

**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 línea¹ 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 2015² (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 SUIT³ 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 necesitaban⁴; 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 pesos⁵; en el 2015, la solicitud de pensiones ante Colpensiones se presentó un fraude cercano a los 4.500 millones de pesos⁶ 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 suplantación⁷.

Esta problemática se presenta en situaciones presenciales pero también cuando se hace uso de los medios tecnológicos. De acuerdo con las cifras de la DIJIN⁸, 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 cibernéticos⁹.

¹ 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>

² 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”

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

⁴ 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>

⁵ 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>

⁶ 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

⁷ 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>

⁸ 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>

⁹ 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 información¹⁰, 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 posible¹¹.

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 electrónica¹². 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 usuarios¹³.

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)¹⁴. 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

¹⁰ 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://estrategiacolombia.co/estadisticas/stats.php?&pres=content&jer=4&cod=&id=134#TTC>

¹¹ 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

¹² 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.

¹³ *Ibid.*

¹⁴ 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

realiza 62 trámites a lo largo de su vida¹⁵, 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 13.884.000¹⁶, 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 pesos¹⁷, 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 gobierno¹⁸.

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 solicitante¹⁹. La dificultad en este proceso radica en encontrar a las personas a las cuales se debe notificar²⁰.

El Ministerio de Educación Nacional por ejemplo, realizó 822 notificaciones mediante aviso en su página web entre 2013 y 2014²¹. De igual manera, la Dirección de Impuestos y Aduanas Nacional realiza en promedio 380 notificaciones quincenales por aviso correspondientes a obligaciones tributarias²². 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.

¹⁵ 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.

¹⁶ 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>.

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

¹⁸ 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>

¹⁹ 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”.

²⁰ 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”.

²¹ 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>

²² 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 documentos²³.

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.

²³ 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 personas²⁴ 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 documentos²⁵ 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.

²⁴ Ciudadanos y empresas colombianas.

²⁵ 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 Desarrollo²⁶, en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo²⁷ 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

Autenticación electrónica	Carpeta Ciudadana	Interoperabilidad
<p>Reconocer y validar la identidad de las personas 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>Firmar electrónicamente documentos²⁸ 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>Recibir documentos, comunicaciones y notificaciones. 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>Compartir documentos. 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>Habilitar y consumir servicios: 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 MINTIC²⁹, de forma que puedan ser compartidos o consumidos por otras entidades para construir cadenas de trámites³⁰ 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>Virtualizar datos. Las entidades públicas podrán, a través de los operadores, recopilar grandes volúmenes de datos provenientes de diversas fuentes al interior de</p>

²⁶ Ley 1753 de 2015, Artículo 45.

²⁷ Ley 1437 de 2011, Artículo 53 y siguientes

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

²⁹ 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>

³⁰ 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>Custodiar documentos: 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 70³¹ realizaron gestiones con el Estado haciendo uso de medios digitales³². 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 mantiene³³.

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 beneficios³⁴. 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

³¹ 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.

³² 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.

³³ 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.

³⁴ 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 everis³⁵

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 beneficios³⁶. 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 empresas³⁷. 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 mantiene³⁸.

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

³⁵ 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.

³⁶ 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.

³⁷ Esta cifra es tomada de las metas de conectividad del MINTIC.

³⁸ 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 everis³⁹

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 Excelencia⁴⁰ 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.

³⁹ 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.

⁴⁰ Mayor información sobre esta iniciativa se puede consultar en: <http://estrategia.gobiernoonlinea.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	2	1	1	1	1	1		98.369.880

Fuente: Elaboración propia con cifras del estudio de la Corporación Colombia Digital⁴¹

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

⁴¹ 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 restringida⁴² 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 acceso⁴³ 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 recurso⁴⁴.

⁴² 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.

⁴³ 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>.

⁴⁴ 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 impedirlo⁴⁵.

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 documentos⁴⁶ que se generen y compartan tienen la validez y fuerza probatoria que le confieren a los mismos las disposiciones del Código General del Proceso⁴⁷. 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.

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

⁴⁶ 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.

⁴⁷ 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 servicios⁴⁸ 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.*

⁴⁸ 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”

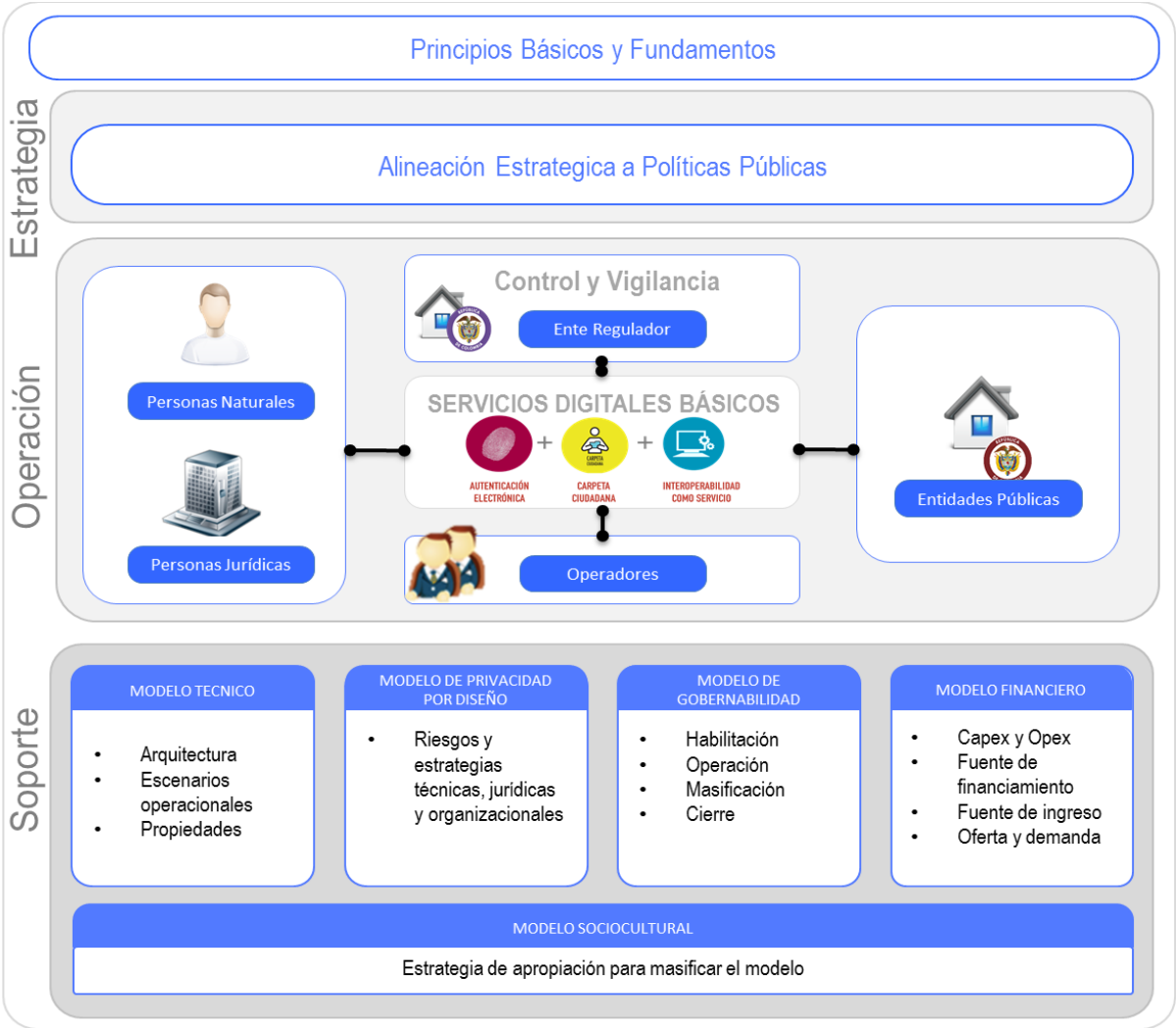
De otro lado, el artículo 113 de la Constitución Política consagra como base fundamental de la organización de los poderes públicos y de las relaciones entre ellos, la exigencia de su colaboración armónica, en estos términos, que en lo esencial se encontraban en la Carta de 1886: *"Los diferentes órganos 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.

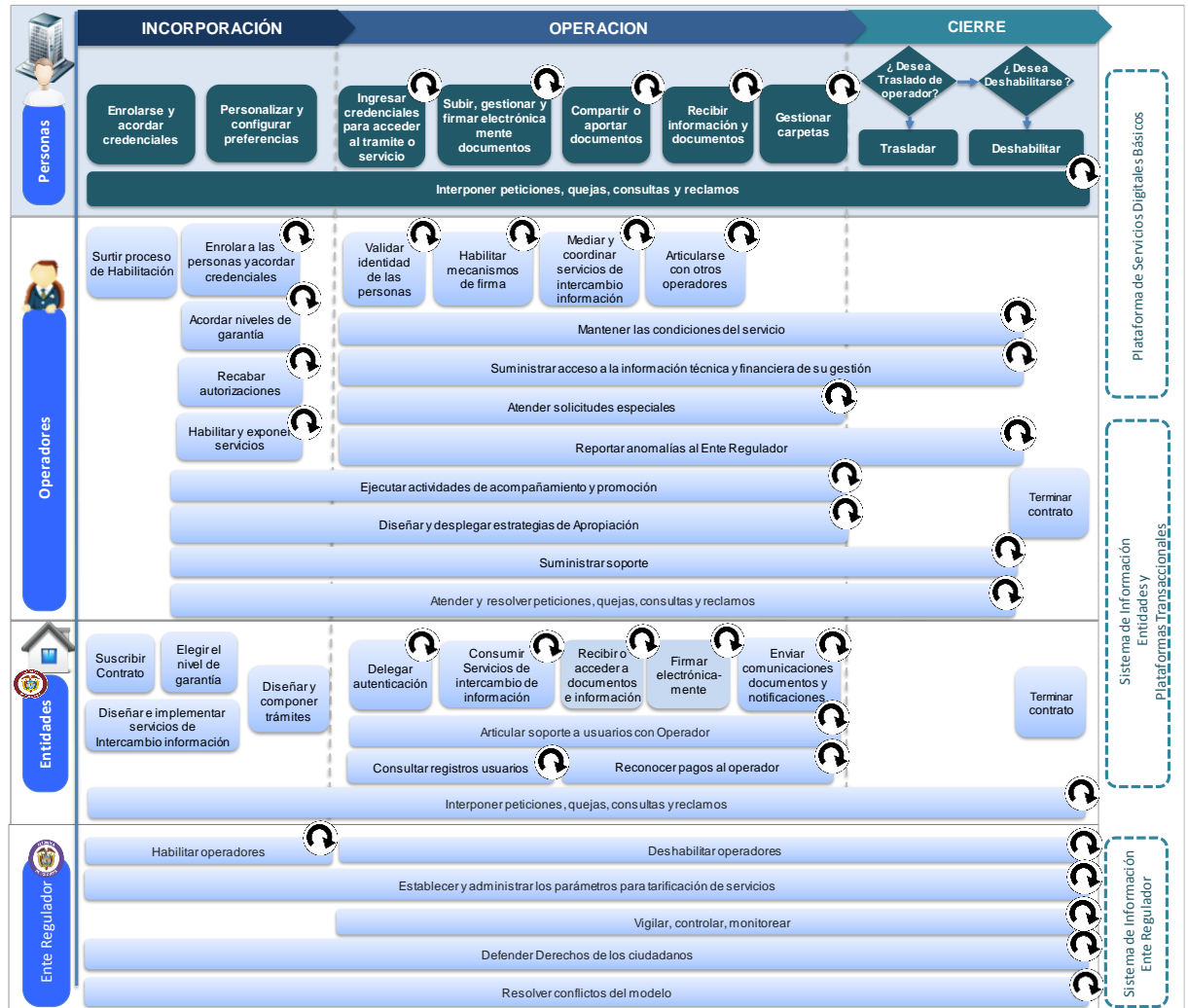
Ilustración No. 1 Modelo de Servicios Digitales Básicos



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 Regulador.

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.⁴⁹
- *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

⁴⁹ 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.⁵⁰ 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.

⁵⁰ 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

plataformas transaccionales centralizadas, como el Sí Virtual (www.sivirtual.gov.co) o las ventanillas únicas. Se incluyen los sistemas misionales y de apoyo de las entidades públicas que deben interactuar entre sí para ofrecer servicios conjuntos y permitir aumentar la eficiencia administrativa de cara a ofrecer unos servicios óptimos al ciudadano.

- **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.

9.2 Modelo Técnico

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.

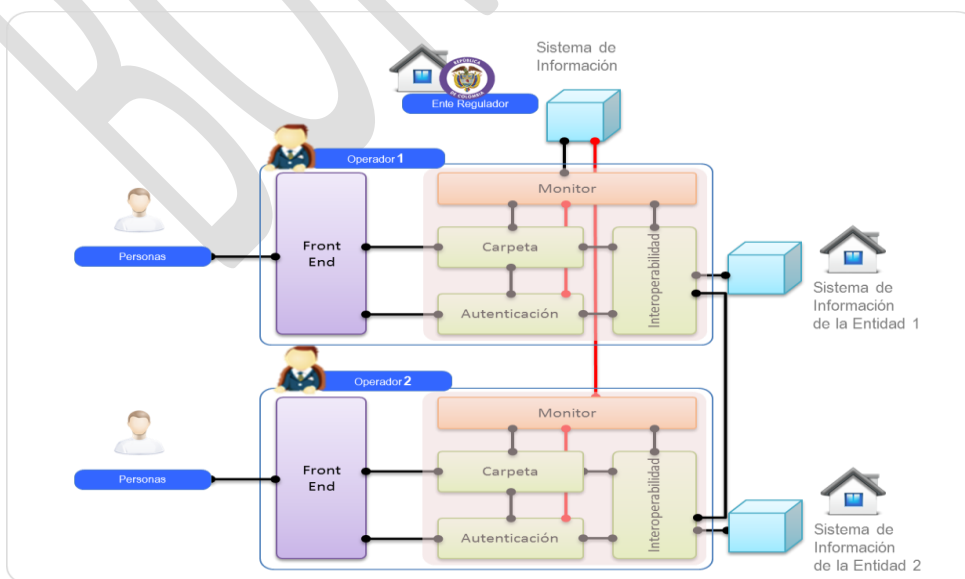
9.2.1 Arquitectura

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*.

Front-end, que es la interfaz de la plataforma con la cual va a interactuar el ciudadano, el representante legal de una empresa, los operadores tecnológicos y el ente regulador. Este componente brindará las interfaces de usuario necesarias para llevar a cabo los procesos de identificación de usuarios a la plataforma de servicios digitales básicos, las gestiones de sus cuentas, alertas, credenciales, custodia de documentos y demás escenarios operacionales que posteriormente se detallarán.

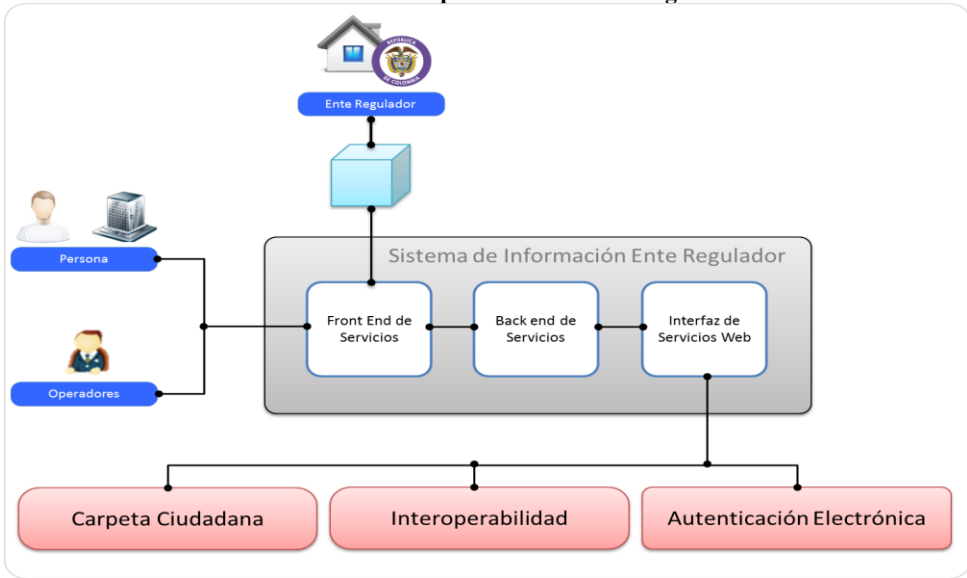
Back-end, que comprende todos los componentes necesarios para que la plataforma pueda ejecutar los procesos lógicos requeridos para soportar los servicios a los diferentes actores. Implementa toda la lógica de negocio necesaria para soportar las interacciones de los diferentes actores definidos para 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.

Ilustración No. 3 Arquitectura de la plataforma de Servicios Digitales Básicos



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
PERSONAS		
Enrolarse y acordar credenciales	Gestionar enrolamiento	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: <ul style="list-style-type: none">Solicitar enrolamiento ante un operadorIdentificarse ante el sistema para enrolamientoAcordar 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.

