

**El futuro digital  
es de todos**

**Gobierno  
de Colombia  
MinTIC**

# **Anexo 1 Guía de Lineamientos de los Servicios Ciudadanos Digitales**

**Septiembre 2020**

**Ministerio de Tecnologías de la Información y las Comunicaciones**  
**Viceministerio de Transformación Digital**  
**Dirección de Gobierno Digital**

**Equipo de trabajo**

Karen Abudinen Abuchaibe - Ministra de Tecnologías de la Información y las Comunicaciones

German Rueda - Viceministro de Transformación Digital

Aura María Cifuentes - Directora de Gobierno Digital

Gerson Castillo - Subdirector de Estándares y Arquitectura de TI

José Ricardo Aponte Oviedo – Equipo Servicios Ciudadanos Digitales

Ángela Janeth Cortés Hernández – Coordinadora grupo interno de seguridad y privacidad

Juan Carlos Noriega – Equipo de Política Dirección de Gobierno Digital

Marco E. Sánchez Acevedo – Abogado - Equipo de Política Dirección de Gobierno Digital

Equipo Subdirección de Estándares y Arquitectura de TI

Versión	Observaciones
Versión 1 Septiembre 2020	<b>Guía de Lineamientos de los Servicios Ciudadanos Digitales</b> Dirigida al articulador de los Servicios Ciudadanos Digitales

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico:  
[gobiernodigital@mintic.gov.co](mailto:gobiernodigital@mintic.gov.co)

Guía de Lineamientos de los Servicios Ciudadanos Digitales



Esta guía de la Dirección de Gobierno Digital se encuentra bajo una [Licencia Creative Commons Atribución 4.0 Internacional](https://creativecommons.org/licenses/by/4.0/).

# Tabla de Contenido

<b>1</b>	<b>INTRODUCCIÓN .....</b>	<b>8</b>
<b>2</b>	<b>ALCANCE DE LA GUÍA .....</b>	<b>11</b>
<b>3</b>	<b>DEFINICIONES .....</b>	<b>13</b>
<b>4</b>	<b>MARCO JURÍDICO .....</b>	<b>18</b>
<b>5</b>	<b>MODELO CONCEPTUAL DE LOS SERVICIOS CIUDADANOS DIGITALES .....</b>	<b>24</b>
<b>6</b>	<b>MODELO DE INTENCIÓN DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD .....</b>	<b>33</b>
<b>6.1</b>	<b>MODELO ESTRATÉGICO DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD .....</b>	<b>37</b>
<b>7</b>	<b>MAPA DE CAPACIDADES DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD .....</b>	<b>40</b>
<b>8</b>	<b>MODELO DEL SERVICIO DE INTEROPERABILIDAD .....</b>	<b>47</b>
<b>8.1</b>	<b>ALINEACIÓN DEL SERVICIO DE INTEROPERABILIDAD Y EL MARCO DE INTEROPERABILIDAD.....</b>	<b>50</b>
<b>8.2</b>	<b>OBJETIVOS DEL SERVICIO DE INTEROPERABILIDAD .....</b>	<b>51</b>
<b>8.3</b>	<b>VISTA DE CONTEXTO DEL SERVICIO DE INTEROPERABILIDAD .....</b>	<b>53</b>
<b>8.4</b>	<b>MAPA DE CAPACIDADES DEL SERVICIO DE INTEROPERABILIDAD.....</b>	<b>61</b>
<b>8.5</b>	<b>MODELO DE DESPLIEGUE DEL SERVICIO DE INTEROPERABILIDAD .....</b>	<b>61</b>
<b>8.6</b>	<b>SERVICIOS TECNOLÓGICOS DE LA PLATAFORMA DE INTEROPERABILIDAD.....</b>	<b>68</b>
<b>8.6.1</b>	<b>CARACTERÍSTICAS DE LA PLATAFORMA DE INTEROPERABILIDAD .....</b>	<b>68</b>
<b>8.6.2</b>	<b>REQUISITOS TÉCNICOS ASOCIADOS A LA PLATAFORMA.....</b>	<b>70</b>
<b>8.6.3</b>	<b>SUMINISTRO, ADMINISTRACIÓN Y OPERACIÓN DE LA PLATAFORMA .....</b>	<b>71</b>
<b>8.6.4</b>	<b>PROCEDIMIENTOS DE GESTIÓN DEL SERVICIO DE LA PLATAFORMA.....</b>	<b>71</b>
<b>8.6.5</b>	<b>SOPORTE DE LA PLATAFORMA DE INTEROPERABILIDAD .....</b>	<b>72</b>
<b>8.6.6</b>	<b>GESTIÓN DE LOS SERVICIOS DE INFORMACIÓN PUBLICADOS EN LA PLATAFORMA.....</b>	<b>73</b>
<b>8.6.7</b>	<b>GOBIERNO DE LOS SERVICIOS DE INTERCAMBIO DE INFORMACIÓN.....</b>	<b>73</b>
<b>8.6.8</b>	<b>PROCESO DE DESPLIEGUE DEL SERVICIO DE INTERCAMBIO DE INFORMACIÓN.....</b>	<b>74</b>
<b>8.6.9</b>	<b>DISEÑO, DESARROLLO, IMPLEMENTACIÓN Y MANTENIMIENTO DE SERVICIOS DE INTERCAMBIO DE INFORMACIÓN.....</b>	<b>75</b>
<b>8.6.10</b>	<b>OPERACIÓN DE LA PLATAFORMA.....</b>	<b>76</b>
<b>9</b>	<b>MODELO DEL SERVICIO DE AUTENTICACIÓN DIGITAL .....</b>	<b>78</b>
<b>9.1</b>	<b>OBJETIVOS DEL SERVICIO .....</b>	<b>82</b>

<b>9.2</b>	<b>CONTEXTO DEL SERVICIO .....</b>	<b>83</b>
<b>9.3</b>	<b>MAPA DE CAPACIDADES DEL SERVICIO.....</b>	<b>87</b>
<b>9.4</b>	<b>MODELO DE DESPLIEGUE DEL SERVICIO .....</b>	<b>87</b>
<b>9.5</b>	<b>REQUISITOS OPERATIVOS DEL SERVICIO DE AUTENTICACIÓN DIGITAL.....</b>	<b>97</b>
9.5.1	CONDICIONES DE OPERACIÓN DEL SERVICIO DE AUTENTICACIÓN DIGITAL.....	97
9.5.2	PROCESO DE REGISTRO Y VERIFICACIÓN DE ATRIBUTOS DIGITALES DEL USUARIO .....	99
9.5.3	REGISTRO DE PERSONAS NATURALES MAYORES DE EDAD .....	101
9.5.4	REGISTRO DE PERSONAS NATURALES MENORES DE 18 AÑOS.....	101
9.5.5	REGISTRO DE EXTRANJEROS.....	102
9.5.6	REGISTRO DE PERSONAS JURÍDICAS.....	102
9.5.7	REGISTRO DE FUNCIONARIOS PÚBLICOS Y PARTICULARES QUE DESEMPEÑEN FUNCIONES PUBLICAS	104
9.5.8	PROCESO DE EMISIÓN DE LAS CREDENCIALES DE AUTENTICACIÓN .....	104
9.5.9	PROCESO DE AUTENTICACIÓN DIGITAL.....	110
9.5.10	ENRUTAR SOLICITUDES DE AUTENTICACIÓN .....	115
9.5.11	GESTIÓN DE LA BASE DE DATOS MAESTRA.....	116
9.5.12	PROCESO DE FIRMADO ELECTRÓNICO CON LAS CREDENCIALES DE AUTENTICACIÓN DIGITAL .....	116
9.5.13	DESVINCULACIÓN DEL USUARIO FRENTE AL SERVICIO DE AUTENTICACIÓN DIGITAL .....	117
9.5.14	COMUNICACIÓN ENTRE PRESTADORES DE SERVICIO .....	118
9.5.15	INTEGRACIÓN DE AUTENTICACIONES YA OFERTADAS POR OTRAS AUTORIDADES PUBLICAS.....	118
<b>10</b>	<b>MODELO DEL SERVICIO DE CARPETA CIUDADANA .....</b>	<b>119</b>
<b>10.1</b>	<b>OBJETIVOS DEL SERVICIO DE CARPETA CIUDADANA DIGITAL .....</b>	<b>121</b>
<b>10.2</b>	<b>CONTEXTO DEL SERVICIO CARPETA CIUDADANA DIGITAL .....</b>	<b>122</b>
<b>10.3</b>	<b>MODELO DE CAPACIDADES DEL SERVICIO CARPETA CIUDADANA DIGITAL .....</b>	<b>128</b>
<b>10.4</b>	<b>MODELO DE DESPLIEGUE DEL SERVICIO CARPETA CIUDADANA DIGITAL .....</b>	<b>128</b>
<b>11</b>	<b>REQUERIMIENTOS NO FUNCIONALES DE LOS SERVICIOS CIUDADANOS DIGITALES ....</b>	<b>133</b>
<b>11.1</b>	<b>ATRIBUTO DE CALIDAD: FUNCIONAMIENTO.....</b>	<b>134</b>
<b>11.2</b>	<b>ATRIBUTO DE CALIDAD: ESCALABILIDAD .....</b>	<b>137</b>
<b>11.3</b>	<b>ATRIBUTO DE CALIDAD: MONITOREO .....</b>	<b>138</b>
<b>11.4</b>	<b>ATRIBUTO DE CALIDAD: USABILIDAD.....</b>	<b>140</b>
<b>11.5</b>	<b>ATRIBUTO DE CALIDAD: DISPONIBILIDAD .....</b>	<b>144</b>
<b>11.6</b>	<b>ATRIBUTO DE CALIDAD: CONFIABILIDAD .....</b>	<b>146</b>
<b>11.7</b>	<b>ATRIBUTO DE CALIDAD: PRIVACIDAD POR DEFECTO.....</b>	<b>148</b>
<b>12</b>	<b>REQUISITOS TÉCNICOS DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD .....</b>	<b>153</b>
<b>12.1</b>	<b>REQUISITOS TÉCNICOS DE LOS SCD .....</b>	<b>154</b>
<b>12.2</b>	<b>SISTEMAS DE ADMINISTRACIÓN DE RIESGOS .....</b>	<b>157</b>



12.3	REQUISITOS DE INFRAESTRUCTURA .....	159
12.4	REQUISITOS DE RED .....	163
12.5	REQUISITOS A NIVEL DE APLICACIÓN .....	166
12.6	ALMACENAMIENTO DE INFORMACIÓN .....	168
13	SEGURIDAD Y PRIVACIDAD.....	169
14	ANS DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD .....	181
14.1	SOBRE LA REDES DE DATOS DE LOS SERVICIOS CIUDADANOS DIGITALES .....	185
15	TÉRMINOS Y CONDICIONES DE USO .....	188

## Lista de Ilustraciones

Ilustración 1 - Modelo conceptual de los Servicios Ciudadanos Digitales.....	29
Ilustración 2 - Lienzo del modelo de negocio SCD .....	34
Ilustración 3 - Modelo estratégico de SCD .....	38
Ilustración 4 - Mapa de capacidades SCD .....	41
Ilustración 5 – Servicio de Intercambio de Información.....	48
Ilustración 6 - Alineación modelo / Marco de Interoperabilidad.....	51
Ilustración 7 – Modelo de contexto del servicio IO.....	60
Ilustración 8 - Modelo de despliegue IO .....	62
Ilustración 9 – Modelo de despliegue nivel 2 IO.....	65
Ilustración 10 – Modelo de contexto del servicio de Autenticación Digital .....	83
Ilustración 11 - Modelo de despliegue servicio de Autenticación Digital .....	88
Ilustración 12 - Componente CORE del servicio de Autenticación Digital.....	88
Ilustración 13 – Modelo de contexto del servicio de Carpeta Ciudadana Digital .....	125
Ilustración 14 – Modelo de despliegue del servicio de Carpeta Ciudadana Digital base. .....	129

## Lista de Tablas

Tabla 1 – Descripción de las entidades del modelo conceptual.....	30
Tabla 2 – Descripción de las capacidades de nivel 1 de los SCD .....	42
Tabla 3 – Capacidades de Nivel 2 de los Servicios Ciudadanos Digitales.....	43
Tabla 4 – Relaciones del Modelo de contexto servicio de Interoperabilidad (IO) .....	60
Tabla 5 – Descripción de las relaciones del modelo de despliegue de IO.....	63
Tabla 6 – Descripción de las relaciones del modelo de despliegue de IO Nivel 2 .....	66
Tabla 7 - Relaciones del modelo de contexto .....	85
Tabla 8 – Descripción de las relaciones del modelo de despliegue .....	89
Tabla 9- Relaciones del modelo de contexto de Carpeta Ciudadana Digital, CCD.....	126
Tabla 10 – Descripción de las relaciones del modelo del servicio de CCD .....	130
Tabla 11 – Descripción de los elementos del atributo de funcionamiento.....	134
Tabla 12 – Descripción de los elementos del atributo de escalabilidad .....	137
Tabla 13 – Descripción de los elementos del atributo de monitoreo.....	138
Tabla 14 – Descripción de los componentes del atributo usabilidad .....	141
Tabla 15 – Descripción de los elementos del atributo de disponibilidad .....	144
Tabla 16 – Descripción elementos del atributo de confianza .....	146
Tabla 17 – Descripción de los elementos del atributo de privacidad por defecto. ....	148
Tabla 18 - Requisitos técnicos para el Articulador .....	154
Tabla 19 – ANS Asociados a los Servicios Ciudadanos Digitales.....	183
Tabla 20 – Lineamientos de seguridad y requisitos mínimos .....	185





El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), de acuerdo con la Ley 1341 de 2009, desarrolla políticas y planes enfocados a las Tecnologías de la Información y las Comunicaciones que constituyen un componente vital para el crecimiento y desarrollo del sector, con el fin de brindar acceso a toda la población, en el marco de la expansión y diversificación de las TIC, y conforme al principio de “masificación del gobierno en línea” hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de dicha ley, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

Con base en lo anterior, MinTIC tiene establecido dentro de sus funciones: “1. Diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. 2. 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”. En este sentido, MinTIC ha conceptualizado y diseñado un modelo integral que incorpora los proyectos de Interoperabilidad, Autenticación Digital y Carpeta Ciudadana, bajo el nombre de ‘Servicios Ciudadanos Digitales’, este modelo tiene por objeto, facilitar a los ciudadanos su interacción con la administración pública y optimizar la labor del Estado.

En consecuencia, MinTIC ha establecido la necesidad de garantizar la transformación digital de los trámites y servicios mediante el modelo de los Servicios Ciudadanos Digitales (SCD), para enfrentar los retos que imponen los entornos digitales entre ellos:

- a) Interoperabilidad, mejorando las condiciones de intercambio de información. Las entidades públicas deben estar interconectadas y operar de manera articulada como un único gran sistema.
- b) Autenticación Digital, mitigando los riesgos en la suplantación de la identidad y transformando al Estado colombiano para que funcione como una sola institución que le brinde a los ciudadanos información trámites y servicios seguros.
- c) Carpeta Ciudadana Digital, permitiendo la visualización de los datos que las entidades públicas tienen de cada ciudadano o empresa.

El presente documento tiene como fin, establecer las condiciones necesarias que el Articulador debe cumplir, con el fin de garantizar la correcta prestación de los servicios ciudadanos digitales, entre otros, este Ministerio determina los estándares de implementación de los Servicios Ciudadanos Digitales contenidos en la guía de lineamientos de los servicios ciudadanos digitales <sup>1</sup>.

---

<sup>1</sup> <http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30019521>





El presente documento define el modelo que establece las condiciones para garantizar la correcta prestación de los Servicios Ciudadanos Digitales (SCD), incluyendo todos sus componentes, relaciones, modelo de intención, procesos, obligatoriedad, requerimientos técnicos, lineamientos y estándares necesarios, buscando que el articulador de los Servicios Ciudadanos Digitales desarrolle las capacidades para adelantar las interacciones con los distintos actores involucrados en la prestación de los Servicios Ciudadanos Digitales tanto en la operación como en la articulación de estos, con el fin de lograr una coordinación y disposición adecuada de dichos servicios.

En esta guía se dan algunas indicaciones para permitir la compatibilidad de aplicaciones, así como la correcta operación y desarrollo de los servicios a ofrecer a las entidades públicas que se vinculen a los SCD. Sin embargo, están fuera de su alcance la definición de los protocolos de comunicación, los tipos de bases de datos, y las soluciones tecnológicas concretas de los componentes que soporten los SCD.



