nacional (DANE)	48.742.553	49.286.435	49.829.048	50.369.268	50.906.520
B. Población entre 16-70 años (64% del total). $B=A*64\%$	32.835.341	33.303.159	33.758.685	34.204.189	34.637.844
C. % Población que realiza transacciones electrónicas con el Estado	68%	72%	76%	76%	76%
D. Población que realiza transacciones electrónicas con el Estado $D=B*C$	22.328.031	23.978.274	25.656.600	25.995.183	26.324.761
E. Población dispuesta a usar Carpeta Ciudadana (15%). $E=B*15\%$	4.925.301	4.995.474	5.063.803	5.130.628	5.195.677
F. Población potencial que usaría Carpeta (59%). $F=B*59\%$	19.372.851	19.648.864	19.917.624	20.180.471	20.436.328
G. Población dispuesta a usar carpeta y que realiza transacciones con el Estado $G=E*C$	3.349.205	3.596.741	3.848.490	3.899.278	3.948.714
H. Población potencial que usaría carpeta y transa con el Estado $G=F*C$	13.173.539	14.147.182	15.137.394	15.337.158	15.531.609

<sup>31</sup> Si bien, la población entre 7 y 16 años es potencialmente beneficiaria del servicio de Autenticación Electrónica esta no se incluye en la estimación y proyecciones debido al bajo nivel de interacciones con el Estado las cuales en su mayoría están mediadas por uno de los padres. Así mismo para las proyecciones de población de Carpeta Ciudadana se asume que la cifra de personas entre los 16 y 17 años incluida en los estudios y que interactúa con el Estado a través de medios digitales no afecta significativamente el resultado proyectado.

<sup>32</sup> Esta cifra es tomada de los estudios y sondeos que realiza anualmente la Dirección de Gobierno en Línea del MINTIC para medir el conocimiento y uso de medios electrónicos de los ciudadanos de todo el país para relacionarse con el Estado.

<sup>33</sup> Esto se hace considerando las metas anuales de aumento en la cifra de personas que realizan transacciones con el Estado, las cuales prevén un crecimiento de 4 puntos porcentuales anuales hasta 2018.

<sup>34</sup> Esta cifra es tomada del *Estudio de Evaluación de Conceptos y Levantamiento de Línea Base de Carpeta Ciudadana*, el cual fue llevado a cabo por la Dirección de Gobierno en Línea del MINTIC en el año 2015.

Criterio	2016	2017	2018	2019	2020
I. Población que definitivamente utilizaría el servicio de Autenticación Electrónica y que realiza transacciones con el Estado (26,3%) $I=D*26,3\%$	5.872.272	6.306.286	6.747.686	6.836.733	6.923.412
J. Población potencial que usaría el servicio de Autenticación Electrónica y que realiza transacciones con el Estado (84,5%) $J=D*84,5\%$	18.867.186	20.261.642	21.679.827	21.965.930	22.244.423

Fuente: Elaboración propia con base en el estudio de everis<sup>35</sup>

De acuerdo con lo anterior, en un escenario conservador, es decir, tomando las personas dispuestas a usar los servicios y que realizan transacciones, la población beneficiada en un periodo de cinco años para el servicio de Carpeta Ciudadana, oscila entre 3.34 y 3.94 millones. Si al grupo anterior se suma aquella población que estaría dispuesta a usar la Carpeta, una vez comprobados sus beneficios, la cifra de beneficiados puede ubicarse entre 13.17 y 15.53 millones de personas en el mismo periodo de 5 años.

Por su parte, tomando las personas que definitivamente utilizarían el servicio de Autenticación Electrónica y que realiza transacciones con el Estado, la población beneficiada en un periodo de cinco años, está entre 5.87 y 6,92 millones. Si al grupo anterior se suma aquella población que utilizaría solo en algunos casos el servicio, la cifra de beneficiados puede estar entre 18.86 y 22.24 millones de personas en el mismo periodo de 5 años.

Si bien la Carpeta Ciudadana se enfoca en las personas naturales, existe la posibilidad de integrar esta solución a personas jurídicas. Las cifras de empresas dispuestas a usar la Carpeta señalan que el 11% sí la utilizaría y el 54% posiblemente, dependiendo sus beneficios<sup>36</sup>. Esto significa que la población empresarial dispuesta a usar la Carpeta oscila entre el 11% y el 65%. Para realizar la proyección hasta el año 2020 se asume que este porcentaje se mantiene en los próximos años. Sin embargo, es importante realizar un ajuste con las cifras de conectividad que para 2018 el cubrimiento será de un 70% de las empresas<sup>37</sup>. En este caso, para realizar la proyección en los próximos años se asume el incremento estimado de esta meta de gobierno de conectividad hasta el año 2018 y a partir de allí se mantiene<sup>38</sup>.

A partir de los anteriores escenarios se calcula la población empresarial potencial a beneficiar con la plataforma de servicios digitales básicos específicamente con la Carpeta Ciudadana y el servicio de Autenticación Electrónica, la cual aparece en la siguiente tabla:

**Tabla 3. Estimación potencial de empresas**

Criterio	2016	2017	2018	2019	2020
A. Universo Empresas (DANE)	1.268.177	1.268.177	1.268.177	1.268.177	1.268.177
B. % de empresas conectadas a Internet	66%	68%	70%	70%	70%
C. Empresas dispuestas a usar carpeta (11%) $C= A*0,11$	139,499	139,499	139,499	139,499	139,499
D. Empresas potenciales que usaría carpeta (65%) $D = A*0,65$	824,315	824,315	824,315	824,315	824,315
E. Empresas que definitivamente siempre utilizaría AE (41,3%). $E= A*0,413$	523,757	523,757	523,757	523,757	523,757
F. Empresas potenciales que usarían AE - La utilizaría solo en algunos casos (43,4%). $F = A*0,434$	550,389	550,389	550,389	550,389	550,389
G. Empresas dispuesta a usar carpeta (conectadas a Internet). $G= B*C$	91,372	94,86	97,65	97,65	97,65

<sup>35</sup> Everis 2015. Carpeta Ciudadana y Autenticación Electrónica, en el marco del contrato de consultoría no. 0000535 de 2015 para la conceptualización y diseño del modelo y la estrategia de implementación de los proyectos de “carpeta ciudadana” y “autenticación electrónica” del plan vive digital 2014 – 2018.

<sup>36</sup> Esta cifra es tomada del *Estudio de Evaluación de Conceptos y Levantamiento de Línea Base de Cuatro Proyectos Estratégicos para Gobierno en Línea*, el cual fue llevado a cabo por la Dirección de Gobierno en Línea del MINTIC en el año 2015.

<sup>37</sup> Esta cifra es tomada de las metas de conectividad del MINTIC.

<sup>38</sup> Esto se hace considerando metas para los años 2016 al 2018, y de ahí en adelante constante.

H. Empresas potenciales que usaría carpeta (conectadas a Internet). $H = B * D$	539,926	560,534	577,021	577,021	577,021
I. Empresas que utilizarían AE (conectadas a Internet) $I = B * E$	345,68	356,155	366,63	366,63	366,63
J. Empresas potenciales que usarían AE (conectadas a Internet). $J = B * F$	363,257	374,264	385,272	385,272	385,272

*Fuente:* Elaboración propia con base en el estudio de everis<sup>39</sup>

Nuevamente en un escenario conservador, es decir, tomando las empresas dispuestas a usar la Carpeta conectadas a Internet, la población beneficiada en un periodo de cinco años, está entre 91.372 y 97.650. Si al grupo anterior se suman aquellas empresas que estarían dispuestas a usar la Carpeta, una vez comprobados sus beneficios, la cifra de beneficiados puede oscilar entre 539 y 577 mil empresas en el mismo periodo de 5 años.

Del mismo modo, tomando las empresas que definitivamente utilizarían el servicio de Autenticación Electrónica y que realiza transacciones con el Estado, las empresas beneficiadas en un periodo de cinco años, está entre 345 mil y 366 mil. Si al grupo anterior se suman aquellas empresas que utilizarían solo en algunos casos el servicio, la cifra de beneficiados puede estar entre 363 mil y 385 mil empresas en el mismo periodo de 5 años.

Desde la perspectiva de la Interoperabilidad como servicio, se infiere que los cálculos de población y empresas beneficiadas por los servicios de Carpeta Ciudadana y Autenticación Electrónica se constituyen como beneficiarios finales de los servicios digitales básicos que surjan del intercambio de información e interoperabilidad de las Entidades del Estado.

No obstante lo anterior y dada la naturaleza y enfoque del servicio de interoperabilidad, se consideran beneficiarios potenciales directos el universo de entidades públicas del nivel nacional y territorial que deban intercambiar servicios e información para la atención a los ciudadanos, destacándose que se focalizarán esfuerzos en los servicios y entidades incluidos en la Ruta de Excelencia<sup>40</sup> de la estrategia de Gobierno en Línea. Las transacciones en el año, corresponden al número de solicitudes de los trámites por parte de los ciudadanos recibidas en el periodo y fueron obtenidas a partir de la información consolidada a Diciembre 2015 por el equipo Ruta de Excelencia.

<sup>39</sup> Everis 2015. Carpeta Ciudadana y Autenticación Electrónica, en el marco del contrato de consultoría no. 0000535 de 2015 para la conceptualización y diseño del modelo y la estrategia de implementación de los proyectos de “carpeta ciudadana” y “autenticación electrónica” del plan vive digital 2014 – 2018.

<sup>40</sup> Mayor información sobre esta iniciativa se puede consultar en: <http://estrategia.gobiernoenlinea.gov.co/623/w3-article-9404.html>.

**Tabla 4. Trámites y Servicios de la Ruta de Excelencia potenciales usuarias de Interoperabilidad**

TRAMITES y SISTEMAS DE LA RUTA DE EXCELENCIA		ENTIDAD																															31 Entidades involucradas	TOTAL TRANSACCIONES 2015
		Registraduría Nacional del Estado Civil	Delegaciones Registraduría Nacional del Estado Civil	Registradurías Locales	Ministerio de Relaciones Exteriores y Consulados	Ministerio de Salud y Protección Social	Unidad de Gestión Pensional y Parafiscales - UGPP	Secretarías de Salud	Ministerio de Defensa	Dirección de Impuestos y Aduanas Nacionales - DIAN	Ministerio de Educación Nacional	Instituto Geográfico Agustín Codazzi	Oficinas de Registro y Catastro municipales	Secretarías de Hacienda	Ministerio de Hacienda y Crédito Público	Agencia Nacional para la Superación de la Pobreza Extrema - ANSPE	Instituto Colombiano de Bienestar Familiar - ICBF	Ministerio del Interior	Instituto Colombiano de Desarrollo Rural - INCODER	Instituto Nacional de Vigilancia sobre Medicamentos y Alimentos - INVIMA	Unidad de Restitución de Tierras	Unidad de Atención y Reparación Integral a las Víctimas - UARIV	Superintendencia de Notariado y Registro	Consejo Superior de la Judicatura	Fiscalía General de la Nación	Presidencia de la República	Ministerio de Trabajo	Unidad Nacional para la Gestión del Riesgo Desastres	Policía Nacional	Dirección Nacional Bomberos de Colombia	Dirección de Reclutamiento del Ejército Nacional	Defensa Civil Colombiana		
1	Registro Civil																																3	884.921
2	Historia Clínica Electrónica																																2	22.000.000
3	Tarjeta Militar																																11	200.000
4	Cédula de ciudadanía																																4	1.204.499
5	Pasaporte																																2	686.466
6	Convalidación de títulos																																3	8.000
7	Afiliación única a la Seguridad Social																																4	700.000
8	Solicitud de citas médicas y autorización de servicios médicos y medicamentos																																2	43.761.534
9	Inscripción y actualización en el SISBEN																																4	2.500.000
10	Impuesto Predial																																5	15.759.206
11	Creación de empresa																																2	300.000
12	Factura Electrónica																																2	-
13	Impuestos de Industria y Comercio																																3	10.100.000
14	Registro sanitario																																3	16.750
15	Historia laboral																																3	173.504
16	Atención de conflictos familiares en línea																																1	75.000
17	Sistema Nacional del Proceso de Restitución de Tierras (SNPRT)																																9	
18	Sistema Nacional de Atención y Reparación Integral de Víctimas (SNARIV)																																8	
19	Sistema Integrado de Seguridad y Emergencias (SIES) a nivel territorial y nacional.																																7	
TOTALES		11	1	2	5	6	1	1	2	6	3	2	4	2	5	1	2	1	2	1	2	3	2	2	2	2	2	1	1	1	1	1		98.369.880

Fuente: Elaboración propia con cifras del estudio de la Corporación Colombia Digital<sup>41</sup>

## 6. BENEFICIOS DE LOS SERVICIOS DIGITALES BÁSICOS

Se han identificado los siguientes beneficios potenciales de la implementación de los servicios digitales básicos.

- Garantizar a los ciudadanos y empresas la igualdad en el acceso a la Administración por medios digitales, transformando y masificando la prestación de servicios del Estado que son apoyados en las Tecnologías y las Comunicaciones de tal manera que:
  - Adelanten trámites con diligencia, eliminando barreras propias de los trámites por mecanismos tradicionales y presenciales.
  - Sean reconocidos por medios digitales, mitigando el riesgo de suplantación de su identidad cuando adelanten trámites y servicios provistos por el Estado.
  - No tengan que registrarse de manera independiente en cada uno de los sistemas de información de las entidades públicas, ocasionando que tengan que memorizar diferentes y numerosas claves para acceder a las plataformas digitales de las entidades públicas cuando requieren demostrar su identidad.
  - Se fortalezca la protección de los datos personales.
  - Reciban, custodien y compartan información, documentos y notificaciones fruto de sus actuaciones y relacionamiento con el Estado

<sup>41</sup> Corporación Colombia Digital. 2016. Modelo de Interoperabilidad Autosostenible – en el marco del Contrato Interadministrativo N° 000376 de 2015 para los Servicios de acompañamiento especializado al Ministerio TIC en la implementación de las iniciativas: Fortalecimiento de la Gestión de TI en el Estado y la Estrategia de Gobierno en Línea.

- Eviten desplazamientos y costos para reunir y aportar información que ya reposa en las entidades públicas y que puede ser intercambiada e integrada a los trámites por parte de estas sin convertir al ciudadano en mensajero del Estado que debe actuar como uno sólo.
- b) Garantizar las capacidades en las entidades para intercambiar, integrar, compartir información en el marco de sus procesos, con el propósito de facilitar la entrega de servicios digitales a los ciudadanos, empresas y a otras entidades, funcionando el Estado colombiano como uno sólo.
- c) Crear las condiciones de confianza en el uso de los medios digitales a través de las medidas necesarias para garantizar la calidad y eficacia en la atención así como la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos y las comunicaciones.

## 7. PRINCIPIOS BÁSICOS Y FUNDAMENTOS DE LOS SERVICIOS DIGITALES BÁSICOS

Los servicios digitales básicos atenderán los siguientes principios:

- **Seguridad, privacidad y circulación restringida de la información.** Toda la información de las personas que se genere, almacene o transmita en el marco de los servicios digitales básicos debe ser protegida y custodiada bajo los más estrictos esquemas de seguridad y privacidad con miras a garantizar la confidencialidad, el acceso y circulación restringida<sup>42</sup> de la información y evitar el indebido tratamiento de los datos personales. Igualmente, se deben respetar siempre los derechos al buen nombre, la intimidad y a la protección de datos personales de conformidad con la ley 1581 de 2002.
- **Gratuidad para el usuario.** Los servicios digitales básicos deberán ser gratuitos para los usuarios.
- **Voluntariedad.** Los usuarios serán quienes acojan voluntariamente el uso de los servicios digitales básicos y autorizarán a su elección con cuáles de las aplicaciones o sistemas de información de las entidades públicas desea establecer vínculo para acceder a los servicios ofrecidos por estas y con cuáles autoriza recibir y compartir su información.
- **Simplicidad de uso, acceso e integración.** El proceso de recibir, custodiar y compartir documentos así como la validación de la identidad de los usuarios que realizan actuaciones ante el Estado por medios digitales debe ser sencillo y fácil de usar. Para las entidades, por su parte, debe ser fácil su integración con los diferentes sistemas o plataformas tecnológicas que soportan sus servicios/procesos.
- **Acceso y uso.** Se garantizará el acceso<sup>43</sup> y uso de los servicios digitales a cualquier persona independientemente de su condición física, social o económica y no debe dar lugar a discriminación o beneficios especiales para personas o grupos determinados.
- **Eficacia y Eficiencia.** Las entidades y operadores buscarán que los procedimientos logren su finalidad procurando la efectividad del derecho material; para ello se removerán los obstáculos formales, se garantizará un uso eficiente de los recursos públicos y se promoverá la convergencia de esfuerzos y de diversas fuentes de recurso<sup>44</sup>.

<sup>42</sup> La circulación restringida de la información es un principio de la Ley de protección de datos personales (Ley 1581 de 2012) que implica que las actividades de recolección, procesamiento y divulgación de información están sometidas a límites específicos determinados en el objeto de la recolección de datos y en la autorización para su tratamiento y circulación que otorgue el titular.

<sup>43</sup> El artículo 53 de la Ley 1437 de 2011 (CPACA) establece que siempre las entidades del estado deben garantizar la igualdad en el acceso asegurando la existencia de mecanismos suficientes y adecuados para el acceso gratuito a los medios electrónicos. Ver <http://www.mintic.gov.co/portal/604/w3-article-5437.html>.

<sup>44</sup> Principio establecido a la luz del artículo 3 numeral 11 de la ley 1437 de 2011.

- **Neutralidad tecnológica.** Se garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible.
- **Facilitación.** Las entidades facilitarán el intercambio de la información con otras entidades evitando la duplicidad de acciones y excluyendo exigencias o requisitos que puedan obstruirlo o impedirlo<sup>45</sup>.

Adicionalmente a los anteriores principios, los Servicios Digitales Básicos se sustentan en los siguientes fundamentos en los que además se enmarca de manera general la estrategia de Gobierno en Línea:

- **Privacidad por diseño y por defecto.** Se adoptarán las medidas preventivas en toda la gestión del ciclo de la información, las tecnologías, el tratamiento y los procesos, entendiendo la privacidad como una opción por defecto, garantizando la seguridad y privacidad de los datos de carácter personal.
- **Responsabilidad demostrada.** Los responsables del tratamiento de datos personales deberán adoptar medidas apropiadas y efectivas para cumplir sus obligaciones legales. Adicionalmente, tendrá que evidenciar y demostrar el correcto cumplimiento de sus deberes.
- **Validez y fuerza probatoria.** Los documentos<sup>46</sup> que se generen y compartan tienen la validez y fuerza probatoria que le confieren a los mismos las disposiciones del Código General del Proceso<sup>47</sup>. Las alternativas de identificación electrónica deberán ser jurídicamente válidas y permitirán demostrar tanto la identidad de las personas como las actuaciones que realizan frente al Estado utilizando mecanismos digitales. Así mismo, la solución debe permitir a las entidades públicas las notificaciones electrónicas en los términos de ley.
- **Preservación de archivos a largo plazo.** Los usuarios podrán almacenar y custodiar los documentos que se generen a lo largo de su vida y los operadores deberán implementar medidas durante su gestión para garantizar la preservación de los mismos en el tiempo.
- **Portabilidad.** Los usuarios podrán acceder a los servicios digitales a través de cualquier sistema operativo, navegador o sistema de información.
- **Movilidad.** Los usuarios tendrán el derecho a trasladarse entre operadores, sin restricción alguna y conservando los mismos derechos y servicios mínimos.
- **Escalabilidad.** La habilitación de la plataforma de servicios debe asegurar que ante el incremento de demanda y uso, sea posible mantener las mismas condiciones de servicio incrementando recursos y adicionando nuevas capacidades.
- **Viabilidad y sostenibilidad.** Se promoverá el desarrollo de soluciones viables, innovadoras y sostenibles que reconozcan las oportunidades proporcionadas por las tendencias del sector de las TIC para producir cambios que generen nuevo y mayor valor público que además procuren su continuidad en el largo plazo.

## 8. ALINEACIÓN ESTRATÉGICA DE LOS SERVICIOS DIGITALES BÁSICOS

Los servicios digitales básicos se constituyen en uno de los proyectos más relevantes para contribuir a las políticas de buen gobierno, al proveer a los ciudadanos, empresas y entidades públicas de una plataforma que promueva la mejora en los servicios del gobierno y facilite los mecanismos de comunicación e interacción Estado-Personas.

<sup>45</sup> Este principio está orientado a apoyar la interoperabilidad a la luz del artículo 3 de la Ley 1712 de 2014.

<sup>46</sup> El Código General del Proceso (Ley 1564 de 2012) en su artículo 243 define documentos así: Son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares.

<sup>47</sup> Ley 1564 de 2012 por el cual se expide el Código General de Proceso antes Código de Procedimiento Civil.



Los servicios digitales básicos se alinean con el Plan Nacional de Desarrollo 2014-2018 y con el Plan Vive Digital 2014-2018, además de contribuir positivamente a los Objetivos de Desarrollo Sostenible de la ONU, establecidos en la Agenda 2030, para lo cual se suscribió la Declaración de Compromiso con la Agenda Post 2015. Así mismo, impulsan el principio de colaboración armónica establecido en el artículo 113 de la Constitución Política.