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"> • Obtener credenciales de acceso. • Suscribir términos y condiciones con el operador.
Personalizar y configurar preferencias Trasladar Deshabilitar	Gestionar cuenta en la plataforma de Servicios Digitales Básicos	<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"> • Identificarse ante el sistema • Ingresar a la plataforma de servicios digitales básicos • Gestionar PQRs • Cancelar cuenta/Deshabilitarse
	Gestionar servicio de Autenticación Electrónica	<p>Le permitirá al usuario realizar todas las gestiones necesarias para administrar el servicio:</p> <ul style="list-style-type: none"> • Configurar alertas de acceso • Visualizar registros de acceso • Descargar registros de acceso • Bloquear y desbloquear servicio
	Configurar servicio de Carpeta Ciudadana	<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 <darse de alta para recibir notificaciones electrónicas, aviso de notificaciones por otros canales, selección por entidad o trámite, vigencia></p>
	Suscribir a los servicios de envío de información de las entidades	<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>
	Gestionar credenciales de acceso	<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"> • Consultar el estado y la vigencia de sus credenciales de acceso • Solicitar la revocación de credenciales • Renovar credenciales (a nivel lógico)
Ingresar credenciales para acceder a trámites y servicios	Usar autenticación	<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"> • Instalar el componente de autenticación (en caso de que se requiera). <p>Usar el componente de autenticación de acuerdo al nivel de garantía requerido por la entidad.</p>
Subir, gestionar y firmar electrónicamente documentos Recibir información y documentos	Usar mecanismos de firma	<p>Le permitirá al usuario usar los mecanismos necesarios para firmar documentos por medios digitales. Permitirá:</p> <ul style="list-style-type: none"> • Instalar el componente de firma. • Usar el componente de firma
	Usar servicios criptográficos	<p>Le permite al usuario realizar las siguientes operaciones:</p> <ul style="list-style-type: none"> • Cifrar/Descifrar documento • Estampar documentos • Verificar firma electrónica o digital de documentos • Verificar estampas cronológicas • Verificar certificados para firmar documentos
	Gestionar documentos	<p>Le permitirá al usuario realizar las siguientes operaciones relacionadas con la gestión de los documentos:</p> <ul style="list-style-type: none"> • Subir documento • Visualizar documento • Mover documento a una carpeta seleccionada • Eliminar y restaurar documento • Renombrar documento • Buscar documento

Operaciones de los Actores	Escenario Operacional	Descripción
		<ul style="list-style-type: none"> • Descargar documento a un dispositivo de almacenamiento externo • Firmar documento
Gestionar carpetas	Gestionar carpetas	<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"> • Modificar carpetas • Eliminar carpetas • Cortar y pegar (mover) carpetas • Visualizar carpetas por defecto fijas <entrada, compartidos, eliminados, cargados por el usuario> • Gestionar esquemas de organización de carpetas del usuario • Gestionar esquema de organización de carpetas para personas dependientes.
Compartir o aportar documentos	Aportar/compartir documentos con terceros	<p>Le permitirá al usuario realizar las siguientes operaciones:</p> <ul style="list-style-type: none"> • Compartir un documento con uno o varios usuarios de Carpeta Ciudadana. <enlace> • Aportar documentos en un trámite/servicio de una entidad <URL, archivo físico, FTP, API> • Visualizar un documento que he o me han compartido • Cancelar compartir documento • Bloquear usuarios para que me compartan documentos • Gestionar los permisos de acceso al documento • Buscar y filtrar sobre documentos que he o me han compartido.
Interponer peticiones, quejas, consultas y reclamos.	Gestión de Peticiones, Quejas y Reclamos a los Operadores y al Ente regulador	<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"> • Radicar Peticiones, Quejas y Reclamos • Consultar Peticiones, Quejas y Reclamos • Ver estado o respuesta de las Peticiones, Quejas y Reclamos • Adicionalmente debe ofrecer vínculos a los sistemas de Peticiones, Quejas y Reclamos del Ente regulador.
ENTIDADES PÚBLICAS		
Suscribir contrato Terminar contrato	Gestionar servicios de la plataforma de Servicios Digitales Básicos	<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"> • Darse de alta en un operador. • Acceder a algún servicio de provisto por la plataforma. Es necesario introducir las credenciales de identificación provistas por el operador • Configurar el servicio. • 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. • Configurar por tipo de documento ofrecido en la Carpeta Ciudadana <nombre; formato: PDF, JPG,T IFF, XML; medio de entrega del documento: URL, FTP, físico; periodo de validez; medio de notificación; tamaño>. • Configurar usuarios internos de la aplicación, bloquear y desbloquear servicio. • Cancelar servicio. • Habilitar la activación y desactivación de los diferentes servicios de la Plataforma de Interoperabilidad.
Elegir nivel de garantía	Análisis del trámite y servicio	<p>La entidad podrá realizar un análisis del trámite o servicio o plataforma digital.</p> <ul style="list-style-type: none"> • Evaluar el riesgo del trámite o servicio o plataforma digital que requiera el servicio de Autenticación Electrónica. • 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.
Delegar autenticación	Acordar protocolo de Autenticación Electrónica	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
	Delegar los servicios de autenticación	<p>La entidad podrá validar la identidad de las personas.</p> <ul style="list-style-type: none"> • Delegar servicios de autenticación de las personas a la plataforma de Autenticación Electrónica.
Firmar electrónicamente	Delegar los servicios de firma	La entidad podrá ofrecer el servicio de firma de documentos por medios digitales haciendo uso de la plataforma:

Operaciones de los Actores	Escenario Operacional	Descripción
		<ul style="list-style-type: none"> Delegar servicios de firma electrónica de las personas a la plataforma de Servicios Digitales Básicos
Diseñar e implementar servicios de intercambio de información Diseñar y componer trámites	Componer y/o orquestar servicios para intercambio de información	<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"> Definir las reglas y políticas de los servicios Diseñar y componer los trámites a partir de los servicios internos y externos
	Habilitar y exponer servicios	<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"> Habilitación de servicios o micro servicios Definición del servicio y metadatos asociados al mismo Configuración de los servicios Aseguramiento y control de accesos Administración de reglas y políticas asociadas al servicio en su ejecución o definición Seguimiento de la operación del servicio
	Virtualizar datos	<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>
	Estandarizar servicios para intercambio de información	<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"> Revisión y verificación de los 5 dominios de interoperabilidad Definición de las estructuras a partir de las cuales se intercambiarán los datos.
Consumir servicios de intercambio de información	Consumir servicios de intercambio de información	<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"> Permitir el consumo (uso) de la plataforma, a través de un programa o una persona que solicita un servicio de las Entidades Apoyar la interacción e integración de los consumidores; es decir, la capacidad de capturar la entrada del usuario (consumidor) y proporcionar la respuesta Permitir la creación de una interface de usuario para el consumo de servicios
Recibir o acceder a documentos e información	Importar documentos como parte de un trámite	<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 <consumo del servicio>; solicitar documento adicional a un trámite ya generado <consumo del servicio>.</p> <p>Dichos documentos tendrán validez jurídica.</p>
Enviar comunicaciones, documentos y gestionar notificaciones	Gestionar comunicaciones, documentos y notificaciones	<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"> Enviar comunicaciones y documentos Enviar avisos por diferentes canales Enviar comunicaciones y documentos masivamente Gestionar notificaciones Consultar reportes
Consultar registros de usuarios	Consultar registros de usuarios	<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>
Reconocer pagos al operador	Consultar la información de la facturación del servicio	<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>
Interponer peticiones, quejas, consultas y reclamos.	Gestionar peticiones, quejas y reclamos	<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"> Radicar Peticiones, Quejas y Reclamos

Operaciones de los Actores	Escenario Operacional	Descripción
		<ul style="list-style-type: none"> Consultar Peticiones, Quejas y Reclamos Ver estado o respuesta del Peticiones, Quejas y Reclamos
ENTES REGULADORES		
Vigilar, controlar y monitorear	Monitorear operadores	<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"> Para el servicio de Carpeta Ciudadana: <ul style="list-style-type: none"> Reporte del número de usuarios enrolados en la plataforma de Carpeta Ciudadana Reporte del espacio total utilizado Reporte del espacio promedio utilizado por usuario Reporte del número de documentos asociados a cada usuario. Para el servicio de Autenticación Electrónica: <ul style="list-style-type: none"> Reporte del número de usuarios identificados en la plataforma Reporte del número de transacciones por operador Reporte de los sistemas de información que usan el servicio Para el servicio de IOAAS <ul style="list-style-type: none"> Reporte del número de servicios habilitados (Activos/inactivos) Valores para los parámetros de cada servicio Reporte del número de transacciones por servicio Reporte de entidades consumidoras de servicios y sus trámites Reporte de entidades que publican servicios y su uso por otras entidades Reporte de servicios con análisis de desempeño, disponibilidad y atención de fallas Reporte de los tiempos de ejecución Permisos de acceso y uso, periodicidad de uso máxima permitida
	Gestionar funcionamiento	<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>
Habilitar operadores	Habilitar operador de Servicios Digitales Básicos	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.
	Exponer servicio de habilitación de Operador	El Ente regulador deberá exponer el servicio de habilitación del Operador.
	Revocar operador de Servicios Digitales Básicos	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.
Tarificar servicios	Gestionar servicios prestados y sus tarifas asociadas	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
Funcionamiento	<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>
Seguridad	<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>
Privacidad y debido tratamiento de datos personales	<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>
Escalabilidad	<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>
Capacidad de monitoreo	<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>
Accesibilidad	<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
Disponibilidad	<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>
Confiabilidad	<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>
Recuperación	<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>
Mantenimiento	<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>
Soporte	<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>
Conformidad	<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"> • Deben estar en conformidad con todas las disposiciones legislativas y regulatorias que apliquen a la naturaleza del Operador y a la jurisdicción. • 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 • 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. • Debe ser compatible con el almacenamiento de archivos utilizando formatos de archivo y codificación estandarizada o totalmente documentada. • Debe ajustarse a las normas locales aplicables para admisibilidad jurídica y valor probatorio de la información digital. • El sistema no debe incluir funciones que sean incompatibles con la protección de datos a nivel nacional, la libertad de información u otra legislación. • 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

Propiedad	Descripción
Preservación a largo plazo y obsolescencia de la tecnología	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"> • La degradación de los medios de comunicación • La obsolescencia de hardware • La obsolescencia de formato

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*⁵¹, 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
UBICACIÓN DE LOS DATOS	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"> ▪ Marco regulatorio aplicable al almacenamiento y procesamiento de datos ▪ Acuerdo con el operador para que el tratamiento de los datos se subyugue al marco legal de Colombia. ▪ Almacenamiento y procesamientos de datos en Colombia ▪ 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. ▪ Certificaciones de seguridad. ▪ Controles de acceso a los datos
CONFORMIDAD	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"> ▪ Conformidad con especificaciones, estándares, normas o leyes establecidas en el país. ▪ La posesión de certificaciones de seguridad o la realización de auditorías externas por parte del operador. ▪ La legislación y normativa local relacionada con privacidad y seguridad. ▪ Tecnologías y soluciones estándar ▪ Almacenamiento y procesamiento de datos en Colombia ▪ Integridad y transparencia en los términos de uso

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

CATEGORIA	RIESGO	ESTRATEGIA DE MITIGACIÓN
INFORMACIÓN	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"> 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.
PROPIEDAD DE LOS DATOS	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"> 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.
GESTIÓN DE RIESGOS	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"> 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.
ABUSO EN LOS SERVICIOS	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"> Implementar un sistema de registro de acceso más restrictivo mediante el proceso de Autenticación Electrónica. Coordinar y monitorizar el tráfico de clientes para la detección de posibles actividades ilícitas. Comprobar las listas negras públicas para identificar si los rangos IP de la infraestructura han entrado en ellas.
PÉRDIDA DE INFORMACIÓN	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"> Implementar API potentes para el control de acceso Proteger el tránsito de datos mediante el cifrado de los mismos Analizar la protección de datos desde el diseño como en la ejecución Proporcionar mecanismos potentes para la generación de claves, almacenamiento y destrucción de la información 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
ROBO DE SESIÓN	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"> Prohibir, mediante políticas, compartir credenciales entre usuarios y servicios Aplicar técnicas de autenticación de doble factor siempre que sea posible Monitorizar las sesiones en busca de actividades inusuales
USUARIOS CON PRIVILEGIOS DE ACCESO	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"> 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.
GESTIÓN DE USUARIOS	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"> Nombres Apellidos Tipo de documento Número del documento de identificación. Correo Electrónico Pseudónimo <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"> Numero de celular Información Biométrica (en el caso de usar la biometría como uno de los factores de autenticación) Otros <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"> ▪ 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. ▪ Punto de enrolamiento ▪ Identificador de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (AFIS) provisto por la Registraduría Nacional del Estado Civil RNEC. ▪ Estampa cronológica de la confirmación de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (AFIS) provisto por la RNEC. ▪ Firma electrónica de la transacción que corresponda al funcionario o persona a cargo que facilitó la verificación. <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"> ▪ 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. ▪ Punto de enrolamiento ▪ Identificador de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (AFIS) provisto por la Registraduría Nacional del Estado Civil RNEC. ▪ Estampa cronológica de la confirmación de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (AFIS) provisto por la RNEC. ▪ Firma electrónica de la transacción que corresponda al funcionario o persona a cargo que facilitó la verificación.
	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"> ▪ un servicio de notificación cuando se modifiquen los atributos de identidad de las personas ▪ un servicio de notificación cuando se modifiquen las autorizaciones dadas por las personas ▪ 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
	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.
 AISLAMIENTO DE DATOS 	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"> ▪ El operador debe garantizar el aislamiento de los datos de los respectivos usuarios. ▪ Implementar técnicas de cifrado de los datos aislados para reducir grandemente el riesgo de exposición mientras conserva la economía de escala
 RECUPERACIÓN 	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"> ▪ Se debe exigir a los proveedores los datos sobre la viabilidad de una recuperación completa y el tiempo que podría tardar. ▪ Los operadores de servicio deben tener una política de recuperación de datos en caso de desastre. ▪ Los datos sean replicados en múltiples infraestructuras para evitar que sean vulnerables a un fallo general. ▪ Se debe exigir un plan de copias de seguridad que permita reiniciar rápidamente el servicio ante un desastre.
 VIABILIDAD A LARGO PLAZO DEL OPERADOR 	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"> ▪ 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. ▪ Los operadores deben mostrar como retornaran los datos y en qué formato para poder importarlos en una nueva aplicación.
 RESPUESTA A INCIDENTES 	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"> ▪ Entender y negociar los contratos de servicio de los operadores, así como los procedimientos para la respuesta a incidentes requeridos por los usuarios.
 DISPONIBILIDAD 	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"> ▪ Asegurarse que durante una interrupción del servicio, las operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente.

CATEGORIA	RIESGO	ESTRATEGIA DE MITIGACIÓN
VALOR CONCENTRADO	La Carpeta Ciudadana puede ser objetivo de ataques porque, en cierto modo, concentra gran cantidad de información personal.	<ul style="list-style-type: none"> 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. 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.
CIFRADO DE DATOS	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"> 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. Securización de las comunicaciones ante la interceptación de los datos <i>on-the-air</i>. <ul style="list-style-type: none"> * Utilización de canales de comunicación cifrados entre el cliente y los servicios. * 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.
PÉRDIDA DE CREDENCIALES	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"> Procedimientos de gestión de claves adecuados.
ORDENES JUDICIALES	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"> Cumplimiento de políticas que en la materia sean definidas por el Ente Regulador en el marco de la legislación vigente.
PROTECCIÓN DE DATOS	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"> Marco regulatorio aplicable en materia de protección de datos. Imposición de sanciones administrativas, civiles e incluso penales. Divulgación de información sobre prácticas de procesamiento de datos de los operadores de servicio. Certificación sobre actividades de procesamiento y seguridad de datos y los controles de datos.

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 Seguridad⁵² 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.

⁵² Consultar en http://www.MINTIC.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

Tabla 8. Requisitos de Privacidad de la Información

CATEGORIA	REQUISITOS MINIMOS	REFERENTES
POLÍTICAS Y PROCEDIMIENTOS 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"> 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>. 2. Publicar y garantizar el entendimiento y apropiación de las políticas de privacidad para las prácticas en los servicios. 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. 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. 	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 ⁵³
PRIVACIDAD POR DISEÑO 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"> 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. 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. 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. 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. 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. <p>Dentro de las características a tener en cuenta para implementar la privacidad por diseño se encuentran las ocho (8) estrategias de Hoepman⁵⁴ 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
GESTIÓN DEL RIESGO 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"> 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 2. Garantizar que los costos de inversión cubren el ciclo de vida de cada sistema e incluye todos los recursos presupuestales requeridos. 	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

⁵³ 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>

⁵⁴ 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
		<p>Buena práctica internacional: Apéndice J. <i>Control AR-2 Evaluación de riesgos e impacto de la Privacidad</i>- NIST Special Publication 800-53</p> <p>Template for a PIA report.</p> <p>Proyecto «Privacy Impact Assessment Framework». Bruselas-Londres</p> <p>ISO/IEC 27005 Information Technology. Security Techniques. Information security risk management.</p> <p>ISO 31010. Gestión del riesgo.</p> <p>Técnicas de apreciación del riesgo.</p> <p>Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)</p>
MEDIDAS DE SEGURIDAD Aplicación de los controles adecuados para garantizar la confidencialidad, integridad y disponibilidad de la información personal.	<ol style="list-style-type: none"> 1. Establecer medidas administrativas, técnicas y físicas para garantizar la seguridad y la confidencialidad de los registros y datos. 2. Garantizar que la Evaluación de Impacto a la Privacidad identifica cómo la información será asegurada (controles administrativos y técnicos) 	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.
ROLES ASIGNADOS, RESPONSABILIDADES, Y RENDICIÓN DE CUENTAS 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"> 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. 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. 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. 4. Todos los empleados y contratistas deben ser conscientes de la privacidad y su obligación para proteger la información en forma identificable. 	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
SENSIBILIZACIÓN Y PROGRAMAS DE CAPACITACIÓN BASADO EN FUNCIONES 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"> 1. Capacitar a cada persona implicada en el tratamiento de datos personales en las reglas de conducta y sanciones en caso de incumplimiento. 2. Informar y educar a los empleados y contratistas de su responsabilidad para proteger información en forma identificable. 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. 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>. 	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
DIVULGACIÓN PÚBLICA 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
DERECHOS INDIVIDUALES. PARTICIPACIÓN INDIVIDUAL 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
NOTIFICACIÓN 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
CONSENTIMIENTO 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
MÍNIMO NECESARIO 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
USO ACEPTABLE 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
EXACTITUD DE LOS DATOS 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
AUTORIZACIÓN DE NUEVOS USOS 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
CADENA DE CONFIANZA 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
MONITOREO Y MEDICIÓN 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
NOTIFICACIÓN Y RESPUESTA ANTE INCIDENTES 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
PRESENTACIÓN DE INFORMES	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
MINIMIZAR 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"> ▪ Nombres ▪ Apellidos ▪ Tipo de documento ▪ Número del documento de identificación. ▪ Correo Electrónico ▪ Pseudónimo 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"> ▪ Numero de celular ▪ Información biométrica ▪ Dirección postal ▪ Otros Dentro del registro se deberán almacenar datos generados en el enrolamiento, tales como: <ul style="list-style-type: none"> ▪ Punto de enrolamiento ▪ Identificador de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (Afis) provisto por la Registraduría Nacional del Estado Civil RNEC ▪ Estampa cronológica de la confirmación de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (Afis) provisto por la RNEC ▪ Firma electrónica de la transacción que corresponda al funcionario o persona a cargo que facilitó la verificación.
PROTEGER 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.
SEPARAR 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.
AGREGAR 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: Nivel 1: 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
	Nivel 2: 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.
INFORMAR 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"> ▪ 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. ▪ Mantener los registros de la trazabilidad de autenticaciones e información adicional a la mínima del ciudadano que se compartió con cualquier sistema de información. ▪ 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. ▪ 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. ▪ 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.
CONTROLAR 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"> ▪ 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. ▪ 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. ▪ Un mecanismo para divulgar al titular cuando el punto anterior ocurra. ▪ La posibilidad de la portabilidad dentro de los servicios de información de identificación personal, de acuerdo con la normatividad y las políticas aplicables. ▪ Permitir revocar en cualquier momento el acceso concedido a su información adicional y mensajes de datos. ▪ Permitir el asignar una vigencia en tiempo de los permisos de acceso a su información adicional de autenticación y a los documentos. ▪ 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. ▪ 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.
CUMPLIR 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>
DEMOSTRAR Esta estrategia busca ser capaz de demostrar el cumplimiento de la política de privacidad por parte del operador.	<p>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.</p>

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

- 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
OPERADORES				
Registro y Prestación de servicios	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	Operación de los servicios digitales básicos: Las condiciones de operación y deberes de los operadores se realizará conforme a lo descrito en los	Informes de gestión 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>Normatividad: 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"> - Ley 527 de 1999 - Ley 594 de 2000 - Ley 1341 de 2009 - Ley 1437 de 2011 - Decreto Ley 019 de 2012 - Ley 1753 de 2015 - Decreto 1074 de 2015 - Decreto 1078 de 2015 - Decreto 1080 de 2015 - Resolución 5633 de 2016 <p>Instrumento jurídico de habilitación: 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>Contratación de servicios por parte de las Entidades públicas: La oferta de servicios podrá hacerse mediante acuerdos marco⁵⁵ 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"> 1. Informe de la estrategia de masificación de servicios. 2. Informe cualitativo y cuantitativo de la forma en la que se están cumpliendo con los requisitos técnicos y financieros para operar. 3. Informe sobre indicadores de calidad de servicio. 	<ol style="list-style-type: none"> 1. Por solicitud expresa el operador. 2. Por orden del Ministerio TIC una vez se haya surtido el procedimiento administrativo sancionatorio. 3. En caso de liquidación de la persona jurídica. 4. Por incumplimiento de los deberes y responsabilidades a cargo del operador.