A los efectos de la presente guía se deberán seguir los conceptos señalados en el artículo 2.2.17.1.4 del Decreto 1078 de 2015, que define los estándares y lineamientos generales en el uso y operación de los servicios ciudadanos digitales, además de los siguientes:

1. **Autenticidad:** Es el atributo generado en un mensaje de datos, cuando existe certeza sobre la persona que lo ha elaborado, emitido, firmado, o cuando exista certeza respecto de la persona a quién se atribuya el mensaje de datos.
2. **Atributos digitales:** Característica o propiedad de un usuario que puede ser utilizada para describir su estado, apariencia u otros aspectos. Dichos atributos corresponden a datos e información suministrados por diversas fuentes de atributos.
3. **Articulador:** Es la Agencia Nacional Digital, que será encargada de proveer y gestionar de manera integral los servicios ciudadanos digitales, además de apoyar técnica y operativamente al Ministerio de Tecnologías de la Información y las Comunicaciones para garantizar el pleno funcionamiento de tales servicios.
4. **Disponibilidad:** Es la propiedad de la información que permite que ésta sea accesible y utilizable cuando se requiera.
5. **Fuente de atributos:** Entidades públicas o particulares que poseen información de usuarios y que la disponen dentro de un contexto determinado, y sobre las cuales se puede hacer afirmaciones acerca de la validez de los valores de los atributos digitales.
6. **Guía de lineamientos de los Servicios Ciudadanos Digitales:** Es el documento expedido y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, el cual incluye las condiciones necesarias que el Articulador de los SCD debe cumplir con el fin de garantizar la correcta prestación de los servicios ciudadanos digitales.
7. **Guía para la vinculación y uso de los Servicios Ciudadanos Digitales:** Es el documento expedido y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones destinado a las autoridades referidas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015, que indica cuáles son las condiciones necesarias y los pasos que deben realizar para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán vincular a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad y carpeta ciudadana digital.

8. **Firma digital:** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación,
9. **Firma electrónica:** Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.
10. **Identidad de persona natural:** Es el conjunto de características o rasgos propios que individualizan a una persona de las demás, lo cual permite el reconocimiento de sus derechos y hacer efectivo el cumplimiento de sus deberes
11. **Identificación de persona natural:** es el proceso que permite reconocer a un individuo a través de diversos métodos o técnicas de identificación
12. **Integridad:** es la condición que garantiza que la información consignada en un mensaje de datos permanezca completa e inalterada, salvo la adición autorizada de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.
13. **Mapa de capacidades:** conjunto de capacidades (técnicas, de proceso y de habilidades del talento humano) necesarias dentro de un sistema o modelo para implementar lo planteado en su intención. Se pueden agrupar y presentar por niveles más detallados.
14. **Marco de interoperabilidad:** Es la estructura de trabajo común donde se alinean los conceptos y criterios que guían el intercambio de información. Define el conjunto de principios, recomendaciones y directrices que orientan los esfuerzos políticos, legales, organizacionales, semánticos y técnicos de las entidades, con el fin de facilitar el intercambio seguro y eficiente de información<sup>2</sup>.
15. **Mecanismos de autenticación:** son las firmas digitales o electrónicas que, utilizadas por su titular, previamente identificado, permiten atribuirle la autoría de un mensaje de datos, sin perjuicio de la autenticación notarial.

---

<sup>2</sup> <http://lenguaje.mintic.gov.co/marco-de-interoperabilidad>



16. **Mecanismo de identificación de los colombianos:** Es el proceso mediante el cual la Registraduría Nacional le asigna un único atributo a un colombiano a través del documento de identidad (cédula de ciudadanía o cédula digital) para que pueda ser plenamente identificado en diferentes sistemas
17. **Modelo:** representación de una realidad, definida de forma correcta y suficiente mediante conceptos, instancias, atributos, valores y relaciones.
18. **La Plataforma De Interoperabilidad – PDI:** son el conjunto de herramientas necesarias que permite que los sistemas de información del Estado conversen entre sí mediante interfaces estándar de comunicación entre procesos y sistemas de información
19. **Política de Gobierno Digital:** establecida mediante Decreto 1008 del 14 de junio de 2018, cuyo objetivo es incentivar el uso y aprovechamiento de las TIC para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores que generen valor público en un entorno de confianza digital<sup>3</sup>.
20. **Prestadores de Servicios Ciudadanos Digitales:** Entidades pertenecientes al sector público o privado, quienes, mediante un esquema coordinado y administrado por el Articulador, pueden proveer los servicios ciudadanos digitales a ciudadanos y empresas, siempre bajo los lineamientos, políticas, guías, que expida el Ministerio de Tecnologías de la Información y las Comunicaciones.
21. **Privacidad por diseño y por defecto:** Desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se deben adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional, humana, procedimental) para evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como fallas de seguridad o indebidos tratamientos de datos personales. La privacidad y la seguridad deben hacer parte del diseño, arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan.
22. **Servicios Ciudadanos Digitales:** Es el conjunto de soluciones y procesos transversales que brindan al Estado capacidades y eficiencias para su transformación digital y para lograr una adecuada interacción con el ciudadano,

---

<sup>3</sup> <https://www.mintic.gov.co/portal/604/w3-article-74903.html>





garantizando el derecho a la utilización de medios electrónicos ante la administración pública. Estos servicios se clasifican en servicios base y servicios especiales.

23. **Servicios Ciudadanos Digitales Base:** son los servicios que se consideran fundamentales para brindar al Estado las capacidades en su transformación digital. Estos son Interoperabilidad, Autenticación Digital y Carpeta Ciudadana Digital.
24. **Servicios Ciudadanos Digitales Especiales:** Son servicios que brindan soluciones que por sus características realizan nuevas ofertas de valor y son adicionales a los servicios ciudadanos digitales base, o bien, corresponden a innovaciones que realizan los prestadores de servicio a partir de la autorización dada por el titular de los datos y de la integración a los servicios ciudadanos digitales base. bajo un esquema coordinado por el Articulador.
25. **Usuario de los servicios ciudadanos digitales:** Es la persona natural. nacional o extranjera, o la persona jurídica, de naturaleza pública o privada. que haga uso de los servicios ciudadanos digitales.
26. **Vista:** elementos de un modelo en donde aparecen los conceptos y relaciones (directas y calculadas) expresadas desde una perspectiva o punto de vista, que cumplen con reglas previamente definidas.



La Constitución Política en su artículo 2° establece como uno de los fines esenciales del Estado “(...) servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución (...)”.

Que la Ley 527 de 1999, “por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”, estableció 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. De la misma manera, el Decreto 2364 de 2012 por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica.

Que de conformidad con el artículo 266 de la Constitución Política modificado por el Acto Legislativo 02 de 1 de julio de 2015 en concordancia con el Decreto Ley 2241 de 1986 y el Decreto Ley 1010 de 2000, corresponde a la Registraduría Nacional del Estado Civil ejercer, entre otras, la dirección y organización de las elecciones, el registro civil y la identificación de las personas.

Conforme al principio de “masificación del gobierno en línea” hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

En virtud del artículo 17 de la Ley 1341 de 2009, “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–(...)”, modificado por el artículo 13 de la Ley 1978 de 2019, el Ministerio de Tecnologías de la Información y las Comunicaciones tiene entre sus objetivos “(...) 2. 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”.

Que la Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”, desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información personal que se haya

recogido en las bases de datos o archivos, con pleno respeto a los principios establecidos en el artículo 4, determinando en los artículos 10, 11, 12 y 13, entre otros asuntos, las condiciones bajo las cuales las entidades públicas pueden hacer tratamiento de datos personales y pueden suministrar información en ejercicio de sus funciones legales.

El artículo 45 de la Ley 1753 de 2015, “por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”, atribuye al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en coordinación con las entidades responsables de cada uno de los trámites y servicios, la función de definir y expedir los estándares, modelos, lineamientos y normas técnicas para la incorporación de las TIC, que deberán ser adoptados por las entidades estatales, incluyendo, entre otros, autenticación electrónica, integración de los sistemas de información de trámites y servicios de las entidades estatales con el Portal del Estado Colombiano, y la interoperabilidad de datos como base para la estructuración de la estrategia. Según el mismo precepto, se podrá ofrecer a todo ciudadano el acceso a una carpeta ciudadana electrónica.

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, “Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”, la Política de Gobierno Digital será definida por MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Según el mismo artículo 2.2.9.1.2.1, los habilitadores transversales de la Política de Gobierno Digital, son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha Política.

El artículo 2° de la Ley 1955 de 2019, establece que el documento denominado “Bases del Plan Nacional de Desarrollo 2018-2022: Pacto por Colombia, pacto por la equidad”, hace parte integral de esta ley. Que en las “Bases del Plan Nacional de Desarrollo 2018-2022”: Pacto por Colombia, pacto por la equidad en el pacto VII “por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento”, se incorpora como objetivo la promoción de la digitalización y

automatización masiva de trámites, a través de la implementación e integración de los servicios ciudadanos digitales, (carpeta ciudadana, autenticación electrónica e interoperabilidad de los sistemas del Estado), de forma paralela a la definición y adopción de estándares tecnológicos, al marco de arquitectura TI, a la articulación del uso de la tecnología, y todo lo anterior en el marco de la seguridad digital.

El artículo 147 de la Ley 1955 de 2019, señala la obligación de las entidades estatales del orden nacional, de incorporar en sus respectivos planes de acción el componente de transformación digital, siguiendo los estándares que para este propósito defina el MinTIC. De acuerdo con el mismo precepto, los proyectos estratégicos de transformación digital se orientarán entre otros, por los principios de interoperabilidad, vinculación de las interacciones entre el ciudadano y el Estado a través del Portal Único del Estado colombiano, y empleo de políticas de seguridad y confianza digital, para ello, las entidades públicas deberán implementar el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital y las acciones contenidas en el Conpes 3995 de 2020 cuyo fin es desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

El mismo artículo 147 de la Ley 1955 de 2019, indica que aquellos trámites y servicios que se deriven de los principios enunciados podrán ser ofrecidos tanto por personas jurídicas privadas como públicas, incluyendo a la entidad que haga las veces de articulador de servicios ciudadanos digitales, o la que defina el MinTIC para tal fin.

El artículo 9 del Decreto 2106 de 2019 “Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, señala que, para lograr mayor nivel de eficiencia en la administración pública y una adecuada interacción con los ciudadanos y usuarios, garantizando el derecho a la utilización de medios electrónicos, las autoridades deberán integrarse y hacer uso del modelo de Servicios Ciudadanos Digitales. Este mismo artículo dispone que el Gobierno nacional prestará gratuitamente los Servicios Ciudadanos Digitales base y se implementarán por parte de las autoridades de conformidad con los estándares que establezca el MinTIC.



Por ello, surge la obligación de expedir los estándares de implementación de los Servicios Ciudadanos Digitales contenidos en la guía de lineamientos de los servicios ciudadanos digitales y la guía para vinculación y uso de estos, según se desprende del artículo 2.2.17.4.1. del DURT-TIC, en concordancia con el numeral 2, literal a. del artículo 18 de la Ley 1341 de 2009.

En ese mismo sentido, con el fin de lograr una adecuada interacción con el ciudadano, garantizando el derecho a la utilización de medios electrónicos ante la administración pública, reconocido en el artículo 54 de la Ley 1437 de 2011, se han desarrollado los Servicios Ciudadanos Digitales, entendidos como el conjunto de soluciones y procesos transversales que brindan al Estado capacidades y eficiencias para su transformación digital y para lograr una adecuada interacción con el ciudadano, estos servicios se clasifican en servicios base y servicios especiales.

Para materializar lo anterior, MinTIC dispone los lineamientos que se deben cumplir para la prestación de los Servicios Ciudadanos Digitales y para facilitar a los usuarios el acceso a la administración pública a través de medios digitales, desde la aplicación de los principios de accesibilidad inclusiva, escalabilidad, gratuidad, libre elección y portabilidad, privacidad por diseño y por defecto, seguridad, privacidad y circulación restringida de la información y usabilidad.

Por lo cual, el articulador señalado en el numeral 3 del artículo 2.2.17.1.5. del Decreto 1078 de 2015, deberá cumplir las condiciones y estándares establecidos en la Guía de lineamientos de los servicios ciudadanos digitales que se encuentran señaladas, con el fin de garantizar la correcta prestación de los servicios ofertados, y, las autoridades señaladas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015, deberán cumplir las condiciones y estándares establecidos en la Guía para vinculación y uso de los servicios ciudadanos digitales que se encuentran señaladas para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán integrar a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad, carpeta ciudadana digital y vincularlos al Portal Único del Estado colombiano.

De acuerdo con lo mencionado, se ha determinado la necesidad de presentar los estándares de implementación de los Servicios Ciudadanos Digitales contenidos en la

guía de lineamientos de los servicios ciudadanos digitales. Esto incluye en el articulado las mejoras funcionales del modelo de los Servicios Ciudadanos Digitales que permitan al Articulador tener el rol de prestador de servicios para las entidades públicas, así mismo, se incluyeron mejoras a las definiciones y características de los servicios, se fortalecen los mecanismos de vinculación que estarán a disposición de las entidades para el uso y aprovechamiento de los SCD en su transformación digital.



## **5 Modelo Conceptual de los Servicios Ciudadanos Digitales**



Los Servicios Ciudadanos Digitales (SCD) proponen una solución integrada que toma en consideración las problemáticas que comúnmente tienen los ciudadanos cuando interactúan con las entidades públicas a través de canales digitales, por ejemplo, la dificultad en el intercambio de información entre las entidades, la solicitud de documentos que el ciudadano ya ha presentado y la complejidad para autenticar digitalmente a las personas en el mundo digital. Es por esto que se presentan los tres servicios base dentro del modelo de servicios ciudadanos digitales:

- a. Interoperabilidad
- b. Autenticación Digital
- c. Carpeta Ciudadana Digital

Esto con el fin de proporcionar y mejorar la interacción digital de los usuarios, atendiendo y garantizando las condiciones de calidad, seguridad, interoperabilidad, disponibilidad y acceso a la información que se consideran en la normativa vigente, adoptando las medidas necesarias para garantizar los derechos de las personas en condición de discapacidad e incluir soluciones acordes a sus necesidades.

El modelo de los Servicios Ciudadanos Digitales se presta a las entidades públicas y usuarios de manera integrada, generando mejoras en la calidad de vida de los ciudadanos y eficiencia en las entidades públicas. De esta forma, los SCD son el conjunto de soluciones y procesos transversales que brindan al Estado las capacidades y eficiencias para su transformación digital y para lograr una adecuada interacción con el ciudadano, garantizando el derecho a la utilización de medios electrónicos ante la administración pública. Estos servicios se clasifican en servicios base y servicios especiales.

El modelo de los Servicios Ciudadanos Digitales considera seis (6) actores cuyos roles se describen a continuación:

- Los usuarios de los SCD son los principales beneficiarios de los Servicios Ciudadanos Digitales, son la persona natural, nacional o extranjera, o la persona jurídica, de naturaleza pública o privada, que haga uso de los servicios ciudadanos digitales.

- Los organismos y entidades establecidos en el artículo 2.2.17.1.2 del Decreto 1078 de 2015. son los encargados de brindar los trámites y servicios a los ciudadanos y empresas, custodiar datos de los ciudadanos, empresas y colaborar armónicamente con otras entidades para intercambiar información en el ámbito de sus funciones.
- El articulador es la Agencia Nacional Digital, que será encargada de proveer y gestionar de manera integral los servicios ciudadanos digitales, además de apoyar técnica y operativamente al Ministerio de Tecnologías de la Información y las Comunicaciones para garantizar el pleno funcionamiento de tales servicios ; así mismo, es el encargado de coordinar los SCD y prestar los Servicios Ciudadanos Digitales Base a las entidades públicas siguiendo las definiciones y lineamientos que defina MinTIC, es el único con la potestad de proveer y gestionar el servicio ciudadano digital de Interoperabilidad.
- Los prestadores de SCD, serán entidades pertenecientes al sector público o privado, quienes, mediante un esquema coordinado y administrado por el Articulador, pueden proveer los servicios ciudadanos digitales a ciudadanos y empresas, siempre bajo los lineamientos, políticas, guías, que expida el Ministerio de Tecnologías de la Información y las Comunicaciones.
- El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) es la entidad encargada de generar los lineamientos, estándares, políticas, guías y reglamentación que garanticen un adecuado uso de los SCD.
- Entidades de vigilancia y control son las autoridades que en el marco de sus funciones constitucionales y legales ejercerán vigilancia y control sobre las actividades que involucran la prestación de los SCD.

El modelo de los SCD se enfoca en lograr una adecuada interacción del ciudadano con el Estado, permitiendo garantizar el derecho a la utilización de medios digitales ante la administración pública, reconocido en los artículos 53 y 54 de la Ley 1437 de 2011, estos servicios se clasifican como base y especiales.