De acuerdo con lo señalado en las bases del Plan Nacional de Desarrollo 2014-2018, los servicios básicos digitales hacen parte de los instrumentos para procurar un país más competitivo. Se entiende entonces que la competitividad del país requiere no sólo empresas más productivas sino también un aparato estatal más accesible y efectivo en la solución de problemas y provisión de servicios<sup>48</sup> y es así como en el Artículo 45 de la Ley 1753 de 2015 se señala:

*“ARTÍCULO 45. ESTÁNDARES, MODELOS Y LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PARA LOS SERVICIOS AL CIUDADANO. Bajo la plena observancia del derecho fundamental de hábeas data, el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), en coordinación con las entidades responsables de cada uno de los trámites y servicios, definirá y expedirá los estándares, modelos, lineamientos y normas técnicas para la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC), que contribuyan a la mejora de los trámites y servicios que el Estado ofrece al ciudadano, los cuales deberán ser adoptados por las entidades estatales y aplicarán, entre otros, para los siguientes casos:*

- a) Agendamiento electrónico de citas médicas.*
- b) Historia clínica electrónica.*
- c) Autenticación electrónica.*
- d) Publicación de datos abiertos.*
- e) Integración de los sistemas de información de trámites y servicios de las entidades estatales con el Portal del Estado colombiano.*
- f) Implementación de la estrategia de Gobierno en Línea.*
- g) Marco de referencia de arquitectura empresarial para la gestión de las tecnologías de información en el Estado.*
- h) Administración, gestión y modernización de la justicia y defensa, entre otras la posibilidad de recibir registrar, tramitar, gestionar y hacer trazabilidad y seguimiento de todo tipo de denuncias y querellas, así como el reporte de control de las mismas.*
- i) Sistema integrado de seguridad y emergencias (SIES), a nivel territorial y nacional.*
- j) Interoperabilidad de datos como base para la estructuración de la estrategia que sobre la captura, almacenamiento, procesamiento, análisis y publicación de grandes volúmenes de datos (Big Data) formule el Departamento Nacional de Planeación.*
- k) Servicios de Telemedicina y Telesalud.*
- l) Sistema de seguimiento del mercado laboral.*
- m) El registro de partidos, movimientos y agrupaciones políticas a cargo del Consejo Nacional Electoral, y en especial el registro de afiliados.*

---

<sup>48</sup> Departamento Nacional de Planeación DNP 2015, *Bases para el Plan Nacional de Desarrollo 2014-2018*, Gobierno de Colombia, Bogotá, visto el 29 de Septiembre de 2015,  
<https://colaboracion.dnp.gov.co/cdt/prensa/bases%20plan%20nacional%20de%20desarrollo%202014-2018.pdf>



*PARÁGRAFO 1o. Estos trámites y servicios podrán ser ofrecidos por el sector privado. Los trámites y servicios que se presten mediante los estándares definidos en los literales a), b) y c) serán facultativos para los usuarios de los mismos. El Gobierno nacional reglamentará la materia.*

**PARÁGRAFO 2o. El Gobierno nacional, a través del MinTIC, diseñará e implementará políticas, planes y programas que promuevan y optimicen la gestión, el acceso, uso y apropiación de las TIC en el sector público, cuya adopción será de obligatorio cumplimiento por todas las entidades estatales y conforme a la gradualidad que para el efecto establezca el MinTIC. Tales políticas comportarán el desarrollo de, entre otros, los siguientes temas:**

**a) Carpeta ciudadana electrónica. Bajo la plena observancia del derecho fundamental de hábeas data, se podrá ofrecer a todo ciudadano una cuenta de correo electrónico oficial y el acceso a una carpeta ciudadana electrónica que le permitirá contar con un repositorio de información electrónica para almacenar y compartir documentos públicos o privados, recibir comunicados de las entidades públicas, y facilitar las actividades necesarias para interactuar con el Estado. En esta carpeta podrá estar almacenada la historia clínica electrónica. El Min- TIC definirá el modelo de operación y los estándares técnicos y de seguridad de la Carpeta Ciudadana Electrónica. Las entidades del Estado podrán utilizar la Carpeta Ciudadana Electrónica para realizar notificaciones oficiales. Todas las actuaciones que se adelanten a través de las herramientas de esta carpeta tendrán plena validez y fuerza probatoria.**

*b) Director de Tecnologías y Sistemas de Información. Las entidades estatales tendrán un Director de Tecnologías y Sistemas de Información responsable de ejecutar los planes, programas y proyectos de tecnologías y sistemas de información en la respectiva entidad. Para tales efectos, cada entidad pública efectuará los ajustes necesarios en sus estructuras organizacionales, de acuerdo con sus disponibilidades presupuestales, sin incrementar los gastos de personal. El Director de Tecnologías y Sistemas de Información reportará directamente al representante legal de la entidad a la que pertenezca y se acogerá a los lineamientos que en materia de TI defina el MinTIC”*

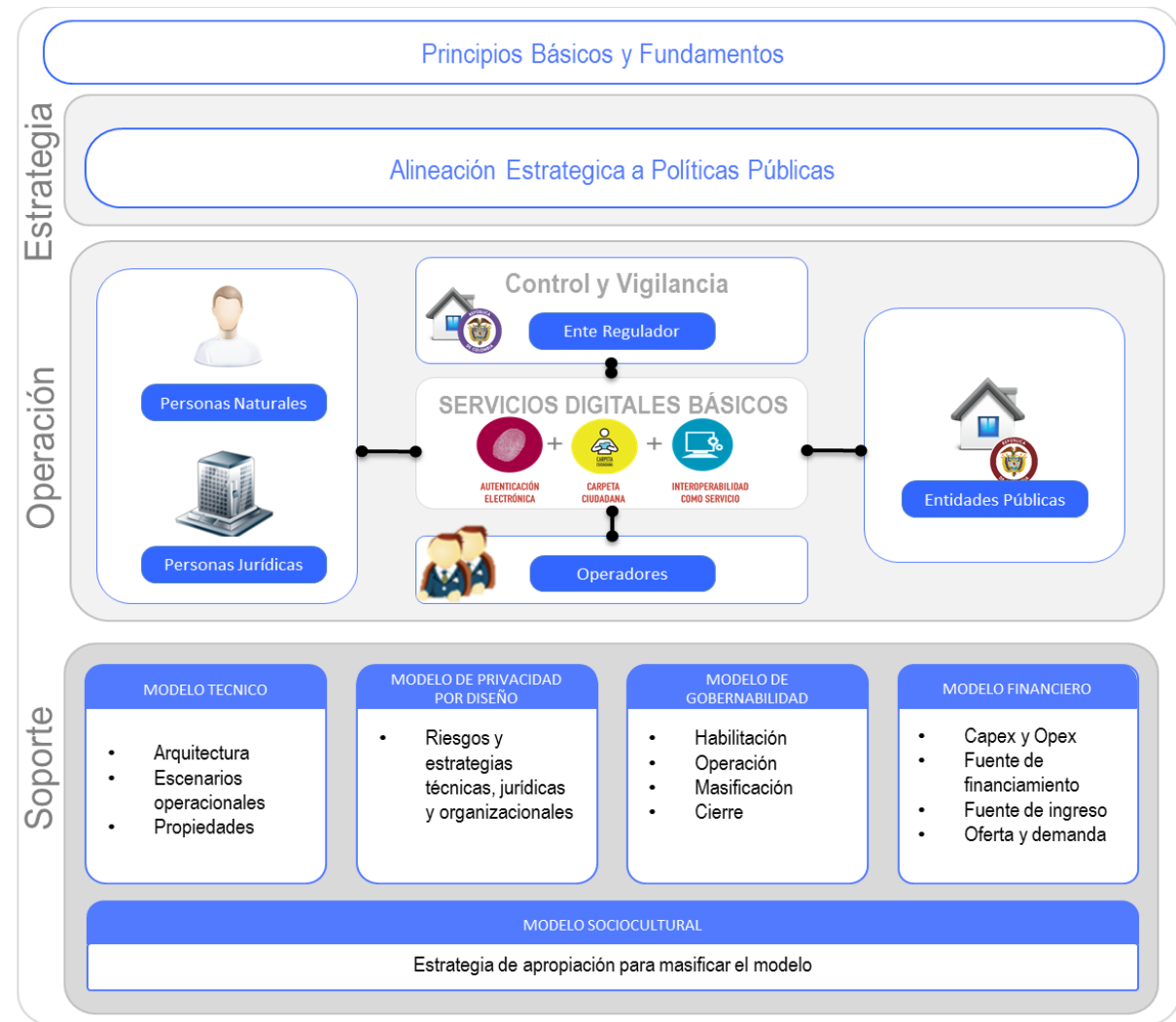
De otro lado, el artículo 113 de la Constitución Política consagra como base fundamental de la organización de los poderes públicos y de las relaciones entre ellos, la exigencia de su colaboración armónica, en estos términos, que en lo esencial se encontraban en la Carta de 1886: *"Los diferentes órganos del Estado tienen funciones separadas pero colaboran armónicamente para la realización de sus fines"* En desarrollo de este mandato constitucional, el artículo 6° de la ley 489 de 1998 define el principio de coordinación en estos términos: *"En virtud del principio de coordinación y colaboración, las autoridades administrativas deben garantizar la armonía en el ejercicio de sus respectivas funciones con el fin de lograr los fines y cometidos estatales. En consecuencia, prestarán su colaboración a las demás entidades estatales para facilitar el ejercicio de sus funciones y se abstendrán de impedir o estorbar su cumplimiento por los órganos, dependencias, organismos y entidades titulares."* "...." de lo expuesto se desprende que hay un solo Estado que se compone de múltiples órganos y entidades, y que todos ellos deben actuar al unísono con el fin de realizar los fines propios de la organización política que le dan sentido y lo legitiman lo cual da cabida a acciones y aprovechamiento de Tecnologías de Información que faciliten la coordinación y articulación entre entidades del Estado en materia de integración e **interoperabilidad** de información y servicios, creando sinergias y optimizando los recursos para converger en la prestación de mejores servicios al ciudadano.

## **9. MODELO DE IMPLEMENTACIÓN DE LOS SERVICIOS DIGITALES BÁSICOS**

El modelo parte de considerar que los Servicios Digitales Básicos que se van a suministrar gratuitamente a las personas naturales y jurídicas, en el marco de sus actuaciones con las entidades públicas, serán provistos por múltiples operadores especializados habilitados previamente por el Ministerio de Tecnologías de la Información y las Comunicaciones, y su implementación obedecerá a un enfoque obligatorio pero gradual bajo el cual las Entidades Públicas contratarán y reconocerán económicamente los servicios a los operadores y migrarán sus servicios digitales al modelo unificado de Autenticación Electrónica, Interoperabilidad o intercambio de información entre entidades así como la gestión de documentos, comunicaciones y notificaciones aportados por los ciudadanos desde su Carpeta Ciudadana.

El modelo, bajo el rigor de los principios y fundamentos definidos y en el marco de la alineación estratégica, define los roles de los actores, las reglas o escenarios de operación y el soporte técnico, financiero y jurídico que garantizarán su sostenibilidad y se representan de manera general mediante la ilustración No. 2.

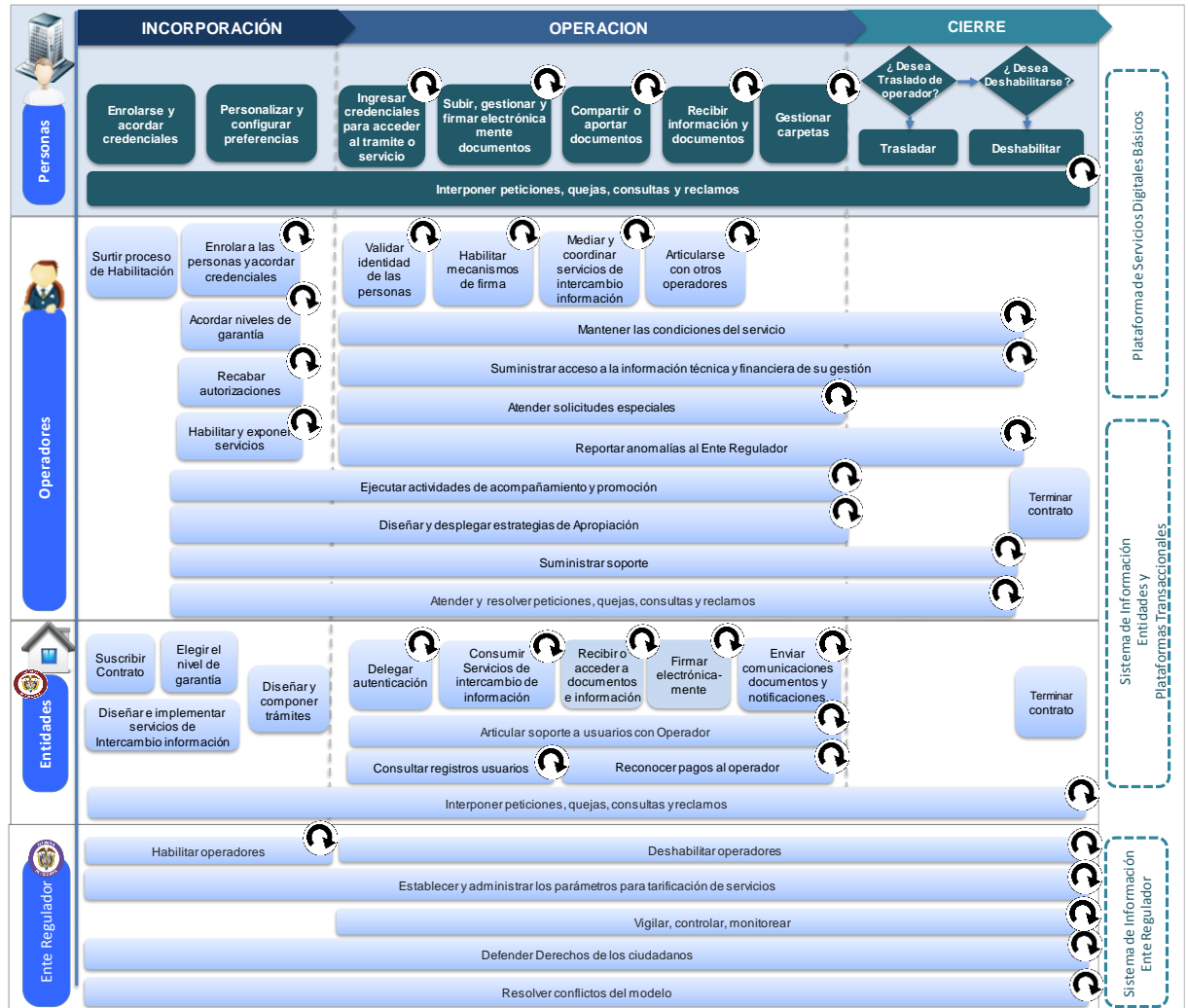
**Ilustración No. 1 Modelo de Servicios Digitales Básicos**



### 9.1 Modelo Operativo

El modelo operativo de servicios digitales básicos propuesto se representa a través de la siguiente gráfica que señala los diferentes actores y la secuencia de operaciones esenciales del modelo a través de las fases de alistamiento, trámite y servicio, gestión y deshabilitación y así mismo señala los sistemas de información que soportan el modelo, a saber, la plataforma de servicios digitales básicos, los sistemas de información de las entidades públicas, plataformas transaccionales y, el sistema del Ente Regulator.

**Ilustración No. 2 Modelo Operativo y flujo de proceso Servicios Digitales Básicos**



Proceso repetitivo

### 9.1.2 Operaciones de los Actores:

**Personas:** Los ciudadanos y empresas tienen los siguientes procesos básicos y relacionamientos dentro del modelo:

- *Enrolarse y acordar credenciales.* Las personas podrán enrolarse voluntariamente y de manera gratuita eligiendo al operador de su preferencia, luego de consultar los servicios ofrecidos por éstos, así como los términos y condiciones de uso, para lo cual suscribirá un acuerdo formal con el operador. El enrolamiento se efectuará presencialmente a través de los puntos que sean habilitados a nivel nacional y para colombianos en el exterior en donde el operador validará la identidad de las personas mediante verificación contra la base de datos biográfica y biométrica de la Registraduría Nacional del Estado Civil. Durante el mismo proceso de enrolamiento se les otorgarán a las personas un conjunto de credenciales de acceso, las cuales podrán ser usadas en procesos de Autenticación Electrónica y firma de mensajes de datos al emplear los sistemas de información de las Entidades Públicas y plataformas transaccionales del Estado. El usuario gestionará sus credenciales lo cual le permitirá elegir las, renovarlas, revocarlas, y recuperar los registros de auditoría generados a razón del uso de sus

credenciales. Se le entregarán dos tipos de credenciales a las personas, correspondientes a los niveles de garantía medio y alto.<sup>49</sup>

- *Personalizar y configurar preferencias.* Las personas podrán aceptar, actualizar y revocar las autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de la Carpeta Ciudadana y para el tratamiento de sus datos personales. De igual forma podrán configurar alarmas y notificaciones cada vez que se utilicen sus credenciales de acceso.
- *Ingresar credenciales para acceder al trámite o servicio.* Las personas que deseen interactuar por medios digitales con alguna entidad, deberán ingresar al portal o sistema de información de la misma, seleccionar el trámite o servicio al que requiera acceder e ingresar sus credenciales, las cuales serán validadas por el operador permitiendo o denegando el acceso.
- *Subir, gestionar y firmar electrónicamente documentos.* Las personas podrán subir, almacenar y gestionar los documentos públicos o privados a la Carpeta Ciudadana los cuales requiera dentro de una actuación con el Estado, y firmarlos electrónicamente haciendo uso de los mecanismos habilitados desde la plataforma garantizando así la confidencialidad e integridad de estos de la misma manera que lo haría a través de su firma autógrafa en documentos físicos.
- *Compartir o aportar documentos.* Las personas con su consentimiento previo podrán compartir documentos con usuarios seleccionados de la carpeta, o aportarlos a un trámite o servicio ante una entidad pública.
- *Recibir información y documentos.* Las personas podrán recibir comunicaciones, documentos y notificaciones provenientes de las entidades públicas como resultado de sus actuaciones. Sólo recibirán documentos de las entidades emisoras que las personas hayan seleccionado según se indicó en la actividad de personalización y configuración de preferencias.
- *Gestionar Carpetas.* Estarán disponibles las funcionalidades para que las personas puedan dentro de su Carpeta organizar y gestionar información y documentos que surjan como resultado de sus actuaciones ante las entidades públicas (descargar, renombrar, imprimir, organizar, borrar, etc.) y guardar documentos privados que requiera a futuro dentro de una actuación.
- *Interponer peticiones, quejas, consultas y reclamos* ante el operador frente a desviaciones en la calidad, anomalías en los servicios recibidos y de la integridad y privacidad de la información personal.
- *Trasladar.* Las personas podrán solicitar el traslado desde un operador de servicios a otro sin perjuicio de los servicios recibidos y de la integridad de la información que administra en la Carpeta Ciudadana.
- *Deshabilitar.* Las personas podrán solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su deshabilitación de la plataforma de servicios en cuyo caso podrá descargar su información a un medio propio de almacenamiento.

**Entidades:** Tienen varios procesos esenciales dentro del modelo:

- *Suscribir contrato.* Eligiendo al operador de servicios digitales básicos que más le convenga, con la posibilidad de realizar cambio de operador cuando así lo considere. La contratación se surtirá a través de procesos públicos con los operadores previamente habilitados y con sujeción a las normas de contratación pública. Para ello, se deberá generar una articulación del operador de los servicios digitales básicos contratado por cada entidad para aprovisionar los servicios que garanticen los esquemas de autenticación, carpeta ciudadana e interoperabilidad a los sistemas de información, ventanillas únicas y sedes electrónicas de las entidades. Lo anterior, de conformidad con la gradualidad que defina el MINTIC y en cumplimiento del artículo 45 del Plan Nacional de Desarrollo.
- *Elegir el nivel de garantía.* Analizando con el operador cada servicio y trámite, evaluado riesgos y eligiendo el nivel de garantía de cada uno de los trámites y servicios que requieran Autenticación Electrónica. Los niveles de garantía a elegir tendrán dos categorías: nivel de garantía medio y alto. El primero da alguna confianza en que la identidad presentada es precisa; por su parte, el nivel de garantía

<sup>49</sup> En el Nivel de Garantía Medio: Da alguna confianza en que la identidad declarada es precisa. Pueden emplearse una serie de tecnologías de autenticación, incluyendo la autenticación de un solo factor, los tokens de conocimiento pre-registrado, tokens fuera de banda y dispositivos de contraseña de un solo uso. (Equivalente a nivel de Garantía 2 (NdG2) establecido en las recomendaciones de la ITU X.1254, ISO 29115 y NIST Special Publication 800-63-2)

En el Nivel de Garantía Alto: Posee un nivel muy alto de confianza en la exactitud de la identidad declarada y se emplea para el acceso a datos muy restringidos. Se exigen por lo menos dos factores de autenticación. El proporcionar autenticación remota con la más alta seguridad práctica y está basado en la posesión de tokens criptográficos basados en hardware. (Equivalente a nivel de Garantía 4 (NdG4) establecido en las recomendaciones de la ITU X.1254, ISO 29115 y NIST Special Publication 800-63-2).

alto posee un mayor nivel de confianza respecto del nivel medio en la exactitud de la identidad presentada y se emplea para el acceso a datos muy restringidos.

- *Diseñar e implementar servicios de intercambio de información.* Definiendo reglas y políticas que deben ser consideradas por el operador en el intercambio de la información de un servicio determinado, lo anterior en el marco de interoperabilidad para que las entidades que requieran esta información en sus procesos puedan consumirla.
- *Diseñar y componer trámites.* Definiendo reglas y políticas que deben ser consideradas por los operadores en la composición de un trámite a partir de los servicios de intercambio de información de las entidades que intervienen en el mismo.
- *Delegar autenticación.* Autorizando formalmente a los operadores de servicios digitales básicos para ejecutar los procesos de reconocimiento y validación de la identidad de las personas cuando adelanten algún trámite por medios digitales. En este caso a la entidad se le garantizará técnica y jurídicamente la validación de identidad de las personas en medio digital, de acuerdo al nivel de garantía elegido.
- *Consumir servicios de intercambio de información.* Haciendo uso de los servicios de intercambio de información publicados a través de la plataforma con el objeto de optimizar sus procesos y automatizar los trámites y servicios al ciudadano. También recibiendo o accediendo a documentos que comparte el ciudadano desde su Carpeta para integrarlos dentro de un trámite o actuación.
- *Recibir o acceder a documentos e información* que comparte el ciudadano desde su Carpeta Ciudadana, previo consentimiento del mismo, e integrarlos dentro de un trámite o actuación sin exigir que sean presentados en medios físicos.
- *Firmar electrónicamente.* Haciendo uso de los mecanismos habilitados desde la plataforma para la firma electrónica o digital en aquellas actuaciones que así lo requieran.
- *Enviar comunicaciones, documentos y gestionar notificaciones electrónicas.* Gestionando la remisión de comunicaciones, documentos, gestionando las notificaciones electrónicas dirigidas a los usuarios del servicio de la Carpeta Ciudadana y garantizando su recepción.
- *Consultar registros de usuarios.* La entidad podrá consultar los registros básicos de usuarios que hacen uso de sus sistemas de información por medio de los servicios digitales básicos.
- *Articular con los Operadores los esquemas de soporte al usuario* de tal manera que sean escalados adecuadamente los casos que competan a la plataforma de Servicios Digitales Básicos sin perjuicio de los niveles de servicios y soporte que le competen a la entidad pública en el marco de la administración de sus sistemas de información.
- *Interponer peticiones, quejas y reclamos* ante el operador frente a desviaciones en la calidad y anomalías en los servicios recibidos.
- *Reconocer pagos al operador.* Pagando por transacción dentro de un trámite o servicio habilitado en la plataforma de servicios digitales los cuales estarán relacionadas con:
  - Autenticación Electrónica de los usuarios de un trámite o servicio
  - Envío de documentos del trámite a la Carpeta del Ciudadano
  - Consumo de servicios de intercambio información – Interoperabilidad con otros sistemas de información
- *Terminar contrato.* Finalizando su relación contractual y por tanto las delegaciones y acuerdos de confianza con el operador de servicios seleccionado para vincularse con otro sin perjuicio de los servicios recibidos y de la integridad de la información que administra a través de la plataforma de servicios digitales básicos. Se adoptarán medidas para garantizar el traslado oportuno de la información a otro operador con miras a que los servicios al ciudadano se presten sin interrupción (sin solución de continuidad).