⁵⁵ 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
Requisitos técnicos y financieros	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.
Vigilancia y Control	-	<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>Superintendencia de Industria y Comercio (SIC): 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"> 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. 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. <p>Registraduría Nacional del Estado Civil: 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>Ministerio Público: 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>Archivo General de la Nación: 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>MINTIC: 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"> Diseñar el marco reglamentario y la expedición del correspondiente decreto que fije el marco normativo para el desarrollo del modelo. Establecer un proceso de registro de operadores, previa verificación de requisitos habilitantes. Establecer un seguimiento periódico sobre el cumplimiento de dichos requisitos. Hacer seguimiento y supervisión a la operación del modelo a través de indicadores y el análisis periódico. 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. 		
Tratamiento de Datos personales	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	Decreto: 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. Resolución de carácter Particular 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.	<p>El operador podrá prestar sus servicios una vez haya sido autorizado mediante acto administrativo de carácter particular proferido por el Ministerio TIC.</p> <p>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.</p> <p>Los acuerdos marco de precios establecerán el mecanismo de compensación entre prestadores así como los Acuerdos de Niveles de Servicio.</p>	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

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

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

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

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

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

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

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

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”

ANEXO TÉCNICO

Nombre del servicio		Autenticación Electrónica		
Alcance del servicio		<p>El servicio de Autenticación electrónica permitirá reconocer y validar la identidad de las personas 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>Para el correcto funcionamiento del servicio se requiere un enrolamiento que permita registrar a los ciudadanos al servicio de Autenticación Electrónica, verificando plenamente su identidad y mediante un flujo de información que representa los procesos de demostración, verificación y pruebas de que un ciudadano real está asociado con una identidad, asignándole credenciales que vinculen al ciudadano con un nombre o pseudónimo y otros atributos asociados, y así permitiéndole realizar transacciones por medios digitales. Para ello el ciudadano deberá realizar la solicitud de enrolamiento de modo presencial y no podrá ser delegada. El operador deberá facilitarle la etapa de enrolamiento a cada ciudadano que lo requiera a lo largo del país, permitiéndole completar esta etapa de manera satisfactoria.</p>		
	Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
1	Acceso al enrolamiento	El ciudadano podrá realizar la solicitud de enrolamiento ante el operador que seleccione. El operador deberá facilitarle la etapa de enrolamiento a cada usuario que lo requiera a lo largo del país y a usuarios colombianos en el exterior, permitiéndoles completar esta etapa de manera satisfactoria.	NA	
2	Verificación Biométrica	Este proceso implica la demostración, verificación y pruebas de que un ciudadano real está asociado con una identidad, para ello el usuario deberá demostrar que es quien dice ser, mediante la verificación con la información biométrica de la Registraduría Nacional del Estado Civil RNEC. Esta verificación deberá generar un identificador de la transacción que deberá ser almacenado dentro de los campos del registro y la transacción deberá tener estampado cronológico.	Verificación contra el Sistema Automatizado de Identificación Dactilar Colombiano (Afis) provisto por la RNEC, según lo dispuesto en la Resolución 5633 de 2016 de la RNEC	
3	Verificación no Biométrica	En los casos en los que el usuario tenga alguna dificultad médica que le impida validar su identidad contra la información biométrica de la RNEC, este deberá presentar certificación médica que demuestre la dificultad. El usuario deberá presentar el documento original de identificación (cédula de ciudadanía, cédula de extranjería, tarjeta de identidad, pasaporte). La identidad deberá verificarse contra el Archivo General de identificación de la Registraduría Nacional del Estado Civil. Deberá proporcionar información que probablemente sólo esta persona conozca y esta información se corroborará con fuentes de otros contextos, lo suficiente como para asegurar la identidad.	NA	
4	Registro en el servicio	Este es el proceso de registro de los atributos relacionados con la identidad del usuario La recopilación de datos en el momento del enrolamiento deberá tener la plena aprobación de la persona a enrolar y respetar la debida protección de datos personales, de conformidad y en los términos de la ley 1581 de 2012. No deberá aportarse por parte del usuario información adicional, como por ejemplo (dirección física, entre otros) a los operadores y/o a los sistemas de información. 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 mínimos necesarios.	Para el registro se solicitarán los siguientes datos: o Nombres o Apellidos o Tipo de documento o Número del documento de identificación. o Correo electrónico o Pseudónimo	Prevía justificación ante el MinTIC y con su correspondiente autorización, se podrán solicitar otros datos únicamente si son requeridos para la expedición de las credenciales, tales como: o Número de celular o Información biométrica o Otros


	Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
5	Base de datos primaria	Para que el usuario 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.		La base de datos primaria deberá contener únicamente los siguientes campos: o Número del documento de identificación. o Identificador del Operador que enroló al usuario
6	Actualización de base de datos primaria	La base de datos primaria deberá ser compartida y actualizada entre los operadores por medio de un servicio que cada operador deberá publicar a través del servicio de interoperabilidad.	La actualización de la base de datos primaria de cada operador deberá realizarse cada 3 horas	
7	Protección de la información	Cualquier información de datos personales que se reciba o procese por parte del operador debe estar protegida.	<ul style="list-style-type: none"> - Deben adoptarse las medidas técnicas y administrativas necesarias para proteger la información contra la destrucción accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, en particular cuando el procesamiento implique la transmisión de datos por una red, y contra toda forma ilícita de procesamiento. - Implementar el uso de criptografía, con el objetivo de permitir el cifrado fuerte de información, conforme a lo recomendado en la NIST Special Publication 800-78-4 	
8	Preferencias para compartir información	Los usuarios deben tener el control sobre el servicio de autenticación y el tratamiento de sus datos, permitiéndole al usuario que sea él quien defina sus preferencias. Los usuarios tienen el derecho de acceder, modificar y suprimir su información personal.		
9	Expedición de credenciales	<p>El operador deberá proveer dos tipos de credenciales a los usuarios correspondientes a los niveles de garantía Medio y Alto.</p> <p><i>En el Nivel de Garantía Medio:</i> Puede 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.</p> <p><i>En el Nivel de Garantía Alto:</i> Se exigen por lo menos dos factores de autenticación. Debe proporcionar autenticación remota con la más alta seguridad práctica y está basado en la posesión de tokens criptográficos basados en hardware.</p>	<p>El Nivel de Garantía Medio es equivalente al 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>Nivel de Garantía Alto es 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>	
10	Entrega de credenciales	Antes de hacer la vinculación de una credencial a un usuario el operador debe tener la suficiente garantía de que la credencial está y sigue estando vinculada a la persona correcta.	NA	
11	Credenciales basadas en secretos compartidos almacenamiento	Las credenciales basadas en secretos compartidos requeridos en los niveles de garantía medio (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), no deberán almacenarse en texto plano, para ello se usarán funciones hash y valores salt para frenar ataques de fuerza bruta (brute-force attack) o ataques a la tabla arcoíris (rainbow table).	Mínimo implementación de mecanismos criptográficos de derivación de claves como PBKDF2 descrito en el RFC 2898 y lo recomendado en la NIST Special Publication 800-78-4.	

	Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
12	Credenciales basadas en secretos compartidos formato de creación	Será obligatoria la utilización de contraseñas robustas (por ejemplo, cadenas complejas sin significado que contengan una combinación de mayúsculas, minúsculas, números y caracteres especiales). No se utilizarán nombres de cuentas ni contraseñas por defecto (por ejemplo, datos del fabricante).		
13	Credenciales basadas en hardware	Las credenciales incluidas en un dispositivo de hardware se pondrán en estado de bloqueo al final del proceso de creación y deberán hacer uso de criptografía fuerte.	Implementar el uso de criptografía, con el objetivo de permitir el cifrado fuerte de información, conforme a lo recomendado en la NIST Special Publication 800-78-4	
14	Política de protección de credenciales	La política de protección para las credenciales almacenadas deberá describirse en la documentación asociada a la utilización de estas credenciales, puesta a disposición de los usuarios.		
15	Datos del proceso de enrolamiento	Dentro del registro se deberán almacenar datos básicos generados en el enrolamiento que permitan tener la trazabilidad en la validación de una identidad y las credenciales otorgadas	<ul style="list-style-type: none"> o Punto de enrolamiento o Identificador de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (Afis) provisto por la Registraduría Nacional del Estado Civil RNEC. o Estampa cronológica de la confirmación de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (Afis) provisto por la RNEC o Firma electrónica de la transacción que corresponda al funcionario o persona a cargo que llevó a cabo el enrolamiento. o Descripción de credenciales otorgadas. o Firma de aceptación de términos y condiciones por parte del usuario. 	
16	Niveles de garantía del servicio	En este proceso el operador deberá acompañar, asesorar, recomendar y orientar 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 sea precisa, mientras que 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.	El Nivel de Garantía Medio es equivalente al nivel de Garantía 2 (NdG2) y el Nivel de Garantía Alto es equivalente a nivel de Garantía 4 (NdG4) establecidos en las recomendaciones de la ITU X.1254, ISO 29115 y NIST Special Publication 800-63-2.	
17	Acceso de personas	Le debe permitir al usuario que lo requiera, acceder a un servicio de información de una entidad.	<p>El operador contratado por la entidad deberá proveer un formulario que le permita al ciudadano el ingreso de los siguientes datos.</p> <ul style="list-style-type: none"> o Tipo de documento o Número de documento de identificación. o Numero de NIT (en caso de requerir acceso representando a una persona jurídica) <p>Con esta información el operador podrá consultar la base de datos primaria de usuarios para determinar qué operador deberá resolver la solicitud de autenticación.</p>	
18	Autenticación mutua	El sistema de información o página web de la entidad deberá identificarse ante el sistema de información del operador por medio de protocolos y mecanismos de autenticación mutua.	Uso de protocolos criptográficos que proporcionan comunicaciones seguras, como Transport Layer Security	

	Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
19	Autenticación del servicio ante la persona	Para que las personas puedan estar seguras de que están ingresando al servicio provisto por el operador, se deberán ofrecer mecanismos de autenticación del servicio ante la persona, como frase e imagen de seguridad personalizadas por usuario.	Uso de estrategias como frase e imagen de seguridad personalizadas por usuario para identificar el sitio web.	
20	Controles para ataques por phishing	Se efectuarán controles concebidos concretamente para detectar ataques de phishing	Filtros bayesianos, listas negras IP, filtros URL, esquemas heurístico	
21	Verificación de enrolamiento del usuario	<p>En caso de que el usuario requiera acceder a un servicio de información de una entidad, el operador contratado por la entidad que dispone de dicho servicio, deberá validar en qué operador se enroló el ciudadano por medio de la base de datos primaria de usuarios.</p> <p>Si el usuario se encuentra registrado en el operador contratado por la entidad, este mismo operador resolverá la solicitud de autenticación.</p> <p>Si el usuario no se encuentra registrado con 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.</p> <p>Si el usuario no se encuentra registrado en la base de datos primaria de usuarios, el operador contratado por la entidad deberá realizar una consulta a los demás operadores, y así verificar si efectivamente se encuentra enrolado ante alguno de estos. (Esta validación se realizará con el fin de verificar al usuario que requiera acceder a un servicio de información de una entidad, en un espacio de tiempo en el que no se han sincronizado la base de datos primaria de usuarios entre operadores).</p> <p>Si el ciudadano no se encuentra registrado en la 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 el operador de su preferencia, y así ser un usuario del servicio.</p>	NA	
22	Bloqueo por intentos fallidos	Se deberá utilizar un mecanismo de anulación o bloqueo tras un cierto número de intentos infructuosos de introducir una contraseña.		Máximo 3 intentos fallidos permitidos
23	Registro de accesos fallidos	<p>Se mantendrá un registro de verificación de los accesos fallidos para analizar modelos de intentos de obtención directa de contraseñas en línea, esto por usuario y por grupos de usuarios.</p> <p>En el caso de los registros por grupos de usuarios se deberá tener en cuenta 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.</p>		
24	Delegación	En los casos en que se presente la situación en la que el usuario no se encuentra registrado con el operador contratado por la entidad, este deberá reenviar la solicitud al operador que enroló al usuario con el fin de que sea este último quien resuelva la solicitud de autenticación, en ese caso, se producirá una delegación de la autenticación, de modo tal que el operador en el que el usuario se encuentra registrado sea quien resuelva la solicitud de autenticación, y efectúe las etapas de intercambio de protocolo de Autenticación Electrónica, Validación de credenciales y aseveración		
25	Intercambio de protocolo de Autenticación Electrónica	Este flujo de información representa el intercambio de mensajes de protocolo para la autenticación del ciudadano por parte del operador	Los operadores deberán soportar el protocolo SAML 2.0 (UIT-T X.1141) y OpenId con OAuth 2.0 (UIT-T Y.2723).	No se permite el uso de protocolos adicionales.
26	Solicitud del nivel de garantía	Como parte de los metadatos enviados por el sistema de información de la entidad, deberá estar incluido el nivel de garantía requerido, con el fin que se le soliciten las credenciales adecuadas al trámite que se requiera acceder.		

	Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
27	Validación de credenciales	El operador deberá proveer un flujo de información que represente el intercambio de información entre el usuario y el operador para validar las credenciales presentadas contra las almacenadas.	El flujo de información deberá estar encriptado	
28	Verificación de atributos ciudadano	Para una adecuada validación se requiere que los atributos del ciudadano sean precisos y deben mantenerse actualizados.	Para ello 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, el operador debe realizar 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, sin reserva legal y que haga parte de la información de identidad requerida: nombres, apellidos, vigencia del documento de ciudadanía.	
29	Verificación de atributos representante legal privado	Debe permitir que una persona natural pueda hacer un trámite o servicio como representante legal de una persona jurídica de naturaleza privada.	El operador deberá validar que esta persona natural cuenta con esos permisos, para ello deberá validar la información para empresas privadas, contra el Registro Único Empresarial y Social de Confecámaras (RUES)	
30	Verificación de atributos representante legal público	Debe permitir que una persona natural pueda hacer un trámite o servicio como representante legal de una persona jurídica de naturaleza pública.	El operador deberá validar que esta persona natural cuenta con esos permisos, para ello deberá validar la información para Entidades públicas, contra el Sistema de Información y Gestión del Empleo Público (SIGEP).	
31	Aseveración	Debe permitir el intercambio de información entre el operador y una entidad en el cual notifica el resultado de la validación, informando si su autenticación es satisfactoria o no.		
32	Sesiones	El sistema de información deberá implementar una política de manejo y administración de tiempos de sesión en la cual el usuario debe ingresar periódicamente sus datos de acceso a la plataforma de autenticación electrónica a partir de un tiempo de inactividad. Adicionalmente, para operaciones críticas (i.e. Nivel de Garantía Alto) el usuario siempre deberá confirmar la operación por medio de su contraseña de acceso.		
33	Usar mecanismos de firma	El operador le deberá permitir al usuario firmar electrónicamente documentos.	Se deben seguir los lineamientos estipulados en el Decreto 2364 de 2012 y garantizando la autenticidad, integridad y disponibilidad del documento firmado. Para la firma de documentos, se exigirá el uso de credenciales correspondientes al nivel de garantía alto.	
34	Alertas	Deberá permitir a los usuarios aceptar, actualizar y revocar las autorizaciones de autenticación y envío de atributos a las entidades públicas a su elección. De igual forma podrán configurar alarmas y alertas cada vez que se utilicen sus credenciales de acceso.	<ul style="list-style-type: none"> o Un servicio de alarmas cuando se modifiquen los atributos de identidad de las personas o Un servicio de alarmas cuando se modifiquen las autorizaciones dadas por las personas o Un servicio de alarmas a los propietarios de la identidad sobre transacciones de autenticación o Un servicio de alarmas y alerta a los propietarios de la identidad sobre transacciones de autenticación interpretadas por el operador como una amenaza a sus credenciales e información 	
35	Administración del servicio de autenticación	Deberá permitir al usuario realizar todas las gestiones necesarias para administrar el servicio de Autenticación Electrónica.	<ul style="list-style-type: none"> o Configurar alertas de acceso o Visualizar registros de acceso o Descargar registros de acceso o Bloquear y desbloquear servicio 	
36	Gestionar credenciales de acceso	El operador le deberá permitir 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	<ul style="list-style-type: none"> o Consultar el estado y la vigencia de sus credenciales de acceso o Solicitar la revocación de credenciales o Renovar credenciales 	

	Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
37	Manejo de datos personales	Con el fin de generar mayores garantías en materia de privacidad de la información de identificación personal, los operadores y las entidades deben respetar un conjunto de principios.	<ul style="list-style-type: none"> o Solicitud de recolección y transmisión de datos mínimos, adecuados, pertinentes y no excesivos por parte del operador. o La información debe recabarse para fines específicos, explícitos y legítimos y no debe procesarse de manera incompatible con dichos fines o La información debe mantenerse durante no más tiempo del estrictamente necesario para los fines para los cuales se recabaron y/o procesaron o La información no debe intercambiarse entre aplicaciones para fines distintos a los solicitados por las personas o La información debe limitarse al mínimo necesario para un objetivo específico 	
38	Historial de credenciales	El operador mantendrá un registro de las credenciales. La duración de retención deberá especificarse en la política del operador.	El registro deberá contener mínimo: <ul style="list-style-type: none"> o Inscripción o Historia o Estado de cada credencial (incluida la revocación) 	

		MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estudio de mercado ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos	
Nombre del servicio		Carpeta Ciudadana	
Alcance del servicio		<p>La carpeta ciudadana es un servicio en donde las personas puedan recibir, custodiar y compartir de manera segura y confiable la información digital generada en su interacción con el Estado.</p> <ul style="list-style-type: none"> • Recibir documentos, comunicaciones y notificaciones. 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. • Firmar electrónicamente documentos 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 • Compartir documentos. 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 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. • Custodiar documentos: 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. 	
Característica requerida		Descripción del requerimiento	Característica mínima requerida
1	Configurar el servicio de Carpeta ciudadana	Permite la configuración y definición de parámetros que le permiten al usuario definir las reglas con las que desea ejecutar el servicio.	Permite la configuración de reglas del servicio o de información personal del usuario.
			Permite iniciar el servicio de la carpeta ciudadana.
			Permite el cambio de un operador de carpeta a cualquier otro operador habilitado, previa autorización del administrador del modelo.
			Permite bloquear de manera temporal el servicio de la carpeta ciudadana. De igual manera permite volver a habilitar el servicio
			Permite configurar el periodo de validez de cada uno de los tipos de documentos cargados por el ciudadano
			Permite configurar las reglas de conservación de cualquier documento como la conservación indefinida, destrucción, transferencia o mover entre carpetas.
			Permite configurar conjuntos de elementos de metadatos adecuados a las distintas clases de documento.
			Permite cancelar de manera definitiva el servicio de la carpeta ciudadana.
2	Gestionar documentos	Permite realizar las acciones que se pueden realizar sobre cada uno de los documentos que se encuentran en la carpeta ciudadana.	Permite establecer los mecanismos definidos por el usuario para la notificación de un trámite y el envío de avisos complementarios a las acciones de la carpeta
			Permite el cargue e incorporación de un nuevo documento a la carpeta ciudadana y que se encuentre en alguno de los siguientes formatos:
			· PDF/A simple y PDF/A firmado electrónicamente. (véase la norma ISO 19005);
			· XML simple y XML firmado electrónicamente.
			· Imágenes JPG, TIFF, PNG.(véase Especificación TIFF 6.0);(véase la norma ISO 15444 , requiere sólo si se admite el color);
			· Los formatos de los tipos de documentos admitidos deben ser ampliables en la medida que se introducen nuevos formatos.
			Permite asociar un documento a un esquema de organización de carpetas y a una o más carpetas;
			Permite incorporar información sobre el documento, fecha de creación y otros metadatos tales como: asunto, autor, fecha de creación, derechos de acceso, nivel de seguridad, metadatos de conservación de conformidad con las normas MOREQ, firmas electrónicas, versión, información sobre la encriptación, fechas de recibo y de envío etc.
			Permite la visualización de un documento cargado en la carpeta ciudadana.
			Permite mover un documento entre alguna de las carpetas configuradas en el espacio de trabajo de un ciudadano de forma manual o mediante un proceso automático.
			Permite eliminar de las carpetas un documento que será borrado en un tiempo configurado por el ciudadano.
			Permite quitar un documento de la carpeta ciudadana para liberar el espacio de almacenamiento que tiene cada usuario.
			Permite modificar el nombre de un archivo cargado en el modelo de carpeta ciudadana.
			Permite identificar un documento cargado en la carpeta ciudadana a través de una serie de parámetros de búsqueda.
			Permite la descarga local de un documento cargado en la carpeta ciudadana.
			Permite firmar electrónicamente un documento cargado en el sistema y que no contaba con ella.