Se consideran servicios ciudadanos digitales base, aquellos que son fundamentales para brindarle al Estado las capacidades en su transformación digital. A continuación, se definen de manera general las características y funcionalidades esenciales de esta clase de servicios:

- a. **Servicio de interoperabilidad:** Es el servicio que brinda las capacidades necesarias para garantizar el adecuado flujo de información e interacción entre los sistemas de información de las entidades, permitiendo el intercambio, la integración y la compartición de la información. con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad.
- b. **Servicio de autenticación digital:** Es el procedimiento que, utilizando mecanismos de autenticación, permite verificar los atributos digitales de una persona cuando adelanten trámites y servicios a través de medios digitales. Además, en caso de requerirse, permite tener certeza sobre la persona que ha firmado un mensaje de datos, o la persona a la que se atribuya el mismo en los términos de la Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen, y sin perjuicio de la autenticación notarial.
- c. **Servicio de carpeta ciudadana digital:** Es el servicio que le permite a los usuarios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las entidades señaladas en el artículo 2.2.17.1.2 del Decreto 1078 de 2015. Adicionalmente, este servicio podrá entregar las comunicaciones o alertas que las entidades señaladas tienen para los usuarios, previa autorización de estos.

Los **servicios digitales especiales:** Son servicios que brindan soluciones que por sus características realizan nuevas ofertas de valor y son adicionales a los servicios ciudadanos digitales base, o bien, corresponden a innovaciones que realizan los prestadores de servicio a partir de la autorización dada por el titular de los datos y de la integración a los servicios ciudadanos digitales base, bajo un esquema coordinado por el Articulador.

El servicio de Interoperabilidad para las entidades del Estado será prestado de forma exclusiva por el Articulador. Los prestadores de servicios ciudadanos digitales podrán conectarse con la plataforma de interoperabilidad del Estado, de conformidad con las condiciones que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones.

El servicio ciudadano de carpeta ciudadana digital será prestado por el Articulador de conformidad con las condiciones dadas en la presenta guía.

El servicio ciudadano digital de autenticación digital será prestado de conformidad con las disposiciones sobre firma electrónica y digital contenidas en la Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen, siguiendo los lineamientos que para tal efecto señale el Ministerio de Tecnologías de la Información y las Comunicaciones en el marco de sus competencias.

Con el objetivo de describir los conceptos principales de los Servicios Ciudadanos Digitales y la relación entre cada uno ellos, se ilustra el modelo conceptual, que corresponde a un diagrama de clases en notación de Lenguaje Unificado de Modelado (UML, por sus siglas en inglés, *Unified Modeling Language*). Adicional a la ilustración que se expone a continuación, se indica en la Tabla No. 1 la descripción de cada una de las entidades del modelo.



El modelo general de los SCD presentado en la anterior ilustración contempla que el articulador sea el encargado de coordinar y administrar las interacciones con los distintos actores involucrados en la prestación de los Servicios Ciudadanos Digitales, siendo prestador de los SCD base para los usuarios.

Las entidades como actores del modelo podrán:

- Autorizar y permitir el acceso a los trámites y servicios que ellas mismas ofrecen.
- Reducir los riesgos de suplantación de identidad.
- Evitar que en el intercambio de información con otras entidades, los usuarios aporten documentos que las entidades ya tienen.
- Permitir el acceso a los usuarios a la información que las entidades custodian.

La interacción de los usuarios con las entidades públicas se realizará teniendo en cuenta la integración y utilización del Portal Único del Estado colombiano, GOV.CO como canal de comunicación.

Tabla 1 – Descripción de las entidades del modelo conceptual.

Nombre del concepto	Descripción
ServicioCiudadanosDigitales	Los Servicios Ciudadanos Digitales pueden ser servicios digitales base o servicios digitales especiales. Los servicios base son tres (servicio de Carpeta Ciudadana Digital, servicio Autenticación Digital y servicio de Interoperabilidad).
ANS (Acuerdos de Niveles de Servicio)	Son los acuerdos de nivel de servicio, los cuales están asociados a cada uno de los Servicios Ciudadanos Digitales.
Articulador	Es el encargado de proveer y gestionar de manera integral los Servicios Ciudadanos Digitales, además de apoyar técnica y operativamente al Ministerio de Tecnologías de la Información y las Comunicaciones para garantizar el pleno funcionamiento de los Servicios Ciudadanos Digitales.
CarpetaPersonal	Es el acceso a la consulta de un conjunto de datos que custodia la administración pública de cada usuario.
CatálogoServicios	Es el catálogo de servicios de intercambio de información.
ConjuntoDatos	El conjunto de datos a intercambiar que genera un servicio de intercambio de información.

Nombre del concepto	Descripción
Dato	Identifica y define la unidad básica de información, a partir de la cual se realiza el intercambio de información de acuerdo con los requerimientos funcionales definidos dentro del proceso o servicio de intercambio de información.
DiccionarioDatos	El diccionario de datos contiene todos los metadatos y definición de los elementos de datos, conceptualizados por las entidades del estado, para el estándar de Lenguaje Común de Intercambio de Información.
Entidad	La entidad pública o privada.
FuenteAtributos	La fuente de atributos contiene datos que permiten verificar los atributos digitales asociados a la identidad de un usuario.
MecanismoAutenticación	Son las firmas digitales o electrónicas que utilizadas por su titular permiten atribuirle la autoría de un mensaje de datos. Sin perjuicio de la autenticación notarial.
MensajeComunicación	Los mensajes de comunicación generados por las entidades a los usuarios.
Metadato	Corresponde a un metadato asociado a un servicio de intercambio de información. Los metadatos describen y facilitan el entendimiento de los servicios de intercambio de información, lo que permite el acceso y la reutilización de los mismos.
MinTIC	El Ministerio de Tecnologías de la Información y las Comunicaciones.
NivelGarantía	Es el grado de confianza en los procesos que conducen a la Autenticación Digital, los cuales se clasifican en orden ascendente según su nivel de confianza entre bajo, medio, alto y muy alto.
Norma	Los elementos normativos de los Servicios Ciudadanos Digitales.
Usuario	Es la persona natural, nacional o extranjera, o la persona jurídica, de naturaleza pública o privada que haga uso de los Servicios Ciudadanos Digitales.
PrestadorServicio	Personas jurídicas, pertenecientes al sector público o privado, quienes, mediante un esquema coordinado y



Nombre del concepto	Descripción
	administrado por el articulador, pueden proveer los Servicios Ciudadanos Digitales a ciudadanos y empresas, siempre bajo los lineamientos, políticas, guías, que expida el Ministerio de Tecnologías de la Información y las Comunicaciones.
Registro	El registro generado del proceso mediante el cual los usuarios se incorporan a los servicios ciudadanos digitales como usuarios
ServicioAutenticacionDigital	Es el servicio de Autenticación Digital, que hace parte de los tres Servicios Ciudadanos Digitales base.
ServicioCarpetaCiudadana	Es el servicio de Carpeta Ciudadana Digital, que hace parte de los tres Servicios Ciudadanos Digitales base.
ServicioCuidadanoDigital	Servicios Ciudadanos Digitales es el agrupador de los servicios base y los servicios especiales.
ServicioEspecial	Son los Servicios Ciudadanos Digitales Especiales que hace parte de los Servicios Ciudadanos Digitales
ServicioIntercambioInformacion	Recurso tecnológico que mediante el uso de un conjunto de protocolos y estándares permite el intercambio de información.
ServicioInteroperabilidad	Es el servicio de Interoperabilidad, que hace parte de los tres Servicios Ciudadanos Digitales base.
TramiteServicio	Los trámites o procesos o procedimientos de las entidades públicas.
Verificacion	La verificación que se hace al registro de un usuario contra las fuentes de atributos.

Para que este modelo de SCD inicie su operación, MinTIC pone a disposición esta Guía de lineamientos de los Servicios Ciudadanos Digitales en la que se consignan las condiciones de carácter general y técnico que el articulador debe cumplir para la prestación de los Servicios Ciudadanos Digitales.



## **6 Modelo de Intención de los Servicios Ciudadanos Digitales, SCD**

Con el objetivo de ofrecer un entendimiento de la propuesta de valor de los Servicios Ciudadanos Digitales, se presenta el modelo de intención utilizando el lienzo de modelo de negocio (*Business Model Canvas* - BMC). Este modelo permite documentar y comunicar la propuesta de valor y la relación con los segmentos de clientes, las actividades clave, el modelo de ingresos y egresos, los socios clave y los recursos.

Al finalizar el diagrama se encuentran las convenciones que se utilizaron para los elementos de Carpeta Ciudadana Digital, Interoperabilidad, Autenticación Digital y para los elementos transversales.

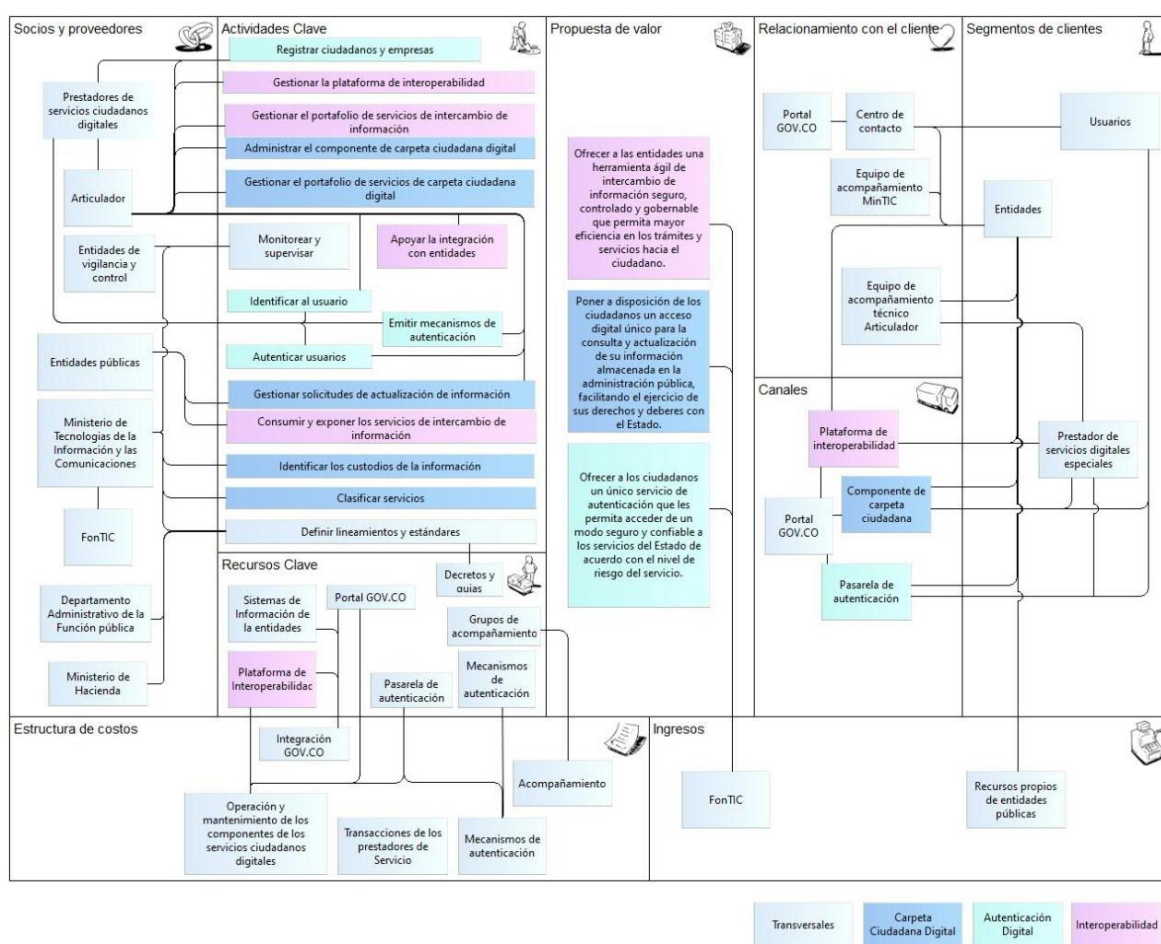


Ilustración 2 - Lienzo del modelo de negocio SCD

### **Interoperabilidad - IO:**

La propuesta de valor de interoperabilidad dirigida a las entidades públicas es ofrecer una plataforma tecnológica eficiente que permita realizar el intercambio de información entre entidades del Estado, de forma segura, controlada y gobernable buscando la eficiencia en los trámites y servicios hacia los usuarios. Las funcionalidades más relevantes que ofrece el servicio ciudadano de interoperabilidad son: gestionar la plataforma de interoperabilidad, gestionar el portafolio de servicios de intercambio de información, apoyar a las autoridades con la integración de sus servicios en la plataforma de interoperabilidad, así como consumir y exponer los servicios de intercambio de información.

### **Autenticación Digital - AD:**

La propuesta de valor para este servicio está orientada a ofrecer a los usuarios, previamente identificados, un único servicio de autenticación, que les permita acceder de un modo seguro y confiable a los trámites, procesos y procedimientos que ofrece el Estado de acuerdo con el nivel de riesgo del servicio o trámite. Para acceder a este servicio, los usuarios acceden a la pasarela de autenticación integrada al Portal Único del Estado GOV.CO. Las funcionalidades que ofrece este servicio son: autenticar y registrar usuarios, emitir los mecanismos de autenticación y autenticar a los usuarios que acceden a través de la pasarela de autenticación.

### **Carpeta Ciudadana Digital - CCD:**

La propuesta de valor del servicio de Carpeta Ciudadana Digital está dirigida a los usuarios. Este servicio ofrece un acceso digital único a comunicaciones e información que las entidades de la administración pública producen, recolectan o almacenan de ellos. Las funcionalidades claves que ofrece este servicio son administrar el componente de Carpeta Ciudadana Digital, gestionar el portafolio de servicios de CCD, visualizar los datos que las entidades públicas tienen de los usuarios y clasificar los servicios. Así mismo, este servicio les permite a los usuarios, solicitar la actualización y/o corrección de los datos ante la administración pública, por lo que se requiere generar la capacidad en el articulador de direccionar estas solicitudes a las entidades públicas. La CCD podrá

entregar las comunicaciones o alertas que las entidades tienen para los usuarios, previa autorización de estos.

## Elementos Transversales

Los elementos transversales son aquellos relacionados a más de un SCD. Para el bloque 'Segmentos de cliente' El MinTIC ha identificado a: las entidades públicas y usuarios, a quienes están dirigidas las propuestas de valor de todos los SCD. Los prestadores de SCD corresponden a los encargados de ofrecer los Servicios Ciudadanos Digitales Base y Especiales, según corresponda.

- a) **Bloque de relacionamiento:** se incluye el centro de contacto de segundo nivel el cual será ofrecido por el articulador a los usuarios. Adicionalmente se identifican los equipos de trabajo de MinTIC y del Articulador, quienes estarán acompañando a las entidades públicas en la implementación de los Servicios Ciudadanos Digitales. El Articulador adicionalmente prestará el acompañamiento a los prestadores de servicio.
- b) **Los ingresos** que soportan la implantación del modelo de los servicios ciudadanos digitales base provienen del Fondo de Tecnologías de la Información y las Comunicaciones, FONTIC. La implementación e infraestructura de las entidades públicas de los servicios de intercambio de información, la vinculación al servicio de Autenticación Digital y la Carpeta Ciudadana Digital proviene de los recursos propios de cada entidad.
- c) **Canales:** la plataforma de interoperabilidad es para las entidades el principal medio para ofrecer los trámites, procesos y procedimientos a los usuarios, quienes a su vez acceden por el Portal Único del Estado Colombiano – GOV.CO en donde adicionalmente encontraran integrado la pasarela de autenticación y el componente de Carpeta Ciudadana Digital.
- d) **Bloque de recursos:** Hacen parte del bloque de recursos, los sistemas de información de las entidades públicas productoras de información, para ofrecer servicios de intercambio de información a través de los cuales se debe realizar el intercambio de información entre las entidades públicas. El Portal Único del

Estado Colombiano GOV.CO, la pasarela de autenticación y los mecanismos de autenticación serán los recursos más importantes para ofrecer los servicios de Autenticación Digital. Adicionalmente, los grupos de acompañamiento serán un recurso muy importante para garantizar el uso y apropiación de los Servicios Ciudadanos Digitales en las entidades públicas.