**Operador de Servicios Digitales Básicos:** Sus procesos esenciales dentro del modelo incluyen:

- *Surtir el proceso de habilitación* y posterior mecanismo de contratación con las Entidades Públicas a la luz del régimen aplicable y vigente.
- *Enrolar a las personas y acordar credenciales.* Registrando a las personas en la plataforma de servicios digitales básicos una vez que estas acepten los términos y condiciones de uso establecidos mediante contrato formal y luego que el proceso de verificación y validación de la identidad por medio de las huellas dactilares sea superado de manera satisfactoria. Esta validación deberá realizarse de manera presencial en todo el territorio nacional y para ciudadanos en el extranjero verificando la identidad de las personas contra la base de datos biográfica y biométrica de la Registraduría Nacional del Estado

Civil.<sup>50</sup> Posteriormente se deberán acordar credenciales, asignando a las personas dos tipos de credenciales correspondientes a los niveles de garantía medio y alto.

Para que el ciudadano pueda ingresar a un servicio de información de una entidad por medio del servicio de Autenticación Electrónica de la Plataforma de Servicios Digitales, cada operador deberá tener una base de datos de sus usuarios (en adelante base de datos primaria de usuarios), la cual deberá ser actualizada posterior a cada registro, así como compartida y sincronizada con los demás operadores. Estas bases de datos deberán contener únicamente los siguientes campos:

- Número del documento de identificación.
- Identificador del Operador que enroló al ciudadano.

Las bases de datos primarias de usuarios deberán ser compartidas y actualizadas entre los operadores cada 2 horas por medio de un servicio web que cada operador deberá publicar por medio del servicio de interoperabilidad

- *Acordar niveles de garantía.* Acompañando a las entidades en la evaluación de los riesgos para acordar los niveles de garantía de los servicios y trámites que requieran Autenticación Electrónica. Los niveles de garantía a elegir tendrán dos categorías: nivel de garantía medio y alto. El primero, da alguna confianza en que la identidad presentada es precisa, por su parte, el nivel de garantía alto, posee un nivel muy alto de confianza en la exactitud de la identidad presentada y se emplea para el acceso a datos muy restringidos.
- *Recabar las autorizaciones de los usuarios* para tratar y suministrar datos personales, cumplir los requerimientos probatorios en esta materia y recibir comunicaciones o notificaciones electrónicas desde y hacia las Entidades Públicas.
- *Diseñar y componer trámites.* Acompañando a las entidades en la creación, diseño u orquestación de los trámites en sus sistemas de información a partir de los servicios digitales que estén habilitados para intercambio de información en el marco de interoperabilidad.
- *Habilitar y exponer servicios.* Registrando en un directorio general de servicios de intercambio de información, configurando y exponiendo los servicios para intercambio de información de una entidad específica que podrán ser consumidos por otra entidad en la atención al ciudadano
- *Validar la identidad de las personas.* Verificando las credenciales presentadas por las personas en el momento que acceden a un trámite o servicio del Estado. En este proceso se debe realizar una validación con la Registraduría Nacional del Estado Civil, con el fin de actualizar la información de naturaleza pública y datos sin reserva legal, incluyendo la vigencia del documento. Para lograr validar la identidad de las personas, el operador le debe permitir al ciudadano ingresar la siguiente información inicial:
  - Tipo de documento
  - Número de documento de identificación.

Con esta información el operador podrá consultar la base de datos primaria de usuarios para determinar que operador deberá resolver la solicitud de autenticación. Si el ciudadano se encuentra registrado en el operador contratado por la entidad, este mismo operador resolverá la solicitud de autenticación. Si el ciudadano no se encuentra registrado en el operador contratado por la entidad, este deberá reenviar la solicitud al operador que enroló al ciudadano, con el fin de que sea este último quien resuelva la solicitud de autenticación.

Si el ciudadano no se encuentra registrado en base de datos primaria de usuarios, el operador contratado por la entidad, deberá realizar una consulta a los servicios web los demás operadores, y así verificar si efectivamente se encuentra enrolado en ante alguno de estos. Esta validación se realizará con el fin de verificar al ciudadano que requiera acceder a un servicio de información de una entidad, en un espacio de tiempo en el que no se han sincronizado las bases de datos primarias de usuarios entre operadores.

Si el ciudadano no se encuentra registrado en base de datos primaria de usuarios de ninguno de los operadores, el operador contratado por la entidad deberá comunicarle al ciudadano que debe llevar a cabo el proceso de enrolamiento ante un operador de su preferencia.

---

<sup>50</sup> Para la verificación contra las bases de datos biométricas se hará uso de las huellas dactilares del ciudadano, que como mecanismo de Autenticación Electrónica, tiene fundamento en el artículo 17 de la Ley 527 de 1999, los artículos 18 y 161 del Decreto Ley 019 de 2012, el Decreto 2364 de 2012 y la Resolución 5633 de 2016 de la RNEC. A través de este mecanismo, permite identificar a la persona por la creación de una serie de características técnicas de la huella denominadas minucias, las cuales son un conjunto de puntos únicos sobre la completitud de la huella que permiten establecer un perfil biométrico de cada persona. Esto permitirá verificar la identidad de una persona en medios electrónicos, por medio de la comparación de la minucia de la huella capturada, contra una fuente de datos confiable de comparación como es la base de datos de la Registraduría Nacional del Estado Civil. Por tal motivo, el acceso a tales datos lo dará la Registraduría Nacional del Estado Civil a través de un operador biométrico y aliado tecnológico que se encuentre habilitado ante la Registraduría respecto del proceso de verificación de identidad. Los operadores del servicio de Autenticación Electrónica no podrán guardar, copiar o replicar la información proveniente de la base de datos de la Registraduría, de acuerdo con lo establecido en las normas a este respecto.

- *Habilitar los mecanismos de firma* para que los ciudadanos y entidades puedan garantizar la integridad y autenticidad de los documentos.
- *Mediar y coordinar servicios de intercambio de información.* Integrando los servicios de intercambio de información habilitados o expuestos en la plataforma de conformidad con las reglas y políticas predeterminadas generando interoperabilidad entre entidades y con los otros operadores.
- *Articularse con los otros operadores* del modelo de servicios digitales básicos para el intercambio y la circulación oportuna, segura y eficiente de la información de los servicios y usuarios, por ejemplo el operador asignado al usuario, autorizaciones y revocatorias de los usuarios, etc.
- *Mantener las condiciones del servicio* tanto técnicas, como financieras y jurídicas a lo largo de toda la ejecución, para garantizar los estándares mínimos de seguridad, privacidad, acceso, neutralidad tecnológica y continuidad en el servicio, así como las condiciones acordadas con sus usuarios y entidades públicas vinculadas, sin imponer o cobrar servicios que no hayan sido aceptados expresamente por el usuario.
- *Suministrar acceso a la información técnica y financiera y de su gestión* requerida para las acciones de monitoreo y control permanente por parte del Ente Regulador.
- *Atender solicitudes especiales* emitidas por los ciudadanos, entidades o por autoridades judiciales en cuanto a información administrada respetando siempre el principio de privacidad, circulación restringida y seguridad de los datos personales.
- *Reportar al Ente Regulador anomalías* que se registren en la prestación del servicio.
- *Ejecutar actividades de acompañamiento y promoción* a las Entidades públicas y empresas privadas buscando su participación activa como proveedor o consumidor de servicios básicos digitales.
- *Diseñar y desplegar estrategias de apropiación* del modelo entre los ciudadanos, empresas y entidades públicas, proceso que realizará conjuntamente con el MINTIC.
- *Suministrar soporte* a los usuarios y entidades de acuerdo con los lineamientos, políticas, directrices generadas por MINTIC y de conformidad con el marco regulatorio vigente.
- *Atender y resolver las Peticiones, Quejas, Consultas y Reclamos* de los usuarios y entidades públicas vinculadas.
- *Terminar contrato.* Dando por terminada su relación contractual y por tanto las delegaciones y acuerdos de confianza con las Entidades sin perjuicio de la continuidad del servicio e integridad de la información que administra a través de la plataforma de servicios digitales básicos. En este caso, debe adoptar medidas para garantizar el traslado oportuno de la información a otro operador con miras a que los servicios al ciudadano se presten sin interrupción (sin solución de continuidad). Una vez hecho lo anterior, deberá eliminar de sus archivos o sistemas de información la información que administró o trató con ocasión de la prestación de sus servicios como operador de servicios digitales básicos.

**Entes Reguladores:** Actores encargados de realizar los siguientes procesos:

- *Habilitar operadores.* Autorizando la entrada de los operadores de Servicios Digitales Básicos previo cumplimiento de requisitos técnicos, jurídicos y financieros que sean establecidos.
- *Vigilar, controlar, monitorear.* Ejerciendo seguimiento a los indicadores de calidad, la operación y el servicio prestado por los operadores. En ejercicio de esta función podrá solicitar una auditoria especial sobre la gestión de los operadores.
- *Defender, dentro de sus competencias,* los derechos de los ciudadanos.
- *Resolver conflictos* que surjan en el modelo y promover la competencia leal.
- *Establecer y administrar los parámetros para la tarificación de los servicios.*
- *Deshabilitar* o restringir a los operadores de Servicios Digitales Básicos.

### 9.1.3 Sistemas de Información:

- **Plataforma de Servicios Digitales Básicos:** Plataforma tecnológica que permite reconocer y validar la identidad de las personas cuando adelanten trámites con el Estado por medios digitales para mitigar el riesgo de suplantación de su identidad, ofrecer un servicio seguro de gestión de información para recibir, almacenar y compartir documentos y, habilitar mecanismos para el intercambio información entre entidades públicas de manera estandarizada, eficiente y segura.
- **Sistema de información de la Entidad:** Sistema de información que delegará la validación de identidad de sus usuarios a la plataforma de servicios digitales básicos y utilizará los servicios expuestos para intercambio de información y datos desde otras entidades, para llevar a cabo un trámite o servicio del ciudadano e integrar los documentos necesarios desde o hacia la Carpeta Ciudadana. Hacen parte de esta categoría, las

- **Sistema de información del Ente Regulador:** Sistema de información que consumirá los servicios de monitoreo de cada uno de los operadores con el objetivo de verificar el correcto funcionamiento, la calidad del servicio y tener información estadística general de los operadores.

El modelo técnico está compuesto por la arquitectura, los escenarios operacionales y las propiedades. La arquitectura contiene el marco estructural básico de cada uno de los servicios digitales básicos; los escenarios operacionales dan cuenta de los procesos básicos entre los actores y sistemas y son la base para definir los requerimientos funcionales; las propiedades son las condiciones en las cuales deben darse los procesos y con base en ellas se determinan los requerimientos no funcionales.

Desde el punto de vista técnico, la plataforma a habilitar por parte de los operadores tiene dos componentes: el *front-end* y el *back-end*.

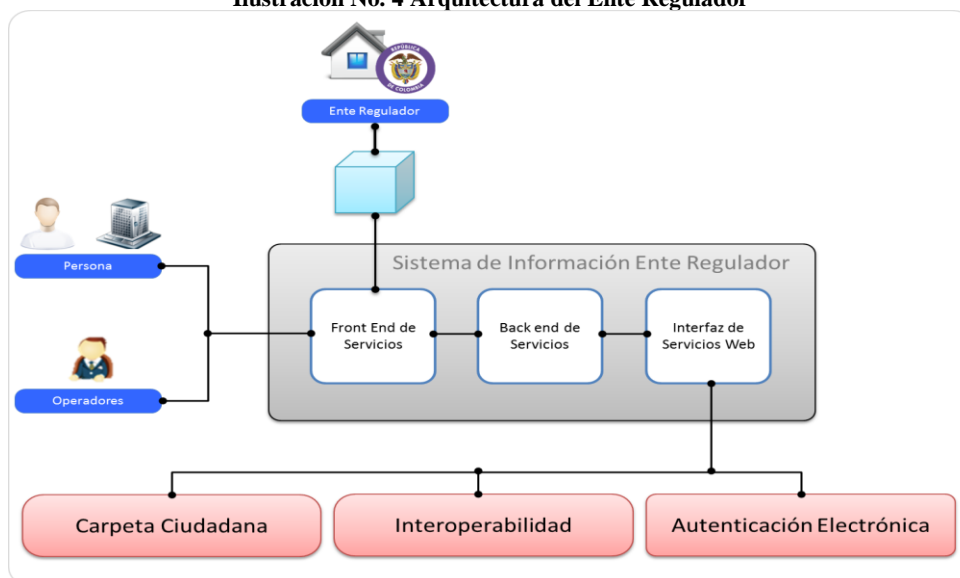
**Back-end**, que comprende todos los componentes necesarios para que la plataforma pueda ejecutar los procesos lógicos requeridos para soportar los servicios a los diferentes actores. Implementa toda la lógica de negocio necesaria para soportar las interacciones de los diferentes actores definidos para la plataforma de servicios digitales. Adicionalmente, orquesta la interacción de todos los componentes que sean definidos y se encarga de llevar a cabo labores de persistencia del modelo de datos. Incluye el monitor de servicios que expone los servicios de monitoreo tanto de las transacciones llevadas a cabo por la plataforma como los indicadores de calidad de sus servicios.

El diagrama ilustra la arquitectura de un sistema de información. En la parte superior, se muestra el 'Ente Regulador' (con un icono de casa y un sello) conectado al 'Sistema de Información' (un cubo azul). El sistema central está dividido en dos secciones, cada una con un 'Operador' (Operador 1 y Operador 2) y un 'Front End' (un cubo azul). Los operadores interactúan con el 'Front End', que a su vez se conecta con un 'Monitor' (un cubo azul). El 'Monitor' está dividido en tres partes: 'Carpeta', 'Autenticación' y 'Interoperabilidad'. El 'Front End' también se conecta directamente con 'Carpeta' y 'Autenticación'. El 'Monitor' interactúa con el 'Sistema de Información' (un cubo azul) y el 'Sistema de Información de la Entidad' (un cubo azul). El 'Sistema de Información de la Entidad' también interactúa con el 'Sistema de Información' central. El diagrama muestra la interacción entre los operadores, el sistema central y los sistemas de información de la entidad.



Frente al ente regulador, vale la pena señalar que este representa un actor que interactúa con los diferentes operadores tecnológicos de servicios digitales por medio de un sistema de información. Este actor es el encargado de ejercer de forma eficiente y automática actividades de habilitación, vigilancia, inspección y control sobre todos los operadores autorizados. En su arquitectura de primer nivel el ente regulador interactúa con los diferentes operadores legalmente constituidos y autorizados de la siguiente manera:

**Ilustración No. 4 Arquitectura del Ente Regulador**



En esta arquitectura se identifican tres componentes principales: (i) *Front-end* de Servicios, (ii) *Back-end* de servicios, (iii) Interfaz de servicios web:

- (i) **Front-end de servicios:** Componente mediante el cual las personas, el representante legal de una empresa, el operador tecnológico y el ente regulador interactúan con la plataforma. Este componente brindará las interfaces de usuario necesarias para llevar a cabo los escenarios operacionales propios del ente regulador.
- (ii) **Back-end de servicios:** Implementa toda la lógica de negocio necesaria para soportar las interacciones de los diferentes actores definidos para el sistema de información. Adicionalmente, el back-end de servicios orquesta la interacción de todos los componentes definidos para el sistema de información y se encarga de llevar a cabo labores de persistencia del modelo de datos.
- (iii) **Interfaz de servicios web:** Contiene la definición de todos los servicios web que deberán consumir los operadores tecnológicos para reportar, en línea y en tiempo real, los indicadores de calidad del servicio y las estadísticas de uso de sus plataformas.

## 9.2.2 Escenarios Operacionales

Se describen a continuación los escenarios mínimos identificados los cuales se encuentran divididos por cada uno de los actores, en este caso, personas, entidad y ente regulador así:

**Tabla 5. Escenarios operacionales**

Operaciones de los Actores	Escenario Operacional	Descripción
<b>PERSONAS</b>		
<b>Enrolarse y acordar credenciales</b>	<b>Gestionar enrolamiento</b>	<p>Le permitirá al usuario enrolarse de forma segura al servicio de Autenticación Electrónica de la Plataforma de Servicios Digitales, (el operador deberá garantizar la seguridad de la actividad), esta actividad deberá realizarse de modo presencial para verificar de forma fehaciente la identidad de la persona. Incluye las siguientes actividades:</p> <ul style="list-style-type: none"> <li>Solicitar enrolamiento ante un operador</li> <li>Identificarse ante el sistema para enrolamiento</li> <li>Acordar con el operador los mecanismos de autenticación Se le deberán entregar dos tipos de credenciales a las personas, correspondientes a los niveles de garantía medio y alto.</li> </ul>

Operaciones de los Actores	Escenario Operacional	Descripción
		<p>En el Nivel de Garantía Medio: Pueden emplearse una serie de tecnologías de autenticación, incluyendo la autenticación de un solo factor, los tokens de conocimiento pre-registrado, tokens fuera de banda y dispositivos de contraseña de un solo uso. (Equivalente a nivel de Garantía 2 (NdG2) establecido en las recomendaciones de la ITU X.1254, ISO 29115 y NIST Special Publication 800-63-2).</p> <p>En el Nivel de Garantía Alto: Se exigen por lo menos dos factores de autenticación. El proporcionar autenticación remota con la más alta seguridad práctica y está basado en la posesión de tokens criptográficos basados en hardware. (Equivalente a nivel de Garantía 4 (NdG4) establecido en las recomendaciones de la ITU X.1254, ISO 29115 y NIST Special Publication 800-63-2).</p> <ul style="list-style-type: none"> <li>• Obtener credenciales de acceso.</li> <li>• Suscribir términos y condiciones con el operador.</li> </ul>
<b>Personalizar y configurar preferencias</b>  <b>Trasladar</b>  <b>Deshabilitar</b>	<b>Gestionar cuenta en la plataforma de Servicios Digitales Básicos</b>	<p>Le permitirá al usuario gestionar la propia cuenta o cancelarla en función del nivel de acceso a la Plataforma de Servicios Digitales Básicos:</p> <ul style="list-style-type: none"> <li>• Identificarse ante el sistema</li> <li>• Ingresar a la plataforma de servicios digitales básicos</li> <li>• Gestionar PQRs</li> <li>• Cancelar cuenta/Deshabilitarse</li> </ul>
	<b>Gestionar servicio de Autenticación Electrónica</b>	<p>Le permitirá al usuario realizar todas las gestiones necesarias para administrar el servicio:</p> <ul style="list-style-type: none"> <li>• Configurar alertas de acceso</li> <li>• Visualizar registros de acceso</li> <li>• Descargar registros de acceso</li> <li>• Bloquear y desbloquear servicio</li> </ul>
	<b>Configurar servicio de Carpeta Ciudadana</b>	<p>Le permitirá usuario la configuración y definición de parámetros para definir las reglas con las que desea ejecutar el servicio: personalizar los datos, darse de alta en el servicio, cambiar de operador, bloquear y desbloquear el servicio, cancelar el servicio, establecer periodos de validez por tipo de documento subidos por el ciudadano, cancelar el servicio, configuración de las tablas de acceso a la información, configurar de notificaciones &lt;darse de alta para recibir notificaciones electrónicas, aviso de notificaciones por otros canales, selección por entidad o trámite, vigencia&gt;</p>
	<b>Suscribir a los servicios de envío de información de las entidades</b>	<p>Le permitirá al usuario realizar la suscripción a cualquiera de los servicios que ofrecen las entidades y que se encuentran dentro del modelo de servicios digitales: consultar servicios ofrecidos por las entidades, consultar y aceptar los términos y condiciones del servicio, registrar el identificador del usuario frente al servicio de la entidad, consultar el estado de suscripción de un servicio, actualizar, revocar o cancelar la suscripción de un servicio.</p>
	<b>Gestionar credenciales de acceso</b>	<p>Le permitirá al usuario consultar el estado de sus credenciales de acceso y podrá solicitar la renovación o revocación de sus credenciales si sospecha que estas se encuentran comprometidas:</p> <ul style="list-style-type: none"> <li>• Consultar el estado y la vigencia de sus credenciales de acceso</li> <li>• Solicitar la revocación de credenciales</li> <li>• Renovar credenciales (a nivel lógico)</li> </ul>
<b>Ingresar credenciales para acceder a trámites y servicios</b>	<b>Usar autenticación</b>	<p>Le permitirá al usuario usar los mecanismos necesarios para validar su identidad y acceder a trámites y servicios o gestiones administrativa por medios digitales, de acuerdo a los niveles de garantía requeridos:</p> <ul style="list-style-type: none"> <li>• Instalar el componente de autenticación (en caso de que se requiera).</li> </ul> <p>Usar el componente de autenticación de acuerdo al nivel de garantía requerido por la entidad.</p>
<b>Subir, gestionar y firmar electrónicamente documentos</b>  <b>Recibir información y documentos</b>	<b>Usar mecanismos de firma</b>	<p>Le permitirá al usuario usar los mecanismos necesarios para firmar documentos por medios digitales. Permitirá:</p> <ul style="list-style-type: none"> <li>• Instalar el componente de firma.</li> <li>• Usar el componente de firma</li> </ul>
	<b>Usar servicios criptográficos</b>	<p>Le permite al usuario realizar las siguientes operaciones:</p> <ul style="list-style-type: none"> <li>• Cifrar/Descifrar documento</li> <li>• Estampar documentos</li> <li>• Verificar firma electrónica o digital de documentos</li> <li>• Verificar estampas cronológicas</li> <li>• Verificar certificados para firmar documentos</li> </ul>
	<b>Gestionar documentos</b>	<p>Le permitirá al usuario realizar las siguientes operaciones relacionadas con la gestión de los documentos:</p> <ul style="list-style-type: none"> <li>• Subir documento</li> <li>• Visualizar documento</li> <li>• Mover documento a una carpeta seleccionada</li> <li>• Eliminar y restaurar documento</li> <li>• Renombrar documento</li> <li>• Buscar documento</li> </ul>