Característica requerida		Descripción del requerimiento	Característica mínima requerida
3	Gestionar Carpetas	Permite la configuración y definición del esquema de organización de las carpetas en las que se almacenan los documentos.	Permite la creación de las carpetas que el ciudadano establezca para organizar sus documentos.
			Permite el cambio del nombre de una carpeta que se haya creado en el esquema de organización de un ciudadano.
			Permite ubicar una carpeta en otra ubicación del esquema de organización, copiando todo el contenido de la carpeta y colocándolo en la nueva ubicación establecida por el ciudadano
			Permite la eliminación de una carpeta del esquema de organización
			Permite la visualización de cuatro carpetas por defecto que no podrán ser modificadas por el ciudadano dentro de su esquema de organización. Estas carpetas son: 1. Recibidos, 2. Eliminado, 3. Compartidos, 4. Cargados
			- Recibidos
			- Eliminados
			- Compartido
			- Cargados por el usuario
			- Esquema de navegación propio que como mínimo contenga las siguientes por default: <Identificación, Académico, Laboral, Patrimonial, Fiscal, Servicios públicos, Salud
			Permite al usuario la creación de un conjunto de carpetas con los niveles que el considere para organizar los documentos que se encuentran almacenados en su espacio de carpeta ciudadana.
			Permitir al usuario la navegación y la exploración, en un entorno visual, de las carpetas y de la estructura del esquema de carpetas, así como la selección, la recuperación y la presentación de las carpetas y su contenido por medio de tal mecanismo.
			Permitir al usuario añadir o modificar los metadatos de un documento una vez cargado y soportar los metadatos de las carpetas del esquema de organización.
			Permite la creación y uso simultaneo de un esquema de organización de carpetas independiente para los documentos de un hijo del ciudadano o de una persona que se encuentre jurídicamente a su cargo.
4	Aportar o compartir documentos con tercero	Permite compartir documentos con otros usuarios de la carpeta ciudadana o aportarlos al trámite de una de las entidades.	Permite compartir un documento con uno o varios usuarios que se encuentran registrados y activos dentro del modelo de la carpeta ciudadana.
			Permite compartir un documento a una entidad para realizar un trámite configurado en el servicio de carpeta ciudadana.
			Permite la visualización de un documento que ha sido compartido por un ciudadano o una entidad.
			Permite cancelar el permiso de compartir un documento que había sido compartido con anterioridad.
			Permite bloquear a un usuario registrado y activo del servicio de carpeta ciudadana para que no me pueda compartir documentos
			Permite al usuario configurar los privilegios de acceso al documento que me han compartido. En este sentido permitirá establecer si el usuario al que se le comparte el documento podrá consultar, descargar, eliminar, o compartir entre otros.
			Permite la búsqueda de un documento compartido a través de una serie de filtros que me permitirán ubicar un documento compartido específico.
5	Usar servicios criptográficos	Permite implementar los diferentes servicios criptográficos que se pueden implementar sobre cada uno de los documentos que se encuentran dentro del servicio de la carpeta ciudadana.	Permite la firma electrónica de un documento por parte del usuario del servicio de carpeta ciudadana.
			Permite cifrar y descifrar un documento cargado en el servicio.
			Permite realizar el estampado de un documento cargado en el servicio.
			Permite verificar el certificado de un usuario de la carpeta ciudadana para poder realizar el proceso de firma de un documento.
			Permite realizar la verificación y validación de la firma electrónica de un documento cargado. Este proceso se podrá realizar de manera automática por el sistema una vez se cargue o se comparta un documento, o podrá realizarse de manera manual para los documentos que defina el usuario.
			Permite realizar el proceso de validación y verificación de las estampas cronológicas incluidas en un documento cargado en el servicio de la carpeta ciudadana.
6	Suscribir a servicios de envío de información de otras entidades	Permite que un ciudadano realice la suscripción a cualquiera de los trámites que ofrecen las entidades y que se encuentran dentro del modelo de la carpeta ciudadana.	Permite consultar el listado completo de servicios ofrecidos por todas las entidades que se encuentran dentro del modelo de la carpeta ciudadana.
			Permite consultar los términos y las condiciones del servicio que establecen cada una de las entidades para que el ciudadano pueda consultarlos y aceptarlos como parte de la confirmación de la suscripción.
			Permite al ciudadano ingresar su identificador único frente al servicio a suscribir. Este identificador dependerá de la configuración que hacen las entidades para cada uno de los servicios que ofrecen, por ejemplo, el número de la factura, su número de cuenta, su cedula de ciudadanía, etc.
			Permite consultar el estado de la suscripción de un ciudadano con relación a cualquiera de sus trámites.
			Permite la cancelación de la suscripción de un servicio para dejar de recibir documentos relacionados con el servicio que ofrece la entidad.
7	Gestionar Peticiones, Quejas y Reclamos - PQR's	Permite que un ciudadano realice peticiones de información a su operador, o que registre cualquier reclamación o descontento que tenga sobre el servicio ofrecido. En este sentido se hace importante aclarar que los operadores podrán integrar a la carpeta ciudadana los sistemas de PQR's con los que cuenten actualmente, en caso de no contar con ninguno de estos sistemas deberán garantizar el cumplimiento mínimo de las siguientes funcionalidades:	Permite consultar el listado de las diferentes peticiones, quejas o reclamos que ha radicado ante su operador.
			Permite radicar o registrar peticiones, quejas o reclamos que tenga el ciudadano con relación al servicio presentado por su operador.
			Permite consultar el estado en el que se encuentra su petición, queja o reclamo. De igual manera debe permitir consultar cualquiera de las respuestas que ha generado el operador con respecto a su solicitud.

Característica requerida		Descripción del requerimiento	Característica mínima requerida
8	Gestionar comunicaciones y documentos	Permite la gestión de las comunicaciones y documentos que realiza una entidad, dirigidas a los usuarios de un servicio publicado en la carpeta ciudadana	Permite el envío de comunicaciones documentos dirigidas a un usuario de la carpeta ciudadana que está suscrito a uno de los servicios que ofrece. En este punto se hace necesario aclarar que hace referencia cada uno de estos elementos:
			· Comunicaciones: Envío de información por parte de la entidad y que está orientada a comunicar algún tema relevante al ciudadano. En términos generales es información que no está asociada a un trámite o documento en particular, y está orientada más al conjunto general de usuarios de la entidad. Como ejemplo de comunicaciones se pueden identificar, resoluciones, calendarios del trámite, cambios o modificaciones del servicio, etc.
			· Documentos: Corresponde a archivos físicos resultantes de la ejecución de un trámite o servicio ofrecido por la entidad. Estos archivos pueden ser generados en sistemas transaccionales de la entidad y ser enviados a la carpeta ciudadana a través de alguno de los siguientes métodos:
			o Link: URL de referencia a un servicio web o a un repositorio de la entidad en donde se encuentra el archivo físico. Este tipo de documentos se encuentra en cada una de las entidades y no hace parte del almacenamiento de documentos definido en la carpeta ciudadana
			o Archivo físico: Corresponde a un archivo físico generado por la entidad como resultado de un trámite o servicio publicado en la carpeta ciudadana y que se encuentra en alguno de los siguientes formatos:
			§ PDF/A simple y PDF/A firmado electrónicamente.
			§ XML simple y XML firmado electrónicamente.
			§ Imágenes JPG, TIFF, PNG.
			Permite comunicar al ciudadano de los pasos o del resultado de alguno de los tramites solicitados a través de los diferentes medios definidos en la carpeta ciudadano y que el ciudadano ha configurado.
			Permite que una entidad pueda enviar comunicaciones o documentos a un grupo de usuarios de manera masiva.
9	Gestionar notificaciones	Permite la gestión de las notificaciones que realiza una entidad, dirigidas a los usuarios de un servicio publicado en la carpeta ciudadana.	Permite consultar los diferentes reportes relacionados con la información de los servicios prestados.
			Permite la consulta de las diferentes notificaciones generadas por una entidad y dirigidas a un usuario de la carpeta ciudadana que está suscrito a uno de los servicios que ofrece.
			Permite el envío de notificaciones entendidas como las comunicaciones oficiales por medio de las cuales las entidades podrán notificar al ciudadano de todos los resultados de un servicio o tramite de acuerdo a los lineamientos definidos en el código contencioso administrativo.
			Permite garantizar el proceso de acuse de recibido que existe entre una notificación enviada por la entidad (Iniciador) y el ciudadano que la recibe (Receptor) de acuerdo a la normatividad vigente que rige en esta materia.
			Permite que una entidad pueda enviar notificaciones a un grupo de usuarios de manera masiva.
			Permite consultar los términos y las condiciones del servicio de notificación con el fin que exista un acuerdo expreso entre el ciudadano y la entidad para la recepción de las notificaciones
			Permite consultar el estado de la suscripción del conjunto de notificaciones o de una notificación en particular para consultar los diferentes servicios de notificación que ha aceptado el ciudadano.
			Permite que el ciudadano cancele el servicio de notificaciones que ha aceptado de manera general o de algún trámite o documento específico.
			Permite la interoperabilidad de los sistemas de carpeta ciudadana con los sistemas transaccionales de las entidades para que estas entreguen las notificaciones resultado de un servicio o tramite de acuerdo a los lineamientos definidos en el código contencioso administrativo.
			Permite la interoperabilidad de los sistemas de carpeta ciudadana con los sistemas transaccionales de las entidades para que estas entreguen los documentos adjuntos a notificaciones resultado de un servicio o tramite de acuerdo a los lineamientos definidos en el código contencioso administrativo. Este servicio es completamente independiente al anterior, permitiendo la radicación independiente de documentos o de notificaciones.
			Permite la interoperabilidad de los sistemas de carpeta ciudadana con los sistemas transaccionales de las entidades para que estas entreguen las notificaciones resultado de un servicio o tramite de acuerdo a los lineamientos definidos en el código contencioso administrativo y sean almacenadas en un espacio seguro de la carpeta, ofreciéndole a las entidades la tranquilidad y confiabilidad de acceder siempre y en todo momento a las notificaciones generadas.
			Permite el envío de avisos a través de diferentes medios sobre las notificaciones que han sido enviadas por las entidades y que aún no han sido leídas por el ciudadano.

Característica requerida		Descripción del requerimiento	Característica mínima requerida
10	Gestionar servicio de carpeta ciudadana	Permite la configuración y definición de parámetros que le permiten al usuario de las entidades definir las reglas con las que desea interactuar con el servicio.	Permite iniciar el servicio de la carpeta ciudadana por parte de las diferentes entidades.
			Permite configuración y definición de parámetros que le permiten al usuario de las entidades definir las reglas con las que desea ejecutar el servicio.
			Permite la creación de usuarios internos por parte de la entidad para que puedan ingresar al servicio de carpeta ciudadana de acuerdo a los permisos y accesos que ellos consideren necesarios.
			Permite bloquear de manera temporal el servicio de la carpeta ciudadana desde la perspectiva de la entidad. De igual manera permite volver a habilitar el servicio.
			Permite cancelar de manera definitiva el servicio de la carpeta ciudadana por parte de una entidad.
			Permite que la entidad pueda configurar en el sistema un nuevo servicio o documento a ofrecer permitiendo establecer entre otros, la siguiente información: <ul style="list-style-type: none"> Nombre del trámite o del documento. Formato del documento (pdf, xml, tiff). Medio de entrega del documento (url, físico, ftp). Periodos de validez de un documento ofrecidos. Medio de notificación. Tamaño.
11	Consultar la información de la información del servicio	Permite la consulta de la información generada por la prestación de los diferentes servicios y tramites ofrecidos por cada una de las entidades.	Permite que la entidad pueda tener el detalle de la facturación del servicio ofrecido por el operador en un periodo de tiempo.
			Permite que la entidad pueda tener el detalle de la facturación del servicio ofrecido por el operador durante todo el tiempo de suscripción al servicio de carpeta ciudadana.
			Permite que la entidad pueda tener el detalle de los diferentes movimientos y transacciones realizados para cada uno de sus trámites o documentos ofrecidos en un determinado periodo de tiempo.
			Permite que la entidad pueda tener el detalle de los diferentes movimientos y transacciones realizados para cada uno de sus trámites o documentos ofrecidos durante todo el tiempo de suscripción al servicio de carpeta ciudadana.
12	Gestionar información de prestación de servicios	Permite al operador exponer a través de servicios web la información relacionada con la operación y la prestación de los servicios o tramites ofrecidos, mediante un conjunto de indicadores que han definido los administradores del modelo de carpeta ciudadana.	Permite exponer a través de un servicio web la información de los indicadores establecidos por los administradores del modelo de carpeta ciudadana y relacionados con: <ul style="list-style-type: none"> La información de los usuarios enrolados La información de las empresas suscritas al servicio La información de los tramites o documentos inmersos en el modelo de carpeta ciudadana La información de los servicios y las tarifas
			Permite exponer a través de un servicio web la información de los indicadores establecidos por los administradores del modelo de carpeta ciudadana y relacionados con las siguientes estadísticas de uso: <ul style="list-style-type: none"> No de usuarios enrolados Reporte de espacio total Espacio promedio Numero de documentos asociados a un usuario Información de servicios de interoperabilidad (Reportes) Reportes sobre la gestión de PQR's
13	Transferir carpetas ciudadanas a otro operador	Permite que un operador pueda hacer el traslado de la información de su carpeta ciudadana de un operador a otro. Esto se puede dar por que el usuario decide pasar de un operador a otro por mejores condiciones en el servicio, o por decisión de los administradores del modelo, cuando se deshabilita un operador.	Para que un operador pueda hacer el traslado de la información de una carpeta a otro operador deberá tener en cuenta al menos la siguiente información:
			Permite que un operador exporte los documentos y los metadatos asociados a la carpetas y a los documentos a otro operador, sin importar el estado en el que se encuentren los documentos.
			Permite que un operador elimine de manera física y definitiva la información de los documentos del ciudadano que está transfiriendo sus documentos a otro operador de modo que no se degrade el contenido ni la estructura de los documentos y se conserven todos los vínculos entre el documento, sus metadatos y las carpetas.
			Permite exportar de manera masiva la información de las entidades que se encuentran asociadas al servicio de la carpeta
			Permite exportar todo el registro de auditoría que se ha realizado sobre las transacciones y movimientos realizados por el ciudadano al que se le está transfiriendo la carpeta.
			Permite exportar las configuraciones del usuario al igual que las configuraciones de cada una de las entidades
14	Registrar o habilitar entidad	Permite registrar la información de las diferentes entidades que ofrecerán los documentos, o tramites al interior de la carpeta ciudadana de un operador, permitiendo la gestión de la entidad como uno de sus clientes.	Permite al operador registrar los datos básicos de una entidad que se incluirá dentro del modelo de carpeta ciudadana
			Permite al operador registrar los datos de contacto técnico o funcional de una de las entidades que ha registrado dentro de la carpeta ciudadana.
			Permite al operador registrar los datos de las tarifas de cada uno de los servicios de las entidades que ha registrado dentro de la carpeta ciudadana.
			Permite al operador registrar el alta de una entidad para que pueda iniciar a ofrecer sus trámites o documentos dentro del modelo de la carpeta ciudadana.


Característica requerida		Descripción del requerimiento	Característica mínima requerida
15	Interacción entre operadores	Permite al operador identificar los diferentes servicios web que deberá consumir con el fin de interactuar con el sistema del administrador del modelo de carpeta ciudadana, así como interactuar con cada una de las carpetas de los diferentes operadores habilitados en el modelo. Entre los diferentes servicios se pueden identificar los siguientes:	Permite consumir el servicio web que le devolverá el listado de usuarios enrolados en las diferentes sistemas de carpeta ciudadana de los diferentes operadores
			Permite consumir el servicio web que le devolverá el listado de todas las entidades que se encuentren suscritas al servicio de carpeta ciudadana de los diferentes operadores
			Permite consumir el servicio web que le devolverá el listado de los diferentes tipos de documentos configurados por las entidades suscritas al modelo de carpeta ciudadana.
			Permite consumir el servicio web que les devolverá la autorización de ingreso a los operadores que estén habilitados dentro del modelo de carpeta ciudadana.
			Permite consumir el servicio web que maneja los procesos de autenticación y que son ofrecidos por los operadores de Autenticación electrónica para garantizar el ingreso de los ciudadanos a los sistemas de carpeta ciudadana.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Nombre del servicio		Interoperabilidad - Capa Capacidades de infraestructura		
Alcance del servicio		<p>Todos los elementos de infraestructura necesarios para el despliegue y ejecución de los programas, plataformas, servidores de aplicaciones, contenedores y los entornos de ejecución, aplicaciones empaquetadas, máquinas virtuales, etc., que se encuentran en el hardware y son necesarios para apoyar la PDI. Incluye:</p> <ul style="list-style-type: none"> - Toda la infraestructura de software y hardware necesario para soportar la PDI y sus componentes en tiempo de ejecución y tiempo de diseño - Todos los elementos de alojamiento operativo y tiempo de ejecución de los componentes del sistema físicos subyacentes - Todos los activos necesarios para dar soporte a la funcionalidad de los servicios en la PDI, incluyendo aplicaciones empaquetadas o personalizadas, nuevos servicios, los servicios creados a través de la composición o la orquestación, servicios de infraestructura, etc. 		
Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
1	Tecnología	El Operador debe suministrar el servicio utilizando tecnología que le permita cumplir los ANS y características técnicas definidas en esta ficha.	NA	NA
2	Tipo de equipos	El Operador debe suministrar el servicio utilizando equipos que le permitan cumplir los ANS y características técnicas definidas en esta ficha.	NA	NA
3	Conexión a NAP Colombia	Debe incluir conexión al NAP Colombia garantizando el ancho de banda contratado.	NA	NA
4	Entorno de Ejecución	<p>Esta categoría de capacidades es necesaria para proporcionar un entorno de ejecución que representa la infraestructura en tiempo de ejecución para la PDI. Esto incluye la capacidad para soportar tanto los componentes necesarios para sostener la funcionalidad del servicio y las operaciones necesarias para ejecutar los componentes de la PDI. Esto incluye capacidades para el hardware, componentes del sistema operativo.</p> <ul style="list-style-type: none"> -Capacidad de soportar plataformas para el alojamiento en tiempo de ejecución de los servicios de la PDI -Capacidad para soportar los tiempos de ejecución de los programas informáticos necesarios para correr la implementación del servicio de PDI -Capacidad para soportar los tiempos de ejecución y el software necesarios para desplegar las implementaciones de servicios en la PDI -Capacidad de soportar el entorno de software en el que se ejecuta los servicios de las entidades sobre la PDI 	Una (1) instancia	Pueden existir tantas instancias como sean requeridas dependiendo de los formatos de mensaje, protocolos de comunicación y demás características asociadas a las tecnologías de exposición de Trámites y Servicios de las Entidades hacia el exterior de la PDI.
5	Servicios de infraestructura o de virtualización	<p>Esta categoría de capacidades proporciona la infraestructura subyacente, como la potencia de computación, red, almacenamiento, etc., en forma nativa o una virtualizado.</p> <ul style="list-style-type: none"> -Capacidad de proporcionar la infraestructura necesaria para la PDI -Capacidad de proporcionar la infraestructura de una manera virtualizada a las plataformas -Capacidad de proporcionar la infraestructura de una manera virtualizada para dar servicio a la implementación de microservicios a las entidades -Capacidad de gestión de la infraestructura y la infraestructura virtualizada -Capacidad para proporcionar un único punto de control para la seguridad de la operacionales de la infraestructura 	NA	NA