- e) **Socios y colaboradores:** el Ministerio de Tecnologías de la Información y las Comunicaciones junto con el Departamento Administrativo de la Función Pública y el Ministerio de Hacienda y Crédito Público serán los encargados de definir los elementos normativos (decretos, resoluciones) aplicables a los Servicios Ciudadanos Digitales, de otra parte el Ministerio de Tecnologías de la Información y las Comunicaciones genera los estándares de implementación de los Servicios Ciudadanos Digitales contenidos en la guía de lineamientos de los servicios ciudadanos digitales, lo anterior con la debida articulación y colaboración armónica de la Registraduría Nacional del Estado Civil. El articulador, será el encargado de ejecutar las actividades relacionadas con la gestión de la plataforma de interoperabilidad, la pasarela de autenticación, el componente de Carpeta Ciudadana Digital, la administración del catálogo de servicios de intercambio de información, el registro de los usuarios, la emisión de los mecanismos de autenticación, la gestión de los prestadores de servicio y la gestión de las solicitudes de los usuarios, entre otras. Adicionalmente, el articulador será el único actor encargado de la plataforma de Interoperabilidad, las entidades públicas son aliadas en la implementación de los Servicios Ciudadanos Digitales quienes deberán consumir y exponer los servicios de intercambio de información e integrarse con el servicio de Autenticación Digital y Carpeta Ciudadana Digital. Los entes de control y vigilancia realizarán las actividades de vigilancia y control a los SCD en el ámbito de sus funciones.

## 6.1 Modelo Estratégico De Los Servicios Ciudadanos Digitales, SCD

El modelo estratégico muestra de qué manera los SCD permiten dar cumplimiento a la Política de Gobierno Digital. Esta relación se muestra en la siguiente ilustración:

# Política de Gobierno Digital



Ilustración 3 - Modelo estratégico de SCD

La Política de Gobierno Digital se desarrolla por medio de dos componentes:

- TIC para el Estado: tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades, a través del uso de las Tecnologías de la Información y las Comunicaciones.
- TIC para la sociedad: tiene como objetivo fortalecer la relación de la sociedad con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas y la identificación de soluciones a problemáticas de interés común.

Adicionalmente, la Política de Gobierno Digital tiene cinco propósitos:

- Servicios digitales de confianza y calidad
- Procesos internos seguros y eficientes
- Decisiones basadas en datos

- Empoderamiento ciudadano a través de un Estado Abierto
- Territorios y Ciudades Inteligentes a través de las TIC

Todos ellos desarrollados por medio de los habilitadores transversales, entre ellos los Servicios Ciudadanos Digitales.

## **7 Mapa de Capacidades de los Servicios Ciudadanos Digitales, SCD**



Este mapa describe las principales capacidades que el articulador debe desarrollar y mantener para prestar los Servicios Ciudadanos Digitales. Cada capacidad cuenta con un identificador único, un nombre y una descripción que pueden ser consultadas en la tabla al finalizar el diagrama. Este mapa está dividido en capacidades estratégicas, misionales y de apoyo, las cuales deberán ser desarrolladas por el articulador y aquellas en las que Ministerio de Tecnologías de la Información y las Comunicaciones realiza apoyo de acuerdo con la siguiente imagen. Para las capacidades estratégicas y de apoyo se utiliza el nivel uno (CXX) y para las misionales se desagregaron a nivel dos (CXX.XX). Las capacidades de nivel tres se encuentran en el Anexo 1 Mapa de Capacidades SCD.xlsx.



Ilustración 4 - Mapa de capacidades SCD

Tabla 2 – Descripción de las capacidades de nivel 1 de los SCD

CÓDIGO	NOMBRE	DESCRIPCIÓN
<b>C01</b>	Gestionar la estrategia de los SCD	Definir, mantener y hacer seguimiento a la estrategia de Servicios Ciudadanos Digitales con el objetivo de definir la misión y la visión estratégica que genere valor a los ciudadanos.
<b>C02</b>	Gestionar las comunicaciones de los SCD	Generar las comunicaciones externas con el objetivo de dar a conocer los Servicios Ciudadanos Digitales a los actores involucrados.
<b>C03</b>	Gestionar la normatividad de los SCD	Generar normatividad relacionada con los Servicios Ciudadanos Digitales.
<b>C04</b>	Gestionar la implementación de los Servicios Ciudadanos Digitales	Realizar la identificación de las necesidades en las entidades para la implementación de los Servicios Ciudadanos Digitales.
<b>C05</b>	Gestionar el Servicio de Autenticación Digital	Administrar integralmente el servicio de autenticación digital en la verificación, registro, emisión de los mecanismos de autenticación y la autenticación de los usuarios, así como la administración de los mecanismos utilizados.
<b>C06</b>	Gestionar la atención al usuario	Administrar la atención al usuario gestionando las solicitudes y comunicaciones a los usuarios de los servicios ciudadanos digitales.
<b>C07</b>	Gestionar el servicio de Carpeta Ciudadana Digital	Administrar y configurar el servicio de Carpeta Ciudadana Digital y los servicios que se incorporan en ella.
<b>C08</b>	Gestionar los prestadores de servicio	Integrar y administrar los prestadores de servicio que ofrecen los servicios ciudadanos digitales base y especiales.
<b>C09</b>	Gestionar la plataforma de interoperabilidad	Administrar, configurar y dar soporte de la plataforma de Interoperabilidad.
<b>C10</b>	Gestionar tecnología e información	Planear, ejecutar y mantener los servicios de tecnología e información, en especial los incidentes de TI, problemas y requerimientos de los Servicios Ciudadanos Digitales, así

CÓDIGO	NOMBRE	DESCRIPCIÓN
		como el desarrollo de nuevos servicios de intercambio de información.
<b>C11</b>	Gestionar los servicios administrativos y jurídicos	Gestionar los servicios jurídicos asociados a los SCD, gestionar el talento humano que permite ofrecer los SCD, gestionar los procesos contractuales requeridos para la implementación de los SCD.
<b>C12</b>	Gestionar la seguridad de la información	Gestionar las políticas, controles, incidentes de seguridad y privacidad de la información que permiten garantizar la disponibilidad, integridad y confidencialidad de los SCD.

Tabla 3 – Capacidades de Nivel 2 de los Servicios Ciudadanos Digitales

COD	CAPACIDAD NIVEL 2	DESCRIPCIÓN
<b>C01.01</b>	Definir la estrategia de SCD	Construir la estrategia de los SCD.
<b>C01.02</b>	Hacer seguimiento a la estrategia de los SCD	Monitorear los indicadores asociados a la estrategia de SCD y ejecutar las acciones de mejora en caso de ser necesario.
<b>C02.01</b>	Definir el plan de comunicaciones de los SCD	Construir el plan de comunicaciones de los SCD.
<b>C02.02</b>	Ejecutar el plan de comunicaciones de los SCD	Poner en marcha el plan de comunicaciones de los SCD.
<b>C02.03</b>	Monitorear el plan de comunicaciones de los SCD	Realizar seguimiento y control a la ejecución del plan de comunicaciones de los SCD.
<b>C03.01</b>	Elaborar la normatividad de los SCD	Definir políticas y lineamientos asociados a los SCD.
<b>C03.02</b>	Publicar la normatividad de los SCD	Publicar las políticas y lineamientos asociados a los SCD.
<b>C03.03</b>	Mantener actualizada la normatividad de los SCD	Actualizar de forma periódica la normatividad asociada a los SCD.

COD	CAPACIDAD NIVEL 2	DESCRIPCIÓN
<b>C04.01</b>	Identificar los servicios de intercambio de información	Realizar la identificación de los servicios de intercambio de información realizando la definición de cada uno en el catálogo de servicios.
<b>C04.02</b>	Gestionar los custodios de los datos	Identificar y definir la entidad que custodia los datos de los servicios de intercambio de información.
<b>C04.03</b>	Gestionar el diccionario de datos	Construir, publicar y mantener actualizado el diccionario de datos de los SCD.
<b>C04.04</b>	Gestionar los ANS	Definir y hacer seguimiento a la medición de los Acuerdos de Niveles de Servicio (ANS) para garantizar las condiciones de calidad de los servicios de intercambio de información utilizados para los SCD.
<b>C05.01</b>	Verificar identificación de usuarios	<p>El prestador de servicios debe obtener del usuario los atributos relacionados con la identidad de la persona a registrar y verificar que estos sean los que le correspondan.</p> <p>En el caso de ciudadanos colombianos, la verificación de identificación se realiza con la Registraduría Nacional del Estado Civil.</p>
<b>C05.02</b>	Registrar usuarios	Si es superada satisfactoriamente la verificación de los atributos relacionados al usuario, el prestador de servicios debe realizar el proceso de registro del usuario.
<b>C05.03</b>	Autenticar usuarios	Cuando el usuario requiere acceder a un servicio en línea, inicia sesión autenticándose en el sistema con los mecanismos de autenticación emitidos durante el registro.
<b>C05.04</b>	Administrar los mecanismos de autenticación	Administrar y configurar los mecanismos de Autenticación Digital para garantizar su seguridad.
<b>C06.01</b>	Gestionar las solicitudes	Recibir, analizar y remitir a las entidades públicas las solicitudes de los usuarios de los SCD cuando proceda y atender las solicitudes que corresponda al prestador de servicio
<b>C06.02</b>	Gestionar los mensajes al usuario	Generar los mensajes de comunicación para los usuarios sobre los Servicios Ciudadanos Digitales.
<b>C06.03</b>	Acompañar a las entidades públicas	Realizar el acompañamiento técnico a las entidades públicas que lo requieran durante la implementación y operación de los SCD.
<b>C07.01</b>	Administrar los servicios de Carpeta Ciudadana	Configurar y clasificar los servicios de información que están disponibles en la Carpeta Ciudadana Digital.



COD	CAPACIDAD NIVEL 2	DESCRIPCIÓN
<b>C07.02</b>	Gestionar componente de Carpeta Ciudadana	Configurar el componente de Carpeta Ciudadana Digital.
<b>C08.03</b>	Monitorear la prestación de servicio	Realizar el monitoreo de los servicios para garantizar la correcta prestación.
<b>C08.04</b>	Administrar los SCD especiales	Identificar, planear y coordinar los SCD especiales.
<b>C09.01</b>	Integrar nuevos servicios en la plataforma	Integrar los nuevos servicios de intercambio de información en la plataforma de Interoperabilidad.
<b>C09.02</b>	Administrar la seguridad de la plataforma de interoperabilidad	Administrar los mecanismos de seguridad en la plataforma de Interoperabilidad.
<b>C09.03</b>	Administrar la plataforma de interoperabilidad	Administrar y realizar mantenimiento a la plataforma de Interoperabilidad.
<b>C09.04</b>	Operar la plataforma de interoperabilidad	Operar la plataforma de Interoperabilidad.
<b>C09.05</b>	Gestionar reportes de información	Generar los reportes sobre el estado y uso de la plataforma de Interoperabilidad.
<b>C10.01</b>	Gestionar los requerimientos	Gestionar los requerimientos funcionales nuevos de las soluciones tecnológicas que soportan los Servicios Ciudadanos Digitales.
<b>C10.02</b>	Gestionar los incidentes de TI	Gestionar los incidentes de las soluciones tecnológicas que soportan los Servicios Ciudadanos Digitales.
<b>C10.03</b>	Implementar Política De Gobierno Digital	Implementar el habilitador transversal de SCD de la Política De Gobierno Digital.
<b>C10.04</b>	Implementar las mejoras a los SCD	Implementar las mejoras de las soluciones tecnológicas que soportan los Servicios Ciudadanos Digitales.
<b>C10.05</b>	Gestionar infraestructura tecnológica	Gestionar la infraestructura tecnológica de las soluciones que soportan los Servicios Ciudadanos Digitales.
<b>C10.06</b>	Gestionar la Configuración	Gestionar la configuración de los servicios tecnológicos que soportan los Servicios Ciudadanos Digitales.
<b>C10.07</b>	Gestionar los cambios	Gestionar los cambios asociados a las soluciones de tecnología e información que soportan los SCD.



COD	CAPACIDAD NIVEL 2	DESCRIPCIÓN
<b>C10.08</b>	Desarrollar soluciones de tecnología e información	Gestionar el desarrollo de los requerimientos funcionales y no funcionales de las soluciones de tecnología e información que soportan los Servicios Ciudadanos Digitales mediante un proceso formal de desarrollo de software.
<b>C11.01</b>	Gestionar procesos contractuales	Ejecutar los procesos contractuales que permitan adquirir los bienes y servicios asociados a los Servicios Ciudadanos Digitales.
<b>C11.02</b>	Gestionar servicios jurídicos	Prestar los servicios relacionados con la defensa jurídica asociada a los Servicios Ciudadanos Digitales.
<b>C11.03</b>	Gestionar información financiera y contable	Gestionar los recursos financieros asociados con los Servicios Ciudadanos Digitales.
<b>C12.01</b>	Gestionar los riesgos	Gestionar los riesgos de seguridad de la información asociados a la prestación de los SCD.
<b>C12.02</b>	Gestionar los controles de seguridad de la información	Realizar la definición de las políticas de seguridad de la información e implementación de controles asociados a los Servicios Ciudadanos Digitales.
<b>C12.03</b>	Gestionar las políticas de seguridad de la información	Realizar la definición de las políticas de seguridad de la información e implementación de controles asociados a los Servicios Ciudadanos Digitales.



Bajo un escenario tradicional de Interoperabilidad, cuando una entidad pública requiere información necesaria para la prestación de un servicio en el que tenga que ver otra entidad, debe obtenerla directamente de la entidad involucrada o productora de la información, y no solicitándola al usuario, a través del intercambio de información automatizado sobre la plataforma de interoperabilidad del Estado. La misma dinámica aplica para cualquier intercambio de información que se produzca entre entidades públicas.

Este concepto se denomina servicio de intercambio de información y se representa en la Ilustración 5 – Servicio de Intercambio de Información.

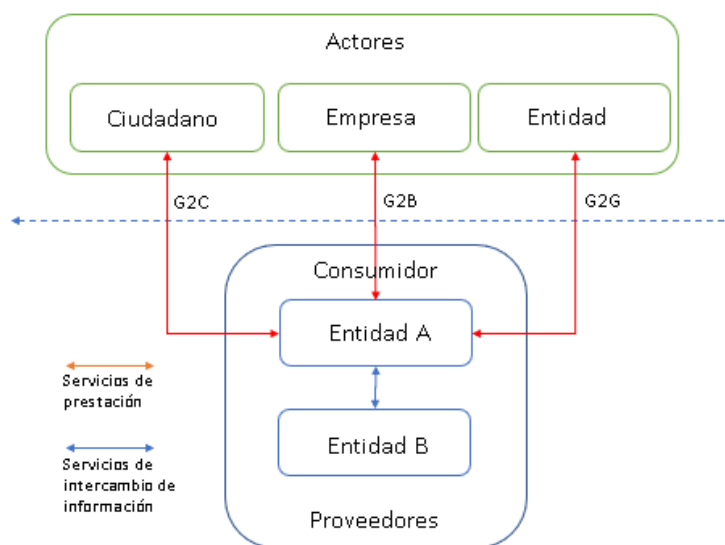


Ilustración 5 – Servicio de Intercambio de Información

El servicio de intercambio de información es el resultado de la forma en la que dos o más entidades coordinan su actuar, para garantizar que el intercambio de información entre ellas se realice de forma legal, correcta y eficiente. Esta concepción permite que su puesta en funcionamiento resulte fundamentalmente más sencilla desde el punto de vista legal y político.

Teniendo en cuenta lo anterior, la política de Gobierno Digital espera que el servicio de interoperabilidad se convierta en un instrumento que les permita a las entidades públicas poner en funcionamiento el intercambio de información desde el dominio técnico definido en el Marco de interoperabilidad para Gobierno Digital, el cual define el conjunto de elementos que orientan el intercambio de información a nivel público. Sin embargo, desde



el dominio técnico, con el rápido desarrollo de soluciones diversas en el ámbito de la integración de aplicaciones, ha surgido la necesidad de la normalización de las capacidades de una plataforma que permita facilitar la materialización de los servicios de intercambio de información entre las entidades, a la vez que se procure la máxima eficiencia y una fácil integración dentro de la dinámica de la administración pública. Se debe garantizar un desarrollo escalable, replicable y funcional, que también facilite la diversificación y un mayor número de elementos entre los cuales elegir a la hora de desarrollar proyectos de Interoperabilidad en las entidades y usuarios.

Para que las entidades públicas puedan alcanzar la Interoperabilidad, es fundamental que los servicios de intercambio de información, las aplicaciones y los sistemas de información de los cuales disponen, tengan las capacidades y funcionalidades necesarias para este intercambio, sin embargo, no todas las entidades desarrollan la interoperabilidad con los niveles de seguridad, confiabilidad, oportunidad, trazabilidad y valor probatorio suficiente y ajustados a los lineamientos de la política de gobierno digital ni del marco de interoperabilidad, ya sea por dificultades técnicas, operativas o de costos. Es aquí donde el servicio de interoperabilidad apoyará a las entidades con el fin de vincularlas a la plataforma para ofrecer una interoperabilidad fluida.