Operaciones de los Actores	Escenario Operacional	Descripción
		<ul style="list-style-type: none"> <li>• Descargar documento a un dispositivo de almacenamiento externo</li> <li>• Firmar documento</li> </ul>
<b>Gestionar carpetas</b>	<b>Gestionar carpetas</b>	<p>Le permitirá al usuario la organización de documentos por medio de funcionalidades de gestión de carpetas la cuales se podrán</p> <p>Crear carpetas</p> <ul style="list-style-type: none"> <li>• Modificar carpetas</li> <li>• Eliminar carpetas</li> <li>• Cortar y pegar (mover) carpetas</li> <li>• Visualizar carpetas por defecto fijas &lt;entrada, compartidos, eliminados, cargados por el usuario&gt;</li> <li>• Gestionar esquemas de organización de carpetas del usuario</li> <li>• Gestionar esquema de organización de carpetas para personas dependientes.</li> </ul>
<b>Compartir o aportar documentos</b>	<b>Aportar/compartir documentos con terceros</b>	<p>Le permitirá al usuario realizar las siguientes operaciones:</p> <ul style="list-style-type: none"> <li>• Compartir un documento con uno o varios usuarios de Carpeta Ciudadana. &lt;enlace&gt;</li> <li>• Aportar documentos en un trámite/servicio de una entidad &lt;URL, archivo físico, FTP, API&gt;</li> <li>• Visualizar un documento que he o me han compartido</li> <li>• Cancelar compartir documento</li> <li>• Bloquear usuarios para que me compartan documentos</li> <li>• Gestionar los permisos de acceso al documento</li> <li>• Buscar y filtrar sobre documentos que he o me han compartido.</li> </ul>
<b>Interponer peticiones, quejas, consultas y reclamos.</b>	<b>Gestión de Peticiones, Quejas y Reclamos a los Operadores y al Ente regulador</b>	<p>Le permitirá integrarse con el sistema de Peticiones, Quejas y Reclamos con el que cuenta cada Operador y en caso de no disponer del sistema ofrecer las siguientes funcionalidades:</p> <ul style="list-style-type: none"> <li>• Radicar Peticiones, Quejas y Reclamos</li> <li>• Consultar Peticiones, Quejas y Reclamos</li> <li>• Ver estado o respuesta de las Peticiones, Quejas y Reclamos</li> <li>• Adicionalmente debe ofrecer vínculos a los sistemas de Peticiones, Quejas y Reclamos del Ente regulador.</li> </ul>
<b>ENTIDADES PÚBLICAS</b>		
<b>Suscribir contrato</b> <b>Terminar contrato</b>	<b>Gestionar servicios de la plataforma de Servicios Digitales Básicos</b>	<p>Le permitirá a la entidad realizar las siguientes operaciones mínimas en la plataforma de servicios digitales básicos:</p> <ul style="list-style-type: none"> <li>• Darse de alta en un operador.</li> <li>• Acceder a algún servicio de provisto por la plataforma. Es necesario introducir las credenciales de identificación provistas por el operador</li> <li>• Configurar el servicio.</li> <li>• Configurar el nivel de garantía de cada uno de los trámites y servicios que requieran Autenticación Electrónica. Los niveles de garantía a elegir tendrán dos categorías: nivel de garantía medio y alto. El nivel de garantía medio, da alguna confianza en que la identidad presentada es precisa, por su parte, el nivel de garantía alto, posee un nivel muy alto de confianza en la exactitud de la identidad presentada y se emplea para el acceso a datos muy restringidos.</li> <li>• Configurar por tipo de documento ofrecido en la Carpeta Ciudadana &lt;nombre; formato: PDF, JPG,T IFF, XML; medio de entrega del documento: URL, FTP, físico; periodo de validez; medio de notificación; tamaño&gt;.</li> <li>• Configurar usuarios internos de la aplicación, bloquear y desbloquear servicio.</li> <li>• Cancelar servicio.</li> <li>• Habilitar la activación y desactivación de los diferentes servicios de la Plataforma de Interoperabilidad.</li> </ul>
<b>Elegir nivel de garantía</b>	<b>Análisis del trámite y servicio</b>	<p>La entidad podrá realizar un análisis del trámite o servicio o plataforma digital.</p> <ul style="list-style-type: none"> <li>• Evaluar el riesgo del trámite o servicio o plataforma digital que requiera el servicio de Autenticación Electrónica.</li> <li>• Relacionar el trámite según el nivel de riesgo identificado, contra un nivel de garantía apropiado, eligiendo entre las categorías: nivel de garantía medio y alto.</li> </ul>
<b>Delegar autenticación</b>	<b>Acordar protocolo de Autenticación Electrónica</b>	<p>La integración del servicio de Autenticación Electrónica con otros sistemas de información se deberá llevar a cabo por medio de un protocolo de Autenticación Electrónica, basado en estándares abiertos y validados internacionalmente, tales como: SAML2.0, OAuth 2.0, OpenID</p>
	<b>Delegar los servicios de autenticación</b>	<p>La entidad podrá validar la identidad de las personas.</p> <ul style="list-style-type: none"> <li>• Delegar servicios de autenticación de las personas a la plataforma de Autenticación Electrónica.</li> </ul>
<b>Firmar electrónicamente</b>	<b>Delegar los servicios de firma</b>	<p>La entidad podrá ofrecer el servicio de firma de documentos por medios digitales haciendo uso de la plataforma:</p>

Operaciones de los Actores	Escenario Operacional	Descripción
		<ul style="list-style-type: none"> <li>Delegar servicios de firma electrónica de las personas a la plataforma de Servicios Digitales Básicos</li> </ul>
<b>Diseñar e implementar servicios de intercambio de información</b>  <b>Diseñar y componer trámites</b>	<b>Componer y/o orquestar servicios para intercambio de información</b>	<p>Provee las funcionalidades para la representación de un proceso o tramites mediante la composición de servicios individuales publicados en la plataforma, proporciona bloques de construcción para la agregación de servicios débilmente acoplados como una secuencia de procesos alineados con los objetivos de la Entidad. El flujo de datos y el flujo de control se utilizan para permitir interacciones entre los servicios y el trámite o proceso de negocio en Entidad. La interacción puede existir dentro de una o varias Entidades.</p> <p>Incluye funcionalidades como:</p> <ul style="list-style-type: none"> <li>Definir las reglas y políticas de los servicios</li> <li>Diseñar y componer los trámites a partir de los servicios internos y externos</li> </ul>
	<b>Habilitar y exponer servicios</b>	<p>La Entidad podrá acceder a las funcionalidades para exponer un conjunto de datos o información definida en lenguaje común de intercambio de información a otras entidades en la plataforma de interoperabilidad.</p> <p>Incluye funcionalidades como:</p> <ul style="list-style-type: none"> <li>Habilitación de servicios o micro servicios</li> <li>Definición del servicio y metadatos asociados al mismo</li> <li>Configuración de los servicios</li> <li>Aseguramiento y control de accesos</li> <li>Administración de reglas y políticas asociadas al servicio en su ejecución o definición</li> <li>Seguimiento de la operación del servicio</li> </ul>
	<b>Virtualizar datos</b>	<p>Permite a las entidades contar con una forma de recopilar grandes volúmenes de datos provenientes de diversas fuentes al interior de sus áreas funcionales y mostrarlos de forma centralizada para su posterior uso, facilitando y agilizando la provisión de información a los trámites y servicios que ofrecen a los usuarios con el fin de mejorar el rendimiento y hacer más oportuna la respuesta.</p>
	<b>Estandarizar servicios para intercambio de información</b>	<p>Permite a las entidades aplicar el marco de interoperabilidad a los servicios que desea exponer en la plataforma y estandarizar los datos a intercambiar o compartir en el Lenguaje Común de Intercambio de información. Incluye actividades como:</p> <ul style="list-style-type: none"> <li>Revisión y verificación de los 5 dominios de interoperabilidad</li> <li>Definición de las estructuras a partir de las cuales se intercambiarán los datos.</li> </ul>
<b>Consumir servicios de intercambio de información</b>	<b>Consumir servicios de intercambio de información</b>	<p>Permite la ejecución o llamada a los servicios digitales expuestos por una entidad cuya respuesta se puede recibir de manera sincrónica o asincrónica, incluye funcionalidades como:</p> <ul style="list-style-type: none"> <li>Permitir el consumo (uso) de la plataforma, a través de un programa o una persona que solicita un servicio de las Entidades</li> <li>Apoyar la interacción e integración de los consumidores; es decir, la capacidad de capturar la entrada del usuario (consumidor) y proporcionar la respuesta</li> <li>Permitir la creación de una interface de usuario para el consumo de servicios</li> </ul>
<b>Recibir o acceder a documentos e información</b>	<b>Importar documentos como parte de un trámite</b>	<p>Le permitirá al sistema de información de la entidad, previa autorización del ciudadano, generar un enlace de acceso a un documento en la Carpeta Ciudadana que el ciudadano autorice aportar en un trámite/servicio es decir consumir el servicio a un link de descarga &lt;consumo del servicio&gt;; solicitar documento adicional a un trámite ya generado &lt;consumo del servicio&gt;.</p> <p>Dichos documentos tendrán validez jurídica.</p>
<b>Enviar comunicaciones, documentos y gestionar notificaciones</b>	<b>Gestionar comunicaciones, documentos y notificaciones</b>	<p>Le permitirá a la entidad la gestión de las comunicaciones y documentos dirigidas a los usuarios de un servicio publicado en la Carpeta Ciudadana</p> <ul style="list-style-type: none"> <li>Enviar comunicaciones y documentos</li> <li>Enviar avisos por diferentes canales</li> <li>Enviar comunicaciones y documentos masivamente</li> <li>Gestionar notificaciones</li> <li>Consultar reportes</li> </ul>
<b>Consultar registros de usuarios</b>	<b>Consultar registros de usuarios</b>	<p>La entidad podrá consultar los registros básicos de usuarios que hacen uso de sus sistemas de información por medio de los servicios digitales básicos.</p>
<b>Reconocer pagos al operador</b>	<b>Consultar la información de la facturación del servicio</b>	<p>Le permitirá a la entidad realizar consultas de la facturación del servicio, movimientos por periodo y acumulados, consultar la facturación del servicio acumulada, consultar los movimientos del servicio por periodo, consultar los movimientos del servicio acumulado</p>
<b>Interponer peticiones, quejas, consultas y reclamos.</b>	<b>Gestionar peticiones, quejas y reclamos</b>	<p>Gestionar Peticiones, Quejas y Reclamos ante los operadores y ver Reportes de Peticiones, Quejas y Reclamos relacionadas con sus usuarios y servicios habilitados sobre la plataforma de servicios digitales básicos. Le permitirá integrarse con el sistema de Peticiones, Quejas y Reclamos con el que cuenta cada Operador y en caso de no tenerlo ofrecer las siguientes funcionalidades:</p> <ul style="list-style-type: none"> <li>Radicar Peticiones, Quejas y Reclamos</li> </ul>

Operaciones de los Actores	Escenario Operacional	Descripción
		<ul style="list-style-type: none"> <li>Consultar Peticiones, Quejas y Reclamos</li> <li>Ver estado o respuesta del Peticiones, Quejas y Reclamos</li> </ul>
<b>ENTES REGULADORES</b>		
<b>Vigilar, controlar y monitorear</b>	<b>Monitorear operadores</b>	<p>Mecanismo mediante el cual el Ente regulador consume en línea y en tiempo real los indicadores de calidad asociados a la prestación de los servicios del Operador. Entre otras, las siguientes estadísticas son importantes para evaluar el impacto social y la penetración del servicio en la sociedad colombiana</p> <ul style="list-style-type: none"> <li><b>Para el servicio de Carpeta Ciudadana:</b> <ul style="list-style-type: none"> <li>Reporte del número de usuarios enrolados en la plataforma de Carpeta Ciudadana</li> <li>Reporte del espacio total utilizado</li> <li>Reporte del espacio promedio utilizado por usuario</li> <li>Reporte del número de documentos asociados a cada usuario.</li> </ul> </li> <li><b>Para el servicio de Autenticación Electrónica:</b> <ul style="list-style-type: none"> <li>Reporte del número de usuarios identificados en la plataforma</li> <li>Reporte del número de transacciones por operador</li> <li>Reporte de los sistemas de información que usan el servicio</li> </ul> </li> <li><b>Para el servicio de IOAAS</b> <ul style="list-style-type: none"> <li>Reporte del número de servicios habilitados (Activos/inactivos)</li> <li>Valores para los parámetros de cada servicio</li> <li>Reporte del número de transacciones por servicio</li> <li>Reporte de entidades consumidoras de servicios y sus trámites</li> <li>Reporte de entidades que publican servicios y su uso por otras entidades</li> <li>Reporte de servicios con análisis de desempeño, disponibilidad y atención de fallas</li> <li>Reporte de los tiempos de ejecución</li> <li>Permisos de acceso y uso, periodicidad de uso máxima permitida</li> </ul> </li> </ul>
	<b>Gestionar funcionamiento</b>	<p>El sistema de información del Ente regulador deberá informar en todo momento cuántos operadores se encuentran habilitados, cuántos se encuentran en procesos de autorización y a cuántos se les ha revocado el permiso de funcionamiento.</p> <p>El sistema deberá proveer los mecanismos electrónicos necesarios para que el aspirante a Operador tecnológico pueda enviar los documentos requeridos para su acreditación y para agendar sus visitas de auditoría de control en sitio. De la misma manera, el Ente regulador tendrá a su disposición un flujo de trabajo de habilitación de operadores en el cual podrán subir, para cada etapa, las evidencias y observaciones del trabajo llevado a cabo de forma presencial.</p> <p>Adicionalmente, el sistema deberá proveer los mecanismos necesarios para revocar la autorización de funcionamiento de un operador específico. En este caso el Ente regulador podrá subir la resolución o la justificación que respalda la decisión tomada.</p>
<b>Habilitar operadores</b>	<b>Habilitar operador de Servicios Digitales Básicos</b>	El ente regulador deberá contar con una interfaz que le permita gestionar los operadores autorizados o en proceso de autorización para la prestación de los servicios. En esta interfaz el Ente regulador podrá listar, crear, filtrar y actualizar el estado de los operadores de la plataforma de Servicios Digitales Básicos.
	<b>Exponer servicio de habilitación de Operador</b>	El Ente regulador deberá exponer el servicio de habilitación del Operador.
	<b>Revocar operador de Servicios Digitales Básicos</b>	El ente regulador podrá revocar los permisos de funcionamiento de un operador siempre y cuando existan las pruebas técnicas suficientes para tomar esta decisión. En este se deberá realizar una migración de los servicios a los operadores disponibles y que se encuentran en estado activo.
<b>Tarificar servicios</b>	<b>Gestionar servicios prestados y sus tarifas asociadas</b>	Cada operador tecnológico deberá disponer de un conjunto de servicios para que el sistema de información del Ente regulador consulte las tarifas de los servicios adicionales ofrecidos al ciudadano. Esta consulta deberá generar gráficos estadísticos e información tabular en el cual se informe de todos los servicios adicionales prestados por cada operador y sus costos asociados.

### 9.2.3 Propiedades

Aplican para todos los procesos e interacciones que se den en el modelo de Servicios Digitales Básicos las siguientes propiedades

**Tabla 6. Propiedades**

Propiedad	Descripción
<b>Funcionamiento</b>	<p>El funcionamiento se relaciona con la respuesta, eficiencia y rendimiento de los procesos internos de la plataforma y depende de la infraestructura, el ancho de banda, la capacidad de procesamiento y respuesta, la capacidad de la memoria, la cantidad de espacio de almacenamiento del sistema y el espacio asignado a cada usuario, entre otros. Se establecerán acuerdos de niveles de servicio sobre el funcionamiento que estime por ejemplo, el tiempo que debe tomar una transacción, el cargar un documento, el tiempo que debe tomar una consulta y recuperar un documento, tiempo de descarga de un documento, el número de usuarios soportados y número de usuarios concurrentes, etc.</p> <p>En lo que concierne a la Carpeta Ciudadana se refiere al rendimiento al ser cargada y usada por todos los usuarios potenciales identificados y para Autenticación Electrónica el operador deberá garantizar un ancho de banda suficiente para suplir la demanda de autenticación en sistemas de información altamente transaccionales. Este ancho de banda será directamente proporcional a su número de usuarios registrados y su proyección de incremento anual. En complemento con el ancho de banda, se deberán implementar mecanismos de balanceo de carga con estrategia Round Robin.</p> <p>Los tiempos de consulta de documentos no deberán superar un segundo de espera. Estos resultados deberán estar debidamente paginados de a 30 resultados. Los tiempos de descarga dependerán del tamaño del documento y estos no deberán superar los 2 segundos por un MB de información.</p>
<b>Seguridad</b>	<p>La seguridad se relaciona con la integridad externa de la plataforma y su capacidad para evitar el acceso no autorizado, piratería o manipulación, virus, y otras formas accidentales o maliciosas de daño. El sistema debe estar diseñado e implementado para satisfacer varios estándares de seguridad como ISO 27000, pruebas de penetración, regulación nacional. La plataforma deberá ser: físicamente segura, segura en sus datos, segura frente al acceso no autorizado, segura en sus comunicaciones, segura internamente.</p> <p><i>No repudio</i> - Ninguno de los actores deberá poder denegar de manera total o parcial las operaciones en las que ha tomado parte dentro de la plataforma o sistema debido al uso de técnicas para obtención de pruebas de la ocurrencia o no de un evento o acción dentro de la misma.</p> <p><i>Trazabilidad</i> - Se debe implementar el registro de acciones realizadas (usuario, fecha, hora) y registros del sistema con la creación, modificación y eliminación de datos. El sistema debe almacenar información de las transacciones realizadas por un usuario, se debe considerar que se realizan invocaciones de servicios independientes sin guardar estado entre llamadas, por lo que el log debe usar un mecanismo único para identificar las transacciones, almacenando información durante el progreso de las mismas en su paso por los módulos del sistema, centralizando los datos lo que permite realizar un análisis de la información recolectada para cada transacción de forma individual.</p> <p>Para precisar los requisitos referirse al modelo de Seguridad y Privacidad por diseño incluido en este documento.</p>
<b>Privacidad y debido tratamiento de datos personales</b>	<p>Es importante que la plataforma de servicios digitales básicos respete los derechos de las personas a su intimidad y el debido tratamiento de sus datos personales, teniendo en cuenta la naturaleza de la información que se utilizará. Por eso, el operador debe tomar las medidas necesarias para garantizar los mandatos constitucionales y legales sobre la materia e implementar políticas de protección de la privacidad y de los datos personales desde el diseño y por defecto, así como programa integral de privacidad y de gestión de datos personales como mecanismo operativo proteger los citados derechos y materializar el principio de responsabilidad demostrada en esta materia.</p> <p>Para precisar los requisitos referirse al modelo de Seguridad y Privacidad incluido en este documento.</p>
<b>Escalabilidad</b>	<p>La escalabilidad se relaciona con el funcionamiento y la capacidad del sistema en el tiempo y bajo una carga que aumenta de acuerdo a los usuarios potenciales estimados por periodo. Al aumentar el número de autenticaciones y documentos al mismo tiempo que el número de usuarios y la consecuente carga al sistema, el operador deberá prever la escalabilidad ya sea aumentando el tamaño y la capacidad del sistema o balancear el aumento de carga entre diferentes sistemas, o a través de múltiples servicios.</p> <p>El sistema provisto por el operador deberá estar en la capacidad de expandir y mejorar el sistema con nuevas capacidades sin tener que realizar cambios importantes a la infraestructura del sistema, en particular, la introducción de una función adicional al sistema no debe requerir cambios en servicios ya en operación que no tienen relación con dicha funcionalidad.</p>
<b>Capacidad de monitoreo</b>	<p>La plataforma de servicios digitales básicos debe tener una previsión para su propio manejo y administración. Se consideran aspectos relacionados con la administración técnica (instalación, configuración, monitoreo, espacio de almacenamiento, registro de errores, problemas técnicos) y la administración del sistema desde la perspectiva del ente regulador (reportes, estadísticas de uso, auditoría).</p>
<b>Accesibilidad</b>	<p>La plataforma debe ser asequible a todo tipo de usuario, con diferentes capacidades, incluyendo aquellos con discapacidades específicas. Uno de los principales proponentes para la evaluación activa de los requerimientos no funcionales para la accesibilidad es el World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI). El W3C WAI provee las guías para el acceso al contenido en la red, las cuales cubren recomendaciones para hacer el contenido de la red más accesible. También son válidos referentes normativos como la <i>Norma Técnica ICONTEC 5854</i>.</p>