ANS		Descripción	Medición
1	Disponibilidad	<p>La disponibilidad se mide usando la siguiente ecuación:</p> $\left(1 - \frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes facturado} \times 24 \text{ horas} \times 60 \text{ minutos}}\right) \times 100\%$ <p>La indisponibilidad es el número total de minutos, durante el mes facturado, en los que el servicio de intercambio de datos en la PDI no está disponible, dividido en el número total de minutos en el mes facturado.</p> <p>La medición la hace el Operador monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el Operador para que puedan ser consultados por la Entidad Compradora o MinTIC en cualquier momento durante la duración del servicio. La información mantenida por el Operador le debe permitir a la Entidad Compradora o MinTIC verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.</p>	<p>Disponibilidad exigida >=99.98% mensual</p> <p>Penalidad por no conformidad - Descuento en facturación 99.9%<=Disponibilidad<99.98%: 10% de descuento sobre el costo del servicio. 99.8%<=Disponibilidad<99.9%: 20% de descuento sobre el costo del servicio. 99.7%<=Disponibilidad<99.8%: 50% de descuento sobre el costo del servicio. Disponibilidad<99.7%: 100% de descuento sobre el costo del servicio.</p>
2	RTO	<p>El RTO por sus siglas en inglés es Recovery Time Objective o en español Tiempo Objetivo de Recuperación.</p> <p>El RTO es el tiempo máximo que el que la PDI puede estar fuera de servicio una vez se ha producido una Interrupción. Una Interrupción se define como una pérdida total del servicio que implica que no hay intercambio de datos sobre la PDI.</p> <p>La medición la hace el Operador monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el Operador para que puedan ser consultados por la Entidad Compradora o MinTIC en cualquier momento durante la duración del servicio. La información mantenida por el Operador le debe permitir a la Entidad Compradora o MinTIC verificar los tiempos de recuperación históricos de las Interrupciones que se han presentado en meses anteriores y en el mes en curso.</p>	<p>RTO <= 8 minutos</p> <p>Penalidad por no conformidad - Descuento en facturación 8 min<RTO<=15 min: 10% de descuento sobre el costo total de este servicio. 15 min<RTO<=25 min: 20% de descuento sobre el costo total de este servicio. 25 min<RTO<=45 min: 50% de descuento sobre el costo total de este servicio. 45 min<RTO: 100% de descuento sobre el costo total de este servicio.</p>
3	Interrupciones máximas	<p>El ANS Interrupciones máximas hace referencia a el número máximo de Interrupciones durante el mes facturado.</p> <p>Una Interrupción se define como una pérdida total del servicio que implica que no hay intercambio de datos sobre el enlace a Internet.</p> <p>La medición la hace el Operador monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el Operador para que puedan ser consultados por la Entidad Compradora y MinTIC en cualquier momento durante la duración del servicio. La información mantenida por el Operador le debe permitir a la Entidad Compradora y MinTIC verificar el número de Interrupciones histórico de meses anteriores y el número de Interrupciones acumuladas para el mes en curso.</p>	<p>Interrupciones máximas en un mes 1 Interrupción.</p> <p>Penalidad por no conformidad - Descuento en facturación 2 Interrupciones: 20% de descuento sobre el costo de este servicio. 3 Interrupciones: 50% de descuento sobre el costo de este servicio. >4 Interrupciones: 100% de descuento sobre el costo de este servicio.</p>

ANS		Descripción	Medición
4	MTBF	<p>El MTBF por sus siglas en inglés es Mean Time Between Failures o en español Tiempo Medio Entre Fallas.</p> <p>El MTBF es un indicador de confiabilidad definido como el promedio aritmético acumulado del tiempo entre Fallas asumiendo que el enlace a Internet se recupera de forma inmediata cuando se produce la Falla.</p> <p>Una Falla se define como una degradación del servicio de interoperabilidad con respecto a las condiciones pactadas para el modelo de Servicios Digitales.</p> <p>La medición la hace el Operador monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el Operador para que puedan ser consultados por la Entidad compradora y MinTIC en cualquier momento durante la duración del servicio. La información mantenida por el Operador le debe permitir a la Entidad Compradora y a MINTIC verificar el MTBF acumulado en cualquier momento durante la prestación del servicio.</p> <p>Nota aclaratoria: Una Falla es diferente a una Interrupción. La Falla esta asociada a la confiabilidad del servicio y la Interrupción esta asociada a la disponibilidad del servicio.</p>	<p>MTBF >4320 horas</p> <p>Penalidad por no conformidad - Descuento en facturación 2160 horas <= MTBF < 4320 horas: 10% de descuento sobre el costo total de este servicio. 1440 horas <= MTBF < 2160 horas: 20% de descuento sobre el costo total de este servicio. 1080 horas <= MTBF < 1440 horas: 50% de descuento sobre el costo total de este servicio. MTBF<1080 horas: 100% de descuento sobre el costo total de este servicio.</p>
5	Latencia	<p>Mide el tiempo promedio en el mes ,por servicio, que tarda una transacción en ir y volver entre los siguientes puntos:</p> <ul style="list-style-type: none"> - Desde la Entidad Compradora hasta el Operador. - Desde el Operador hasta la Entidad Consumidora. <p>La medición la hace el Operador a través de muestras diarias tomadas durante todo el tiempo de servicio. Los resultados de las muestras son mantenidas por el Operador para que puedan ser consultadas por la Entidad Compradora y MinTIC durante la duración del servicio con el fin de verificar la latencia promedio histórica de meses anteriores y el valor promedio acumulado para el mes en curso.</p> <p>En los casos en que la Entidad Compradora sospeche que existe una Falla, el Operador debe medir y reportar la latencia en el momento y con la frecuencia que la Entidad Compradora lo requiera.</p>	<p>Latencia máxima < 16 ms < 36 ms < 50 ms</p> <p>Penalidad por no conformidad - Descuento en facturación Latencia máxima < Latencia <= Latencia máxima * (1.3): 10% de descuento sobre el costo del servicio Latencia máxima * (1.3)< Latencia <= Latencia máxima * (1.6): 20% de descuento sobre el costo del servicio Latencia máxima * (1.6)< Latencia <= Latencia máxima * (2): 50% de descuento sobre el costo del servicio Latencia >Latencia máxima *(2): 100% de descuento sobre el costo del servicio</p>
6	Ancho de banda	<p>El ancho de banda corresponde al rango de frecuencias que ocupan los datos transmitidos por el enlace sin que se presente distorsión o pérdida de información, para proveer o consumir los servicios de información.</p> <p>La medición la hace el Operador una vez lo solicite la Entidad Compradora o MinTIC por el tiempo y con la frecuencia que la Entidad Compradora o MinTIC lo requiera. Los resultados de la medición deben ser mantenidos por el Operador para que puedan ser consultadas por la Entidad Compradora o MinTIC durante la duración del servicio.</p>	<p>Ancho de banda Debe ser mayor o igual al ancho de banda contratado</p> <p>Penalidad por no conformidad - Descuento en facturación Si se evidencia una reducción del 10% sobre el ancho de banda contratado: 40% de descuento sobre el costo del servicio Si se evidencia una reducción del 20% sobre el ancho de banda contratado: 50% de descuento sobre el costo del servicio Si se evidencia una reducción >= 30% sobre el ancho de banda contratado: 100%</p>
8	Calidad y oportunidad en los reportes entregados	<p>El Operador debe garantizar la calidad de la información que contienen los reportes que entrega a la Entidad Compradora y a MINTIC.</p> <p>Con el fin de garantizar la calidad de los reportes se define el número máximo de</p>	<p>Devoluciones máximas por cada reporte <= 2 devoluciones de un mismo reporte</p> <p>Penalidad por no conformidad - Descuento en facturación</p>

		MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estudio de mercado ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos	
Nombre del servicio		Interoperabilidad - Capa Componentes del servicio	
Alcance del servicio		<p>Se encarga de la gestión de los servicios de información de las entidades en tiempo de ejecución o el despliegue de la solución en la plataforma de interoperabilidad y en particular de:</p> <ul style="list-style-type: none"> - soportar la exposición de un servicio de una manera compatible con los estándares definidos en el lenguaje común de intercambio de información favoreciendo la interoperabilidad y haciendo uso de protocolos como son (SOAP / REST / J2EE, etc.) - Capacidad para exponer el servicio a través de integración de la plataforma de interoperabilidad con los la infraestructura y sistemas de información subyacente en las Entidades en el que reside la funcionalidad de servicio. - Posibilidad de publicar e implementar el componente de servicio en sí: exponer servicios de manera interoperable; publicar la información de contrato de servicio de manera interoperable y compatible con los estándares; desplegar el servicio 	
Característica requerida		Descripción del requerimiento	Característica mínima requerida
1	Implementación del servicio	<ul style="list-style-type: none"> - Realizar las actividades relacionadas para el análisis, diseño e implementación de servicios para interoperabilidad, entre ellas se consideran las necesarias para la conexión a fuentes de datos, extracción, transformación, publicación o consumo de datos o información, así como, combinar, ensamblar servicios, conectar aplicaciones, servicios web y cualquier otro tipo de mecanismos de interoperables a través de adaptadores, todo lo anterior en concordancia con lo definidos en el marco de interoperabilidad y el lenguaje común de intercambio de información 	ver hoja (A1. Desarrollo sis información)
2	Publicación y exposición del servicio	<ul style="list-style-type: none"> - Apoyar la exposición y publicación de servicios de la Entidad, incluyendo se contrato o definición - Proporcionar la información sobre los metadatos del servicio a los componentes de la plataforma de interoperabilidad para su integración con las demás capas o entre ellas calidad del servicio, consumo y repositorio de servicio 	<ul style="list-style-type: none"> - Soporta tanto la publicación de servicios Web SOAP estándar, como la de servicios REST, XML-RPC y sus correspondientes descriptores o definiciones, también debe darse soporte a protocolos de transporte como HTTP, SMTP, FTP
3	Despliegue del servicio	<ul style="list-style-type: none"> - Proporcionar el despliegue físico del servicio en la plataforma de interoperabilidad en la condiciones pactadas con la Entidad 	<ul style="list-style-type: none"> - Ensamblar los artefactos necesarios para habilitar los servicios de la Entidad y disponerlos para su invocación y consumo
4	Invocación de servicios	<ul style="list-style-type: none"> - Soportar la invocación en tiempo de ejecución del servicio de la entidad 	<ul style="list-style-type: none"> - Soporta tanto la invocación de servicios Web SOAP estándar, como la de servicios REST, XML-RPC, también debe darse soporte a protocolos de transporte como HTTP, SMTP, FTP
5	Agrupación de servicios	<ul style="list-style-type: none"> - Soportar la integración de los servicios de las Entidades a la Plataforma de interoperabilidad. 	<ul style="list-style-type: none"> - Soportar la integración de los servicios de las Entidades a la Plataforma de interoperabilidad. - Convertir la descripción del servicio a invocaciones del servicio que estén soportados por la plataforma de interoperabilidad (en el caso de un servicio web WSDL, la conversión del descriptor WSDL a la invocación de servicio deseada) - Transformar la entrada y salida de los servicios a estándares compatibles para el consumo de las entidades - Hacer cumplir las políticas de control de acceso

Interoperabilidad como Servicio (IOAAS) - Desarrollo de servicios de información Servicio que puede ser tomado de forma opcional por las entidades		
Características		Descripción del requerimiento mínimo y/o tipo de tecnología
El proveedor debe definir una arquitectura de solución para el servicio de información	IOAAS_DEV_001	El proveedor debe definir una Arquitectura de solución para el servicio desarrollado, aplicando las Arquitecturas de referencia definidas en la entidad. LI.SIS.04 - Arquitecturas de solución de sistemas de información
El proveedor debe transferir a la institución los derechos patrimoniales sobre los productos desarrollados	IOAAS_DEV_002	El proveedor debe transferir a la institución los derechos patrimoniales sobre los productos desarrollados. LI.SIS.06 - Derechos patrimoniales sobre los sistemas de información
El proveedor debe proveer y seguir una metodología de referencia para el desarrollo de los servicios de información	IOAAS_DEV_003	El proveedor debe contar con metodologías de referencia que definan los componentes principales de un proceso de desarrollo del software, que considere sus fases o etapas, las actividades principales y de soporte involucradas, roles y responsabilidades, y herramientas de apoyo al ciclo de vida, así como los ámbitos de aplicación. Las metodologías de referencia deben dar cobertura a todas las soluciones de software de los sistemas de información que la institución construya o adapte, independientemente de su tecnología. Las metodologías deben incorporar mejores prácticas de la industria.
El servicio de información desarrollado debe funcionar sobre la Arquitectura de información definida para la institución	IOAAS_DEV_004	El servicio de información desarrollado debe funcionar sobre la Arquitectura de información definida para la institución y debe dar soporte a los componentes de información allí incluidos. LI.SIS.10 - Implementación de Componentes de información
El proveedor debe contar y ejecutar un plan de pruebas que cubra lo funcional y lo no funcional.	IOAAS_DEV_005	El proveedor debe contar y ejecutar un plan de pruebas que cubra lo funcional y lo no funcional. La aceptación de cada una de las etapas de este plan debe estar vinculada a la transición del servicio de información a través de los diferentes ambientes. LI.SIS.14 - Plan de pruebas durante el ciclo de vida de los sistemas de información
Plan de capacitación y entrega del servicio de información	IOAAS_DEV_006	El proveedor debe contar y ejecutar planes de capacitación y entrenamiento para el personal que designe la entidad, incluyendo al menos los siguientes temas: - Capacitación técnica de la solución. - Instalación de la solución. - Errores comunes


Características		Descripción del requerimiento mínimo y/o tipo de tecnología
El proveedor debe disponer de ambientes independientes y controlados destinados para desarrollo, pruebas y operación	IOAAS_DEV_007	<p>El proveedor debe disponer de ambientes independientes y controlados destinados para desarrollo, pruebas y operación, del servicio de información, y debe aplicar mecanismos de control de cambios de acuerdo con las mejores prácticas.</p> <p>LI.SIS.16 - Ambientes independientes en el ciclo de vida de los sistemas de información</p>
El proveedor debe elaborar y entregar a la entidad la documentación de usuario, técnica y de operación, debidamente actualizada.	IOAAS_DEV_008	<p>El proveedor debe elaborar y entregar a la entidad la documentación de usuario, técnica y de operación, debidamente actualizada, que asegure la transferencia de conocimiento hacia los usuarios, hacia la dirección de Tecnologías y Sistemas de la Información o quien haga sus veces y hacia los servicios de soporte tecnológico.</p> <p>LI.SIS.16 - Manual del usuario, técnico y de operación de los sistemas de información</p>
El proveedor debe aplicar un proceso formal de gestión de requerimientos	IOAAS_DEV_009	<p>El proveedor debe aplicar un proceso formal de manejo de requerimientos, que incluya la identificación, la especificación y el análisis de las necesidades funcionales y no funcionales, la definición de los criterios de aceptación y la trazabilidad de los requerimientos a través del ciclo de vida de desarrollo del servicio de información.</p> <p>LI.SIS.12 - Análisis de requerimientos de los sistemas de información</p>
El proveedor debe incorporar componentes de seguridad en el servicio de información.	IOAAS_DEV_010	<p>En el diseño del servicio de información el proveedor debe incorporar aquellos componentes de seguridad para el tratamiento de la privacidad de la información, la implementación de controles de acceso, así como los mecanismos de integridad y cifrado de la información.</p> <p>LI.SIS.21 - Seguridad y privacidad de los sistemas de información</p>
En el diseño del servicio de información, el proveedor debe tener en cuenta los requerimientos de la institución, las restricciones funcionales y técnicas, y los atributos de calidad.	IOAAS_DEV_011	<p>En el diseño del servicio de información, el proveedor debe tener en cuenta los requerimientos de la institución, las restricciones funcionales y técnicas, y los atributos de calidad.</p> <p>LI.SIS.21 - Criterios no funcionales y de calidad de los sistemas de información</p>
El proveedor debe tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la auditoría y trazabilidad de las acciones realizadas.	IOAAS_DEV_012	<p>En el diseño del servicio de información, el proveedor debe tener en cuenta mecanismos que aseguren el registro histórico para poder mantener la auditoría y trazabilidad de las acciones realizadas.</p> <p>LI.SIS.23 - Auditoría y trazabilidad de los sistemas de información</p>


	MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estudio de mercado ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos
--	--