El servicio de Interoperabilidad les permitirá a las entidades compartir la información y los recursos (datos, documentos y expedientes) que se generan en los diferentes niveles de la administración pública, evitando a usuarios tener que presentar los mismos datos y documentos en diferentes sistemas o entidades, aportando al ciudadano trámites y servicios digitales ágiles aún aquellos que implican a diferentes entidades públicas. Para esto, se espera que las entidades puedan desarrollar los siguientes tipos de intercambio básico:

- **Intercambio de expedientes electrónicos (grandes volúmenes de datos):** automatización del envío de un expediente completo de una entidad a otra en los diferentes escenarios administrativos en los que se puede producir. Esto permite minimizar el gasto en mensajería, agilizar los plazos y facilitar la interacción entre diferentes órganos administrativos, lo que redundará en una mayor eficiencia administrativa y puede conducir hacia una simplificación general de las relaciones del ciudadano con las diferentes administraciones públicas.

- **Intercambio de documentos.** Envío de documentos individuales entre dos entidades (certificaciones, informes técnicos, resoluciones, etcétera): todo ello permite a las administraciones, el ahorro de costos derivados de la progresiva desaparición del formato papel, vinculado tanto a su gestión como a su conservación, como con los costos derivados de todos los movimientos físicos del papel durante su ciclo de vida.
- **Intercambio de datos:** sustitución de documentos que aporta el usuario, por servicios de intercambio de datos que permiten verificar la información necesaria. Este intercambio de datos es un servicio que beneficia a todas las partes: al usuario quien evita gastos y molestias por obtener algún documento; la entidad destino, que elimina la necesidad de gestionar el documento en papel; y la entidad emisora, que reduce la carga de trabajo que supone la generación de documentos para el usuario.

## 8.1 Alineación del servicio de interoperabilidad y el marco de interoperabilidad

El servicio de Interoperabilidad busca lograr la consolidación de un ecosistema de información pública unificado, que permita la adecuada interacción entre los sistemas de información de las entidades del Estado, a través de la provisión de una estructura tecnológica, para enviar y recibir información relevante, que les facilite a los ciudadanos la gestión de trámites y servicios. La utilización del servicio ciudadano digital de Interoperabilidad va acompañada de la adopción del Marco de Interoperabilidad<sup>4</sup>.

Considerar la Interoperabilidad, con y en el Estado, requiere tener en cuenta tanto la diversidad tecnológica de las entidades, como la organizacional, política y cultural con

---

<sup>4</sup> <https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8117.html>

relación a los procesos de generación de información. Esto hace que alcanzar la Interoperabilidad sea un proceso no lineal y complejo, que debe encararse de manera múltiple y considerando la coexistencia de diferentes niveles de desarrollo en cualquiera de las dimensiones que plantea el Marco de Interoperabilidad. Por tal motivo, es indispensable determinar estándares y unificar criterios que permitan el intercambio de información bajo un modelo de Interoperabilidad uniforme. De esta manera, el modelo de Interoperabilidad ubica su accionar como un instrumento dentro de la dimensión técnica del Marco de Interoperabilidad con el fin de facilitar el acceso a recursos tecnológicos que permiten el intercambio electrónico y digital de información.



Ilustración 6 - Alineación modelo / Marco de Interoperabilidad

## 8.2 Objetivos del servicio de interoperabilidad

Los objetivos que se buscan con el servicio de Interoperabilidad se basan en brindar las capacidades técnicas a las entidades del Estado como un elemento transversal habilitador para interoperar con otras entidades públicas, empresas y ciudadanos, como usuarios de los Servicios Ciudadanos Digitales.

- Interacción de usuarios con entidades públicas, desde la Carpeta Ciudadana Digital y la Autenticación Digital para la verificación de atributos digitales.
- Intercambio de datos entre una o más entidades estatales para resolver trámites y dar respuesta a ciudadano/empresa.
- Intercambio de datos para resolver temas propios de las entidades.
- Intercambios de información entre países.

Se espera que este modelo de Interoperabilidad permita a las entidades públicas:

- Ser más sostenibles (en lo social, económico, amigables con el medioambiente).
- Ser más eficientes.
- Mejorar la calidad de los servicios que prestan a los usuarios, mediante el uso de la tecnología.

Estos tres grandes objetivos se concretan en:

- a. Mejorar la calidad de los servicios de intercambio de información prestados, y el control de los contratos de servicios generados, evaluando la evolución de la gestión de dichos servicios en las entidades públicas.
- b. Mejorar el modelo de gobernanza del Marco de Interoperabilidad, optimizando la gestión relacional de las entidades públicas fomentando un mayor alcance de entidades y usuarios.
- c. Aumentar la información disponible y los servicios adicionales que de ella se deriven para los usuarios, mediante difusión a través de la plataforma de Interoperabilidad.
- d. Aportar a un Gobierno abierto, ofreciendo transparencia mediante la apertura de datos de forma estandarizada, consistente, unificada e integral.
- e. Reducir el gasto público y mejorar la coordinación entre diferentes servicios y administraciones públicas.
- f. Apoyar y mejorar la toma de decisiones por parte de los sujetos obligados de la política de Gobierno Digital, a través de información en tiempo real.
- g. Fomentar la innovación y el emprendimiento, favoreciendo con ello el desarrollo de nuevos negocios e ideas.
- h. Mejorar la transparencia de la función pública y la participación ciudadana por medios digitales a través de los trámites de las entidades.

- i. Medir los resultados de la gestión de la Interoperabilidad y su impacto en la administración pública, el relacionamiento con las empresas y la calidad de vida del ciudadano.
- j. Evolucionar hacia un modelo autogestionado y sostenible, tanto en consumo de recursos, como en eficiencia en servicios de intercambio de información.
- k. Ofrecer una plataforma integral de Interoperabilidad como servicio que facilite la circulación de información entre las entidades, incorporar librerías para el intercambio de información, permitir la composición, orquestación y definición de reglas sobre los servicios de intercambio de información, proporcionar interfaces de entrada - salida y la inteligencia del sistema para administrar los recursos.

## 8.3 Vista de contexto del servicio de interoperabilidad

La vista de contexto que se muestra en la ilustración No. 07 del servicio de interoperabilidad presenta cómo se relacionan los actores, y muestra las interacciones que se realizan cuando se presenta un intercambio de información desde los Servicios Ciudadanos Digitales.

Los actores que participan en el modelo de contexto del servicio de Interoperabilidad y sus principales obligaciones y roles, son:

**Ministerio de Tecnologías de la Información y las Comunicaciones:** define y señala la política a seguir en materia de Interoperabilidad. Por esta razón se encarga de:

- Establecer los requisitos, criterios técnicos y condiciones para la plataforma de interoperabilidad.
- Establecer los requisitos, criterios técnicos y condiciones para el acceso y utilización de la plataforma por parte de las entidades públicas.

**Entidades:** Encargadas de vincular a sus sistemas de información los servicios para interoperar con otras entidades y empresas (publicar y consumir servicios de información). Para lo cual deben:

- Definir y acordar junto con las demás entidades públicas participantes, el alcance de sus responsabilidades en la provisión de servicios de intercambio de información.
- Atender los procesos establecidos en los lineamientos del Marco de Interoperabilidad para la provisión de servicios de intercambio de información.
- Desarrollar las competencias y habilidades para usar y prestar los servicios de intercambio de información.
- Proveer y consumir los servicios de intercambio de información a través de la plataforma de Interoperabilidad.
- Adecuar los procesos relacionados con trámites y servicios que ofrecen a usuarios y otras entidades públicas, para propiciar en el menor tiempo posible la utilización de servicios de intercambio de información.
- Solicitar a MinTIC la incorporación de las definiciones semánticas o estándares internacionales al Lenguaje Común de Intercambio de Información.
- Asegurar que los servicios y sistemas de información a su cargo mantengan la capacidad de interoperar, como una cualidad integral desde su diseño.

Dentro del esquema de Interoperabilidad, las entidades pueden cumplir los siguientes roles:

- **Proveedor:** se consideran proveedores de información aquellas entidades públicas o particulares que son fuente de información y que habilitan servicios para suministrar datos a otras entidades que lo requieran, en el ámbito de su competencia.
  - a. Definir las autorizaciones de acceso a los servicios de intercambio de información que ofrece, estableciendo los protocolos y condiciones de acceso, los métodos de consulta permitidos, así como la información a conocer de cada entidad que solicita.
  - b. Definir los casos de rechazo o denegación de una solicitud.
  - c. Definir la política de auditoría y realizará auditorías periódicas sobre el uso del servicio de Interoperabilidad.
  - d. Establecer las condiciones técnicas de acceso y auditoría a los servicios de intercambio de información que ofrece.

- e. Definir los controles y criterios de acceso a los datos necesarios para garantizar la confidencialidad de la información según las políticas y procedimientos de gestión y control de acceso de usuarios y entidades que establezca.
  - f. Definir los Acuerdos de Nivel de Servicio (ANS) para regular las condiciones de prestación de los servicios y mecanismos de respuesta a incidencias específicos acorde a la criticidad del servicio que se está prestando.
  - g. Facilitar la información para el directorio de servicios de intercambio de información, donde estará el registro de sus servicios de intercambio disponibles, que están a disposición de otras entidades para su consulta.
- **Cliente:** hace referencia a aquellas entidades públicas o particulares autorizados para consultar o acceder a los servicios de información publicados en la PDI (Plataforma de Interoperabilidad) con el objeto de optimizar sus procesos de negocio, automatizar los trámites y servicios al usuario.
    - a. Solicitar información en relación con los trámites y procedimientos autorizados por el proveedor y dentro del marco de un procedimiento administrativo.
    - b. Cumplir con las condiciones de acceso a los datos establecidas por el proveedor.
    - c. Utilizar la información obtenida de cada consulta para la finalidad que corresponda en cada caso, realizando una misma consulta tantas veces como sea necesario, y lo requiera el trámite al que se refiera la consulta, atendiendo los principios para el tratamiento de datos personales establecidos en el Art. 4 de la Ley 1581 de 2012, entre otros, el principio de finalidad y el de acceso y circulación restringida"
    - d. Colaborar en las labores de auditoría cuando sea requerido, facilitando al proveedor la información o documentos necesarios para el control de las consultas.

Sin perjuicio de lo anterior, en el tratamiento de datos personales, tanto las entidades proveedoras como las entidades clientes, son responsables del tratamiento, conforme lo establecido en la Ley 1581 de 2012 y el título 17 de la parte 2 del libro 2 del DUR-TIC.

- **Articulador:** La Agencia Nacional Digital será la encargada de proveer y gestionar de manera integral los servicios ciudadanos digitales, además de apoyar técnica y operativamente al Ministerio de Tecnologías de la Información y las Comunicaciones para garantizar el pleno funcionamiento de tales servicios. En este orden, es la entidad encargada de adelantar las interacciones con los distintos actores involucrados en la prestación, entre otros, del Servicio Ciudadano Digital de Interoperabilidad para lograr una prestación coordinada y adecuada de los servicios, y quien provee este servicio a las entidades facilitando el intercambio de los datos desde un punto de vista tecnológico. Su función es proporcionar una plataforma de Interoperabilidad que garantice la comunicación transparente, continua y segura. Como prestador del servicio de Interoperabilidad es responsable del aprovisionamiento, habilitación, configuración, mantenimiento, operación, soporte a usuarios y acompañamiento a entidades, ajustado a los lineamientos, políticas, directrices generadas por MinTIC y de conformidad con el Marco de Interoperabilidad vigente, adicionalmente:
  - a. Coordinar las interacciones con los distintos actores involucrados en la prestación de los servicios ciudadanos digitales.
  - b. Prestar el servicio de interoperabilidad para las entidades del Estado. Para ello, realizará las actividades señaladas en el artículo 2.2.17.4.6 del Decreto 1078 de 2015.
  - c. Proponer para aprobación del Ministerio de Tecnologías de la Información y las Comunicaciones los aspectos técnicos a formalizar en la Guía para vinculación y uso de los servicios ciudadanos digitales.
  - d. Prestar los servicios ciudadanos digitales cuando se requiera.
  - e. Celebrar los acuerdos necesarios con las entidades públicas y particulares que desempeñen funciones públicas para que éstas puedan vincularse e implementar en sus sistemas de información los servicios ciudadanos digitales.
  - f. Administrar los servicios de información necesarios para la integración y unificación de la entrada a los servicios ciudadanos digitales.
  - g. Administrar en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones el directorio de servicios de intercambio de información.



- h. Monitorear los indicadores de calidad y uso de los servicios ciudadanos digitales.
- i. Tramitar y responder las peticiones, quejas, reclamos y solicitudes de información que le presenten los actores del sistema en materia de servicios ciudadanos digitales y que sean de su competencia.
- j. Asistir a todas las reuniones a las que sea convocado por el Ministerio de Tecnologías de la Información y las Comunicaciones para hacer seguimiento a sus labores.
- k. Generar reportes de prestación del servicio, conforme lo disponga la Guía de lineamientos de los servicios ciudadanos digitales.
- l. Diseñar y desarrollar en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones estrategias de comunicación y difusión que permitan dar a conocer los riesgos asociados a la implementación de los servicios ciudadanos digitales.
- m. Comunicar al Ministerio de Tecnologías de la Información y las Comunicaciones la forma en que se estén prestando los servicios ciudadanos digitales, entre otros, comunicar el cumplimiento o incumplimiento de los estándares de seguridad, privacidad, acceso, neutralidad tecnológica, o cualquier otra circunstancia requerida por el Ministerio de Tecnologías de la Información y las Comunicaciones, en el marco de la ejecución del modelo de servicios ciudadanos digitales.
- n. Presentar al Ministerio de Tecnologías de la Información y las Comunicaciones los informes necesarios sobre el nivel de implementación de los servicios ciudadanos digitales por parte de los sujetos obligados, atendiendo al plazo de gradualidad establecido en el artículo 2.2.17.7.1 del Decreto 1078 de 2015.
- o. Comunicar a los prestadores de servicios ciudadanos digitales las modificaciones o actualizaciones de la Guía para vinculación y uso de los servicios ciudadanos digitales.
- p. Atender de manera oportuna los requerimientos que, en cualquier momento, le solicite MinTIC en el marco de la prestación del servicio de interoperabilidad.
- q. Cumplir con las actividades presentadas en el modelo operativo de Interoperabilidad.

- r. Contar con todos los permisos y licencias necesarios para prestar los servicios de Interoperabilidad, con las capacidades y características que se solicitan.
- s. Establecer y ejecutar planes de contingencia cuando ocurran eventos de fuerza mayor o caso fortuito que afecten la prestación de los servicios.
- t. Contar con sistemas de respaldo que permitan la prestación de los servicios de intercambio de información de las entidades cuando haya una interrupción.
- u. Colaborar con las entidades públicas para la configuración y operación de los servicios de intercambio de información y la resolución de fallas e interrupciones.
- v. Aplicar las condiciones técnicas de acceso, los métodos de consulta permitidos, los controles y auditoría técnica sobre los servicios de intercambio de datos que definen las entidades públicas que son proveedoras de datos.
- w. Aplicar los controles y criterios de acceso a los datos necesarios para garantizar la confidencialidad de la información: políticas y procedimientos de gestión y control de acceso de usuarios y entidades.
- x. Asegurar la confidencialidad e integridad de la información intercambiada a través de los mecanismos correspondientes.
- y. Informar sobre la disponibilidad de cada servicio de intercambio bajo su responsabilidad, así como sobre los mecanismos de soporte y resolución de incidencias disponibles en cada caso, incluyendo los datos de contacto para dichos servicios.
- z. Monitorear y alertar sobre el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) que regulan las condiciones de prestación del servicio de interoperabilidad.
- aa. Mantener la trazabilidad de todas las peticiones recibidas y respuestas generadas sobre las plataformas operadas.
- bb. Realizar las labores de supervisión y monitoreo necesarias para mantener un correcto funcionamiento de los servicios de intercambio de información.
- cc. No almacenar información personal de ningún titular derivada de cualquier transacción de intercambio de datos.
- dd. Mantener el sistema en funcionamiento 24/7.

- ee. Dar soporte a las entidades y gestionar todas las comunicaciones e incidencias producidas en la operación del servicio colaborando para ello con proveedores y usuarios a través de una mesa de servicio.
  - ff. Mantener un centro de atención a entidades que canalice todas las incidencias a la mesa de servicio.
  - gg. Elaborar informes de actividad y uso de la Plataforma considerando las consultas realizadas desde y hacia cada entidad.
  - hh. Evolucionar y mantener sus sistemas garantizando la seguridad y privacidad de los datos acorde a la normativa aplicable.
  - ii. Las demás establecidas en el artículo 2.2.17.5.6. del decreto 1078 de 2015.
- **Prestadores de Servicios Ciudadanos Digitales:** Personas jurídicas, públicas o privadas, quienes, mediante un esquema coordinado y administrado por el articulador, pueden proveer los Servicios Ciudadanos Digitales de Autenticación digital y Carpeta Ciudadana Digital y que pueden acceder al servicio de interoperabilidad prestado por el articulador en el contexto de la prestación de los Servicios Ciudadanos Digitales Base o Especiales.
  - **Usuarios:** para el servicio de interoperabilidad serán principalmente las entidades públicas o privadas que cumplen funciones públicas. Sin embargo, también puede representar la persona natural, nacional o extranjera titular de cédula de extranjería, o la persona jurídica, de naturaleza pública o privada, que hace uso de los Servicios Ciudadanos Digitales.
  - **El Portal Único del Estado Colombiano GOV.CO:** Herramienta de la estrategia de integración digital y el punto de acceso digital del usuario a los trámites, procesos y procedimientos, servicios, información pública, ejercicios de participación que ofrece a las entidades públicas un espacio cercano y ágil para desarrollar la Política de Gobierno Digital.