Propiedad	Descripción
<b>Disponibilidad</b>	<p>Los requerimientos de disponibilidad son usualmente expresados como un porcentaje o radio del tiempo de actividad comparado con el tiempo de inactividad. Se requiere acceso y soporte a la plataforma 24X7 (24 horas al día los 7 días de la semana). El nivel de disponibilidad que el sistema puede proporcionar debe estar claramente establecido por el Operador en respuesta a los requerimientos no funcionales. También debe estar incluido en todos los acuerdos de niveles de servicio establecidos.</p> <p>La disponibilidad del sistema deberá estar constantemente monitoreada para observar si las metas del servicio están siendo alcanzadas o si han sido sobrepasadas.</p> <p>La plataforma debe estar en capacidad de tolerar fallas, pudiendo así proveer sus servicios en alta disponibilidad aún en presencia de fallas y debe estar en capacidad de recuperarse automáticamente de las fallas parciales sin afectar el rendimiento global. Se debe garantizar la tolerancia a fallos cuando se reciban mensajes o eventos no anticipados. El operador debe implementar las políticas de réplica y respaldo sobre la información y documentos almacenados por cada uno de los ciudadanos enrolados en la plataforma.</p>
<b>Confiabilidad</b>	<p>La confiabilidad está descrita como la integridad interna de un sistema, la precisión y exactitud de su software, y su resistencia a los defectos, problemas de funcionamiento o inesperadas condiciones de operación. La plataforma de servicios digitales básicos deberá ser capaz de manejar condiciones de error, sin quiebra o falla repentina.</p> <p>Se debe garantizar la exactitud de la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados de forma accidental o intencionada.</p> <p>Los mecanismos de autenticación provistos deben permitir que la información consignada en un mensaje de datos sea íntegra, completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido, será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias relevantes del caso. Para determinar el grado de confiabilidad se seguirán las recomendaciones de la ITU e ISO dispuestas en sus documentos ITU X.1254 e ISO 29115.</p>
<b>Recuperación</b>	<p>Si la plataforma de servicios falla por cualquier razón, es importante que el operador sea capaz de recobrar los servicios con la mayoría de los datos intactos. El operador debe asegurarse de no ser dependiente de la información que ha sido guardada y que sea más antigua de un día, especialmente en ambientes de alto volumen. Es esencial que las necesidades de los usuarios sean evaluadas antes de que ocurra cualquier desastre, y que se tenga un plan de continuidad de negocios completo y comprensivo.</p>
<b>Mantenimiento</b>	<p>La plataforma de servicios digitales básicos debe poder ser mantenida. Esto quiere decir que debe ser relativamente fácil de reparar y actualizar. El operador dispondrá de un sistema de mantenimiento con nuevas versiones, paquetes de servicios o parches. En el caso de que incluyan nuevas características y funciones, el Operador debe considerar nuevas capacitaciones y costos de formación para los usuarios.</p>
<b>Soporte</b>	<p>El operador debe mantener activa la plataforma de servicios digitales. Debe establecer el nivel de mantenimiento y soporte que le da al producto, frecuencias de actualización, fecha de la última versión liberada, y la hoja de ruta del sistema. También se refiere al nivel de soporte suministrado a los usuarios por el Operador o un tercero en representación del operador. Deben existir reglas claras de cómo acceder al servicio de soporte del Operador, como reportar errores, problemas del software, y que tipo de nivel de ayuda in situ y asistencia remota puede esperar un usuario.</p>
<b>Conformidad</b>	<p>La Plataforma de servicios digitales básicos debe estar configurada de conformidad con los estándares de la industria y con las regulaciones nacionales de la siguiente manera:</p> <ul style="list-style-type: none"> <li>• Deben estar en conformidad con todas las disposiciones legislativas y regulatorias que apliquen a la naturaleza del Operador y a la jurisdicción.</li> <li>• Deben estar en conformidad con estándares industriales generalmente aceptados en tecnología, y en las plataformas en donde sea desplegado el sistema. Así por ejemplo, para determinar los requisitos técnicos que deben cumplir los mecanismos de autenticación de acuerdo a nivel de Garantía 2 (NdG2) y 4 (NdG4) establecidos en las recomendaciones de la ITU X.1254, ISO 29115 y NIST Special Publication 800-63-2</li> <li>• Deben estar en conformidad con los formatos de documentos populares, como es el PDF, habilitando la Carpeta Ciudadana para examinar la estructura de estos documentos, extraer sus metadatos, e indexar su contenido para fines de búsqueda.</li> <li>• Debe ser compatible con el almacenamiento de archivos utilizando formatos de archivo y codificación estandarizada o totalmente documentada.</li> <li>• Debe ajustarse a las normas locales aplicables para admisibilidad jurídica y valor probatorio de la información digital.</li> <li>• El sistema no debe incluir funciones que sean incompatibles con la protección de datos a nivel nacional, la libertad de información u otra legislación.</li> <li>• El sistema debe ser compatible con la versión del lenguaje común de intercambio de información en uso al momento de su entrada en servicio. Es necesario tener en cuenta las condiciones de compatibilidad, diseño y evolución del lenguaje común de intercambio para la integración a la plataforma</li> </ul>

Propiedad	Descripción
<b>Preservación a largo plazo y obsolescencia de la tecnología</b>	Hace referencia a los riesgos tecnológicos de cara a la preservación de los documentos a largo plazo desde tres puntos de vista: <ul style="list-style-type: none"> <li>• La degradación de los medios de comunicación</li> <li>• La obsolescencia de hardware</li> <li>• La obsolescencia de formato</li> </ul>

### 9.3 Modelo de Seguridad y Privacidad

La implementación del modelo de Servicios Digitales Básicos propende por la seguridad y privacidad de la información considerando que este involucra intensivamente la gestión de datos y documentos personales. En razón de lo anterior, adicionalmente al cumplimiento normativo y de amplios referentes en materia de seguridad y privacidad, el modelo se ha centrado en el concepto de privacidad por diseño, y su aplicación a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y empresas sobre la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios digitales básicos gestionados por el operador. Según Ann Cavoukian, creadora del concepto de *Privacy by Design*<sup>51</sup>, la Privacidad por Diseño "*promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización*". Su principal premisa es el derecho que tienen las personas de ejercer un control eficiente sobre los mensajes de datos gestionados y que no solo fundamente la privacidad con la firma y/o compromiso de cumplimiento de la legislación y su marco regulador por parte del operador, sino que propone diferentes acciones a ejecutar por parte de las entidades interesadas en el momento de diseñar y desarrollar componentes necesarios para la implementación del modelo, de tal manera que estos se encaminen a garantizar la privacidad y la obtención de control de la información y sus mensajes de datos por parte de las personas, sin requerir realizar configuraciones adicionales.

A continuación se relacionan los riesgos más significativos del modelo identificados frente a la privacidad y seguridad de la información y datos personales:

**Tabla 7. Riesgos y estrategias posibles de mitigación**

CATEGORIA	RIESGO	ESTRATEGIA DE MITIGACIÓN
<b>UBICACIÓN DE LOS DATOS</b>	Localización de los datos fuera del país y ausencia de información acerca de cómo se ha implantado la infraestructura, por lo cual no se tiene prácticamente información de cómo y dónde son almacenados los datos ni de cómo se protegen los mismos. Los marcos legales y regulatorios de los países son diferentes y afectan la forma de tratar los datos. Los datos podrían ser objeto de incursiones de las autoridades locales y los datos o sistemas podrían ser divulgados o confiscados por la fuerza.	<ul style="list-style-type: none"> <li>▪ Marco regulatorio aplicable al almacenamiento y procesamiento de datos</li> <li>▪ Acuerdo con el operador para que el tratamiento de los datos se subyugue al marco legal de Colombia.</li> <li>▪ Almacenamiento y procesamientos de datos en Colombia</li> <li>▪ Los operadores de servicios se hallan sujetos a auditorías externas y al cumplimiento de instrucciones de los organismos de inspección, vigilancia y control, así como a órdenes judiciales para la verificación del cumplimiento de disposiciones legales.</li> <li>▪ Certificaciones de seguridad.</li> <li>▪ Controles de acceso a los datos</li> </ul>
<b>CONFORMIDAD</b>	Incumplimiento por parte del operador de servicios de las especificaciones técnicas, estándares, normas o leyes establecidas en el país para prestar los servicios. El operador no pueda demostrar su propio cumplimiento de los requisitos pertinentes. El operador no permite que se realice una auditoría.	<ul style="list-style-type: none"> <li>▪ Conformidad con especificaciones, estándares, normas o leyes establecidas en el país.</li> <li>▪ La posesión de certificaciones de seguridad o la realización de auditorías externas por parte del operador.</li> <li>▪ La legislación y normativa local relacionada con privacidad y seguridad.</li> <li>▪ Tecnologías y soluciones estándar</li> <li>▪ Almacenamiento y procesamiento de datos en Colombia</li> <li>▪ Integridad y transparencia en los términos de uso</li> </ul>

<sup>51</sup> Cavoukian, A., 2016. "Privacy & Big Data Institute", visto en <http://www.ryerson.ca/pbdi/about/people/cavoukian.html>



CATEGORIA	RIESGO	ESTRATEGIA DE MITIGACIÓN
<b>INFORMACIÓN</b>	Dificultad en el cumplimiento de las obligaciones de un operador en la preservación y generación de documentos para cumplimiento de auditorías o solicitud de información en procedimientos judiciales.	<ul style="list-style-type: none"> <li>Los operadores deben cumplir las obligaciones para la preservación y la generación de los documentos, tales como cumplir con las auditorías y las solicitudes de información en una investigación electrónica.</li> </ul>
<b>PROPIEDAD DE LOS DATOS</b>	Términos ambiguos en la propiedad de los datos recolectados haciendo que el operador haga uso de los mismos para su propio beneficio.	<ul style="list-style-type: none"> <li>Definir de forma clara los derechos sobre los datos estableciendo que el usuario mantiene la propiedad de todos sus datos y que el operador no adquiere derechos o licencias a través de los acuerdos para usar los datos.</li> </ul>
<b>GESTIÓN DE RIESGOS</b>	El operador no lleva a cabo el proceso de identificar y valorar los riesgos realizando los pasos necesarios para reducirlos a un nivel asumible a lo largo de su ciclo de vida.	<ul style="list-style-type: none"> <li>Confirmar que los controles de seguridad están implementados correctamente y cumplen con los requisitos de seguridad establecidos para la protección de los datos, así como las pruebas de la efectividad de dichos controles.</li> </ul>
<b>ABUSO EN LOS SERVICIOS</b>	El abuso afecta principalmente el modelo de servicios y está relacionado con la vinculación poco restrictiva de personas, empresas o entidades con la consecuente proliferación de spammers, creadores de código malicioso y otros criminales.	<ul style="list-style-type: none"> <li>Implementar un sistema de registro de acceso más restrictivo mediante el proceso de Autenticación Electrónica.</li> <li>Coordinar y monitorizar el tráfico de clientes para la detección de posibles actividades ilícitas.</li> <li>Comprobar las listas negras públicas para identificar si los rangos IP de la infraestructura han entrado en ellas.</li> </ul>
<b>PÉRDIDA DE INFORMACIÓN</b>	Comprometer los datos por el borrado o modificación sin tener una copia de seguridad supone una pérdida de datos. Esto deriva en pérdida de imagen del proyecto, del Gobierno, del operador de servicios, daños económicos y, si se trata de fuga de información, problemas legales, infracciones a las normas, etc.	<ul style="list-style-type: none"> <li>Implementar API potentes para el control de acceso</li> <li>Proteger el tránsito de datos mediante el cifrado de los mismos</li> <li>Analizar la protección de datos desde el diseño como en la ejecución</li> <li>Proporcionar mecanismos potentes para la generación de claves, almacenamiento y destrucción de la información</li> <li>Definir, por contrato, la destrucción de los datos antes de que los medios de almacenamiento sean eliminados de la infraestructura, así como la política de copias de seguridad</li> </ul>
<b>ROBO DE SESIÓN</b>	Secuestro de sesión o servicio si un atacante obtiene las credenciales de un usuario del entorno de forma que puede hacerse pasar por este y acceder a actividades y transacciones, manipular datos, devolver información falsificada o redirigir a los clientes a sitios maliciosos.	<ul style="list-style-type: none"> <li>Prohibir, mediante políticas, compartir credenciales entre usuarios y servicios</li> <li>Aplicar técnicas de autenticación de doble factor siempre que sea posible</li> <li>Monitorizar las sesiones en busca de actividades inusuales</li> </ul>
<b>USUARIOS CON PRIVILEGIOS DE ACCESO</b>	Los daños causados por usuarios maliciosos o con privilegios de acceso en el procesamiento o tratamiento de datos sensibles conllevan un riesgo inherente, ya que es posible que estos servicios sorteen los controles físicos, lógicos y humanos siendo, por este motivo, necesario conocer quién maneja dichos datos.	<ul style="list-style-type: none"> <li>Consensuar con el operador los usuarios que tendrán acceso a esos datos, para minimizar así los riesgos de que haya usuarios con elevados privilegios que no deberían tener acceso a los datos.</li> </ul>
<b>GESTIÓN DE USUARIOS</b>	Que el operador en el proceso de enrolamiento y en su operación obtenga información detallada de las personas que afecte la intimidad de los ciudadanos.	<p>Como mecanismo de control se busca que la información personal que se recolecte en el enrolamiento y operación sea mínima y debe limitarse exclusivamente a los datos necesarios para que la entidad pueda prestar un servicio o un recurso a una persona, para ello en la etapa de enrolamiento el operador solo estará autorizado a recolectar la siguiente información:</p> <ul style="list-style-type: none"> <li>Nombres</li> <li>Apellidos</li> <li>Tipo de documento</li> <li>Número del documento de identificación.</li> <li>Correo Electrónico</li> <li>Pseudónimo</li> </ul> <p>Prevía autorización del MINTIC se podrán solicitar otros datos que sean requeridos para la expedición de las credenciales, tales como:</p> <ul style="list-style-type: none"> <li>Numero de celular</li> <li>Información Biométrica (en el caso de usar la biometría como uno de los factores de autenticación)</li> <li>Otros</li> </ul> <p>La recopilación de datos en el momento del enrolamiento, deberán tener la plena aprobación de la persona a enrolar y tener la debida</p>

CATEGORIA	RIESGO	ESTRATEGIA DE MITIGACIÓN
		<p>protección de Datos Personales, de conformidad y en los términos de la ley 1581 de 2012.</p> <p>No deberá aportarse por parte del ciudadano información adicional a la mencionada anteriormente, como por ejemplo (dirección física, entre otros) a los operadores y/o a los sistemas de información que así lo soliciten. Por lo anterior el operador en sus contratos de vinculación y/o términos y condiciones debe indicar de manera clara que los únicos datos a recolectar serán los anteriormente mencionados.</p>
	<p>Que en el momento del enrolamiento una persona suplante la identidad de otro ciudadano.</p> <p>Que un atacante copia una credencial creada por el operador para una persona cuando ésta se transfiere del operador a la persona durante el establecimiento de credencial</p>	<p>El enrolamiento inicial deberá ser presencial, y la identidad de las personas deberá verificarse contra la base de datos biográfica y biométrica de la Registraduría Nacional del Estado Civil con el fin de garantizar la identidad de la persona</p> <p>Deberá establecerse un procedimiento para garantizar que una credencial, o los medios para generarla, se activa únicamente si está bajo el control de la persona que le corresponde.</p>
	Que un atacante haga que un operador cree una credencial basada en una identidad ficticia	<p>Dentro del registro se deberán almacenar datos generados en el proceso de enrolamiento, tales como:</p> <ul style="list-style-type: none"> <li>▪ Identificador de la transacción correspondiente a la autenticación biométrica contra el AFIS de la RNEC, que deberá ser almacenado dentro de los campos del registro, incluyendo el resultado de la validación.</li> <li>▪ Punto de enrolamiento</li> <li>▪ Identificador de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (AFIS) provisto por la Registraduría Nacional del Estado Civil RNEC.</li> <li>▪ Estampa cronológica de la confirmación de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (AFIS) provisto por la RNEC.</li> <li>▪ Firma electrónica de la transacción que corresponda al funcionario o persona a cargo que facilitó la verificación.</li> </ul> <p>Si una credencial, o los medios para producirla, está incluida en un dispositivo de hardware, este dispositivo deberá mantenerse físicamente en un lugar seguro y deberá realizarse un seguimiento del inventario. Por ejemplo, las tarjetas inteligentes no personalizadas deben almacenarse en un sitio seguro y deben registrarse sus números de serie para protegerlas contra el robo e intentos posteriores de crear credenciales no autorizadas.</p>
	Que en el momento de enrolamiento de una persona, el operador no efectúa la autenticación biométrica contra el AFIS de la RNEC o esta validación no es exitosa, y pese a ello se realiza la asignación de credenciales.	<p>Dentro del registro se deberán almacenar datos generados en el proceso de enrolamiento, tales como:</p> <ul style="list-style-type: none"> <li>▪ Identificador de la transacción correspondiente a la autenticación biométrica contra el AFIS de la RNEC, que deberá ser almacenado dentro de los campos del registro, incluyendo el resultado de la validación.</li> <li>▪ Punto de enrolamiento</li> <li>▪ Identificador de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (AFIS) provisto por la Registraduría Nacional del Estado Civil RNEC.</li> <li>▪ Estampa cronológica de la confirmación de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (AFIS) provisto por la RNEC.</li> <li>▪ Firma electrónica de la transacción que corresponda al funcionario o persona a cargo que facilitó la verificación.</li> </ul>
	Que con el fin de generar reportes y estadísticas de uso y mediante un procedimiento de minería de datos se logre acceder a datos privados de los ciudadanos respecto al servicio de Autenticación Electrónica.	Como mecanismo de control se busca que la información personal que se procese tenga el menor detalle y un nivel de agregación que sea imposible particularizar a una persona, de tal manera que la información personal identificable de cada ciudadano se oculte entre toda la información agregada.

CATEGORIA	RIESGO	ESTRATEGIA DE MITIGACIÓN
	Que las personas no conozcan que los sistemas de información de las entidades validan su identidad y un atacante pueda obtener su información de autenticación.	Como mecanismo de control se busca mantener informado a los ciudadanos sobre el uso de sus credenciales, así como la información que se comparte en el proceso de autenticación y/o cualquier proceso que se realice uso de su información. Para lo cual se debe proveer: <ul style="list-style-type: none"> <li>▪ un servicio de notificación cuando se modifiquen los atributos de identidad de las personas</li> <li>▪ un servicio de notificación cuando se modifiquen las autorizaciones dadas por las personas</li> <li>▪ un servicio de notificación y alerta a los propietarios de la identidad sobre transacciones de autenticación interpretadas por el operador como una amenaza a sus credenciales e información</li> </ul>
	Que múltiples plataformas conectadas a la Autenticación Electrónica desean validar la identidad de un ciudadano y obtener información de este.	Como mecanismo de control se busca que los ciudadanos tengan el control sobre el servicio de autenticación y el tratamiento de sus datos, permitiéndole al ciudadano que él sea quien define sus preferencias para compartir información. Las personas tienen el derecho de acceder, modificar y suprimir su información personal.
	Una persona ya enrolada pierde sus derechos civiles y desea acceder a algún tipo de servicios al cual ya no tiene derecho.	Los datos necesarios para el proceso de autenticación deben ser precisos y mantenerse actualizados; deben tomarse las medidas necesarias para garantizar que los datos inexactos o incompletos se suprimen o corrigen, habida cuenta de los fines para los que se ha recabado y/o procesado, por lo cual, como mecanismo de control se busca que el operador realice una validación con el Archivo Nacional de Identificación de la Registraduría Nacional del Estado Civil, con el fin de actualizar la información de naturaleza pública y datos sin reserva legal, incluyendo la vigencia del documento.
<b>AISLAMIENTO DE DATOS</b>	Los datos se comparten con datos de otros clientes en bases de datos o infraestructuras comunes para derivar economías de escala para el operador.	<ul style="list-style-type: none"> <li>▪ El operador debe garantizar el aislamiento de los datos de los respectivos usuarios.</li> <li>▪ Implementar técnicas de cifrado de los datos aislados para reducir grandemente el riesgo de exposición mientras conserva la economía de escala</li> </ul>
<b>RECUPERACIÓN</b>	Pérdida de seguridad en el acceso, control y recuperación de la información. No realizar una copia de seguridad para prevenir cualquier desastre. Pérdida de datos en una recuperación de datos.	<ul style="list-style-type: none"> <li>▪ Se debe exigir a los proveedores los datos sobre la viabilidad de una recuperación completa y el tiempo que podría tardar.</li> <li>▪ Los operadores de servicio deben tener una política de recuperación de datos en caso de desastre.</li> <li>▪ Los datos sean replicados en múltiples infraestructuras para evitar que sean vulnerables a un fallo general.</li> <li>▪ Se debe exigir un plan de copias de seguridad que permita reiniciar rápidamente el servicio ante un desastre.</li> </ul>
<b>VIABILIDAD A LARGO PLAZO DEL OPERADOR</b>	Inviabilidad a largo plazo del operador por inhabilidad, suspensión, deshabilitación o porque es comprado o absorbido. Los clientes deben estar seguros que sus datos permanecerán disponibles.	<ul style="list-style-type: none"> <li>▪ El usuario debe asegurarse que podrá recuperar sus datos aún en el caso de que el operador sea inhabilitado, suspendido, comprado o absorbido por otro o bien contemplar la posibilidad de que los datos puedan ser migrados a la nueva infraestructura de otro operador de servicio.</li> <li>▪ Los operadores deben mostrar como retornaran los datos y en qué formato para poder importarlos en una nueva aplicación.</li> </ul>
<b>RESPUESTA A INCIDENTES</b>	Detección y reconocimiento de los incidentes de seguridad y privacidad que incluye la verificación, el análisis del ataque, la contención, la recolección de evidencias, la aplicación de remedios y la restauración del servicio.	<ul style="list-style-type: none"> <li>▪ Entender y negociar los contratos de servicio de los operadores, así como los procedimientos para la respuesta a incidentes requeridos por los usuarios.</li> </ul>
<b>DISPONIBILIDAD</b>	La disponibilidad puede ser interrumpida de forma temporal o permanente. Los ataques de denegación de servicio, fallos del equipamiento y desastres naturales son todas amenazas a la disponibilidad.  Los tiempos de respuestas en caso de fallo o fuera de servicio están fuera de plazo. No se dispone de infraestructuras de respaldo para poder prestar el servicio mientras se prolonga el periodo de recuperación.	<ul style="list-style-type: none"> <li>▪ Asegurarse que durante una interrupción del servicio, las operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente.</li> </ul>

CATEGORIA	RIESGO	ESTRATEGIA DE MITIGACIÓN
<b>VALOR CONCENTRADO</b>	La Carpeta Ciudadana puede ser objetivo de ataques porque, en cierto modo, concentra gran cantidad de información personal.	<ul style="list-style-type: none"> <li>Autenticación de múltiple nivel: Los servicios deben proporcionar controles de acceso autenticación de múltiple nivel mediante la implementación de sistemas compuestos donde se requiera la utilización de forma conjunta de dos factores para el acceso a los sistemas.</li> <li>Segregación de cuentas con privilegios: Se debe garantizar una correcta segregación de funciones entre los diferentes actores o perfiles que forman parte del grupo de usuarios con privilegios administrativos sobre la infraestructura del servicio.</li> </ul>
<b>CIFRADO DE DATOS</b>	Pérdida del control directo sobre los datos ya que estos dejan de estar alojados en servidores sobre los cuales tienen la gestión directa en todos sus sentidos a estar en servidores donde principalmente están administrados por el proveedor del servicio.	<ul style="list-style-type: none"> <li>Securización de los datos mediante el cifrado de los datos. El cifrado de los datos ofrece un nivel extra de protección para los datos, al limitar el acceso a los mismos.</li> <li>Securización de las comunicaciones ante la interceptación de los datos <i>on-the-air</i>. <ul style="list-style-type: none"> <li>* Utilización de canales de comunicación cifrados entre el cliente y los servicios.</li> <li>* Permitir la realización de copias de seguridad con los datos cifrados, de este modo es posible incrementar la seguridad de los datos respecto a accesos no autorizados a los datos de las copias de seguridad.</li> </ul> </li> </ul>
<b>PÉRDIDA DE CREDENCIALES</b>	Aquí se incluye la divulgación de las claves secretas (SSL, codificación de archivos, claves privadas del usuario etc.) o las contraseñas a las partes maliciosas, la pérdida o corrupción de dichas claves o su uso indebido para la autenticación y el no repudio.	<ul style="list-style-type: none"> <li>Procedimientos de gestión de claves adecuados.</li> </ul>
<b>ORDENES JUDICIALES</b>	Revelación de datos a partes no deseadas por incautación de hardware físico a raíz de una orden judicial de las autoridades.	<ul style="list-style-type: none"> <li>Cumplimiento de políticas que en la materia sean definidas por el Ente Regulador en el marco de la legislación vigente.</li> </ul>
<b>PROTECCIÓN DE DATOS</b>	Dificultad del usuario de comprobar de manera eficaz el procesamiento de datos que lleva a cabo el operador y en consecuencia, tener la certeza de que los datos se gestionan de conformidad con la ley. Infracciones de la seguridad de los datos no notificadas al usuario. Pérdida de control de los datos procesados por el operador de servicio.	<ul style="list-style-type: none"> <li>Marco regulatorio aplicable en materia de protección de datos.</li> <li>Imposición de sanciones administrativas, civiles e incluso penales.</li> <li>Divulgación de información sobre prácticas de procesamiento de datos de los operadores de servicio.</li> <li>Certificación sobre actividades de procesamiento y seguridad de datos y los controles de datos.</li> </ul>

Frente a estas categorías y riesgos así como aquellos específicos que sean identificados en el marco de la operación del modelo los operadores establecerán estrategias puntuales y controles efectivos. En materia de *Seguridad de la información* el modelo demanda la implementación de sistemas de gestión de seguridad y unos controles que permitan disminuir el riesgo asociado a la integridad, confidencialidad y disponibilidad de la información para lo cual los operadores adoptarán prácticas de amplio reconocimiento internacional así como el Modelo de Seguridad<sup>52</sup> habilitado por el Ministerio de Tecnologías de Información y Comunicaciones. En lo que respecta a *Privacidad de la información* se identifican a continuación las categorías de controles de privacidad y protección de datos personales lo que proporciona un conjunto inicial de requisitos que serán implementados por los operadores del modelo incluyendo como ya se mencionó la privacidad por diseño. Este conjunto de requisitos no es exhaustivo, sino más bien un conjunto representativo.