Nombre del servicio		Interoperabilidad - Capa de servicios		
Alcance del servicio		<p>Contiene todos los servicios que se definen dentro de la plataforma de interoperabilidad, se encarga de contener las descripciones de los servicios de las entidades, así como la definición de la infraestructura tecnológica para su despliegue y ejecución. También contienen la información relacionada al contrato de servicio y las descripciones que se utilizarán durante la ejecución.</p> <p>En particular, desde la perspectiva de diseño incluye los activos del servicio como las descripciones, contratos y políticas ligadas al servicio. También se definen las capacidades para su ejecución y despliegue, se debe tener en cuenta que la creación de instancias que habilita estas capacidades están alojados en la capa de infraestructura.</p>		
Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
1	Definición de servicio	Proporcionar la posibilidad de definir la descripción del servicio	Capacidad para definir los servicios en términos de descripciones / contratos. Un servicio se representa típicamente en un lenguaje estándar de descripción (por ejemplo, WSDL) que describe sus interfaces accesibles (por ejemplo, los métodos o funciones firmas). Por lo general, la información del servicio se publica en la capa de Gobierno para la búsqueda y reutilización.	
2	Habilitador de ejecución del servicio	Permitir la prestación, invocación y consumo del servicio a las Entidades consumidoras, desacoplándolo de la implementación en la Entidad proveedora, permitir el versionamiento del servicio.	<ul style="list-style-type: none"> - Apoyar la resolución de las versiones de los servicios de las Entidades para dar soporte a las versiones sucesivas - Permitir la invocación, gestión y almacenamiento de los diferentes servicios de la Entidad - Permitir interactuar al servicio de la Entidad con las capacidades provistas por la Plataforma de interoperabilidad, especialmente lo relacionado con la integración - Permitir enlazar el servicio expuesto en la Plataforma de interoperabilidad, con la implementación dada por la Entidad proveedora - Permitir el alojamiento de servicios de las Entidades Proveedoras de información - Permitir verificar el estado del servicio de la Entidad 	
3	Gestor de políticas	Proporciona la capacidad de administrar y hacer cumplir las políticas asociadas a los servicios. (días y horas de ejecución, derechos de acceso, nivel de seguridad)	<ul style="list-style-type: none"> - Capacidad para soportar la integración con las capas de calidad del servicio donde se describen las políticas de gobierno y calidad que debe cumplir el servicio de la Entidad - Hacer cumplir las políticas dentro de la capa. - Apoyar la auditoría y el registro del uso de los servicios, mediante normas como CBE y XDAS para asegurar que los datos son consistentes e interoperables - Apoyar la vigilancia, auditoría, cumplimiento y gobierno durante la ejecución de un servicio 	
4	Controlador de acceso	Ofrece la posibilidad de gestionar el acceso a los servicios	<ul style="list-style-type: none"> - Capacidad de apoyar la integración con la seguridad en el control de acceso definido en los descriptores del servicios de las capas de gobierno y calidad del servicio 	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Nombre del servicio		Interoperabilidad - Capa de Proceso (Trámite)		
Alcance del servicio		<p>Cubre la representación de un proceso o trámites mediante la composición de servicios, 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>Esta capa incluye el flujo de intercambio de información entre los participantes, los recursos y los procesos en una variedad de formas para lograr el objetivo del trámite o proceso de negocio. La mayor parte de la información intercambiada también puede incluir mensajes que no son estructurados y no transaccionales. La lógica de trámite o proceso de negocio se utiliza para formar el flujo de servicio como tareas en paralelo o secuenciales, sincrónicas o asincrónicas basados en reglas, políticas y otros requisitos.</p>		
Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
1	Definición del trámite / proceso	Capacidad se requerida para la definición de los procesos de trámite / flujo operativo	- Posibilidad de definir los trámites o procesos que representan el comportamiento dinámico del negocio	
2	Controlador de eventos	Capacidades gestiona los eventos de proceso en el contexto de un trámite, tales como emisores de eventos / publicación y suscripción / escucha a eventos de trámite.	- Posibilidad de detectar, emitir y escuchar los eventos generados en el contexto de los trámites o procesos de negocio de las Entidades	
3	Ejecutor del proceso/Trámite	Capacidades que permite el BPM y ayuda a comprender los procesos de trámite en el entorno de ejecución utilizando estándares como BPML, SCA, etc.	<ul style="list-style-type: none"> - Realizar e implementar los procesos del trámite en el entorno de ejecución - Crear y gestionar las instancias individuales de los servicios de las entidades en un proceso / trámite - Ejecutar las instancias de un trámite o proceso, sus sub-procesos y actividades - Gestionar las interacción en los trámites / procesos con los seres humanos 	
4	Gestor de información del proceso	Capacidad que manejar las necesidades de información en un trámite, tales como su estado, transformación los datos en el flujo del proceso, y el mantenimiento de un depósito de activos que indique los resultados de la ejecución del trámite	<ul style="list-style-type: none"> - Gestionar el contexto y estado de un proceso o trámite - Transformar los datos que fluyen a través de un procesos de negocio basados en sus necesidades 	
5	Gestor de reglas	Capacidad que define y gestiona los puntos de decisión y reglas asociadas dentro de un trámite	<ul style="list-style-type: none"> - Posibilidad de gestionar las relaciones entre el trámite o proceso de negocio y los requerimientos no funcionales en el flujo de procesos - Aislar/encapsular las decisiones o reglas que afectan un servicio de la entidad de las decisiones o reglas del flujo de procesos en el que participa 	
6	Integrador de servicios	Capacidad de integrar varios servicios de las entidades componiéndolo como un trámite o proceso de negocio y exponerlo como un único servicio	<ul style="list-style-type: none"> - Hacer disponible un trámite o proceso de negocio que se compone de servicios de las entidades como un servicio único - Posibilidad de programar la ejecución de un trámite o proceso de negocio 	
7	Seguridad y Política de cumplimiento	Capacidades que permiten el control de acceso y la ejecución de políticas en los trámites y procesos de negocio.	<ul style="list-style-type: none"> - Definir políticas, hacerlas cumplir, y verificar el cumplimiento de los elementos del proceso con el conjunto de políticas predefinidas - Controlar el acceso a un flujo de proceso o trámite tanto en el diseño como durante su tiempo de ejecución 	
8	Proceso de Seguimiento y Gestión	Capacidades para monitorear y gestiona los trámites y procesos de negocio, identificar los cuellos de botella y optimiza la asignación de la carga de trabajo a los componentes y capas de la plataforma de interoperabilidad	- Monitorear el trámite o proceso de negocio insertando los puntos en los que pueden ser reunidas métricas, identificar cuellos de botella y optimizar las tareas de carga de trabajo de los servicios de las entidades	

		MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estudio de mercado ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos		
Nombre del servicio		Interoperabilidad - Capa de Consumo		
Alcance del servicio		Esta capa es el punto en el cual las Entidades consumidoras interactúan con la plataforma de interoperabilidad, permite soportar el conjunto de funcionalidades de la plataforma independiente del cliente y el canal. sirve como entrada para todos los consumidores externos como pueden ser otros sistemas, otras plataformas SOA, los consumidores de servicios de nube, e inclusive usuarios humanos.		
Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
1	Consumo de servicios	Capacidad que aborda el apoyo de la interacción con los consumidores (Capturar la entrada y entregar la respuesta)	<ul style="list-style-type: none"> - Permitir el consumo (uso) de la plataforma, a través de un programa o una persona que solicita un servicio de las Entidades - Apoyar la interacción e integración de los consumidores; es decir, la capacidad de capturar la entrada del usuario (consumidor) y proporcionar la respuesta 	
2	Servicios de presentación	Conjunto de capacidades que aborda el apoyo de los servicios permitiendo tener una interfaz de usuario de la plataforma, incluyen una interfaz de usuario para los servicios de las entidades, configuración, composición y control, adicionalmente permite la construcción de interfaz de usuario centrada en los consumidores de los servicios de la plataforma.	<ul style="list-style-type: none"> - Permitir la creación de una interface de usuario para el consumo de servicios - Permitir la composición de servicios para la construcción de tramites o procesos de negocio de forma visual en una interfaz de usuario con un formato adecuado para interactuar - Capacidad de proporcionar lógica de navegación y el flujo para el procesamiento de las interacciones de los consumidores (control de la presentación) - Permitir la configuración de los componentes de la plataforma para establecer los escenarios de consumo del servicio de la Entidad (Reglas, seguridad, políticas, etc. ...) 	
3	Integración con el Backend	Capacidad que se refiere a la integración con sistemas back-end y heredados usando servicios y transformado su información para su incorporación.	<ul style="list-style-type: none"> - Capacidad para mediar los servicios de otras capas de la plataforma, como la capa de procesos (tramite) y la capa de integración con la capa de Consumidor - Capacidad para apoyar la traducción de los datos / contenido de un formato soportado por el usuario o sistema cliente al formato de Lenguaje Común de Intercambio de Información requerido por la plataforma 	
4	Caché y streaming de contenido	capacidades apoya de almacenamiento en búfer de información de manera temporal y el rendimiento, y es compatible con el funcionamiento de la capa de Consumidor.	<ul style="list-style-type: none"> - Capacidad de manejo de streaming de contenido - Capacidad de realizar manejar cache en la interacción del flujo de datos para mejorar el rendimiento y la calidad del servicio de la entidad. 	
5	Seguridad y privacidad	Capacidades que dan soporte y apoyo a la calidad del servicio, protección de información, y seguridad.	<ul style="list-style-type: none"> - Proporcionar acceso a las capacidades de autenticación / autorización (habilitado a través de políticas y reglas) - Filtrar las solicitudes para controlar el acceso a la los componentes y capacidades de la plataforma - Capacidad para supervisar el uso de los componentes de la capa del Consumo 	
6	Acceso	Permite el intercambio de datos y metadatos a través de las capas de la plataforma, como atributos de calidad de servicio, atributos definen las normas comunes para ser utilizados a través de las capas, aplicación de reglas y políticas	<ul style="list-style-type: none"> - Permitir el acceso a datos y metadatos de los servicios 	

		MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estudio de mercado ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos	
Nombre del servicio		Interoperabilidad - Capa de integración	
Alcance del servicio		Capa que proporciona las capacidades de mediación de servicios, incluye la transformación, enrutamiento, conversión de protocolo para el transporte de las solicitudes de la entidad al proveedor de servicio correcto, las capacidades en esta capa deben permitir la integración de servicio mediante adaptadores, así como la interacción, virtualización y el procesamiento de mensaje para los servicios.	
Característica requerida		Descripción del requerimiento	Característica mínima requerida Característica máxima requerida
1	Comunicación, interacción e integración del servicio	Capacidades que permiten enrutar las solicitudes al operador correcto, después de las transformación al mensaje y las conversiones de protocolos necesarias para conectar al consumidor con el proveedor de información y su infraestructura. También ofrece la posibilidad de descubrir los servicios y apoyar su virtualización para que un cambio sobre el servicio o su descripción puedan realizarse sin afectar a los consumidores	<ul style="list-style-type: none"> - Capacidad para permitir a un consumidor de servicios conectar e interactuar con los operadores y proveedores de servicios - Capacidad para manejar las solicitudes y respuestas al servicio - Capacidad de soportar la comunicación a través de múltiples protocolos - Capacidad de soportar varias formas de mensajería como: one-way, pub-sub, request-response - Capacidad para enrutar los mensajes al proveedor de servicio correcto - Capacidad para transformar formatos de protocolo; por ejemplo, de SOAP / HTTP a SOAP / Message Queue o SOAP / JMS - Capacidad de enlazar sistemas que no admite directamente las interacciones con servicios, así como servicios que se pueden ofrecer en entornos heterogéneos - Capacidad de almacenar y reenviar mensajes utilizando una cola de mensajes
2	Procesamiento de mensajes	Capacidades para llevar a cabo las transformación necesarias al mensaje para conectar al consumidor y proveedor de servicios y para publicar y suscribir los mensajes y eventos de forma asíncrona.	<ul style="list-style-type: none"> - Capacidad de transformar formatos de datos, de formatos independientes o de la industria a Lenguaje Común de Intercambio de Información y viceversa - Capacidad de propagar los eventos de los proveedores a los consumidores - Capacidad de agregar (mensajes o datos) a los servicios y proveedores de servicio
3	Calidad de Servicio	Soporte al manejo de las transacciones, excepciones y otros requerimientos no funcionales.	<ul style="list-style-type: none"> - Capacidad de controlar las excepciones durante la invocación del servicio y el paso de mensajes - Capacidad para manejar las transacciones en otras capas, especialmente cuando un servicio integrado invoca una cadena de servicios de un trámite
4	Seguridad	Apoyar la aplicación de los privilegios de acceso y otras políticas de seguridad	<ul style="list-style-type: none"> - Capacidad de autenticar / autorizar la invocación de un servicio y el enrutamiento de mensajes
5	Administración	Capacidades para realizar seguimiento, supervisar y mantener el historial de las invocaciones de los servicios	<ul style="list-style-type: none"> - Capacidad de capturar y grabar el enrutamiento de mensajes y la historia de invocación de los servicios - Capacidad de rastrear y supervisar las actividades de invocación mensaje y enrutamiento de servicios - Capacidad de configurar la capa de integración

	<p style="text-align: center;">MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estudio de mercado ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos</p>
--	---

Nombre del servicio	Interoperabilidad - Capa de calidad del servicio (QoS)		
Alcance del servicio	<p>Esta capa ofrece la gestión de la calidad de servicio en varios aspectos, como la disponibilidad, fiabilidad y seguridad, así como mecanismos de apoyo, seguimiento, supervisión y gestión de la plataforma por medio de un administrador de la solución.</p> <p>Esta capa proporciona las capacidades necesarias para garantizar que las políticas definidas, requisitos no funcionales (NFR), y regímenes de gobierno se cumplan.</p>		
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
1 Comando y Control de Gestión	Ofrecer un centro de mando para la gestión de la seguridad y configuración de la plataforma y sus servicios, así como capacidades operativas de seguridad para los activos y servicios que no son de TI para garantizar la protección, respuesta, continuidad y recuperación. Entre ellos, los activos físicos, como lugares, instalaciones, servicios, inventario, control de acceso físico, la identidad humana, etc.	<ul style="list-style-type: none"> - Proporcionar un centro de mando para la gestión de la seguridad y configuración de la plataforma y sus servicios, así como la de los servicios de las entidades - Garantizar la protección, respuesta, continuidad y recuperación de la plataforma - Aprobar y definir perfiles y autoridades para el manejo de la seguridad - Garantizar la seguridad física y operativa de las localizaciones, activos - Garantizar la seguridad de la solución relacionadas a fallas, daños, errores, accidentes y daños según lo definido por la capa de Gobierno 	
2 Gestión de seguridad	Capacidades que permiten gestionar y supervisar la seguridad, administrar los roles e identidades, privilegios de acceso y derechos, protección de datos estructurados y no estructurados a acceso no autorizado o la pérdida de datos, mantener la seguridad a través de mecanismos proactivos que reaccionan a vulnerabilidades identificadas y nuevas amenazas.	<ul style="list-style-type: none"> - Garantizar la autenticación en función de roles - Garantizarla debida autorización basada en las funciones, reglas y políticas - Garantizar el cifrado de mensajes - Garantizar el registro de auditoría de los mensajes - Asegurar que el acceso a los recursos se ha dado a las identidades adecuadas, en el momento adecuado, con el propósito correcto - Supervisar y auditar el acceso a los recursos para el uso no autorizado o inaceptable - Proteger la plataforma de interoperabilidad de acceso no autorizado o pérdida de datos, esto incluye la protección a los servicios de las entidades - Supervisar y auditar el acceso a los servicios de las Entidades - Mantener la seguridad de la Plataforma de Interoperabilidad a través de cambios proactivos, en respuesta a las vulnerabilidades identificadas y las nuevas amenazas, y a través de la respuesta a incidentes detectado y problemas reportados - Identificar, cuantificar, evaluar e informar sobre los riesgos de seguridad que ocurran en la operacional de los servicios de las entidades, proporcionando todos los elementos para analizar e informar eventos de seguridad. - Hacer cumplir las políticas de control de acceso 	

Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
3	Monitoreo y Gestión de infraestructura TI	Capacidades que permiten el monitoreo y la gestión de la infraestructura que da soporte a la plataforma de Interoperabilidad. Esto incluye: monitorear, captura métricas y el estado de las infraestructura que soporta los sistemas informáticos	Capacidad de monitorear, administrar y configurar: - Hardware de TI, incluidos los sistemas operativos que son parte de la solución para la Plataforma de Interoperabilidad - Hardware de red que son parte de una solución - Hardware de almacenamiento que son parte de una solución	
4	Seguimiento y Gestión de software	Capacidades que permiten el monitoreo y gestión de los servicios de software y aplicaciones. Esto incluye la capacidad de capturar y métricas para supervisar y gestionar las aplicaciones y estado que conforman la plataforma de interoperabilidad, también define condiciones básicas sobre la gestión a desarrollar para la entrega de servicios, documentación y demás artefactos a la finalización o terminación del vínculo con las Entidades	- Coordinar las necesidades generales de la solución frente a la calidad del servicio para la plataforma - Capturar el porcentaje de ejecuciones en los que la plataforma y los servicios de las Entidades no fallan - Capturar el porcentaje de ejecuciones de los servicios de las Entidades que se ejecutan dentro de un periodo de tiempo - Capturar la métrica para el porcentaje de tiempo que los servicios de las Entidades esta disponible - Capturar la métrica para el tiempo de respuesta de acceso a un servicio y la plataforma - Capacidad de reaccionar a los cambios de infraestructura para maximizar la disponibilidad - Capacidad de registro o informes de mediciones sobre la disponibilidad - Capacidad para evaluar las métricas de disponibilidad contra los requerimientos no funcionales y acuerdos de niveles de - servicio (política) - Capturar métricas sobre el rendimiento de los servicios y la plataforma - Posibilidad de cambiar la configuración y la política para asegurar el cumplimiento de los acuerdos de niveles de servicio - Posibilidad de cambiar la configuración y la política para asegurar la optimización del rendimiento - Capacidad para soportar la virtualización de los recursos de apoyo a la optimización del rendimiento - Posibilidad de grabar, realizar un seguimiento y controlar el costo de la ejecución de un servicio de Entidad, la plataforma, y/o solución	
5	Seguimiento y Gestión de servicios	Capacidades que proporcionan el monitoreo y la gestión de las actividades de los servicios y tramites de las entidades. Permite el análisis de información tanto en tiempo real como casi real de los eventos, así como almacenarlos, para revisar y evaluar las actividades de los servicios y tramites con el fin de determinar las respuestas o emitir alertas / notificaciones a las Entidades	- Analizar información de eventos relacionados a los servicios o tramites de las Entidades, tanto en tiempo real / tiempo casi real, así como eventos almacenados - Revisar y evaluar las actividades de los servicios y tramites con el fin de determinar las respuestas o emitir alertas / notificaciones a las Entidades	
6	Gestión de Eventos	Capacidades que ofrecen la posibilidad de gestionar los eventos de la plataforma y los servicios o tramites de las Entidades y permite el procesamiento de eventos complejos	- Obtener eventos de la capa de integración - Controlar la emisión de eventos en la plataforma y de los tramites y servicios de la entidad - Enviar eventos que indique un incumplimiento de los requisitos de calidad de servicio de la plataforma o de los tramites y servicios de la entidad - Posibilidad de que las Entidades se suscribire a los eventos emitidos por la plataforma - Controlar la frecuencia y tamaño de registro de los eventos	

Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
7	Política de Seguimiento y Control	Capacidades que proporcionan un mecanismo para controlar y hacer cumplir las políticas y reglas de asociadas a los servicios o tramites, incluidas las políticas a nivel de la Entidad, políticas de seguridad, privilegios de acceso a los servicios y tramites y las políticas de acceso a datos. Se consideran capacidades como, encontrar y acceder a reglas y políticas, evaluar y hacer cumplir las políticas en los puntos de control o en las métricas definidas, capturar el estado de la plataforma, servicio o tramite de la Entidad, enviar notificaciones y registrar los casos de incumplimiento y cambiar las reglas, políticas, configuración.	<ul style="list-style-type: none"> - Comprobar los requisitos de calidad de servicio sobre reglas válidas - Posibilidad de cambiar las reglas para cumplir con los requisitos de calidad de servicio - Capacidad para enviar eventos por incumplimiento de requisitos de calidad de servicio - Capacidad para evaluar las políticas - Capacidad para resolver conflictos entre las políticas - Capacidad para hacer cumplir las políticas - Capacidad de responder de forma automática y corregir violaciones de las políticas - Posibilidad de habilitar la aplicación de políticas - Capacidad de descubrir, analizar, transformar, distribuir, evaluar y hacer cumplir las políticas de seguridad - Capacidad de gestionar el ciclo de vida de las políticas - Posibilidad de cambiar las políticas - Posibilidad de deshabilitar, descartar las políticas - Capacidad para controlar y capturar las métricas y el estado de la plataforma y de los tramites y servicios de las entidades - Capacidad de encontrar y acceder a las políticas - Capacidad de automatizar el seguimiento de violaciones a las políticas 	
8	Configuración y gestión del cambio	Capacidades que proporcionan la posibilidad de cambiar la configuración de la plataforma y descripciones (Servicio, tramite, reglas, políticas).	<ul style="list-style-type: none"> - Capacidad de capturar la configuración - Posibilidad de cambiar la configuración - Comprobar los requisitos de calidad de servicio para las configuraciones válidas - Capacidad de cambiar la configuración para cumplir con los requisitos de calidad de servicio - Capacidad para enviar eventos por incumplimiento de requisitos de calidad de servicio a las entidades - Capacidad de rastrear y registrar los cambios de configuración, metadatos, políticas, etc., que ocurren en la plataforma y los tramites y servicios de las entidades - Capacidad de recuperarse o incluso reversar los cambios realizados en la plataforma o los tramites y servicios de la Entidad - Asegurar que los cambios se ejecutan en el cumplimiento de las políticas y reglas establecidas - Posibilidad de cambiar los metadatos, incluyendo descripciones de los tramites y servicios de las entidades - Capacidad para propagar los cambios de metadatos a otros repositorios y descripciones 	
9	Almacén de reglas y políticas	capacidad de almacenar y políticas y reglas	<ul style="list-style-type: none"> - Posibilidad de almacenar las políticas y normas de calidad de servicio - Capacidad de localizar / buscar / devolver las políticas y normas de calidad de servicio 	