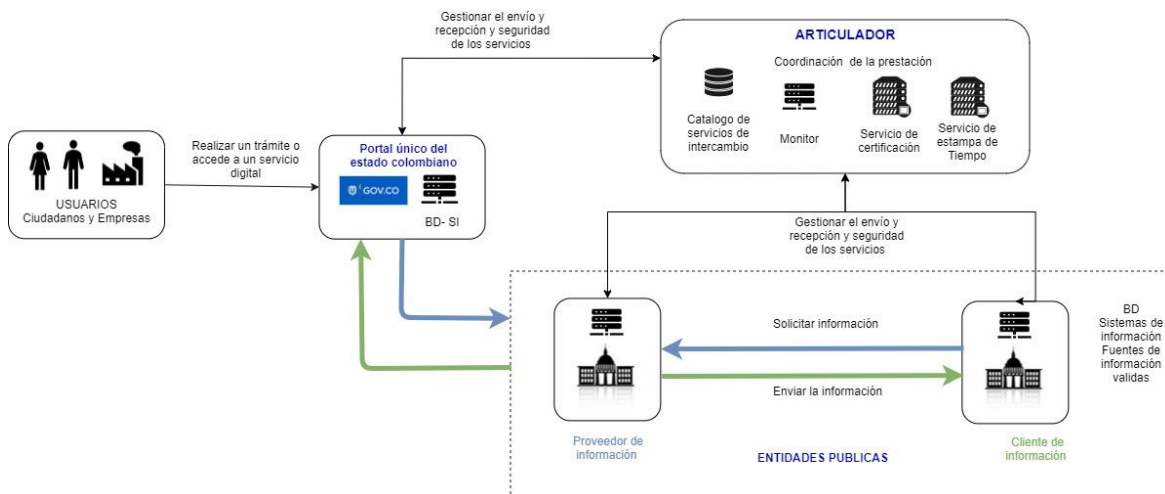


Ilustración 7 – Modelo de contexto del servicio IO

Tabla 4 – Relaciones del Modelo de contexto servicio de Interoperabilidad (IO)

Relaciones del modelo de contexto			
Relación	Origen	Destino	Descripción
<b>Realizar un trámite o acceder a un servicio digital</b>	Usuarios	Portal Único del Estado colombiano (GOV.CO)	Permite utilizar los servicios de intercambio de información a través del Portal Único del Estado colombiano (GOV.CO) o desde el sistema de información de la entidad pública para realizar un trámite o acceder a un servicio digital
<b>Gestionar el envío y recepción de los servicios características de seguridad</b>	Portal Único del Estado colombiano (GOV.CO)	Articulador	Permite la administración de los servicios de intercambio de información, garantiza la integridad de los mensajes de datos que se intercambian entre las entidades y realiza el monitoreo de la operación de la plataforma de Interoperabilidad, como por ejemplo cuántos servicios se han llamado, cuántas veces,
	Entidades públicas o privadas		
	Prestadores de servicio		

Relaciones del modelo de contexto			
Relación	Origen	Destino	Descripción
			cuál es el tiempo de respuesta promedio, etc.
<b>Solicitar información</b>	Cliente de información	Proveedor de información	Permite usar el servicio de intercambio de información enviando una solicitud para pedir los datos de interés al proveedor.
<b>Enviar información</b>	Proveedor de información	Cliente de información	Permite la provisión de los datos al cliente, en respuesta a la solicitud presentada.

## 8.4 Mapa de capacidades del servicio de Interoperabilidad

El mapa de capacidades del servicio de Interoperabilidad (IO) corresponde al tercer nivel del modelo de capacidades de los Servicios Ciudadanos Digitales de la Ilustración 8 de esta guía. Las capacidades de este nivel se pueden consultar en el siguiente anexo: Anexo 2 Mapa de Capacidades SCD.xlsx.

Serán capacidades del servicio de Interoperabilidad aquellas que estén marcadas con "X" en la columna "IO". Adicionalmente, dentro del mapa también se especifica qué actor es necesario para desarrollar la capacidad, marcada con "X" la columna con el nombre del actor (articulador, prestador de servicios, Entidad, MinTIC).

## 8.5 Modelo de despliegue del servicio de Interoperabilidad

A continuación, se presenta el modelo de despliegue de primer nivel del servicio de Interoperabilidad, a partir del cual, se debe cumplir con la oferta del servicio a entregar:

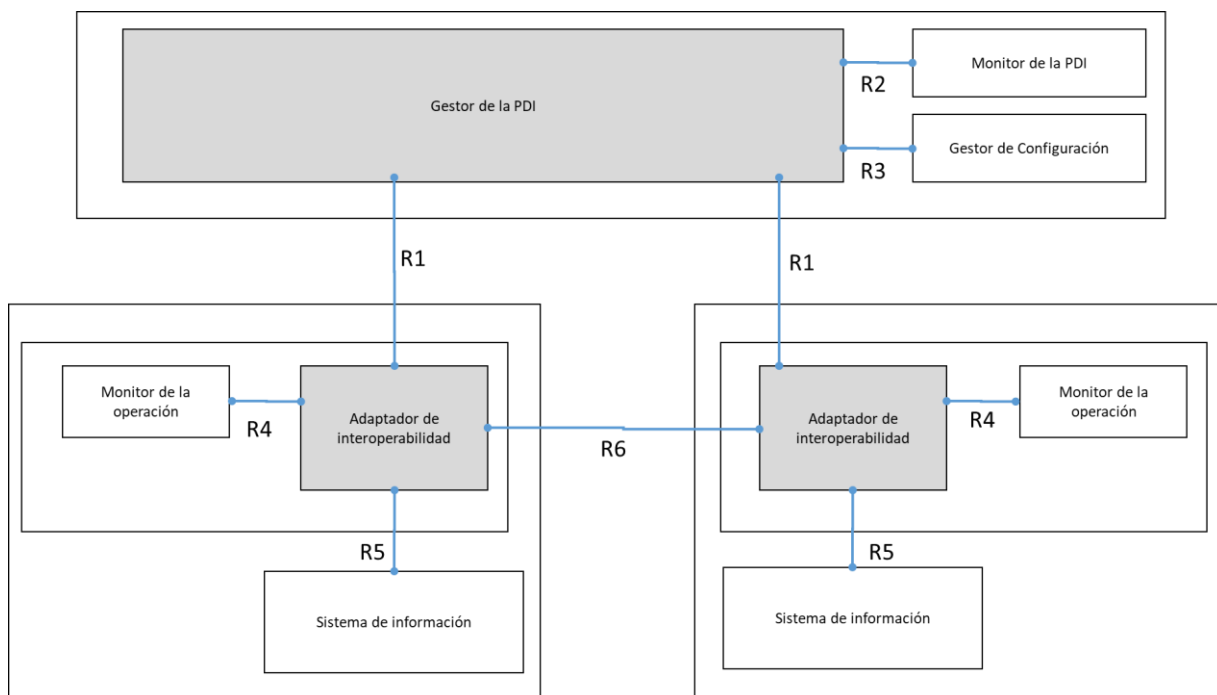


Ilustración 8 - Modelo de despliegue IO

De esta forma a continuación se hace la descripción de los componentes del modelo de despliegue del servicio de Interoperabilidad.

- a) **Gestor de la plataforma de Interoperabilidad:** administra la configuración global de la plataforma de Interoperabilidad, gestiona la agregación y eliminación de entidades, los parámetros de configuración de la plataforma, administra la información de los servicios de intercambio de datos y la política de seguridad mediante los siguientes componentes:
  - Servicio de certificados digitales de autenticación
  - Servicio de certificados digitales para firma
  - Servicio de estampa cronológica de tiempo.
  - Servicios de verificación de estado de los certificados digitales.
- b) **La plataforma central:** proporciona una interfaz para realizar tareas de administración, como agregar y eliminar entidades, servicios, políticas de seguridad.
- c) **Gestor de Configuración:** administra la configuración de la plataforma de Interoperabilidad, es responsable de guardar y compartir la configuración de los servicios de intercambio de información de las entidades y de los aspectos de seguridad.

- d) **Monitor de la PDI:** realiza el monitoreo de la plataforma de Interoperabilidad, PDI, recolecta la información que le envían desde los monitores de operación de los adaptadores en las entidades.
- e) **Adaptador de Interoperabilidad:** gestiona las invocaciones a los servicios de intercambio de información publicados por el proveedor y coordina las respuestas de servicio al cliente que inicia la solicitud. Adicionalmente, encapsula todos los aspectos relacionados con la seguridad para la Interoperabilidad:
- Autenticación y permisos de acceso a los servicios de intercambio.
  - Envío de los mensajes a través de un canal seguro.
  - Firma digital del mensaje de datos.
  - Realizar el estampado de tiempo del mensaje de datos.
- f) **Sistema de información:** sistema misional o transaccional de la entidad responsable de proveer o usar los servicios de intercambio de información.
- g) **Los servicios de intercambio de información:** deben ser estandarizados y certificados en cumplimiento del marco de Interoperabilidad.
- h) **Monitor de la operación:** realiza el monitoreo de la correcta prestación de los servicios de intercambio de información de acuerdo con las condiciones definidas. Es responsable de recolectar y almacenar los detalles de la operación de los servicios de intercambio de información y hacerla disponible externamente al monitor de la PDI.

Tabla 5 – Descripción de las relaciones del modelo de despliegue de IO

Relación	Origen	Destino	Descripción
<b>R1</b>	Adaptador de Interoperabilidad	Gestor de la PDI	Interacción que permite comunicarse con el gestor de la PDI para realizar tareas administrativas como: <ul style="list-style-type: none"> <li>• Registrar o eliminar el proveedor y clientes involucrados en la Interoperabilidad.</li> <li>• Registrar o eliminar el servicio de intercambio de información invocado.</li> <li>• Administrar los servicios de certificación y estampa de tiempo.</li> </ul>
<b>R2</b>	Gestor de la PDI	Monitor de la PDI	Interacción que permite almacenar los datos del monitoreo que se realiza a la PDI y del monitoreo operativo que realizan los

Relación	Origen	Destino	Descripción
			adaptadores de interoperabilidad de las entidades.
<b>R3</b>	Gestor de la PDI	Gestor de configuración	Interacción que permite propagar la configuración de la PDI que se realiza a nivel central.
<b>R4</b>	Adaptador de interoperabilidad	Monitor de la operación	Interacción que permite recolectar los datos de las operaciones realizadas sobre los servicios de intercambio de información de acuerdo con las condiciones definidas.
<b>R5</b>	Sistema de información	Adaptador de Interoperabilidad	Permite la llamada que hace el sistema misional o transaccional de la entidad dentro de su flujo de procesos para usar los servicios de Interoperabilidad ya sea para compartir, solicitar o intercambiar información con otras entidades, acceder a los servicios de Carpeta Ciudadana o Autenticación Digital y de esta forma responder a las solicitudes de los ciudadanos u otras entidades.
<b>R6</b>	Adaptador de Interoperabilidad	Adaptador de Interoperabilidad	Interacción que realiza el intercambio de los mensajes de datos de solicitud y respuesta, resultado de la invocación de un servicio de intercambio de información.



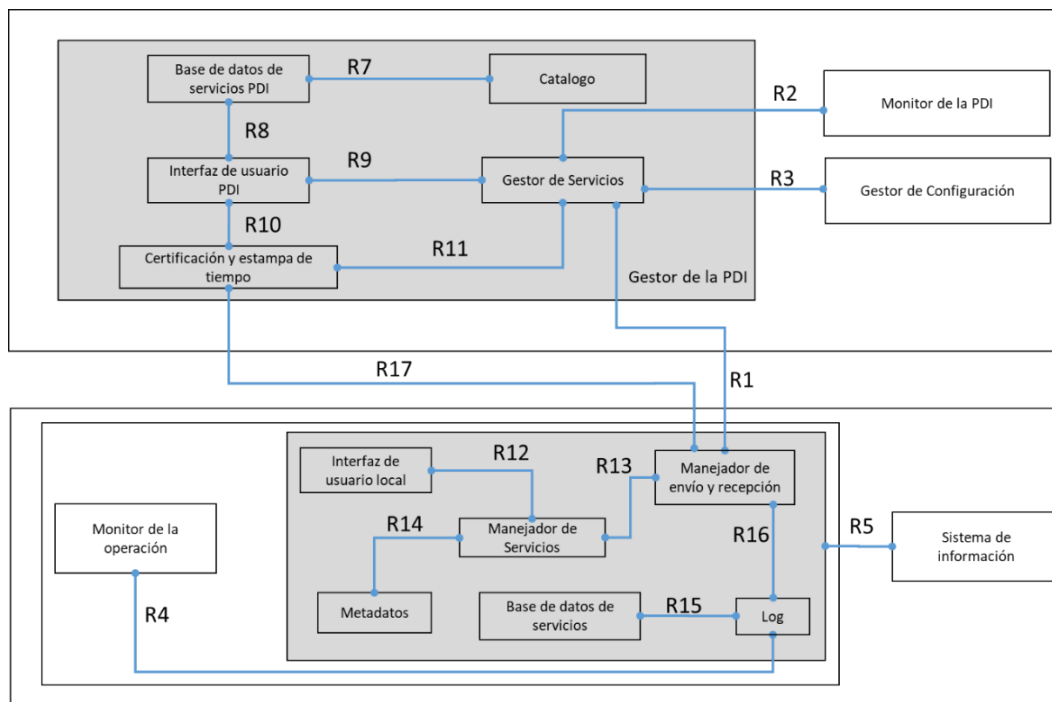


Ilustración 9 – Modelo de despliegue nivel 2 IO

Presentando el Nivel 2 de despliegue del servicio IO, a continuación, se describen los componentes de esta vista:

- Catálogo:** registra la información sobre el directorio de servicios de intercambio de información disponibles que poseen las entidades para su consulta.
- Gestor de servicios:** administra y pone a disposición del adaptador de Interoperabilidad la política de seguridad de la PDI.
- El servidor central:** además de la distribución de la configuración, proporciona una interfaz para realizar tareas de administración, cómo por ejemplo, agregar y eliminar clientes del servidor de seguridad. Estas tareas se invocan desde la interfaz de usuario de los servidores de seguridad. Los servicios de gestión se implementan como servicios de X-Road estándar y se ofrecen a través del servidor de seguridad central.
- Certificación y estampo de tiempo:** el componente responsable de administrar el firmado y estampado de tiempo de los mensajes de datos que intercambian proveedor y cliente, el cual deberá atender las disposiciones sobre firma electrónica y digital contenidas en la Ley 527 de 1999 Y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen.

- e) **Interface de usuario PDI:** permite realizar las tareas de administración sobre la PDI.
- f) **Base de datos de servicios PDI:** repositorio que mantiene y permite obtener una descripción detallada de la configuración de la plataforma de interoperabilidad.
- g) **Manejador de envío y recepción:** administra y media la relación entre los proveedores y clientes de los servicios de intercambio de información, asegura que la comunicación sea segura usando los componentes de firmado, estampado de tiempo e inscripción.
- h) **Manejador de servicios:** gestionar la configuración del servicio de intercambio de información y su definición en términos de seguridad, políticas y reglas, control de acceso, y control de eventos.
- i) **Metadatos:** gestiona la información sobre los metadatos del servicio de intercambio de información y los hace disponibles a la plataforma de Interoperabilidad.
- j) **Log:** registra todos los mensajes generados por los servicios de intercambio de información que pasan a través del adaptador de Interoperabilidad. Los mensajes se almacenan con sus firmas y estampas de tiempo.
- k) **Base de datos de servicios:** repositorio de información con el fin de mantener los datos de los metadatos, log, datos operativos relacionados a los servicios de intercambio de información.
- l) **Interfaz de usuario local:** permite realizar las tareas de administración sobre los servicios de intercambio de información.

Tabla 6 – Descripción de las relaciones del modelo de despliegue de IO Nivel 2

Relación	Origen	Destino	Descripción
<b>R7</b>	Catálogo	Base de datos de servicios PDI	Interacción que permite la consulta de datos de los servicios de intercambio de información disponibles en la PDI.
<b>R8</b>	Interfaz de usuario PDI	Base de datos de servicios PDI	Interacción que guarda en el repositorio la configuración global de la PDI.
<b>R9</b>	Interfaz de usuario PDI	Gestor de servicios	Interacción que permite la actualización y consulta de la configuración de la PDI.