<sup>52</sup> Consultar en [http://www.MINTIC.gov.co/gestionti/615/articles-5482\\_Modelo\\_Seguridad.pdf](http://www.MINTIC.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf)

**Tabla 8. Requisitos de Privacidad de la Información**

CATEGORIA	REQUISITOS MINIMOS	REFERENTES
<b>POLÍTICAS Y PROCEDIMIENTOS</b> Creación de políticas y procedimientos que rijan el uso adecuado de información personal e implementación de controles de privacidad.	<ol style="list-style-type: none"> <li>1. Promulgar las políticas y procedimientos que le competan en su calidad de Responsable de Tratamiento de los Datos para garantizar el cumplimiento los derechos consagrados en los <i>artículos 15 y 20 de la Constitución Política</i> y de la normatividad colombiana vigente y aplicable en especial los requisitos de la <i>Ley 1581 de 2012 de Protección de Datos Personales</i>, del decreto 1377 de 2013 y de la <i>Guía para la implementación de la Responsabilidad Demostrada de la SIC</i>.</li> <li>2. Publicar y garantizar el entendimiento y apropiación de las políticas de privacidad para las prácticas en los servicios.</li> <li>3. Establecer reglas de conducta para las personas involucradas en el diseño, desarrollo, operación, o mantenimiento de cualquier sistema de archivos, o en mantener algún registro.</li> <li>4. Tener un proceso documentado e implementado para la realización y revisión del <i>Programa Integral de Gestión de Datos Personales</i> a la luz de la Guía de la SIC y de <i>Evaluaciones de Impacto en la Privacidad o en la Protección de Datos</i>, más conocidas como PIAs, por sus siglas en inglés (Privacy Impact Assessments) adoptando metodologías reconocidas internacionalmente.</li> </ol>	Artículos 15 y 20 -Constitución Política Artículos 1, 4, 17, 18 y 25 - Ley 1581 de 2012 Artículos 2.2.25.2.8., 2.2.25.3.1, 2.2.25.3.7, 2.2.25.6.1, y 2.2.25.6.2, de Políticas internas efectivas del Decreto 1074 de 2015 Numeral 2.3 <i>Políticas</i> - Guía para la implementación de la Responsabilidad Demostrada de la SIC.  Buena práctica internacional Apéndice J. <i>Control AR-1 Programa de Gobierno y Privacidad</i> - NIST Special Publication 800-53 <sup>53</sup>
<b>PRIVACIDAD POR DISEÑO</b> Implementación de controles y revisiones de privacidad durante todo el ciclo de vida de diseño y desarrollo del sistema-Privacidad por Diseño.	<ol style="list-style-type: none"> <li>1. Realizar y actualizar las <i>Evaluaciones de Impacto a la Privacidad y del Programa Integral de Gestión de Datos Personales</i> cuando cambios del sistema creen nuevos riesgos a la privacidad.</li> <li>2. Incorporar prácticas y procesos de desarrollo necesarios destinadas a salvaguardar la información personal de los individuos a lo largo del ciclo de vida de un sistema, programa o servicio.</li> <li>3. Mantener las prácticas y procesos de gestión adecuadas durante el ciclo de vida de los datos que son diseñados para asegurar que sistemas de información cumplen con los requisitos, políticas y preferencias de privacidad de los ciudadanos.</li> <li>4. Uso de los máximos medios posibles necesarios para garantizar la seguridad, confidencialidad e integridad de información personal durante el ciclo de vida de los datos, desde su recolección original, a través de su uso, almacenamiento, difusión y seguro destrucción al final del ciclo de vida.</li> <li>5. Asegurar la infraestructura, sistemas TI, y prácticas de negocios que interactúan con o implican el uso de cualquier información personal siendo razonablemente transparente y sujeta a verificación independiente por parte de todas las partes interesadas, incluyendo clientes, usuarios y organizaciones afiliadas.</li> </ol> <p>Dentro de las características a tener en cuenta para implementar la privacidad por diseño se encuentran las ocho (8) estrategias de Hoepman<sup>54</sup> para desarrollar proyectos, que como el de Servicios Digitales Básicos, exigen intensivamente la gestión de datos personales. Dichas estrategias, aplicadas al modelo propuesto deben considerar los requerimientos específicos que se presentan en la tabla 9.</p>	Artículos 15 -Constitución Política Artículos 1, 4, 17, 18 y 25 - Ley 1581 de 2012 Artículos 2.2.25.2.8., 2.2.25.3.1, 2.2.25.3.7, 2.2.25.6.1, y 2.2.25.6.2 del Decreto 1074 de 2015 Numeral IV Evaluación y Revisión continua - Guía para la implementación de la Responsabilidad Demostrada de la SIC. Buena práctica internacional: NIST Special Publication 800-53
<b>GESTIÓN DEL RIESGO</b> Evaluación y gestión de riesgos a las operaciones, activos y personas resultado de la recolección, intercambio, almacenamiento, transmisión y uso de información personal. Establecer los controles pertinentes y adecuados frente a cada riesgo.	<ol style="list-style-type: none"> <li>1. Realizar la Evaluación de Impacto a la Privacidad para analizar cómo se maneja la información: garantizar que el manejo se ajusta a la ley, regulación, y requerimientos normativos de la protección de datos; para identificar, medir, controlar y monitorear los riesgos y efectos de recopilar, mantener y difundir información en forma identificable en un sistema de información electrónico; y para examinar y evaluar las protecciones y procesos alternativos para el manejo de la información para mitigar riesgos potenciales de privacidad y protección de datos</li> <li>2. Garantizar que los costos de inversión cubren el ciclo de vida de cada sistema e incluye todos los recursos presupuestales requeridos.</li> </ol>	Artículos 15 -Constitución Política  Artículos 1, 4, 17, 18 y 25 - Ley 1581 de 2012  Artículos 2.2.25.6.1, y 2.2.25.6.2 del Decreto 1074 de 2015  Numeral 2.4 <i>Sistema de Administración de Riesgos asociados al tratamiento de Datos personales</i> - Guía para la implementación de la Responsabilidad Demostrada de la SIC

<sup>53</sup> National Institute of Standards and Technology - Special Publication NIST 800-53 Revisión 4, 2013, "Security and Privacy Controls for Federal Information Systems and Organizations". Visto en: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

<sup>54</sup> Hoepman, J.H, 2012, "Privacy Design Strategies", Institute for Computing and Information Sciences, Radboud University, Nijmegen, The Netherlands, pp. 1-9, visto el 6 de Noviembre de 2015, <https://www.cs.ru.nl/~jhh/publications/pdp.pdf>

CATEGORIA	REQUISITOS MINIMOS	REFERENTES
		Buena práctica internacional: Apéndice J. <i>Control AR-2 Evaluación de riesgos e impacto de la Privacidad</i> - NIST Special Publication 800-53 Template for a PIA report. Proyecto «Privacy Impact Assessment Framework». Bruselas-Londres ISO/IEC 27005 Information Technology. Security Techniques. Information security risk management. ISO 31010. Gestión del riesgo. Técnicas de apreciación del riesgo. Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)
<b>MEDIDAS DE SEGURIDAD</b> Aplicación de los controles adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información personal.	<ol style="list-style-type: none"> <li>1. Establecer medidas administrativas, técnicas y físicas para garantizar la seguridad y la confidencialidad de los registros y datos.</li> <li>2. Garantizar que la Evaluación de Impacto a la Privacidad identifica cómo la información será asegurada (controles administrativos y técnicos)</li> </ol>	Artículos 2.2.2.25.3.7, 2.2.2.25.6.1, y 2.2.2.25.6.2 del Decreto 1074 de 2015.
<b>ROLES ASIGNADOS, RESPONSABILIDADES, Y RENDICIÓN DE CUENTAS</b> Identificación de funciones generales y específicas y las responsabilidades para la gestión y uso de información personal y garantizar la rendición de cuentas para cumplir estas responsabilidades.	<ol style="list-style-type: none"> <li>1. Designar un <i>Oficial de Privacidad o Protección de Datos</i> responsable por el operador de las velar por el cumplimiento de las políticas de privacidad, de las medidas legislativas, reglamentarias, y otras políticas propuestas, las evaluaciones de impacto a la privacidad, del impacto de las tecnologías de información personal, y tecnologías que permiten la auditoría continua de conformidad con las políticas y prácticas de privacidad establecidas.</li> <li>2. Identificar las personas que tienen día a día la responsabilidad en la organización del Operador de la ejecución de políticas de privacidad y el cumplimiento normativo; designar un funcionario(s) de alto nivel apropiado (por ejemplo, CIO) para servir como contacto principal del operador para asuntos de tecnología /web y las políticas de privacidad de la información.</li> <li>3. Establecer un <i>Comité de Privacidad o Protección de Datos</i> para supervisar y coordinar los componentes y la aplicación de los programas así como las evaluaciones y rendición de cuentas.</li> <li>4. Todos los empleados y contratistas deben ser conscientes de la privacidad y su obligación para proteger la información en forma identificable.</li> </ol>	Artículo 2.2.2.25.4.4, del Decreto 1074 de 2015. Numeral 1.2 <i>Oficial de Protección de Datos</i> - Guía para la implementación de la Responsabilidad Demostrada de la SIC
<b>SENSIBILIZACIÓN Y PROGRAMAS DE CAPACITACIÓN BASADO EN FUNCIONES</b> Garantizar que los administradores y usuarios de la información personal son conscientes de los riesgos de privacidad asociados con sus actividades y de las leyes aplicables, políticas y procedimientos relacionados con la privacidad.	<ol style="list-style-type: none"> <li>1. Capacitar a cada persona implicada en el tratamiento de datos personales en las reglas de conducta y sanciones en caso de incumplimiento.</li> <li>2. Informar y educar a los empleados y contratistas de su responsabilidad para proteger información en forma identificable.</li> <li>3. Asegurarse de que todo el personal está familiarizado con las leyes de privacidad de la información, reglamentos y políticas y entender las ramificaciones de acceso inadecuado y revelación.</li> <li>4. Impartir una formación adaptada específicamente a las funciones del personal que maneja datos personales. Esta formación debe ser permanente e incluir la actualización periódica en el contenido del <i>Programa Integral de Gestión de Datos Personales</i> y los resultados de las <i>Evaluaciones de Impacto a la Privacidad</i>.</li> </ol>	Artículos 2.2.2.25.3.7, 2.2.2.25.6.1, y 2.2.2.25.6.2 del Decreto 1074 de 2015. Numeral 2.5 <i>Requisitos de Formación y Educación</i> - Guía para la implementación de la Responsabilidad Demostrada de la SIC Buena práctica internacional: Apéndice J. <i>Control AR-5 Formación y conciencia en Privacidad</i> - NIST Special Publication 800-53

CATEGORIA	REQUISITOS MINIMOS	REFERENTES
<b>DIVULGACIÓN PÚBLICA</b> Revelar públicamente las políticas de privacidad y procedimientos de un programa o sistema, así como los derechos de los titulares de los datos y mecanismos para hacerlos válidos.	1. Publicar las políticas sobre rutinas de uso de los datos personales y registros contenidos en el sistema, propósitos de uso, las políticas y prácticas con respecto al almacenamiento, recuperabilidad, controles de acceso, retención y eliminación de los registros; los mecanismos del operador mediante el cual un ciudadano puede ser notificado a petición de éste si el sistema contiene un registro o dato que le corresponda; los procedimientos mediante los cuales un ciudadano puede ser notificado a su petición y la forma en que puede acceder a cualquier registro que le pertenece y este contenido en el sistema de registros, y cómo él puede impugnar su contenido. 2. Informar a los ciudadanos - Titulares de los datos sobre los derechos que tienen a acceder a sus datos personales, actualizarlos, corregirlos y eliminarlos y revocar las autorizaciones que hayan otorgado, e informa acerca de los mecanismos puestos a disposición por el Operador para ello.	Ley 1581 de 2012 artículos 17 y 18 Sección 3 Capítulo 25 Decreto 1074 de 2015. Capítulo 26 Decreto 1074 de 2015. Numeral 2.8 <i>Comunicación Externa</i> - Guía para la implementación de la Responsabilidad Demostrada de la SIC Buena práctica internacional: Apéndice J. <i>Control TR-3 Difusión del programa de privacidad de Información</i> - NIST Special Publication 800-53
<b>DERECHOS INDIVIDUALES. PARTICIPACIÓN INDIVIDUAL</b> Proporcionando a los ciudadanos la oportunidad de acceder y corregir su información personal y buscar reparación por violaciones a la privacidad.	1. No revelar cualquier registro que se encuentre en un sistema a través de cualquier medio de comunicación a cualquier persona, u otra entidad, sino en virtud de una solicitud por escrito por, o con el consentimiento previo por escrito de la persona a la que se refiere el registro. 2. Atender petición de cualquier ciudadano para acceder a su propio registro o para cualquier información relacionada con lo que está contenido en el sistema bajo su titularidad. 3. Recolectar información en la mayor medida posible directamente desde el ciudadano cuando la información puede dar como resultado determinaciones adversas sobre los derechos del individuo, beneficios o privilegios institucionales. 4. Permitir al ciudadano solicitar la modificación de un registro que le pertenece y realizar cualquier corrección de cualquier porción de la misma que el individuo cree que no es precisa, pertinente, oportuna o completa; o informar a la persona de su negativa a corregir el registro de conformidad con su solicitud, la razón de la negativa, la procedimientos establecidos por el operador para que el ciudadano solicite una revisión de esa negativa por un funcionario designado por el titular de la Entidad o fuente primaria, y el nombre y dirección de ese funcionario.	Ley 1581 de 2012 títulos IV y V. Sección 4 Capítulo 25 Decreto 1074 de 2015. Numeral 2.8 <i>Comunicación Externa</i> - Guía para la implementación de la Responsabilidad Demostrada de la SIC Buena práctica internacional: Apéndice J. <i>Control IP-4 Gestión de Reclamaciones</i> - NIST Special Publication 800-53
<b>NOTIFICACIÓN</b> Aviso de notificación de las prácticas de información a la persona antes de recoger información personal.	1. Informar a las personas en el momento de la recolección y en los medios de recolección de la autoridad que autoriza la solicitud de la información y si la divulgación de dicha información es obligatoria o voluntaria; el propósito(s) de la recolección de información; los usos; y los efectos de no proporcionar la totalidad o parte de la información solicitada. 2. Notificar a un ciudadano cuando cualquier dato o registro de dicha persona se ponga a disposición de cualquier Autoridad bajo un proceso legal obligatorio cuando tales procesos se convierten en un asunto de interés público. 3. Adoptar la tecnología de lectura mecánica que alerte a los usuarios de forma automática sobre si las prácticas de privacidad se ajustan a sus preferencias de su privacidad.	Ley 1581 de 2012 título IV y artículos 4, 17 y 18. Sección 2 Capítulo 25 Decreto 1074 de 2015. Buena práctica internacional: Apéndice J. <i>Controles IP-2 Acceso Individual TR-a Confidencialidad</i> - NIST Special Publication 800-53
<b>CONSENTIMIENTO</b> Obtener consentimiento del ciudadano para utilizar su información personal.	1. No revelar cualquier registro que se encuentre en un sistema de registros por cualquier medio de comunicación a cualquier persona, u otra entidad, sino en virtud de una solicitud por escrito por, o con el consentimiento previo por escrito del ciudadano - titular del derecho al que se refiere el registro.	Ley 1581 de 2012 artículos 11, 17 y 18. Sección 2 Capítulo 25 Decreto 1074 de 2015. Buena práctica internacional: Apéndice J. <i>Control IP-1 Consentimiento</i> - NIST Special Publication 800-53
<b>MÍNIMO NECESARIO</b> Recolectar la cantidad mínima de información personal necesaria para lograr el propósito del negocio.	1. Mantener en los registros sólo la información sobre un ciudadano que sea relevante y necesaria para lograr el propósito del servicio que deba llevarse a cabo por el operador.	Ley 1581 de 2012 título IV y artículos 4, 17 y 18. Sección 2 Capítulo 25 Decreto 1074 de 2015. Buena práctica internacional: Apéndice J. <i>Controles DM Minimización y retención de datos</i> - NIST Special Publication 800-53

CATEGORIA	REQUISITOS MINIMOS	REFERENTES
<b>USO ACEPTABLE</b> Garantizar que la información personal se utiliza sólo en la forma prevista en la notificación, para lo cual el ciudadano aceptó y de acuerdo con las prácticas públicas divulgadas.	1. El nombre y la dirección de una persona no puede ser comercializada o rentada por un operador a menos que dicha actividad está autorizada específicamente por la ley.	Ley 1581 de 2012 artículo 4, 17 y 18. Decreto 1074 de 2015.  Buena práctica internacional: Apéndice J. <i>Controles UI-1 Uso interno y UL-2 Intercambio de Información a terceros</i> - NIST Special Publication 800-53
<b>EXACTITUD DE LOS DATOS</b> Garantizar que la información personal es exacta, sobre todo si daño o negación de beneficios pueden resultar.	1. Tomar las medidas razonablemente necesarias para garantizar que los registros que se usan para hacer las determinaciones acerca de un ciudadano son precisos para garantizar la equidad. 2. Antes de difundir cualquier registro sobre un ciudadano hacer esfuerzos razonables para asegurar que dichos registros son precisos, completos, oportunos y relevantes para los propósitos.	Ley 1581 de 2012 artículo 4, 17 y 18.  Buena práctica internacional: Apéndice J. <i>Control DI-1 Calidad de los Datos</i> - NIST Special Publication 800-53
<b>AUTORIZACIÓN DE NUEVOS USOS</b> Asegurar que el ciudadano autoriza los usos nuevos y secundarios de información personal previamente no identificada en el aviso original de recolección.	1. Ningún registro o dato contenido en un sistema de registros podrá ser comunicado a un destinatario u entidad para su uso en un programa de computación salvo si se efectúa un acuerdo formal entre el titular o la fuente y el organismo receptor.	Ley 1581 de 2012 artículo 4, 17 y 18 y Título IV. Sección 2 Capítulo 25 Decreto 1074 de 2015.  Buena práctica internacional: Apéndice J. <i>Control UL-2 Intercambio de Información a terceros</i> - NIST Special Publication 800-53
<b>CADENA DE CONFIANZA</b> Estableciendo y monitoreando acuerdos de terceros para el manejo de información personal.	1. Todo subcontratista o proveedor del operador, que actúe en su nombre para desarrollar servicios sobre un sistema de registros, debe cumplir con los requisitos de la presente sección sobre privacidad y protección de datos personales. Los contratistas y cualquier empleado de tal contratista deberá ser considerado como un empleado del operador.	Ley 1581 de 2012 artículo 17 y 18 y Título IV. Artículos 2.2.2.25.3.7, 2.2.2.25.6.1, y 2.2.2.25.6.2 del Decreto 1074 de 2015.  Buena práctica internacional: Apéndice J. <i>Control AR-3 Requisitos de privacidad para contratistas y proveedores</i> - NIST Special Publication 800-53
<b>MONITOREO Y MEDICIÓN</b> Supervisar la aplicación de controles de privacidad y medir su eficacia.	1. Llevar a cabo y estar preparados para informar de los resultados de evaluaciones y auditorías de las actividades encomendadas por la Legislación de Protección de datos personales y aplicaciones de buenas prácticas de privacidad, incluyendo contratos, registros, los usos de rutina, exenciones, coordinando los programas, capacitación, violaciones y sistemas de registros.	Ley 1581 de 2012 artículo 17 y 18 y Título IV. Artículos 2.2.2.25.3.7, 2.2.2.25.6.1, y 2.2.2.25.6.2 del Decreto 1074 de 2015.  Buena práctica internacional: Apéndice J. <i>Control AR-4 Monitoreo y Auditoría de la Privacidad</i> - NIST Special Publication 800-53
<b>NOTIFICACIÓN Y RESPUESTA ANTE INCIDENTES</b> Ofrecer a directivos y responsables de supervisión así como a la Autoridad Nacional SIC los resultados de la seguimiento y medición de los controles de privacidad y responder a las violaciones de privacidad.	1. Llevar a cabo y estar preparado para informar sobre los resultados de las siguientes actividades: contratos, prácticas de registros, usos de rutina, excepciones, formación, violaciones, incidentes en los sistemas de registro. 2. Documentar el cumplimiento de las leyes sobre protección de datos, reglamentos y políticas. 3. Documentar los resultados de las auditorías de cumplimiento, acciones correctivas implementadas para remediar las deficiencias identificadas de cumplimiento. 4. Reportar los incidentes a los ciudadanos titulares de la información y a la Superintendencia de Industria y Comercio.	Ley 1581 de 2012 artículo 17 y 18 y Título IV. Artículos 2.2.2.25.3.7, 2.2.2.25.6.1, y 2.2.2.25.6.2 del Decreto 1074 de 2015.  Numeral 2.6 <i>Protocolos de respuesta en el manejo de violaciones e incidentes</i> - Guía para la implementación de la Responsabilidad Demostrada de la SIC.  Buena práctica internacional: Apéndice J. <i>Control SE-2 Respuesta a incidentes de Privacidad e IP-3 Compensación</i> - NIST Special Publication 800-53