Nombre del servicio		Interoperabilidad - Capa de Información		
Alcance del servicio		<p>La capa de información es responsable de la representación unificada de la información y aspectos como la alineación de los servicios de las entidades con el Lenguaje Común de Intercambio de Información, las consideraciones sobre que incluye el contenido de metadatos que se debe almacenar. También permite una capacidad para la virtualización de información para apoyar la consistencia y calidad de los datos.</p> <p>En particular, se debe dar apoyo a:</p> <ul style="list-style-type: none"> - Apoyar una expresión compartida, común y coherente de los datos en Lenguaje Común de Intercambio de Información - Posibilidad de integrar información de la Entidad con el fin de habilitar servicios de información - Compartir los metadatos de los servicios entre capas y con otros servicios - Capacidad de asegurar y proteger la información - Capacidad de virtualización de la información y de trámites y servicios, por lo general implica la capacidad de recuperar datos de diferentes fuentes, transformarla en un formato común, y exponerla a los consumidores que utilizan diferentes protocolos y formatos. 		
Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
1	Servicios de Información	Apoyo a los trámites y servicios de las Entidades, proporcionan una manera uniforme de representar, acceder, mantener, gestionar, analizar e integrar los servicios través de fuentes o proveedores de servicios heterogéneos. Se centra en la integración de servicios	<ul style="list-style-type: none"> - Capacidad para exponer los datos de las Entidades como servicios o datos abiertos, en aplicación del Marco de interoperabilidad, mediante interfaz con la capa de integración. - Capacidad para manejar la representación de datos de diversas fuentes de datos en el formato de datos unificado de acuerdo con el Lenguaje común de intercambio de Información; capacidad de transformar el mapa de datos de un formato a otro y alinear los datos de diferentes recursos. - Capacidad de validar el cumplimiento de la estandarización de los servicios en el Lenguaje Común de intercambio de información - Validar y hacer cumplir las normas de calidad de datos 	
2	Integración de la Información	Apoyo a la integración de los trámites, servicios e información de las Entidades y habilitación de los servicios de información de las Entidades	<ul style="list-style-type: none"> - Capacidad para realizar extracción de datos, transformación y carga (ETL) de una fuente en la Entidad y exponerla a través de un servicio. - Capacidad para realizar Enterprise Information Integration (EII), especialmente para los servicios de virtualización de datos - Capacidad para virtualizar datos que representan los datos reales de los repositorios de Las Entidades, tales como una base de datos o un archivo de Excel - Capacidad para manejar la transformación de datos (incluyendo la transformación de tipos de datos y contenidos) y agregar datos de múltiples fuentes de datos - Capacidad para realizar la normalización y conciliación de datos que incluye la conciliación semántica - Capacidad para limpiar y hacer coincidir los registros de entrada a los datos existentes - Capacidad de mantener datos en caché como apoyo a los servicios de virtualización de datos / información 	

Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
3	Gestión de la Información básica	Apoyo a la gestión de la información, tales como los metadatos y la gestión de datos no estructurados	<ul style="list-style-type: none"> - Capacidad para gestionar y mantener los metadatos en un repositorio común de metadatos y exponerlos a través de un servicio (La exposición de este servicio debe permitir informar a otros Operadores IOAAS, de ingresos, modificaciones, activaciones o inactivaciones de tramites y servicios, se consideran 2 formas broadcast y por solicitud) - Capacidad de crear, configurar, administrar, personalizar y extender metadatos 	
4	Seguridad y Protección de la información	Apoyo a la de seguridad de la información y de protección de los tramites y servicios	<ul style="list-style-type: none"> - Capacidad para manejar los privilegios de acceso de los distintos participantes en los Servicios - Capacidad de controlar el acceso a los elementos de los servicios individuales - Capacidad para controlar y gestionar la trazabilidad de los servicios, un registro típico incluye: quién ha accedido a los servicios, cuándo, desde donde, con que privilegios y roles. 	
5	Análisis de información	Apoyo a las Entidades para el análisis y seguimiento de las actividades de los tramites y servicios, esto permite a las Entidades aprovechar la información para comprender mejor y optimizar el rendimiento de sus tramites y servicios. Incluye la presentación de informes de los análisis detallados, visualización, planificación, métricas estratégicas, accesos y alertas para ejecutar acciones en el tiempo.	<ul style="list-style-type: none"> - Capacidad para analizar la historia de acceso a los servicios y tramites - Realizar interfaz con la capa de Integración y obtener datos de los eventos de la capa de integración; capacidad de analizar esta información - Capacidad para revisar y evaluar la actividad de servicio y determinar las respuestas o emitir alertas / notificaciones 	
6	Definición y Modelado de la información	Capacidades para definir las construcciones fundamentales de información con base en el Marco de interoperabilidad de MinTIC	<ul style="list-style-type: none"> - Capacidad para usar el Lenguaje Común de Intercambio de Información como único vocabulario en la exposición de servicios de las Entidades 	
7	Repositorio de información	Repositorio de información con el fin de mantener los datos de los metadatos, datos maestros, datos analíticos, datos operativos y datos no estructurados.	<ul style="list-style-type: none"> - Capacidad de almacenar información operativa de los tramites y servicios de las Entidades - Posibilidad de almacenamiento de los datos maestros y datos históricos que se registran por los cambios en los Servicios y tramites de las Entidades - Capacidad para almacenar datos analíticos 	

Nombre del servicio		Interoperabilidad - Capa de Gobierno		
Alcance del servicio		<p>La capa de gobierno garantiza que las capacidades de la plataforma de interoperabilidad se adhieran a las políticas, directrices y normas que se definen en función de los objetivos, estrategias y reglamentos aplicados por MinTIC y que los operadores del servicio de interoperabilidad están proporcionando el valor deseado a las Entidades. Las actividades de gobierno se ajustarán a los principios de gobierno del Marco de referencia de Arquitectura TI de MinTIC.</p> <p>Se incluye el gobierno de los procesos, la gestión y la ejecución, así como el ciclo de vida del servicio de las Entidades. Esto abarca todo el ciclo de vida de los servicios y tramites tanto en diseño como en tiempo de ejecución, los acuerdos de nivel de servicio, la capacidad y el rendimiento, la seguridad y vigilancia. Principalmente se aplica a:</p> <ul style="list-style-type: none"> -Definir las políticas, el nivel cumplimiento y características de las excepciones que se pueden dar -Supervisar el estado de los servicios y tramites, de las soluciones que conforman la plataforma, y la gobernabilidad -Los informes sobre el cumplimiento, excepciones, el estado del servicio, y las versiones -Proporciona un punto de consolidación de las reglas de negocio 		
Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
1	Planificación	Planificación de la gobernabilidad	NA	
2	Definición	Definir la gobernabilidad	NA	
3	Activación y aplicación	Implementar la gobernabilidad.	NA	
4	Monitoreo	Controlar la aplicación de las políticas, los procesos, y la efectividad del gobierno.	NA	

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
1	Escalabilidad	Capacidad	
		De acuerdo al plan Nacional de Desarrollo, la meta de uso de la Carpeta ciudadana para el 2018 es de 3.349.205 a 15.000.000 de ciudadanos. Por lo tanto, cada operador autorizado deberá soportar por lo menos este número de carpetas en su infraestructura.	
		El sistema deberá proveer los medios para adicionar capacidad de procesamiento y almacenamiento al sistema sin tener que migrar a un nuevo ambiente teniendo en cuenta las siguientes cifras:	
		a. El número máximo de usuarios simultáneos <1000>	
		b. El número máximo de usuarios concurrentes <1000>	
		c. El número máximo de entidades, incluyendo documentos <50>	
		d. El espacio de almacenamiento usado por el sistema <5Gb por usuario > y	
		e. Las capacidades de procesamiento desplegado para soportar el sistema.	
		Contenido a soportar a tres años	
		El sistema debe considerar el despliegue del sistema más allá de los límites técnicos, asumiendo que el número de usuarios se duplica, y el número de documentos se quintuplica en un período de tres años.	
		Rendimiento al escalar	
		Al escalar el sistema no deberá verse afectado el rendimiento de cada una de sus funciones:	
		a. El rendimiento del sistema descrito	
		b. El tiempo promedio de búsqueda descrito	
		c. El tiempo de búsqueda descrito	
		d. La periodicidad de los procesos de eliminación descrito	
		Tiempos de búsqueda y número de resultados	
		El sistema debe estar en capacidad de encontrar y recuperar un número máximo de resultados de búsquedas de < > al aumentar el número de documentos, entidades y usuarios.	
		El sistema debe tener una estrategia de mitigación en el motor de búsqueda para hacer los primeros resultados de búsqueda más relevantes.	
		Almacenamiento privado limitado	
		Cada ciudadano deberá tener a su disposición 5 Gbytes de almacenamiento para la gestión de sus archivos físicos.	
		Almacenamiento ilimitado	
		Cada ciudadano deberá tener almacenamiento ilimitado solo para recibir y almacenar documentos enviados por las entidades públicas y referencias a documentos externos.	
		Búsquedas complejas	
		El sistema debe permitir a los usuarios encadenar o unir varias consultas de búsqueda para poder responder consultas de búsqueda complejas.	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
 Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
2	Funcionamiento	Tiempo de búsqueda	
		El tiempo debe tomar el encontrar y recuperar un archivo, etc.	
		Naturaleza de los documentos	
		El sistema debe permitir la creación y guardado de los siguientes tipos de archivo: <pdf, jpg, png, tiff, xml >	
		Tamaño y complejidad del despliegue	
		El sistema debe ser capaz de realizar las siguientes consultas:	
		a. Número de usuarios que estén trabajando simultáneamente;	
		b. El porcentaje de uso del sistema por usuario;	
		c. Número de documentos que estén siendo administrados;	
		d. El espacio promedio usado por archivo;	
		e. Cantidad y tipo de espacio de almacenamiento requerido, incluyendo los índices de búsqueda y otros requerimientos del sistema;	
		f. Capacidad de almacenamiento, procesamiento y memoria requerida;	
		El sistema debe ser capaz de realizar despliegues de alcances: pequeño, mediano y grande.	
		Ciclos de uso	
		El sistema debe ser capaz de indicar cuales pueden ser considerados los períodos donde hay picos de trabajo.	
		Rendimiento	
		El sistema debe ser capaz de capturar simultáneamente < > documentos por hora en promedio durante una operación normal y en picos de trabajo por cada despliegue: pequeño, mediano y grande.	
		Tiempo promedio de búsqueda	
		El sistema debe ser capaz de realizar búsquedas a través de tres elementos de metadatos como Emisor, Fecha y Hora de creación, recuperando 100 documentos, en promedio, durante periodos normales y picos de operación.	
		Periodo de espera	
		El tiempo más largo de espera para cualquier búsqueda debe ser < > y puede ser configurada.	
		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 el los 2 segundos por 1 Mbyte de información.	
		Desecho de archivos	
		El sistema puede evaluar el desecho de archivos en tiempo real o periódicamente en intervalos programados y debe ser ejecutado por lo menos diariamente.	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
3	Capacidad de monitoreo	Instalación y configuración del sistema	
		Se debe disponer de la documentación de instalación y configuración del sistema con roles y responsabilidades claras.	
		Monitoreo uso de recursos	
		El sistema debe estar en capacidad de monitorear el uso de recursos para asegurar que el sistema tenga las reservas adecuadas. Medir el uso de recursos implica disponer de:	
		a. Número de usuarios con acceso al sistema, a que horas y en que días;	
		b. La cantidad de almacenamiento que esta siendo usada y el ritmo de aumento;	
		c. Promedio de tiempo de búsqueda y ritmo en incremento o disminución;	
		d. Tiempo de respuesta promedio de todas las funciones; y	
		e. Utilización de procesamiento y memoria.	
		Uso de recursos	
		El personal técnico debe anticipar la demanda de recursos y los suministrará cuando sean necesarios.	
		Comparar reportes	
		El sistema debe estar en capacidad de monitorear y advertir acerca del uso de recursos, comparando reportes estadísticos en el tiempo.	
		Registro de errores	
		El sistema debe permitir el acceso y uso del registro de error.	
		Alertas	
		El sistema debe permitir la utilización de mecanismos de alerta y consolidación de alertas a usuarios autorizados cuando el sistema no realice funciones determinadas.	
		Auditoría	
		El sistema debe estar en capacidad de garantizar y facilitar para la auditoría:	
		a. Que solo los usuarios y grupos apropiados tengan acceso al sistema	
		b. Que todos los usuarios y grupos apropiados tengan acceso al sistema	
		c. Que los controles apropiados de seguridad y acceso estén funcionando	
		d. Que los usuarios no estén accediendo a documentos y otras entidades a las que no tengan permitido el acceso	
		e. Que la clasificación del servicio de configuración sea apropiado para la entidad	
		f. Que los horarios de configuración de servicio de desecho de documentos sea apropiado para el usuario	
		g. Que todos los documentos relevantes sean capturados por el sistema	
		h. Que los documentos estén siendo puestos en las agrupaciones apropiadas	
		i. Que los documentos estén siendo clasificados correctamente	
		j. Que ningún archivo u otra entidad estén siendo eliminados del sistema, fuera del proceso de desecho de documentos	
		k. Que los períodos de desecho estén siendo monitoreados y las fechas límites estén siendo cumplidas	
		l. Que las confirmaciones ocurran dentro de las fechas límite de desecho y que no haya atraso en los documentos que deben eliminarse	
		m. Que el contenido de los documentos esta siendo eliminado correctamente y	
		n. Que las copias de los contenidos de los documentos estén siendo eliminadas de fuentes secundarias dentro del operador inmediatamente después o al tiempo con la eliminación formal del archivo.	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
4	Portabilidad	Usabilidad	
		El sistema debe solicitar solamente la información absolutamente necesaria, no requerir la misma información más de una vez, reutilizar la información de campos y seguir los lineamientos de diseño definidos por el Ministerio de las TIC. En particular la interfaz de experiencia de usuario deberá ser responsive y se deberá adecuar a los dispositivos utilizados por el usuario.	
		Accesibilidad	
		El sistema deberá proveer la opción de alto contraste en la interfaz Web para facilitar la presentación a personas con problemas de visión.	
		Plataformas	
		El sistema debe tener la documentación sobre la(s) plataforma(s) y sistemas operacionales sobre las cuales operan incluyendo módulos y tecnologías de despliegue.	
		Directorio de usuarios	
		El sistema debe administrar o utilizar el directorio de usuarios beneficiarios y suscritos a los servicios de la entidad de manera histórica y preservar esta información.	
		Componentes de software	
		El sistema puede utilizar componentes de software de terceros como tecnologías de bases de datos y motores de búsqueda.	
		Metadatos	
		El sistema debe permitir administrar un modelo de servicio de metadatos para todo tipo de documentos soportando:	
		a. El número de elementos de metadatos de contexto aplicados a un tipo de documento < >	
		b. El número de elementos de metadatos de contexto que pueden ser incluidos en una plantilla < >	
		c. Uso de las plantillas	
		d. Longitud máxima de un campo de metadatos < >	
		e. Tipos de datos soportados en el sistema	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos


Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
5	Seguridad	Autenticación	
		El sistema debe ser solo accesado por un usuario autenticado. El sistema debe soportar uno o varios servicios de autenticación provistos por el operador de autenticación electrónica.	
		Autenticidad.	
		El sistema debe garantizar suficiente confianza en la vinculación entre un usuario y la identidad presentada. Para determinar el grado de confiabilidad requerido se seguirán las recomendaciones de la ITU e ISO dispuestas en sus documentos ITU X.1254 e ISO 29115.	
		Control de acceso	
		El sistema debe adoptar un modelo control de acceso interno e imponer limitaciones en:	
		a. Los roles que están predefinidos y fijados por el sistema	
		b. El número de roles adicionales que pueden ser definidos	
		c. Las definiciones de las funciones que pueden ser incluidas en los roles	
		d. Las entidades que tienen acceso a las listas de control	
		e. La herencia y otras características de acceso del control de entrada	
		Acceso a datos	
		El sistema debe disponer de mecanismos para restringir el acceso a los datos y documentos almacenados.	
		Comunicaciones	
		El sistema debe usar tecnologías para asegurar que la comunicación entre diferentes componentes del sistema y la comunicación con los sistemas externos de las entidades sea seguro.	
		Controles	
		El sistema debe integrar controles y estrategias de seguridad como parte normal del ambiente operacional para prevenir que sea explotado por virus, caballos troyanos, y otro tipo de código malicioso.	
		Complacencia	
		El sistema debe estar diseñado e implementado para satisfacer varios estándares de seguridad como son: ISO 27000, pruebas de penetración, regulación nacional MINTIC:	
		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/gestion/615/articulos-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	
		Integridad	
		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	
		Trazabilidad	
		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.	
		Disponibilidad	
		Mecanismo mediante el cual, el operador a implementa las políticas de réplica y respaldo sobre los documentos almacenados por cada uno de los ciudadanos enrolados en su plataforma.	
		Los usuarios podrán acceder al servicio sin interrupción durante un 99,982% de tiempo de servicio y el usuario puede utilizar sus credenciales de autenticación en cualquier sistema operativo, navegador o sistema de información.	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
6	Privacidad	Privacidad	
		El sistema debe cumplir y ser evaluado de conformidad con las normativas de privacidad como son:	
		a. 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 artículos 15 y 20 de la Constitución Política y de la normatividad colombiana vigente y aplicable en especial los requisitos de la Ley 1581 de 2012 de Protección de Datos Personales, del decreto 1377 de 2013 y de la Guía para la implementación de la Responsabilidad Demostrada de la SIC.	
		b. Buenas prácticas internacionales.	
		Privacidad por Diseño	
		Evaluaciones de Impacto a la Privacidad y del Programa Integral de Gestión de Datos Personales cuando cambios del sistema creen nuevos riesgos a la privacidad.	
		Minimizar	
		Que los datos requeridos para el enrolamiento de un ciudadano en un sistema de información sean los mínimos para validar su identidad, esto es:	
		• Nombres	
		• Apellidos	
		• Tipo de documento	
		• Número del documento de identificación.	
		• Correo Electrónico	
		• Pseudónimo	
		Previa autorización del ciudadano se podrán solicitar otros datos que sean requeridos para la expedición de las credenciales, tales como:	
		• Numero de celular	
		• Información biométrica	
		• Dirección postal	
		• Otros	
		Dentro del registro se deberán almacenar datos generados en el enrolamiento, tales como:	
		• Punto de enrolamiento	
		• Identificador de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (Afis) provisto por la Registraduría Nacional del Estado Civil RNEC	
		• Estampa cronológica de la confirmación de la verificación realizada contra el Sistema Automatizado de Identificación Dactilar Colombiano (Afis) provisto por la RNEC	
		• Firma electrónica de la transacción que corresponda al funcionario o persona a cargo que facilitó la verificación.	
		Proteger	
		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.	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
6	Privacidad	Separar	
		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.	
		Agregar	
		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:	
		Nivel 1: 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.	
		Nivel 2: 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.	
		Informar	
		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.	
		Mantener los registros de la trazabilidad de autenticaciones e información adicional a la mínima del ciudadano que se compartió con cualquier sistema de información.	
		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.	
		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.	
		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.	
		Controlar	
		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:	
		<ul style="list-style-type: none"> • 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. • 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. • Un mecanismo para divulgar al titular cuando el punto anterior ocurra. • La posibilidad de la portabilidad dentro de los servicios de información de identificación personal, de acuerdo con la normatividad y las políticas aplicables. 	

		MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estudio de mercado ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos		
Requisitos No Funcionales				
Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
6	Privacidad	Es importante que el sistema y todo el modelo respete la información y los datos privados de los ciudadanos teniendo en cuenta la naturaleza de la información a transferir y la documentación a guardar. El sistema debe cumplir con las disposiciones que en materia de privacidad de la información personal el país haya adoptado para proteger el derecho de los ciudadanos. En tal sentido el Operador debe tomar las medidas para el tratamiento de datos personales, la notificación a los sujetos cuando sus datos personales están siendo tomados, incluyendo la garantía del derecho a acceder y a objetar, también restricciones al transferir datos personales a países en tercera instancia.	<ul style="list-style-type: none">Permitir revocar en cualquier momento el acceso concedido a su información adicional y mensajes de datos.	
			<ul style="list-style-type: none">Permitir el asignar una vigencia en tiempo de los permisos de acceso a su información adicional de autenticación y a los documentos.	
			<ul style="list-style-type: none">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.	
			<ul style="list-style-type: none">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.	
			Cumplir	
			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.	
			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.	
Demostrar				
	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.			

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
7	Usabilidad	Documentación	
		El sistema debe disponer de personal especializado y documentación técnica para facilitar su evaluación por un centro acreditado del gobierno nacional.	
		Capacitación	
		El operador debe brindar a los usuarios diferentes niveles de capacitación para usar el sistema eficientemente contemplando entre otros cursos de entrenamiento, tutoriales y otros recursos de educación y aprendizaje disponibles para usuarios generales y especializados: ciudadanos, administradores técnicos y de seguridad de las entidades, auditores del Administrador.	
		El sistema debe proporcionar asistencia en línea al usuario en todo momento.	
		Conviene que la ayuda en línea del sistema sea sensible al contexto.	
		Todos los mensajes de error del sistema deben ser significativos, de forma que los usuarios a los que están destinados puedan tomar las medidas adecuadas.	
		El sistema debe utilizar un conjunto único, o un pequeño número de conjuntos, de normas de interfaz de usuario.	
		El sistema debe ser capaz de mostrar varios documentos de forma simultánea.	
		Cuando el sistema recurra a la visualización en pantalla en forma de ventanas, conviene que el usuario pueda configurar cada una de ellas.	
		La interfaz de usuario del sistema debe ser adecuada a usuarios con necesidades especiales, esto es, ha de ser compatible con el software especializado que se pueda utilizar y con las directrices pertinentes sobre interfaces.	
		El sistema debe permitir que, cuando sea conveniente, existan valores por defecto persistentes para la introducción de datos, entre los que convendría que se incluyesen:	
		a. Valores definibles por el usuario	
		b. Valores idénticos a los del elemento anterior	
		c. Valores derivados del contexto, como la fecha, el identificador del usuario, según proceda.	
		Las transacciones más habituales del sistema se han de diseñar de forma que puedan realizarse con un pequeño número de interacciones.	
		Siempre que los usuarios compartan carpetas y documentos conviene que el sistema envíe, en lugar de copias, referencias a tales elementos.	
		Siempre que el sistema utilice una interfaz gráfica de usuario, deberá permitir que sus usuarios la configuren a su gusto. Conviene que algunos aspectos de la personalización abarquen los elementos siguientes, aunque no tienen por qué limitarse sólo a ellos:	
		a. los contenidos de los menús;	
		b. la disposición de las pantallas;	
		c. la utilización de teclas de funciones;	
		d. los colores, las fuentes y el tamaño de las fuentes que se muestran en pantalla;	
		e. las alarmas sonoras.	
		Cuando los usuarios tengan que introducir metadatos de imágenes de documentos impresos, conviene que el sistema ofrezca funciones que permitan recurrir al reconocimiento óptico de caracteres en la captura de estos metadatos (reconocimiento óptico de caracteres por zonas).	
8	Accesibilidad	Complacencia	
		El sistema debe cumplir con los requerimientos establecidos en la WCAG (Web Content Accessibility Guidelines). Éstas guías proveen una clasificación de A (la más baja) o AAA (la más alta).	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
9	Disponibilidad	Disponibilidad anticipada El sistema debe tener una disponibilidad anticipada de < >% al comparar el tiempo de actividad y el de inactividad durante el curso de un año calendario.	
		Acuerdo de nivel de servicio El operador debe disponer en el sistema o por medio de un tercero de las herramientas que permitan medir los porcentajes de disponibilidad mínima.	
		Copias de seguridad El operador debe realizar copias de seguridad completas y copias de seguridad incrementales para cada una de las tecnologías descritas y para cada uno de los despliegues y los escenarios de crecimiento descritos.	
		Horarios El operador debe considerar un horario de administración del sistema para hacer copias de seguridad, mantenimiento o actualizaciones que deben ser reservadas cada día, semana y mes durante el año.	
		Traslado de responsabilidad Si el sistema está alojado por cuenta de un tercero no deben existir limitaciones adicionales de disponibilidad y la garantías deben ser proporcionadas por el sistema anfitrión.	
10	Confiabilidad	Integridad 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 requerido se seguirán las recomendaciones de la ITU e ISO dispuestas en sus documentos ITU X.1254 e ISO 29115	
		Evitar la pérdida de información. Implementar transacciones compensatorias, y mecanismos para realizar Rollback.	
		Revelar lo que esté dispuesto a compartir, bajo ninguna circunstancia debe revelarse lo que no esté autorizado.	
		Calidad en los datos La confiabilidad en la integración puede ser parametrizada a distintos niveles.	
		Recuperabilidad En caso de algún fallo, que el sistema se devuelva al último estado consistente.	
		Inmutabilidad de información 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.	
		Garantizar preservación Los medios de almacenamiento del sistema deben ser utilizados y almacenados en ambientes que son compatibles con la vida útil deseada / esperada, y que estén dentro de la tolerancia de la especificación del fabricante de medios de comunicación.	
		Sustitución El sistema debe permitir el seguimiento y la sustitución de medios de almacenamiento para protegerse contra la degradación de los medios de comunicación.	
		Integridad y comprobación El sistema debe incluir características para la comparación periódica automática de copias de la información, y la sustitución de cualquier copia debido a un defecto, para protegerse contra la degradación de los medios de comunicación.	
		Migración	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
10	Confiabilidad	El sistema debe permitir la migración a granel (interpretación) de los registros (junto con sus metadatos y la información de registro de auditoría) a los nuevos medios y / o sistemas de acuerdo con las normas pertinentes para su formato (s).	
		Actualizaciones de mejoras	
		El proveedor sistema debe tener un programa de actualización del sistema en el lugar para asegurar que la información existente puede seguir siendo visitada y sin cambios en el contenido.	
		Aplicar actualizaciones	
		Cualquier modificación del sistema que se han hecho para el sistema de los requisitos de organización debe permanecer en su lugar después de una actualización del sistema.	
		Comprobaciones	
		El sistema debe ser capaz de informar sobre los formatos de archivo y versiones de los componentes.	
		Invariante	
		El sistema debe ser capaz de convertir desde su formato original (s) a cualquier formato que se especifica a largo plazo la conservación de archivos (s) en el momento de la captura, en cualquier momento posterior, o en la exportación.	
		Siempre que sea posible sin comprometer la integridad de los registros, el sistema debe ser capaz de hacer que los componentes de su formato original a cualquier preservación a largo plazo especificado formato (s) de archivo en el momento de la captura, en ocasiones sucesivas, o en la exportación.	
		Siempre que sea posible, sin comprometer la integridad de los registros, el sistema debe ser capaz de hacer que los componentes de su formato original a cualquier formato especificado a largo plazo la conservación de archivos(s) en el momento de la captura , en una ocasión posterior , o en la exportación.	
		Entrega	
		Siempre que se representan los registros o componentes, el sistema debe permitir al administrador realizar la entrega a introducir un motivo.	
		Preservación	
		Cuando un registro se ha rendido en un formato de archivo de conservación, el sistema debe proporcionar instalaciones adecuadas para recuperar el formato y / o entregas original, según el caso.	
		Exportación de paquete	
		El sistema debe ser capaz de exportar documentos y sus metadatos en forma de un paquete de difusión de la información como se define en el Apéndice 7 de la norma OAIS, ISO 14721.	
		Metadatos	
		El sistema debe contener como mínimo los siguientes metadatos artículos para un componente prestados:	
		• El formato de archivo original y la versión; • Fecha de entrega.	
		Extracción de documentos	
		El sistema debe ser capaz de extraer de un componente, y a continuación, almacenar en forma de metadatos, los metadatos técnicos almacenada en los componentes.	
		Documentación clara	
		Si los términos utilizados cualquier codificación propietaria o estructuras de almacenamiento o bases de datos, éstos deben estar completamente documentados, con estar a disposición de las funciones administrativas de la documentación.	
		Gama de metadatos	
		Las condiciones deberían ser capaces de manejar una amplia gama de elementos de metadatos de preservación de los archivos y sus partes componentes.	
		Preservación del código	
		El código fuente del sistema o bien debe ser abierto, o una copia del código fuente debe ser presentado en depósito con una parte neutral.	

		<div>MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES</div> <div>Estudio de mercado</div> <div>ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos</div>		
Requisitos No Funcionales				
Característica requerida		Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
11	Mantenibilidad	El sistema debe poder ser mantenido. 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.	Localizar cambios	
			Dividir responsabilidades en componentes especializados e independientes, de tal forma que los cambios en algunas funcionalidades, tengan un impacto controlado.	
			Uso de interfases y clases abstractas, para comunicar varios paquetes o componentes de software. De esta forma los cambios en la implementación no se verán.	
			Hacer uso de contratos de comunicación entre paquetes o componentes, ocultando la implementación de los métodos de negocio.	
12	Preservación a largo plazo y obsolescencia de la tecnología	<p>Hace referencia a los riesgos tecnológicos de cara a la preservación de los documentos a largo plazo desde tres puntos de vista:</p> <ul style="list-style-type: none">• degradación de los medios de comunicación;• obsolescencia de hardware;• obsolescencia de formato. <p>Para el ciudadano, el período de conservación se fija en función del tiempo de vida del ciudadano. Después del deceso de un ciudadano esta cuenta podrá ser gestionada por un familiar debidamente autorizado.</p>	Los medios de almacenamiento del sistema deben ser utilizados y almacenados en ambientes compatibles con la vida útil deseada / esperada, y que estén dentro de la tolerancia de la especificación del fabricante de medios.	
			El sistema debe permitir el seguimiento y la sustitución de medios de almacenamiento para protegerse contra la degradación de los medios.	
			El sistema debe incluir características para la comparación periódica automática de copias de información, y la sustitución de cualquier copia debido a un defecto, para protegerse contra la degradación de los medios.	
			El sistema debe permitir la migración en volúmen (interpretación) de archivos (junto con sus metadatos y la información de registro de auditoría) a los nuevos medios y / o sistemas en líneas de acuerdo con los estándares pertinentes para su formato (s).	
			El operador debe tener un programa de actualización del sistema en el lugar para asegurar que la información existente puede seguir siendo visitada y sin cambios en el contenido.	
			Cualquier modificación que se realice al sistema en los requerimientos organizacionales deben permanecer en su lugar después de una actualización del sistema.	
			El sistema debe ser capaz de informar sobre los formatos de archivo y versiones de los componentes.	
			El sistema debe ser capaz de interpretar archivos desde su formato original a cualquier formato de archivo específico de preservación a largo plazo en el momento de la captura, en cualquier momento posterior, o en la exportación.	
			Siempre que sea posible sin comprometer la integridad de los archivos, el sistema debe ser capaz de interpretar los componentes desde su formato original a cualquier formato de archivo específico de preservación a largo plazo en el momento de la captura, en cualquier momento posterior, o en la exportación.	
			Siempre que se representen los registros o componentes, el sistema debe permitir al administrador realizar la interpretación al introducir un motivo.	
			Cuando un registro se ha interpretado en un formato de archivo de preservación, el sistema debe proporcionar facilidades adecuadas para recuperar el formato y / o entregas original, según el caso.	
			El sistema debe ser capaz de exportar archivos y sus metadatos en forma de un paquete de difusión de información como se define en el Apéndice 7 de la norma OAIS, ISO 14721.	
			El sistema debe contener como mínimo los siguientes elementos de metadatos para un componente interpretado	
			• El formato de archivo original y la versión; • fecha de interpretación.	
			El sistema debe ser capaz de extraer desde un componente, y a continuación, almacenar en forma de metadatos, los metadatos técnicos almacenada en los componentes.	
			Si los términos de uso de cualquier codificación propietaria o almacenamiento o estructuras de bases de datos, éstos deben estar completamente documentadas, con la disponibilidad de la documentación a los roles administrativos.	
			El sistema debe ser capaz de manejar una amplia gama de elementos de metadatos para la preservación de los archivos y sus partes componentes.	
			El código fuente del sistema o bien debe ser abierto, o una copia del código fuente debe ser presentado en depósito con una parte neutral.	

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Estudio de mercado
ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
13	Garantía	El operador debe ofrecer un tipo de garantía en términos de calidad y funcionamiento en relación con todas las partes o funcionalidades del sistema.	
		El operador debe ofrecer acuerdos de niveles de servicio que cubran todo el sistema e individuales para los requerimientos no funcionales del sistema como funcionalidad y disponibilidad.	
		El operador debe tener términos y condiciones estándar para los clientes del sistema y disponibles para los usuarios o posibles usuarios. Debe notarse que aún el software de código abierto tiene condiciones de licencia asociadas a él.	
		En caso de que el operador salga del mercado debe ser posible para el administrador obtener acceso al código fuente para el sistema como alojar una copia del código fuente en garantía con un tercero neutral.	
		En caso de que el operador salga del mercado debe ser posible para el administrador obtener acceso a los datos de servicios alojados en el sistema como alojar una copia de datos en garantía con un tercero neutral.	
		El operador es responsable mediante los términos y condiciones por los acuerdos de nivel de servicio, contratos de licencia de todos los componentes del sistema así sean proporcionados por diferentes proveedores y el alojamiento del sistema.	
14	Cumplimiento/conformidad	El sistema debe estar en conformidad con los estándares de la industria y con las regulaciones nacionales de la siguiente manera:	
		Deben estar en conformidad con todas las disposiciones legislativas y regulatorias que apliquen a la naturaleza del Operador y a la jurisdicción.	
		Deben estar en conformidad con estándares Industriales generalmente aceptados en tecnología, y en las plataformas en donde sea desplegado el sistema.	
		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.	
		Compatible con el almacenamiento de archivos utilizando formatos de archivo y codificación estandarizada o totalmente documentada.	
		El sistema debe estar en conformidad con los estándares nacionales o internacionales en cuanto a la administración de documentos o la administración de contenido.	
		El sistema debe estar en conformidad con los marcos regulatorios y legislativos, estándares a nivel nacional o internacional.	
		El sistema debe cumplir las normas de admisibilidad jurídica y de fuerza probatoria de los documentos electrónicos de archivo aplicables en cada caso.	
15	Centro de Operaciones de Seguridad (SOC)	El sistema ha de atenerse a la legislación aplicable en materia de gestión de documentos de archivo.	
		El sistema no debe incluir ninguna característica incompatible con la legislación en materia de protección de datos o de otro tipo.	
		El sistema debe cumplir las exigencias normativas de <Ley 1437 de 2011, Ley 1581 de 2012, Decreto 19 de 2012, Plan Nacional de Desarrollo, Ley 1594 de 2009>	
		El sistema debe proveer un alto nivel de precisión para las marcas de tiempo generadas. Precisión de milisegundo, o mejor, puede ser usada para mantener el orden exacto en el que los eventos ocurren en sistemas de alto rendimiento.	
		El sistema debe utilizar algoritmos adecuados para general identificadores únicos universales para crear grandes números de UUIDs sin repetición, patrón o superposición con otros sistemas.	
		El sistema debe soportar en todo momento el reporte de conformidad del administrador y revisar permanentemente el estado actual del sistema cuando se hace el reporte, para asegurar que no ha sido reconfigurado de manera no conforme.	
		Seguridad Física y Ambiental. Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro del SOC, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro. Las principales amenazas que se prevén en la seguridad física son: 1. Desastres naturales, incendios accidentales, 2. Amenazas ocasionadas por el hombre y 3. Sabotajes internos y externos deliberados. Se analizarán y evaluarán los peligros más importantes que se corren en un centro de operaciones y monitoreo; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.	

 <p>TODOS POR UN NUEVO PAÍS PAZ · EQUIDAD · EDUCACIÓN</p> <p>vive digital para la gente</p> <p> MINTIC</p>	<p align="center">MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Estudio de mercado ANEXO 1. Funcionalidades Técnicas de la plataforma de Servicios Digitales Básicos</p>
--	---

Requisitos No Funcionales			
Característica requerida	Descripción del requerimiento	Característica mínima requerida	Característica máxima requerida
16	Centro de Procesamiento de Datos (CPD)	Disponibilidad y monitorización “24x7x365” un centro de datos diseñado apropiadamente proporcionará disponibilidad, accesibilidad y confianza 24 horas al día, 7 días a la semana, 365 días al año.	
		Fiabilidad: Los centros de datos deben tener redes y equipos altamente robustos y comprobados.	
		Seguridad, redundancia y diversificación: Almacenaje exterior de datos, tomas de alimentación eléctrica totalmente independientes y de servicios de telecomunicaciones para la misma configuración, equilibrio de cargas, sistemas de alimentación ininterrumpida o SAI, control de acceso, etc.	
		Control ambiental y prevención de incendios: El control de ambiente trata de la calidad de aire, temperatura, humedad, inundación, electricidad, control de fuego, y por supuesto, acceso físico.	
		Acceso a internet y conectividad a redes de área extensa WAN para conectividad a Internet: Los centros de datos deben ser capaces de hacer frente a las mejoras y avances en los equipos, estándares y anchos de banda requeridos, pero sin dejar de ser manejables y fiables.	
		Ubicación: El CPD principal deberá estar ubicado en el territorio nacional y el centro de procesamiento de datos redundante deberá estar ubicado en el territorio nacional.	
17	Mesa de Ayuda (Help Desk)	Auditorías de Seguridad Informática: El operador deberá someterse como mínimo a una auditoría en Seguridad Informática al año, por un auditor definido por el Ministerio TIC que escogerá por convocatoria pública. En la auditoría se validará el sostenimiento del cumplimiento de los requerimientos técnicos, jurídicos y administrativos, como operador. Los costos de esta auditoría estarán a cargo del operador.	
		Disponer de un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación (TIC). El personal o recurso humano encargado de Mesa de Ayuda (MDA) debe proporcionar respuestas y soluciones a los usuarios finales, clientes o beneficiarios (destinatarios del servicio), y también puede otorgar asesoramiento en relación con una organización o institución, productos y servicios.	
18	Certificaciones	Deberá aportar la(s) certificación(es) en ISO 9001 expedidas por las entidades certificadoras autorizadas y alguna de las siguientes certificaciones solicitadas: IT MARK, CMMI nivel 3 o superior, ISO 27001, ISO 20000 o ISO 15504.	