Relación	Origen	Destino	Descripción
<b>R10</b>	Interfaz de usuario PDI	Certificación y estampa de tiempo	Interacción que permite la actualización, consulta y administración de los servicios de firmado y estampado de tiempo de los mensajes de datos que intercambian proveedor y cliente.
<b>R11</b>	Gestor de servicios	Certificación y estampa de tiempo	Interacción que permite darle el valor probatorio a largo plazo de los mensajes intercambiados. Estos registros tienen una marca de tiempo para crear una prueba a largo plazo.
<b>R12</b>	Interface de usuario local	Manejador de servicios	Interacción que permite la actualización, consulta y administración de los servicios de intercambio de información que la entidad provee.
<b>R13</b>	Manejador de envío y recepción	Manejador de servicios	Interacción que permite gestionar la provisión del servicio de intercambio de información según la configuración de políticas, reglas y seguridad determinadas.
<b>R14</b>	Manejador de servicios	Metadatos	Interacción que permite suministrar la información sobre los metadatos, reglas y políticas del servicio de intercambio de información.
<b>R15</b>	Log	Base de datos de servicios	Interacción que permite almacenar los datos realizados del monitoreo a los servicios de intercambio de información.
<b>R16</b>	Manejador de envío y recepción	Log	Interacción que permite el registro sobre la recepción de un mensaje de solicitud / respuesta, firmas y tiempo, adicional a la información operativa del adaptador de Interoperabilidad.
<b>R17</b>	Manejador de envío y recepción	Certificación y estampa de tiempo	Interacción que permite realizar el firmado y estampado de tiempo de los mensajes de datos que intercambian proveedor y cliente.

## 8.6 Servicios tecnológicos de la plataforma de Interoperabilidad

Para disponer de la plataforma de interoperabilidad es necesario que el Articulador cuente con los servicios tecnológicos que garanticen su disponibilidad y operación. De esta forma, el Articulador como prestador del servicio de interoperabilidad debe realizar la gestión de la tecnología como servicio permanente que beneficie a todas las entidades públicas, empresas y ciudadanos, permitiendo el suministro, administración y operación de infraestructura tecnológica, la disponibilidad de la plataforma para una operación continua, el soporte y la seguridad.

### 8.6.1 Características de la plataforma de interoperabilidad

Las siguientes son características esenciales de la plataforma de interoperabilidad:

- Recursos Compartidos. Los recursos (almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) del Articulador son compartidos por múltiples entidades públicas, a los que se van asignando capacidades de forma dinámica según sus peticiones.
- Aislamiento de servicios. Se debe garantizar la segmentación de red, los controles de aislamiento de red y de tráfico entrante y saliente y proporcionar las políticas y reglas en los recursos de seguridad de los centros de datos para asegurar el aislamiento con otras entidades. Garantizar que la infraestructura tecnológica utilizada para prestar los servicios esté protegida, segmentada y separada tanto física como lógicamente, asegurando que no se produzcan accesos no autorizados por esta causa. En los casos de afectación a los servicios de una entidad, las demás entidades que comparten los mismos recursos no deben resultar afectadas.
- Elasticidad. Los recursos se asignan y liberan rápidamente, muchas veces de forma automática, lo que permitirá la posibilidad de aumentar o disminuir los recursos y que estos estén siempre disponibles.

- Servicio medido. se debe tener la posibilidad de medir, ha determinado nivel, el servicio efectivamente entregado a cada Entidad pública, de forma que el Articulador y la entidad tengan acceso transparente al consumo real de los recursos.

Funcionalmente las siguientes son las principales características que debe soportar esta plataforma:

- a) Permitir la integración de la información desde diferentes soluciones/sistemas y dispositivos con los que cuenten las entidades públicas.
- b) Capacidad de integración con los servicios y plataformas actualmente en producción en las entidades públicas.
- c) Soportar y basarse en estándares abiertos para garantizar la interoperabilidad de las aplicaciones y su reutilización.
- d) Garantizar la escalabilidad, a medida que crezca el volumen de información y su modularidad para poder extender sus funcionalidades en el futuro. Por tanto, ha de tratarse de una plataforma basada en estándares abiertos.
- e) Garantizar la integridad y seguridad de los datos y de la propia plataforma.
- f) Permitir el desarrollo y la integración de servicios y aplicaciones proporcionados por entidades de forma sencilla ofreciendo APIs, interfaces basadas en estándares para interactuar con la Plataforma de interoperabilidad.
- g) Permitir la gestión y operación de los diferentes servicios de intercambio de información de las entidades que sean desplegados sobre la Plataforma.
- h) Permitir reglar, componer u orquestar los servicios de intercambio de información a través de la gestión organizada de sus interacciones para generar un proceso o trámite.
- i) Capacidad para integrar una gran cantidad de datos generados desde múltiples fuentes y con diferentes estructuras al interior de la entidad para exponerlas como un servicio de intercambio de información través de un enfoque de virtualización de datos que se estandaricen en el Lenguaje Común de Intercambio de Información.
- j) Permitir el análisis eficiente de los eventos gestionados por la plataforma para la toma de decisiones y aprendizaje del comportamiento de la interoperabilidad en el Estado.

Planteadas las características funcionales se detallan las principales capacidades o características técnicas que debe soportar esta plataforma de interoperabilidad, la cual se basa en un modelo de capas siguiendo como referente el modelo de arquitectura SOA.

## 8.6.2 Requisitos técnicos asociados a la plataforma

Debe tenerse en cuenta que los requisitos técnicos de la plataforma de interoperabilidad que soporta el modelo deben ser completos y exigentes:

- Rendimiento: habilidad del sistema para manejar en tiempo real un elevado número de servicios y procesos de manera eficiente.
- Escalabilidad: capacidad de poder incrementar capacidad de proceso sin tener que modificar la arquitectura.
- Robustez y Resiliencia: capacidad para seguir funcionando ante problemas.
- Seguridad: garantías del sistema en cuanto a seguridad, privacidad y confianza se refiere.
- Modularidad: la plataforma debe tener un enfoque modular que permita desplegarla por partes.
- Continuidad operativa o disponibilidad: capacidad del sistema para estar operativo en cualquier momento.
- Capacidad de Recuperación: capacidad para gestionar de forma eficiente los fallos que puedan afectar a la disponibilidad.
- Extensibilidad: capacidad de la plataforma para poder ampliarse para dar soporte a nuevas necesidades.
- Semántica: el uso de conceptos semánticos en la plataforma a partir del Lenguaje Común de Intercambio de Información.
- Integral: la plataforma debe trabajar como un todo, no como piezas desacopladas que no están preparadas para trabajar en conjunto.

### 8.6.3 Suministro, administración y operación de la plataforma

El Servicio de Interoperabilidad comprende que el Articulador realice el suministro y operación ininterrumpida (7x24x365) de la infraestructura tecnológica, almacenamiento de las configuraciones, copias de seguridad de la plataforma, centro de datos, hosting dedicado, conectividad, seguridad física y lógica, monitoreo de infraestructura, mesa de ayuda y servicios de operación y mantenimiento con sus propios recursos, los cuales los entrega a las entidades públicas en forma integral como un servicio por demanda, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de gestión reducido o interacción mínima de las entidades públicas con el Articulador.

### 8.6.4 Procedimientos de gestión del servicio de la plataforma

Se deben establecer mecanismos de seguimiento y gestión de incidencias sobre la plataforma de interoperabilidad provista por el Articulador, las cuales deben identificarse y priorizarse utilizando reconocidas metodologías de gestión de servicios IT como es el caso de ITIL. El Articulador es responsable de realizar la gestión de las Incidencias repetitivas en el servicio, las cuales dan lugar a una actuación de mantenimiento correctivo que elimine el problema raíz.

El Articulador en los procedimientos del plan de comunicaciones debe incluir el mecanismo para informar a MinTIC y a las entidades involucradas sobre las incidencias presentadas en la operación de la plataforma que afecta a los servicios de intercambio de información.

Los procedimientos definidos para el soporte del servicio deberán estar encaminados a utilizar los estándares del modelo CMMI 3 para asegurar aspectos tales como:

- Gestión de Recursos: asegurar que el esfuerzo (infraestructura, personal, soporte) dedicado a cada petición y/o actividad se ajusta a las necesidades del servicio, de

manera que se pueda distribuir y ajustar la dedicación y esfuerzo asociado a cada tarea.

- Gestión de entrega: asegurar la calidad de los entregables relacionados con tareas de soporte, diseño, desarrollo, implementación, mantenimiento, despliegue y operación del servicio.
- Gestión del conocimiento: mantener actualizada la documentación relacionada con el servicio, preguntas frecuentes, incidencias comunes.
- Gestión de riesgos: con el objetivo de anticipar acciones necesarias e involucrar perfiles adecuados para la resolución de solicitudes.
- Gestión de las relaciones: que permita coordinar interlocutores clave, gestión de expectativas y comunicación interna entre niveles de soporte.

El Articulador del servicio debe realizar revisiones periódicas sobre el cumplimiento de los procesos de gestión de la plataforma.

### 8.6.5 Soporte de la plataforma de interoperabilidad

- Herramientas de soporte: El soporte del servicio debe apoyarse en herramientas de gestión específicas, es responsabilidad del Articulador contar con la infraestructura, recursos y licencias necesarias para su funcionamiento. Así mismo ofrecer la posibilidad para que las entidades y MinTIC tengan acceso a los datos históricos de las herramientas de gestión, monitoreo y control que se encuentran en uso.
- Canales de soporte: El Articulador deberá contar con canales de asistencia que podrá utilizar la entidad pública para comunicar nuevas solicitudes tales como teléfono o herramientas de soporte electrónico mediante formularios web o sistema de seguimiento de incidentes. Asimismo, se deben definir y habilitar mecanismos de comunicación entre los distintos niveles de soporte, de cara a simplificar el traspaso de solicitudes y agilizar la ejecución de los procedimientos definidos.
- Procesos de soporte: El Articulador debe construir los procesos de soporte que



garanticen la atención y solución de los actores que interactúen con la plataforma.

- Elasticidad: Dependiendo de los servicios de intercambio de información ofrecidos por la Entidad, es posible que existan períodos de alta o baja demanda, por lo que es conveniente que la plataforma cuente con la capacidad y defina la estrategia particular de soporte, donde se tenga en cuenta la estructura y dimensionamiento del equipo de soporte durante estos períodos.

### 8.6.6 Gestión de los servicios de información publicados en la plataforma

Un aspecto fundamental en la prestación del servicio de interoperabilidad está dado en la administración de los servicios de intercambio de información, en esta forma de gestión, la entidad pública realiza las tareas de administración de los servicios de intercambio de información, ya que el Articulador como prestador del servicio de Interoperabilidad se encarga de los elementos centrales y de seguridad en el transporte del mensaje. Es importante en este modelo definir desde el inicio el alcance de las tareas de administración a realizar por parte del Articulador que deberá entregar a MinTIC el detalle del procedimiento, herramientas y canales de soporte y gestión para solicitud de nuevos usuarios, autorizaciones, roles, perfiles, modificación de tablas maestras o paramétricas, ejecución de scripts y cualquier otro tipo de operaciones de administración a realizar en la plataforma.

### 8.6.7 Gobierno de los servicios de intercambio de información

Si bien el gobierno de los servicios de intercambio de información lo realizan las entidades públicas es importante que el Articulador tenga en cuenta que:

- Las entidades públicas deben hacer disponible su información a través de servicios de intercambio de información que cumplan lo definido en el marco de interoperabilidad.
- Las entidades hacen disponibles sus servicios de intercambio de información a través de la plataforma de interoperabilidad, siguiendo el lineamiento LI.ST.04. Acceso a servicios en la nube del Marco de referencia de Arquitectura Empresarial para la Gestión de TI.
- Las entidades públicas podrán acceder a información y consumir los servicios de intercambio de información disponibles de otras entidades a través de la plataforma de interoperabilidad, y a través de estos mismos acceden a los servicios de carpeta ciudadana y autenticación electrónica.
- La incorporación de nuevos servicios se coordinará con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones y las entidades a través de las mesas de interoperabilidad.
- Los servicios de intercambio de información que las entidades habilitan en la plataforma deben haber alcanzado el nivel dos (2) de cumplimiento del Marco de interoperabilidad.
- El acceso a los servicios de intercambio de información por parte de las entidades se debe realizar en cumplimiento de sus funciones.

## 8.6.8 Proceso de despliegue del servicio de intercambio de información

El Articulador debe dar las pautas generales del proceso para realizar el despliegue de los servicios de intercambio de información. En la plataforma de interoperabilidad, debe contener lo necesario para la instalación y configuración de los componentes de la solución tecnológica de la entidad de forma que se pueda replicar en los ambientes que se requieran. El proceso debe incluir:

- Los planes que permitan a todas las partes coordinar actividades para el despliegue, entre ellas las definiciones de los servicios de intercambio de

información, flujos, procesos, políticas, reglas, controles de acceso, seguridad y demás aplicables al servicio, según lo defina la entidad responsable del servicio

- Asegurar que todas las entregas sean construidas y probadas con los estándares de calidad acordados antes del despliegue entre la entidad y el Articulador,
- Garantizar que los usuarios y personal de soporte estén entrenados y tengan la documentación correcta.

### 8.6.9 Diseño, desarrollo, implementación y mantenimiento de servicios de intercambio de información

En aquellos servicios de intercambio de información en los cuales se incluyan actividades de diseño, desarrollo, implementación y mantenimiento, las autoridades deben establecer un modelo y alcance de estos en el que determinen:

- Niveles y actividades de diseño, desarrollo, implementación y mantenimiento.
- Procedimientos de Gestión.
- Herramientas.
- Canales de soporte.
- La garantía y soporte en diseño, desarrollo e implementaciones tendrán duración de 1 año y contarán a partir de la puesta en producción.

El Articulador cuando preste los servicios de diseño, desarrollo e implementación de servicios de intercambio de información, debe realizar el proceso de cesión de derechos, conforme a la normativa vigente, a la entidad para la cual se prestan dichos servicios y bajo la supervisión de MinTIC.

## 8.6.10 Operación de la plataforma

En la prestación del servicio de interoperabilidad, las autoridades deben considerar algunos procesos de administración, en especial, los relacionados con la gestión de la capacidad, gestión de la continuidad del servicio y gestión de la disponibilidad.

1. **Gestión de la continuidad del servicio / disponibilidad:** La continuidad y disponibilidad de los servicios de intercambio de información de las entidades, constituye uno de los principales requisitos que debe soportar la operación de la plataforma de interoperabilidad. Por ello, resulta conveniente que el Articulador defina y establezca un Plan de Continuidad del Servicio en el que éste determinen todas las acciones para volver a prestar el servicio tras un incidente de fuerza mayor. En dicho plan se debe evaluar el impacto tanto para la entidad que provee el servicio como para la que lo consumen términos del perjuicio que pueden dar sobre una indisponibilidad temporal o prolongada en el tiempo. A partir de lo anterior, el Articulador deberá indicar cuales son las acciones, procesos y elementos mitigadores en caso de indisponibilidad temporal o prolongada del servicio, en concordancia con el lineamiento Continuidad y disponibilidad de los servicios tecnológicos del Marco de referencia de Arquitectura Empresarial para la Gestión de TI.
2. **Gestión de la Capacidad:** Permite planificar la capacidad de procesamiento necesaria para la prestación de las capacidades de la plataforma de interoperabilidad. A través la gestión de la capacidad, el Articulador podrá dimensionar adecuadamente la infraestructura tecnológica para la prestación del servicio en concordancia con el lineamiento LI.ST.07 Capacidad de los Servicios tecnológicos del Marco de referencia de Arquitectura Empresarial para la Gestión de TI. En este contexto, es necesario solicitar a las entidades públicas una planificación del consumo de capacidad del servicio con suficiente antelación y periodicidad como para permitir al Articulador la adecuación de la infraestructura a las necesidades de capacidad previsibles.

3. **Supervisiones Periódicas:** MinTIC podrá establecer revisiones periódicas sobre los servicios ofrecidos por el Articulador, con el fin de verificar el funcionamiento y cumplimiento de las condiciones de esta guía.
4. **Otras consideraciones de operación:** Para la publicación de nuevas versiones, actualizaciones o mantenimientos de la plataforma de interoperabilidad o alguno de sus elementos base en infraestructura, red o software deberán realizarse en horarios que generen un menor impacto en los servicios de intercambio de información de las entidades públicas, Asimismo, se debe establecer procedimientos de comunicación de dichas intervenciones con suficiente antelación informando a las entidades públicas.