CATEGORIA	REQUISITOS MINIMOS	REFERENTES
<b>PRESENTACIÓN DE INFORMES</b>	1. Generar y consolidar informes sobre cumplimiento de privacidad con periodicidad mínima anual incluyendo el seguimiento y ejecución del <i>Programa Integral de Gestión de Datos Personales</i> y acciones frente a las <i>Evaluaciones de Impacto a la Privacidad</i> .	Ley 1581 de 2012 artículo 17 y 18 y Título IV.  Artículos 2.2.2.25.3.7, 2.2.2.25.6.1, y 2.2.2.25.6.2 del Decreto 1074 de 2015.  Numeral 1.3 <i>Presentación de Informes</i> - Guía para la implementación de la Responsabilidad Demostrada de la SIC  Buena práctica internacional: Apéndice J. <i>Control AR-6 Notificación de Privacidad</i> - NIST Special Publication 800-53

**Tabla 9. Requerimientos mínimos frente a Estrategias de Privacidad por Diseño**

ESTRATEGIA PRIVACIDAD POR DISEÑO	REQUERIMIENTO MÍNIMO
<b>MINIMIZAR</b> Esta estrategia establece que la cantidad de datos de carácter personal que se procese debe restringirse a la mínima cantidad posible.	Que los datos requeridos para el enrolamiento de un ciudadano en un sistema de información sean los mínimos para validar su identidad, esto es: <ul style="list-style-type: none"> <li>▪ Nombres</li> <li>▪ Apellidos</li> <li>▪ Tipo de documento</li> <li>▪ Número del documento de identificación.</li> <li>▪ Correo Electrónico</li> <li>▪ Pseudónimo</li> </ul> Prevía autorización del ciudadano se podrán solicitar otros datos que sean requeridos para la expedición de las credenciales, tales como: <ul style="list-style-type: none"> <li>▪ Numero de celular</li> <li>▪ Información biométrica</li> <li>▪ Dirección postal</li> <li>▪ Otros</li> </ul> Dentro del registro se deberán almacenar datos generados en el enrolamiento, tales como: <ul style="list-style-type: none"> <li>▪ Punto de enrolamiento</li> <li>▪ Identificador de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (Afis) provisto por la Registraduría Nacional del Estado Civil RNEC</li> <li>▪ Estampa cronológica de la confirmación de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (Afis) provisto por la RNEC</li> <li>▪ Firma electrónica de la transacción que corresponda al funcionario o persona a cargo que facilitó la verificación.</li> </ul>
<b>PROTEGER</b> Esta estrategia establece que cualquier dato de carácter personal que se procese por parte del operador debe estar protegido.	El operador debe implementar en los servicios de almacenamiento y tránsito de información, el uso de criptografía, con el objetivo de permitir la protección criptográfica fuerte de la información, conforme a estándares reconocidos y aceptados a nivel mundial y en especial a los adoptados por las entidades nacionales, de tal manera que solo el ciudadano pueda descifrar y acceder a la información.  Los nombres asignados a los archivos almacenados no deben permitir identificar al ciudadano dueño de los mismos, de tal manera que al tener acceso al repositorio lógico que almacene los archivos, su nombre no identifique de ninguna manera al ciudadano dueño de los mismos.
<b>SEPARAR</b> Esta estrategia busca siempre que sea posible que el procesamiento de los datos de carácter personal se realice de manera distribuida.	El operador de servicios debe implementar la gestión de los datos biométricos, la gestión de la información para realizar el proceso de autenticación de ciudadano, la base de datos con información mínima del ciudadano y la gestión central de documentos en bases de datos independientes. Cada operador debe implementar la estrategia adecuada que permita evidenciar que esta gestión se realiza de manera distribuida y la relación entre las bases de datos, no cuenta con un parámetro que permita relacionar de manera lógica la información entre ellas, de tal manera que al tomar una muestra de la información almacenada en cada una de las diferentes bases de datos no sea posible relacionar los registros.
<b>AGREGAR</b> Esta estrategia busca que los datos de carácter personal que se procesen tenga el más alto nivel de agregación y con el menor detalle posible.	En los servicios se recomienda que la gestión de evidencias de acceso que están resguardados por parte del operador, sea almacenada en dos (2) niveles de acceso e interpretación:  <b>Nivel 1:</b> Resultado a partir de la información que requiere el MINTIC para el análisis del comportamiento del uso de los servicios y/o cualquier otra estadística que sea requerida y que su finalidad sea publicarla, esta evidencia deberá ser generada y almacenada en un repositorio que permita obtener la información requerida con un nivel de agregación alto, y que no permita a partir de su análisis lograr identificar el comportamiento de un ciudadano en particular.

ESTRATEGIA PRIVACIDAD POR DISEÑO	REQUERIMIENTO MÍNIMO
	<b>Nivel 2:</b> La información requerida a nivel probatorio del uso del servicio por parte del ciudadano y que permita identificar a un nivel detallado los accesos de autenticación, el intercambio de información o la gestión de la carpeta por parte del ciudadano, sea solo accesible por parte del ciudadano y del administrador.
<b>INFORMAR</b> Esta estrategia busca mantener informados a los ciudadanos sobre el uso de sus datos de carácter personal en cualquier proceso de la plataforma.	<ul style="list-style-type: none"> <li>▪ Implementar con los diferentes sistemas que requieran de la información de autenticación del ciudadano o con los cuales se han compartido documentos el protocolo P3P (Plataforma de Preferencias de Privacidad) como mecanismo para declarar las condiciones de uso de la información utilizada de los ciudadanos.</li> <li>▪ Mantener los registros de la trazabilidad de autenticaciones e información adicional a la mínima del ciudadano que se compartió con cualquier sistema de información.</li> <li>▪ Se recomienda mantener acceso a la trazabilidad de accesos y vigencias de la información compartida por el ciudadano, la trazabilidad debe permitir al ciudadano tener acceso de manera detallada de los accesos a los documentos compartidos y la vigencia otorgada por el ciudadano para dicho acceso.</li> <li>▪ Mantener los registros de la trazabilidad de accesos a los documentos por parte del ciudadano y con los cuales se estén compartiendo los documentos y permitir desde la interfaz del ciudadano informar cuales documentos se han compartido, identificando el dato, fecha y sistema de información.</li> <li>▪ Envío de una notificación a los propietarios de la identidad de las amenazas a los sistemas y capacidades de los proveedores de servicio de identidad.</li> </ul>
<b>CONTROLAR</b> Esta estrategia busca que los ciudadanos tengan el control sobre el tratamiento de sus datos y acciones.	<p>En los servicios, se recomienda el desarrollo de componentes que permitan a los ciudadanos realizar las siguientes acciones a fin de garantizar el control de su información:</p> <ul style="list-style-type: none"> <li>▪ Interfaz donde el ciudadano pueda acceder/suprimir/modificar/supervisar/controlar sus preferencias para compartir información a la mínima requerida, incluido el compartir a terceros privados de acuerdo con la normatividad y políticas aplicables.</li> <li>▪ Capacidad de que terceros autorizados (padres, fuerzas de seguridad autorizadas, órganos de imposición legislativa y otros terceros autorizados) puedan acceder/supervisar su información de identidad.</li> <li>▪ Un mecanismo para divulgar al titular cuando el punto anterior ocurra.</li> <li>▪ La posibilidad de la portabilidad dentro de los servicios de información de identificación personal, de acuerdo con la normatividad y las políticas aplicables.</li> <li>▪ Permitir revocar en cualquier momento el acceso concedido a su información adicional y mensajes de datos.</li> <li>▪ Permitir el asignar una vigencia en tiempo de los permisos de acceso a su información adicional de autenticación y a los documentos.</li> <li>▪ El operador deberá implementar técnicas de borrado seguro de la información gestionada por él, cuando el ciudadano decida eliminar sus mensajes de datos por decisión propia o portabilidad a otro operador.</li> <li>▪ Implementar el borrado seguro de los mensajes de datos cuando el ciudadano o el marco regulador así lo exijan, esta información deba ser eliminada de los repositorios del operador.</li> </ul>
<b>CUMPLIR</b> Esta estrategia busca verificar el cumplimiento de las medidas de privacidad propuestas.	<p>Los operadores de servicios deben implementar herramientas de monitoreo de acceso a las bases de datos y a los documentos del ciudadano, estas herramientas deberán permitir auditar a niveles detallados los accesos realizados.</p> <p>La gestión de identidad requiere auditoría, para verificar el cumplimiento de políticas de privacidad y la protección de información de identidad personal, teniendo en cuenta: auditoría respecto a la normatividad, a controles acerca de la información de identificación personal, avisos de privacidad, exactitud de sello de tiempo y trazabilidad.</p>
<b>DEMOSTRAR</b> Esta estrategia busca ser capaz de demostrar el cumplimiento de la política de privacidad por parte del operador.	Respecto a los servicios, se recomienda a los operadores implementar políticas de gestión de incidentes, en donde se reporte al administrador el detalle de los mecanismos implementados, además cuando un incidente se materialice se deberá poner en conocimiento del administrador un informe que detalle el nivel de compromiso de la información gestionada por el operador y que ponga en riesgo la privacidad del ciudadano.

## 9.4 Modelo Financiero

El modelo financiero sobre el cual se soportan los Servicios Digitales Básicos busca definir los parámetros necesarios para establecer la viabilidad financiera del proyecto en un esquema de varios operadores en donde se cumplan los estándares y lineamientos definidos por el modelo de negocio. El modelo financiero debe garantizar un modelo sostenible para cada uno de los operadores en donde se les reconozca una rentabilidad justa por la inversión y a su vez minimizar los costos y riesgos de operación de las diferentes entidades y empresas vinculadas al proyecto.







## Premisas básicas

El modelo financiero se ajusta de acuerdo a las siguientes premisas básicas:

- i. Gratuidad para los ciudadanos de los servicios básicos.
- ii. El modelo financiero debe garantizar la caja suficiente a partir de los ingresos para lograr la sostenibilidad y prestación de los Servicios Digitales a lo largo del tiempo.
- iii. Pagos por transacción por parte de las entidades públicas y privados quienes estarán obligados a implementar sobre la plataforma, de manera gradual, su oferta de servicios y trámites en medios digitales. Las transacciones dentro de un trámite o servicio por los cuales pagará cada entidad pública o privado están relacionadas con:
  - Envío de documentos del trámite a la Carpeta del Ciudadano
  - Validación de la identidad de los usuarios de un trámite o servicio electrónico
  - Consumo de servicios de intercambio de información – Interoperabilidad con otros sistemas de información.
  - Habilitación de servicios de información.

Las transacciones tendrán tarifas según su clasificación, así:

Tabla 10. Clasificación de Transacciones

COMUNES	INTENSAS	SOFISTICADAS
Ocurrencia:  Uso de infraestructura: 	Ocurrencia:  Uso de infraestructura: 	Ocurrencia:  Uso de infraestructura: 
<ul style="list-style-type: none"><li>• Envío a carpeta ciudadana de documentos menores de 500 KB</li><li>• Autenticación electrónica nivel 2</li><li>• Consumo de servicios de información menores a 500 KB</li></ul>	<ul style="list-style-type: none"><li>• Envío a carpeta ciudadana de documentos entre 500 KB y 2 MB</li><li>• Autenticación electrónica nivel 4</li><li>• Consumo de servicios de información entre 500 KB y 1 MB</li></ul>	<ul style="list-style-type: none"><li>• Envío a carpeta ciudadana de documentos mayores a 2 MB</li><li>• Consumo de servicios de información mayores a 1 MB</li></ul>

- iv. Los usuarios podrán voluntariamente suscribir servicios de valor agregado o adicionales de almacenamiento y autenticación ofrecidos por el operador bajo tarifas previamente estipuladas regidas por contratos de servicio.
  - Ciudadanos: espacio adicional al GB incluido.
  - Empresas: envíos a clientes y empleados y espacio de almacenamiento adicional.
- v. Las entidades públicas podrán voluntariamente establecer contratos o suscribir servicios agregados de los operadores para el diseño, desarrollo e implementación de trámites y servicios que serán objeto de intercambio de información en la plataforma de servicios digitales básicos con fundamento en el marco de interoperabilidad y el marco de Arquitectura Empresarial establecidos desde el Ministerio de Tecnologías de la Información y Comunicaciones.
- vi. Los ingresos dependen de la tarifa estipulada por el operador y esta debe ir de acuerdo a los lineamientos de sostenibilidad del modelo financiero en donde los mismos cumplen con la estructura de costos, gastos y requerimientos de capital. El modelo debe ser sostenible y buscar una rentabilidad justa a la inversión realizada de acuerdo a los parámetros. Por ello, las tarifas pueden ser revisadas periódicamente y ajustadas de acuerdo con los objetivos de sostenibilidad del modelo.
- vii. Los operadores deben garantizar el funcionamiento y sostenibilidad del proyecto por medio de inversión (Capital de trabajo, Capex y Opex) de los recursos necesarios para la prestación de los Servicios de Información Digital.
- viii. El modelo financiero busca mitigar los posibles riesgos financieros (Riesgo de mercado, riesgo de liquidez, riesgo de crédito y riesgo de operación) garantizando la sostenibilidad del negocio en el tiempo.

## 9.5 Modelo de Gobernabilidad

El modelo de gobernabilidad determina los arreglos institucionales, normativos y regulatorios que rigen las condiciones de operación y relaciones entre los diferentes actores, con el fin de garantizar la prestación adecuada de los servicios digitales. Dicha gobernabilidad debe darse durante todo el ciclo de prestación del servicio y por tanto contiene las etapas de habilitación y contratación, operación, crecimiento, masificación, madurez y cierre.

Así mismo el modelo de gobernabilidad, identificará las autoridades encargadas de la inspección vigilancia y control de los servicios y de la resolución de conflictos entre operadores. Algunos aspectos se encuentran en la normatividad vigente y otros deberán ser proferidos por el MINTIC mediante un Decreto reglamentario del artículo 45 de la Ley 1753 de 2015, por la cual se adopta el Plan Nacional de Desarrollo 2014-2018.

**Ilustración No. 5. Modelo de Gobernabilidad**

ACTOR	CRITERIO	HABILITACION Y CONTRATACION	OPERACIÓN	CRECIMIENTO, MASIFICACIÓN Y MADUREZ	CIERRE
OPERADOR	Registro y Prestación de servicios	MINTIC			
	Requisitos Técnicos y Financieros	MINTIC			
	Vigilancia y Control		MINTIC, SIC, RNEC, AGN, Colombia Compra Eficiente		
	Tratamiento de Datos Personales	SIC y OPERADORES			
	Transferencia o Trasnmisión de Datos al Exterior		SIC y OPERADORES		
	Masificación y Apropiación	MINTIC y OPERADORES			
MINTIC	Reglamentación	MINTIC			
	Masificación y Apropiación	MINTIC y OPERADORES			
CIUDADANO	Contraprestación	No existe			
	Obligatoriedad	Voluntaria			
	Términos y condiciones	Decreto	SIC		
	Cambio de operador	N/A	Operador		
ENTIDAD	Obligatoriedad	Están obligadas según el artículo 45 de la Ley del PND			
	Compensación	MINTIC: Definir el sistema de compensación entre operadores			
	Contratación	Acuerdo Marco de Precios o Mecanismo que sera aprobado para el Modelo			
	Gradualidad	MINTIC: Instrumento Normativo que formalice el modelo de gradualidad			

A continuación se detalla el modelo de gobernabilidad, señalando los actores y principales instrumentos usados para la prestación de los Servicios Digitales Básicos.

**Tabla No. 11. Detalle del Modelo de Gobernabilidad**

CRITERIO	Habilitación y contratación	Operación	Crecimiento, masificación, madurez	Cierre
<b>OPERADORES</b>				
<b>Registro y Prestación de servicios</b>	El Ministerio TIC definirá un marco regulatorio y operativo que permita realizar la habilitación (operación primaria) de los operadores y la contratación por parte de las	<b>Operación de los servicios digitales básicos:</b> Las condiciones de operación y deberes de los operadores se realizará conforme a lo descrito en los	<b>Informes de gestión</b> El Ministerio TIC conforme a la normativa que establezca el modelo se encargará de solicitar al operador informes de	El Ministerio TIC conforme a la normativa que establezca el modelo se encargará de adelantar el procedimiento de revocatoria o cancelación de la habilitación para prestar los servicios por:

CRITERIO	Habilitación y contratación	Operación	Crecimiento, masificación, madurez	Cierre
	<p>entidades (operación secundaria)</p> <p><b>Normatividad:</b> Los servicios digitales están sujetos a las normas que se relacionan a continuación y se detallan en la sección 7.6.1 marco normativo.</p> <ul style="list-style-type: none"> <li>- Ley 527 de 1999</li> <li>- Ley 594 de 2000</li> <li>- Ley 1341 de 2009</li> <li>- Ley 1437 de 2011</li> <li>- Decreto Ley 019 de 2012</li> <li>- Ley 1753 de 2015</li> <li>- Decreto 1074 de 2015</li> <li>- Decreto 1078 de 2015</li> <li>- Decreto 1080 de 2015</li> <li>- Resolución 5633 de 2016</li> </ul> <p><b>Instrumento jurídico de habilitación:</b> Los interesados en constituirse como operadores de Servicios Digitales Básicos deberán presentar una solicitud formal de registro y habilitación ante el Ministerio Tecnologías de la Información y las Comunicaciones.</p> <p>Los operadores serán habilitados a través de un acto administrativo de carácter particular, que definirá la situación jurídica, particular y concreta para el habilitado.</p> <p><b>Contratación de servicios por parte de las Entidades públicas:</b> La oferta de servicios podrá hacerse mediante acuerdos marco<sup>55</sup> de precios que identifiquen los criterios técnicos bajo los cuales debe suministrarse el servicio y que aplican directamente a los posibles prestadores de servicios. Colombia Compra Eficiente apoyará la construcción y formalización de los acuerdos marco de precios para la adquisición de servicios por parte de las administraciones.</p>	<p>numerales precedentes del documento.</p>	<p>gestión que deberán contener como mínimo:</p> <ol style="list-style-type: none"> <li>1. Informe de la estrategia de masificación de servicios.</li> <li>2. Informe cualitativo y cuantitativo de la forma en la que se están cumpliendo con los requisitos técnicos y financieros para operar.</li> <li>3. Informe sobre indicadores de calidad de servicio.</li> </ol>	<ol style="list-style-type: none"> <li>1. Por solicitud expresa el operador.</li> <li>2. Por orden del Ministerio TIC una vez se haya surtido el procedimiento administrativo sancionatorio.</li> <li>3. En caso de liquidación de la persona jurídica.</li> <li>4. Por incumplimiento de los deberes y responsabilidades a cargo del operador.</li> </ol>

<sup>55</sup> El Acuerdo Marco de Precio (AMP), creado en la Ley 1150 de 2007 y desarrollado especialmente mediante el decreto 1510 del año 2013, establece las condiciones bajo las cuales los proveedores deben prestar servicios o entregar productos, y la forma cómo las entidades públicas deben contratarlos. El AMP es un contrato entre un representante de los compradores, la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente (CCE), y uno o varios proveedores, que contiene la identificación del bien o servicio, el precio máximo (techo) de adquisición, las garantías mínimas y el plazo mínimo de entrega, así como las condiciones a través de las cuales un comprador puede vincularse al acuerdo.

CRITERIO	Habilitación y contratación	Operación	Crecimiento, masificación, madurez	Cierre
<b>Requisitos técnicos y financieros</b>	El Ministerio TIC conforme a la normativa que establezca el modelo verificará que quien quiera ser operador cumpla con los requisitos jurídicos, técnicos y financieros para poder operar.	Su cumplimiento deberá mantenerse a lo largo de toda la ejecución para garantizar los estándares mínimos de seguridad, privacidad, acceso y neutralidad tecnológica, y continuidad en el servicio.		El incumplimiento de alguno de los requisitos técnicos, jurídicos y financieros dará lugar a la cancelación de la habilitación para operar.
<b>Vigilancia y Control</b>	-	<p>Estarán encargadas de la vigilancia y control del modelo dentro de su ámbito de competencia las siguientes entidades que integran al Ente Regulador:</p> <p><b>Superintendencia de Industria y Comercio (SIC):</b> A través de la Delegatura para la Protección de Datos Personales tiene a su cargo la vigilancia de los operadores que realicen tratamiento de los datos personales, de conformidad y en los términos de la ley 1581 de 2012. Considerando lo anterior, corresponde a la SIC las funciones de vigilancia y control de todos los operadores de servicios digitales básicos en los términos del artículo 21 de la ley 1581 de 2012 con especial referencia a los siguientes aspectos:</p> <ul style="list-style-type: none"> <li>La verificación del debido tratamiento de los datos personales de los usuarios por parte de los operadores de servicios digitales básicos bajo los lineamientos técnicos, legales y operativos que se determinen en el marco reglamentario que se expida a través del MINTIC.</li> <li>Impartir instrucciones sobre las medidas y procedimientos pertinentes que considere necesarios para garantizar el debido tratamiento de datos personales por parte de los operadores de servicios digitales (responsables del tratamiento) y los eventuales encargados del tratamiento involucrados en la puesta en marcha y funcionamiento del modelo.</li> </ul> <p><b>Registraduría Nacional del Estado Civil:</b> De conformidad con el Decreto 19 de 2012 y la Resolución 5633 de 2016 de la Registraduría Nacional del Estado Civil, esta entidad autorizará y pondrá a disposición de las entidades interesadas, la consulta de las bases de datos que produce y administra para el cumplimiento de las obligaciones constitucionales y legales (entidades públicas y particulares con funciones públicas) o con el objeto social (particulares autorizados por la ley), según el caso. Dicha disposición estará sujeta al ejercicio de la función a su cargo, a la modalidad de prestación del servicio y a la observancia de las limitaciones técnicas de la Registraduría Nacional del Estado Civil, teniendo en cuenta los términos, procedimientos y condiciones establecidas en dicha resolución, garantizando el cumplimiento de las limitaciones de acceso y uso referidas a la protección de datos personales, al derecho de habeas data, privacidad, reserva estadística, asuntos de defensa y seguridad nacional y en general toda aquella información que tenga el carácter de reserva.</p> <p><b>Ministerio Público:</b> Está encargado de vigilar que se cumpla la Ley 1712 de 2014 (Ley de Transparencia) que tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información. De igual forma, se deberá salvaguardar el interés general y vigilar que se cumplan los fines del Estado. De esta manera, la Procuraduría ejercerá una triple función: Función preventiva, de interventoría y disciplinaria.</p> <p><b>Archivo General de la Nación:</b> se encargará de vigilar los protocolos de gestión documental tanto para las entidades públicas como para las privadas que se encuentren vigiladas por la SIC de conformidad con la Resolución 8934 de 2014. En desarrollo de lo anterior, corresponde al Archivo expedir las normas relacionadas con la preservación de documentos en ambientes o medios digitales, como es el caso de la información y documentos públicos que pudieran ser incorporados en formato digital a la Carpeta Ciudadana.</p> <p><b>MINTIC:</b> Le corresponde el desarrollo del marco reglamentario y, como autoridad sectorial, las funciones que la ley no haya previsto en cabeza de otra entidad, en especial las relacionadas con la verificación de requisitos y registro de quienes se habiliten como operadores de la plataforma de servicios digitales básicos. Las tareas a cargo de esta entidad son:</p> <ul style="list-style-type: none"> <li>Diseñar el marco reglamentario y la expedición del correspondiente decreto que fije el marco normativo para el desarrollo del modelo.</li> <li>Establecer un proceso de registro de operadores, previa verificación de requisitos habilitantes.</li> <li>Establecer un seguimiento periódico sobre el cumplimiento de dichos requisitos.</li> <li>Hacer seguimiento y supervisión a la operación del modelo a través de indicadores y el análisis periódico.</li> <li>Promover el uso y la apropiación de la iniciativa a través de una estrategia de sensibilización de manera coordinada con cada uno de los operadores.</li> </ul>		
<b>Tratamiento de Datos personales</b>	Los operadores habilitados deberán dar cumplimiento a la Ley 1581 de 2012 y sus decretos reglamentarios, la Guía de la SIC en materia de responsabilidad demostrada y las buenas prácticas	Los operadores habilitados deberán dar cumplimiento a la Ley 1581 de 2012, la Guía de la SIC en materia de responsabilidad demostrada y las buenas prácticas internacionales.		Para poder finalizar su operación el operador deberá demostrar que ha cumplido con todos los requerimientos que tenga en trámite con la SIC

CRITERIO	Habilitación y contratación	Operación	Crecimiento, masificación, madurez	Cierre
	internacionales, incluida la privacidad por diseño.			
Transferencia o transmisión de datos al exterior	-	Deberá darse cumplimiento a lo establecido en el artículo 26 de la Ley 1581 de 2012 para lo cual si el operador busca transferir datos al exterior deberá contar con la autorización expresa del usuario. Sin embargo, dentro de los requisitos de entrada deberá consagrarse el que el operador deberá garantizar que los países a los que transfiera datos deberán contar con los estándares adecuados de protección de datos de conformidad con los estándares que la SIC definirá. En el caso eventual de la transmisiones internacionales de datos se deberá observar los establecido en el artículo 25 del decreto 1377 de 2013	La SIC se encargará de vigilar que la transferencia se haga en los términos de la Ley.	Para poder finalizar su operación el operador deberá demostrar que ha cumplido con todos los requerimientos que tenga en trámite con la SIC
Masificación y Apropiación	En lo referente a la estrategia de masificación y sensibilización para promover el uso y la apropiación de la iniciativa se propone que sea diseñada e implementada por MINTIC y de manera coordinada con cada uno de los operadores.			
MINTIC				
Reglamentación	<b>Decreto:</b> El MINTIC debe expedir un Decreto que reglamente el artículo 45 del PND 2014-2018, y el capítulo IV del Título II de la primera parte de la Ley 1437 de 2011, con el fin de establecer los estándares y protocolos que deben cumplir las autoridades para facilitar la utilización de servicios electrónicos y digitales en el procedimiento administrativo, permitiendo que estos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas.  <b>Resolución de carácter Particular</b> El MINTIC deberá proferir actos administrativos de carácter particular que habiliten a los operadores que cumplan con las condiciones técnicas, financieras y jurídicas para operar.	El operador podrá prestar sus servicios una vez haya sido autorizado mediante acto administrativo de carácter particular proferido por el Ministerio TIC.  La oferta de servicios podrá hacerse mediante Acuerdos Marco de Precios que incluyan la identificación del servicio, el precio máximo de adquisición, las garantías mínimas y el plazo implementación, así como las condiciones a través de las cuales las entidades pueden vincularse al acuerdo.  Los acuerdos marco de precios establecerán el mecanismo de compensación entre prestadores así como los Acuerdos de Niveles de Servicio.		En caso que el operador deje de prestar sus servicios, el acto administrativo perderá vigencia.
Masificación y apropiación	En lo referente a la estrategia de masificación y sensibilización para promover el uso y la apropiación de la iniciativa se propone que sea diseñada e implementada por MINTIC y de manera coordinada con los operadores. La estrategia de masificación debe considerar incentivos, garantías de igualdad en el acceso y condiciones de servicio universal.			
PERSONAS				
Contraprestación	No habrá ninguna por parte del ciudadano	No habrá ninguna por parte del ciudadano para el caso de los servicios básicos. Los operadores podrán recibir contraprestaciones por la oferta de servicios adicionales o de valor agregado, por el almacenamiento de información y/o por facilitar la interacción con el sector privado		
Obligatoriedad	El uso de los servicios digitales es facultativo, ya que se presenta como un desarrollo del derecho de acceso a la administración por medios electrónicos, donde el usuario tiene la potestad de ejercer dicho derecho, conforme a lo establecido en el Art 45 Parágrafo 1 del PND y Artículos 53 y 54 del CPACA.			

CRITERIO	Habilitación y contratación	Operación	Crecimiento, masificación, madurez	Cierre
Términos y condiciones	Los derechos de los usuarios estarán definidos en el Decreto reglamentario	Se verificará su cumplimiento por la entidad competente		Su incumplimiento puede ser considerado como causal para la cancelación del registro.
Cambio de operador	Se garantizará el derecho de portabilidad a los usuarios.			
ENTIDADES PÚBLICAS				
Obligatoriedad	De conformidad con el párrafo 2 del artículo 45 de la Ley 1753 de 2015, y atendiendo a los postulados del Artículo 53 y siguientes de la Ley 1437 de 2011, las autoridades deberán garantizar a sus usuarios el acceso a la administración por medios electrónicos (digitales), para lo cual deberán asegurar la igualdad en el acceso y la puesta en disposición de mecanismos suficientes y adecuados para acceder a la administración por medios electrónicos (digitales).			
Gradualidad	El MINTIC establecerá a través del instrumento normativo que formalice el modelo la gradualidad en la contratación de los servicios digitales básicos.			
Tipo de mecanismos de Autenticación Electrónica	Según el nivel de riesgo del trámite o servicio se determinará el tipo de firma a utilizar, el registro o identificación será la regla general, la firma solo se exigirá cuando la norma sustancial la exija. Esta deberá garantizar la autenticidad, integridad, disponibilidad, confiabilidad y no repudio.			
Contratación	Esto será definido por el acuerdo marco de precios o mecanismo de contratación que sea aprobado.			
Compensación	El sistema de compensación entre operadores será definido por el Ministerio TIC y se incluirá en las condiciones de los acuerdos de precio. En todo caso se debe asegurar la continuidad en el servicio, se debe privilegiar los derechos de los usuarios y la prevalencia del interés general sobre el particular.			

### 9.5.1 Marco Normativo

Los servicios digitales básicos están sujetos a los siguientes elementos normativos:

- *La Ley 527 de 1999*, que en sus artículos 5, 6, 7, 9, 10, 11 y 12 establece el reconocimiento jurídico a los mensajes de datos, en las mismas condiciones que se ha otorgado para los soportes que se encuentren en medios físicos.
- *La Ley 594 de 2000*, que en su artículo 19 establece que las entidades públicas podrán contemplar el uso de nuevas tecnologías y soportes para la gestión de documentos y que el Archivo General de la Nación dará pautas y normas técnicas generales sobre conservación de archivos, incluyendo lo relativo a los documentos en nuevos soportes.
- *La Ley 962 de 2005* por la cual se dictan disposiciones sobre la racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos, y establece en su artículo 6º que para atender los trámites y procedimientos de su competencia, los organismos y entidades de la Administración Pública deberán ponerlos en conocimiento de los ciudadanos en la forma prevista en las disposiciones vigentes, o emplear, adicionalmente, cualquier medio tecnológico o documento electrónico de que dispongan, a fin de hacer efectivos los principios de igualdad, economía, celeridad, imparcialidad, publicidad, moralidad y eficacia en la función administrativa.
- *La Ley 1341 de 2009*, que establece dentro de las funciones del Ministerio de las Tecnologías de la Información y las Comunicaciones, el definir, adoptar y promover las políticas, planes y programas tendientes a incrementar y facilitar el acceso de todos los habitantes del territorio nacional, a las Tecnologías de la Información y las Comunicaciones y a sus beneficios. Así mismo, establece que de conformidad con la sociedad de la información y el conocimiento se debe impulsar el uso de medios electrónicos como un objetivo fundamental dentro de la relación entre la administración pública y el ciudadano y que el Ministerio de las Tecnologías de la Información y las Comunicaciones, debe promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación.
- *La Ley 1437 de 2011*; por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, en su artículo 53 establece que los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.
- *El artículo 54 de la Ley 1437 de 2011* que establece que toda persona tiene el derecho de actuar ante las autoridades utilizando medios electrónicos, caso en el cual deberá registrar su dirección de correo electrónico



en la base de datos dispuesta para tal fin. Sí así lo hace, las autoridades continuarán la actuación por este medio, a menos que el interesado solicite recibir notificaciones o comunicaciones por otro medio diferente.

- La *ley 1437 de 2011* que en su artículo 64 faculta al Gobierno Nacional para establecer los estándares y protocolos que deben cumplir las autoridades para incorporar de forma gradual la aplicación de los medios electrónicos en los procedimientos administrativos.
- El *artículo 230 de la Ley 1450 de 2011*, por la cual se expide el Plan Nacional de Desarrollo, 2010-2014, señalando que todas las entidades de la Administración Pública deberán adelantar las acciones señaladas en la Estrategia de Gobierno en línea, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través del cumplimiento de los criterios que éste establezca.
- El *Decreto Ley 019 de 2012*, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública, establece en el artículo 4 que las autoridades deben incentivar el uso de las tecnologías de la información y las comunicaciones y en particular al uso de medios electrónicos como elemento necesario en la optimización de los trámites ante la Administración Pública. En su artículo 9 que cuando se esté adelantando un trámite ante la administración, se prohíbe exigir actos administrativos, constancias, certificaciones o documentos que ya reposen en la entidad ante la cual se está tramitando la respectiva actuación.
- La *Ley 1564 de 2012* que en su artículo 103 permite el uso de las Tecnologías de la Información y las Comunicaciones (TIC) en todas las actuaciones de la gestión y trámites de los procesos judiciales, con el fin de facilitar el acceso a la justicia. Prevé aspectos sobre mensajes de datos.
- La *Ley 1581 de 2012*, por la cual se dictan disposiciones generales para la ley de protección de datos personales, desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en las bases de datos o archivos.
- El *Decreto 1074 de 2015* que en los Capítulos 25 y 26 reglamenta la Ley 1581 de 2012 definiendo las condiciones para hacer la recolección de los datos personales, el ejercicio de los derechos de acceso, actualización, rectificación y supresión, las condiciones para la transferencia y transmisión internacional de datos personales y la información mínima del Registro Nacional de Bases de Datos. Y el capítulo 47 por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- El *Decreto 1080 de 2015* que reglamenta a las leyes 594 de 2000 y 1437 de 2011 y dicta otras disposiciones en materia de Gestión Documental para todas las entidades del Estado. Dicho decreto establece los requisitos para la integridad, autenticidad, inalterabilidad, fiabilidad, disponibilidad, preservación y conservación de los Documentos Electrónicos de Archivo, así como habilita el uso de las firmas electrónicas o digitales, de conformidad con las normas correspondientes para garantizar la autenticidad, integridad y confidencialidad de la información.
- El *Decreto 1078 de 2015* que consagra la estrategia Gobierno en Línea (gobierno electrónico) desarrollada por el Ministerio de Tecnologías de la información y las Comunicaciones cuyo objetivo consiste en construir un Estado más eficiente, más transparente y más participativo a través del uso de las TIC (Tecnologías de la Información y las Comunicaciones). En ese sentido, las entidades estatales deberán incluir la estrategia de Gobierno en Línea de forma transversal en sus planes estratégicos sectoriales e institucionales, donde son de especial relevancia la gestión documental electrónica y el uso de herramientas para optimizar los trámites adelantados por medios electrónicos.
- El *artículo 45 de la Ley 1753 de 2015* que establece que bajo la plena observancia del derecho fundamental de hábeas data, el Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC), en coordinación con las entidades responsables de cada uno de los trámites y servicios, definirá y expedirá los estándares, modelos, lineamientos y normas técnicas para la incorporación de las Tecnologías de la Información y las Comunicaciones (TIC), que contribuyan a la mejora de los trámites y servicios que el Estado ofrece al ciudadano, los cuales deberán ser adoptados por las entidades estatales y aplicarán, entre otros, para los siguientes casos: Autenticación Electrónica, Integración de los sistemas de información de trámites y servicios de las entidades estatales con el Portal del Estado colombiano, Implementación de la estrategia de Gobierno en Línea, marco de referencia de arquitectura empresarial para la gestión de las tecnologías de información en el Estado.
- El *parágrafo 1 del artículo 45 de la Ley 1753 de 2015* establece que estos trámites y servicios podrán ser ofrecidos por el sector privado.
- El *parágrafo 2 literal a) del artículo 45 de la Ley 1753 de 2015* establece que se podrá ofrecer a todo ciudadano el acceso a una Carpeta Ciudadana electrónica que le permitirá contar con un repositorio de información electrónica para almacenar y compartir documentos públicos o privados, recibir comunicados de las entidades públicas, y facilitar las actividades necesarias para interactuar con el Estado. En esta carpeta podrá estar almacenada la historia clínica electrónica. El Min TIC definirá el modelo de operación y los estándares técnicos

y de seguridad de la Carpeta Ciudadana Electrónica. Las entidades del Estado podrán utilizar la Carpeta Ciudadana Electrónica para realizar notificaciones oficiales. Todas las actuaciones que se adelanten a través de las herramientas de esta carpeta tendrán plena validez y fuerza probatoria.

BORRADOR

## Referencias

Cavoukian, A., 2016. "Privacy & Big Data Institute", visto en <http://www.ryerson.ca/pbdi/about/people/cavoukian.html>

Centro Cibernético Policial 2015, Ciberincidentes, Policía Nacional, Gobierno de Colombia, visto el 29 de Enero de 2016, <http://www.ccp.gov.co/ciberincidentes/tiempo-real>

COLPENSIONES Administradora Colombiana de Pensiones 2015, "Notificaciones por aviso. Conozca aquí el listado de ciudadanos notificados por aviso", visto el 5 de Febrero de 2016, [https://www.colpensiones.gov.co/publicaciones/es-CO/841/Notificaciones\\_por\\_aviso](https://www.colpensiones.gov.co/publicaciones/es-CO/841/Notificaciones_por_aviso)

Corporación Colombia Digital. 2016. "Informe Final del Modelo de Interoperabilidad Autosostenible – en el marco del Contrato Interadministrativo N° 000376 de 2015 para los Servicios de acompañamiento especializado al Ministerio TIC en la implementación de las iniciativas: Fortalecimiento de la Gestión de TI en el estado y la Estrategia de Gobierno en línea"

Departamento Administrativo de la Función Pública DAFP, 2016, Sistema Único de Información de Trámites SUIT, 2016, "Trámites y otros procedimientos administrativos disponibles al usuario en el Sistema único de información de trámites – SUIT" 1 de Agosto, visto el 12 de agosto de 2016, [http://www.suit.gov.co/documents/10179/460149/2016-08-01-Total\\_Registros.pdf/d3dbfa77-e727-4546-9ff7-30304b2a162a](http://www.suit.gov.co/documents/10179/460149/2016-08-01-Total_Registros.pdf/d3dbfa77-e727-4546-9ff7-30304b2a162a)

Departamento Administrativo de la Función Pública DAFP, 2016, Sistema Único de Información de Trámites SUIT, 2016, "Trámites y otros procedimientos administrativos en el estado colombiano" 1 de Agosto, visto el 12 de agosto de 2016, [http://www.suit.gov.co/documents/10179/460149/2016-08-01-Total\\_tramites\\_medios.pdf/bd39c38f-54f4-4d02-a83b-23c79b022fe6](http://www.suit.gov.co/documents/10179/460149/2016-08-01-Total_tramites_medios.pdf/bd39c38f-54f4-4d02-a83b-23c79b022fe6)

Departamento Nacional de Planeación DNP 2015, *Bases para el Plan Nacional de Desarrollo 2014-2018*, Gobierno de Colombia, Bogotá, visto el 29 de Septiembre de 2015, <https://colaboracion.dnp.gov.co/cdt/prensa/bases%20plan%20nacional%20de%20desarrollo%202014-2018.pdf>

Departamento Nacional de Planeación. DNP-SPI "Seguimiento a proyectos de Inversión" Visto el 18 de Agosto de 2016, <http://estrategiaticolombia.co/estadisticas/stats.php?&pres=content&jer=4&cod=&id=134#TTC>

Departamento Nacional de Planeación DNP 2016, *Política Nacional de Seguridad Digital – CONPES 3854 de 2016*, Gobierno de Colombia, Bogotá, visto el 19 de Agosto de 2016, <https://colaboracion.dnp.gov.co/CDT/Conpes/Economicos/3854.pdf>

El Espectador, 2012, "Denuncian corrupción en sector educativo por \$132.000 millones", visto el 22 de Febrero de 2016, <http://www.elespectador.com/noticias/educacion/denuncian-corrupcion-sector-educativo-132000-millones-articulo-327449>

El Tiempo, 2015, "Ya son 55 los capturados señalados de estafar y suplantar a víctimas", 14 de Octubre, visto 22 de Febrero de 2016, <http://www.eltiempo.com/politica/justicia/red-estafaba-y-suplataba-a-victimas-del-conflicto/16402746>

FEA Federal Enterprise Architecture, "Security and Privacy Profile", 2006). Visto en: [http://bettergovernment.jp/resources/Security\\_and\\_Privacy\\_Profile\\_v2.pdf](http://bettergovernment.jp/resources/Security_and_Privacy_Profile_v2.pdf)

Hoepman, J.H, 2012, "Privacy Design Strategies", Institute for Computing and Information Sciences, Radboud University, Nijmegen, The Netherlands, pp. 1-9, visto el 6 de Noviembre de 2015, <https://www.cs.ru.nl/~jhh/publications/pdp.pdf>

La República. 2015, "Colpensiones frena más de \$15.000 millones por fraudes", 26 de Agosto, visto el 22 de Febrero de 2016, [http://www.larepublica.co/colpensiones-frena-m%C3%A1s-de-15000-millones-por-fraudes\\_293141](http://www.larepublica.co/colpensiones-frena-m%C3%A1s-de-15000-millones-por-fraudes_293141)

Medina, E. 2016, “En 2015, cibercrimen generó pérdidas por US\$ 600 millones en Colombia”, El Tiempo, 28 de Enero 2016, visto el 22 de Febrero de 2016, <http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604>

MEN, Ministerio de Educación Nacional 2014, “Notificaciones por aviso”, visto el 5 de Febrero de 2016, <http://www.mineducacion.gov.co/1759/w3-propertyvalue-56746.html>

MINTIC, Ministerio de Tecnologías de la Información y las Comunicaciones 2014, “Conocimiento y uso – Ciudadanos”, visto el 5 de Febrero de 2016, <http://estrategia.gobiernoonlinea.gov.co/623/w3-propertyvalue-7654.html>

MINTIC, Ministerio de Tecnologías de la Información y las Comunicaciones 2015. Interoperabilidad. <http://www.MINTIC.gov.co/arquitecturati/630/w3-propertyvalue-8117.html>

MINTIC Ministerio de Tecnologías de la Información y las Comunicaciones 2015, “Estudio de cultura de uso de TIC en los colombianos para relacionarse con el Estado”

MINTIC Ministerio de Tecnologías de la Información y las Comunicaciones 2015, “Notificaciones por aviso cobro coactivo”, visto el 5 de Febrero de 2016, <http://webapp.MINTIC.gov.co/607/w3-propertyvalue-8026.html>

MINTIC, Ministerio de Tecnologías de la Información y las Comunicaciones 2016, “Guía para la Gestión y Clasificación de Activos de Información”, visto el 19 de Julio de 2016, [file:///C:/Users/rbecerraf/Downloads/articles-5482\\_Guia8\\_Gestion\\_Activos.pdf](file:///C:/Users/rbecerraf/Downloads/articles-5482_Guia8_Gestion_Activos.pdf)

MINTIC, Ministerio de Tecnologías de la Información y las Comunicaciones 2016, “Guía de Auto-Evaluación de Seguridad de la Información”, visto el 19 de Julio de 2016, [http://www.MINTIC.gov.co/gestionti/615/articles-5482\\_Guia3\\_Autoevaluacion\\_seguridad.pdf](http://www.MINTIC.gov.co/gestionti/615/articles-5482_Guia3_Autoevaluacion_seguridad.pdf)

MINTIC, Ministerio de Tecnologías de la Información y las Comunicaciones 2016, “Modelo de Seguridad y privacidad de la información”, visto el 19 de Julio de 2016, [http://www.MINTIC.gov.co/gestionti/615/articles-5482\\_Modelo\\_Seguridad.pdf](http://www.MINTIC.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf)

National Institute of Standards and Technology - Special Publication NIST 800-53 Revisión 4, 2013, “Security and Privacy Controls for Federal Information Systems and Organizations”. Visto en: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

4-72 Servicios Postales Nacionales 2015, *Audiencia pública de rendición de cuentas vigencia 2014*, Servicios Postales Nacionales, Gobierno de Colombia, Bogotá, pp. 9-36, visto el 5 de Febrero de 2016, <http://www.4-72.com.co/sites/default/files/TextoImagenArchivo/Presentacion%20APRC%20Vig%202014%20V10.pdf>

Revista Dinero 2015, “Gobierno alista reforma al SISBEN por trampas que cuestan unos \$364.000 millones al año”, 11 de Marzo, visto el 22 de Febrero de 2016, <http://www.dinero.com/economia/articulo/colombia-alista-reforma-sisben-trampas-cuestan-unos-364000-millones-ano/215527>

Superintendencia de Industria y Comercio, 2012, “Guía para la implementación de la Responsabilidad Demostrada”. Visto en: <http://www.sic.gov.co/drupal/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada>

UT Everis – Servinformación, 2015, “Carpeta ciudadana y Autenticación Electrónica - Contrato de consultoría No. 0000535 de 2015 para la Conceptualización y diseño del modelo y la estrategia de implementación de los proyectos de Carpeta Ciudadana y Autenticación Electrónica”