Se debe generar un procedimiento específico para la publicación, despliegue y versionamiento de los servicios de intercambio de información de las entidades públicas que les permita contar con un entorno de integración, reproducción y producción.



El Servicio de Autenticación Digital tiene como objetivo verificar los atributos digitales de una persona cuando se adelanten trámites y servicios a través de medios digitales, afirmando que dicha persona es quien dice ser. El servicio permite generar un ambiente que habilita a los ciudadanos su acceso a los trámites y servicios de entidades públicas y privadas por medios electrónicos, con plenas garantías de confianza y seguridad.

Para la prestación del servicio de autenticación digital se deberán atender las disposiciones sobre firma electrónica y digital contenidas en la Ley 527 de 1999 Y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen.

Para el acceso a este servicio las entidades deben identificar y determinar el riesgo y grado de confianza requerido para sus procesos, y de esta forma elegir el mecanismo de autenticación más acorde a la necesidad, el servicio de autenticación brinda cuatro mecanismos de autenticación clasificados según la confianza y garantía que ofrecen del más bajo al más alto.

Inicialmente, para el acceso a este servicio las entidades deben identificar y determinar el grado de confianza requerido para los procesos:

- **Bajo:** Ofrece un nivel de confianza mínimo en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autenticación errónea es mínimo. Para este nivel las credenciales de usuario estarán asociadas al correo electrónico del usuario, una contraseña de acuerdo con el estándar NIST SP 800-63B de un solo factor OTP.
- **Medio:** Ofrece cierto nivel de confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autenticación errónea es moderado. Para este nivel las credenciales de usuario estarán asociadas al ID del usuario, datos obtenidos en la identificación, correo electrónico, teléfono, dirección, una contraseña de acuerdo con el estándar NIST SP 800-63B de un solo factor OTP, preguntas y respuestas reto, mecanismos de factor múltiple de autenticación de acuerdo con el estándar NIST SP 800-63B Multi-Factor Cryptographic Software y NIST SP 800-63B Multi-Factor.

- **Alto:** Ofrece una gran confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autenticación errónea implica un riesgo considerable. Para este nivel las credenciales de usuario estarán asociadas al uso de certificados digitales.
- **Muy alto:** Ofrece más confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autenticación errónea implica un riesgo muy elevado. Para este nivel las credenciales de usuario estarán asociadas al uso a los mecanismos que disponga la Registraduría Nacional del Estado Civil en el marco de sus funciones.

En caso de los ciudadanos colombianos, la siguiente tabla muestra la relación de trámite, el grado de confianza y el mecanismo de consulta que se requiere a la Registraduría Nacional del Estado Civil.

Tipo de trámite	Grado de confianza	Requiere previa identificación con Registraduría	Consulta requerida
Riesgo de autenticación errónea nulo o mínimo	<b>Bajo</b>		N/A
Riesgo de autenticación errónea moderado	<b>Medio</b>	X	Consulta ANI y Sistema de Información de Registro Civil - SIRC
Riesgo de autenticación errónea considerable	<b>Alto</b>	X	Consulta bases de datos biométricas
Riesgo de autenticación errónea elevada	<b>Muy Alto</b>	X	Cedula Digital

Una vez se tiene definido el grado de confianza, el servicio de autenticación se desarrolla por medio de los siguientes momentos:



**Registro:** el articulador como prestador de servicio debe obtener los atributos relacionados con la identidad de la persona a registrar y verificar que estos le correspondan según el grado de confianza.

Se deben tener las siguientes consideraciones:

- Se deben solicitar a los usuarios los atributos básicos de identificación de acuerdo con el grado de confianza definido.
- Se debe realizar la verificación de la identificación realizando la consulta al Archivo Nacional de Identificación de la Registraduría Nacional del Estado Civil.
- Se debe consultar a través de los mecanismos de Interoperabilidad los atributos de la persona con las fuentes de información facultados para ello.
- Verificar correspondencia de atributos para los grados de confianza alto y muy alto con los datos de la persona a registrar: verificación contra bases de datos externas ABIS de la Registraduría Nacional del Estado Civil.
- Para los extranjeros se efectuará la identificación a través del procedimiento que Migración Colombia estime para ello.

**Inscripción:** si es superada satisfactoriamente la verificación de atributos digitales, el articulador como prestador de servicio debe realizar el proceso de inscripción de la persona, luego de consultar los términos y condiciones de uso. Los datos recopilados en el momento del registro deberán ser los mínimos necesarios requeridos para llevar a cabo los procesos de Autenticación Digital.

**Emisión:** el articulador como prestador de servicio debe emitir y hacer entrega de los mecanismos de autenticación a los usuarios según el grado de confianza.

**Autenticación:** cuando el usuario requiere acceder a un servicio en línea, inicia sesión autenticándose en el sistema con los mecanismos de autenticación emitidos según el grado de confianza.

Este servicio les permitirá a los usuarios acceder a trámites y servicios de las entidades públicas dispuestos por medios electrónicos. De igual forma, la autenticación digital con grado de confianza medio, alto o muy alto podrá ser usada para firmar electrónicamente documentos cuando se quiera garantizar la autenticidad e integridad de un documento.

**Actualización:** este proceso permitirá actualizar los mecanismos de autenticación y los datos utilizados durante el registro.

Posterior a la finalización de la prestación del servicio de Autenticación Digital, y si es superado de modo satisfactorio el proceso de autenticación, se continua con la autorización. En este proceso el sistema de información de la entidad deberá autorizar al usuario el acceso a los recursos, según los privilegios del usuario autenticado. La entidad deberá emplear sus propios mecanismos para determinar los roles y autorizaciones de los usuarios.

**Nota:** en la implementación del servicio de Autenticación Digital el articulador deberá tener en cuenta como base de lineamientos y estándares internacionales como lo son la ITU: X.1251 Marco para el control por el usuario de la identidad digital; X.1253 Directrices de seguridad para los sistemas de gestión de la identidad y X.1254: Marco de garantía de autenticación de entidad y la ISO / IEC/29115:2013 – ‘Information technology — Security techniques — Entity authentication assurance framework’; la NIST: 800-63-3 Digital Identity Guidelines; 800-63A Enrollment and Identity Proofing; 800-63B Authentication and Lifecycle Management y 800-53 Revisión 5, Security and Privacy Controls for Information Systems and Organizations.

## 9.1 Objetivos del servicio

El Servicio de Autenticación Digital tiene un valor estratégico que permite ofrecer a las personas un único conjunto de mecanismos de autenticación para acceder de un modo seguro y confiable a los servicios del Estado, y que las entidades puedan confiar que quien accede a un servicio en línea es quien afirma ser, de acuerdo con el nivel de riesgo del servicio. Para ello la Autenticación Digital permite:

- Definir los lineamientos para que se les asegure a los ciudadanos el derecho de acceso a la administración pública por medios electrónicos en condiciones de calidad.
- Ofrecer un servicio a las entidades públicas y privadas que permita validar la identidad de los usuarios por medios digitales, mitigando los riesgos de

suplantación de identidad, asegurando un nivel de seguridad apropiado para cada servicio o trámite a realizar por medios electrónicos.

- Garantizar autenticidad e integridad a los mensajes de datos dándoles admisibilidad y fuerza probatoria, de acuerdo con el nivel de garantía requerido por la entidad para un servicio específico.
- Proveer los mecanismos necesarios para que los usuarios puedan firmar mensajes de datos y así garantizar la validez jurídica de sus actuaciones con el Estado.
- Mitigar los riesgos de seguridad a los que se ven expuestos los trámites y servicios en línea.

## 9.2 Contexto del servicio

La vista de contexto describe las relaciones entre los actores y sistemas que participan en el servicio de Autenticación Digital, como se presenta en la siguiente ilustración:

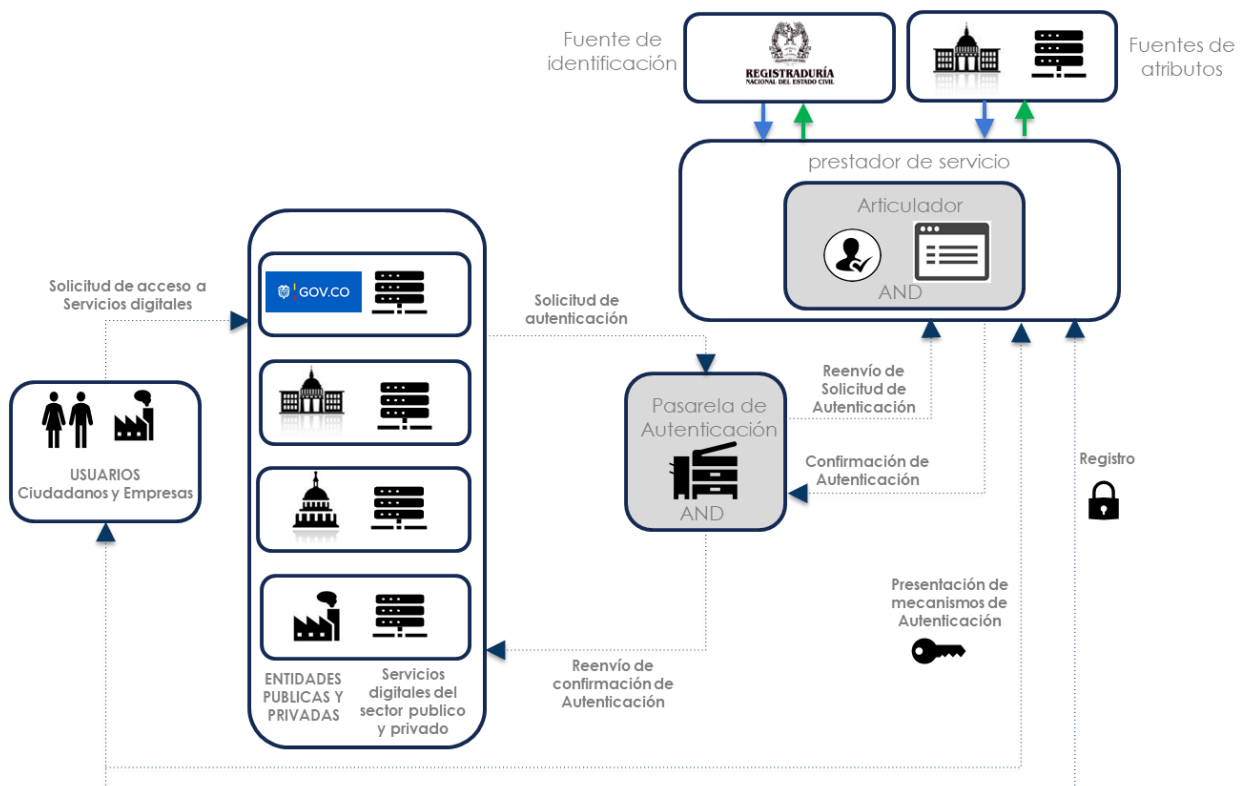


Ilustración 10 – Modelo de contexto del servicio de Autenticación Digital

Del modelo anterior se tienen los siguientes actores:

- **Usuarios:** son las personas naturales, nacionales o extranjeras titulares de cédula de extranjería, o las personas jurídicas, de naturaleza pública o privada, que hagan uso de los Servicios Ciudadanos Digitales.
- **Entidades:** todos los organismos y entidades que conforman las ramas del Poder Público en sus distintos órdenes, sectores y niveles, los órganos autónomos e independientes del Estado, y los particulares que disponen de Servicios Ciudadanos Digitales para el uso de usuarios.
- **Articulador:** La Agencia Nacional Digital. que será la encargada de proveer y gestionar de manera integral los servicios ciudadanos digitales, además de apoyar técnica y operativamente al Ministerio de Tecnologías de la Información y las Comunicaciones para garantizar el pleno funcionamiento de tales servicios.
- **Prestadores de Servicios Ciudadanos Digitales:** personas jurídicas, pertenecientes al sector público o privado, quienes, mediante un esquema coordinado y administrado por el articulador, pueden proveer los Servicios Ciudadanos Digitales, de valor agregado, a ciudadanos y empresas, siempre bajo los lineamientos, políticas y guías que expida el Ministerio de Tecnologías de la Información y las Comunicaciones.
- **Fuentes de atributos:** sistemas de información de entidades públicas y particulares que ejercen funciones públicas, y del sector privado, que brindan información de las personas, que en su conjunto los individualiza y permite identificarlos en entornos digitales.
- **Pasarela de autenticación:** componente de software desarrollado por el articulador que servirá para direccionar los servicios al prestador de servicios de Autenticación Digital con el que cuente el usuario y con el que se conectará cada sistema de las entidades que requieran Autenticación Digital.

Las relaciones que se tienen entre los diferentes actores, de acuerdo con este modelo de contexto, se muestran en la siguiente tabla:

Tabla 7 - Relaciones del modelo de contexto

Relación	Origen	Destino	Descripción
Registro	Usuario	Articulador/ prestadores de servicios	Interacción entre el usuario y articulador o el prestador de servicio quien ingresará al sistema a las personas que lo requieran. Para ello deberá llevar a cabo los procesos para cada persona de: Identificación, inscripción y emisión de mecanismos de autenticación.
Solicitud de acceso a Servicios Ciudadanos Digitales	Usuario	Sistema de información de la Entidad	Interacción entre el usuario y el sistema de información de la entidad, con el fin de solicitar acceso a un servicio digital para realizar un trámite o servicio por medios digitales.
Solicitud de autenticación	Sistema de información de la entidad	Pasarela de autenticación	Interacción entre el Sistema de información de entidad y la pasarela de Autenticación con el fin de generar la solicitud de autenticación de un usuario que realiza una solicitud de acceso a un servicio digital para realizar un trámite o servicio por medios digitales. Para ello deberán estar conectados por medio de Open Id Connect a la pasarela de autenticación con cada sistema de información de las entidades, incluyendo un cliente open id connect.
Reenvío de solicitud de autenticación	Pasarela de autenticación	Articulador o prestadores de servicios	Reenvío de la solicitud de Autenticación Digital desde la pasarela de autenticación al prestador de servicios adecuado con el que se registró el usuario. Para ello deberán estar conectados por medio de Open Id Connect a la

Relación	Origen	Destino	Descripción
			pasarela de Autenticación con cada prestador de servicios, incluyendo un servidor Open Id Connect.
Despliegue de Interoperabilidad	Articulador o prestadores de servicios	Fuentes de atributos	<p>El articulador o prestadores de servicios debe consultar los atributos digitales de una persona a sistemas de información externos, tales como Registraduría Nacional del Estado Civil, Migración Colombia, Departamento Administrativo de la Función Pública, Cámaras de Comercio, etc., que en su conjunto permiten individualizar e identificar a una persona en entornos digitales o hacer afirmaciones acerca de la validez de los valores de los atributos digitales</p> <p>Esta consulta y envío de información deberá hacerse a través del servicio de Interoperabilidad.</p> <p>El transporte de esta información deberá estar cifrado.</p>
Presentación de mecanismos de autenticación	Usuario	Articulador o prestadores de servicios	<p>Interacción en la que se le solicita al usuario el ingreso de los mecanismos de Autenticación con el fin de autenticar a la persona que intenta acceder al servicio digital, provisto por las entidades públicas.</p> <p>El transporte de esta información deberá estar cifrado.</p>
Confirmación de Autenticación	Articulador o prestadores de servicios	Pasarela de Autenticación	Envío del resultado del proceso de Autenticación Digital iniciado por el usuario. En caso de ser superado de modo satisfactorio se enviará la información de autenticación acompañada de los atributos del usuario de acuerdo con el contexto.

Relación	Origen	Destino	Descripción
			Esta información deberá estar cifrada y su contenido no deberá ser conocido por el articulador. El transporte de esta información deberá estar cifrado.
Reenvío de confirmación de Autenticación	Pasarela de Autenticación	Sistema de información de la entidad	Reenvío de la información enviada por el prestador de servicios a la entidad solicitante del proceso de Autenticación Digital.

## 9.3 Mapa de capacidades del servicio

El mapa de capacidades del servicio de Autenticación Digital (AD) corresponde al tercer nivel del modelo de capacidades de los Servicios Ciudadanos Digitales de la sección 16 de esta guía. Las capacidades de este nivel pueden ser consultadas en el siguiente anexo. Anexo 3 Mapa de Capacidades SCD.xlsx.

Serán capacidades del servicio de Autenticación Digital aquellas que estén marcadas con "X" en la columna "AD". Adicionalmente, dentro del mapa también se especifica que actor es necesario para desarrollar la capacidad, marcada con "X" la columna con el nombre del actor (articulador, prestador de servicios, entidad, MinTIC).

## 9.4 Modelo de despliegue del servicio

A continuación, se presenta el modelo de despliegue de primer nivel del servicio de Autenticación Digital, a partir del cual, se debe cumplir con la oferta del servicio a entregar:

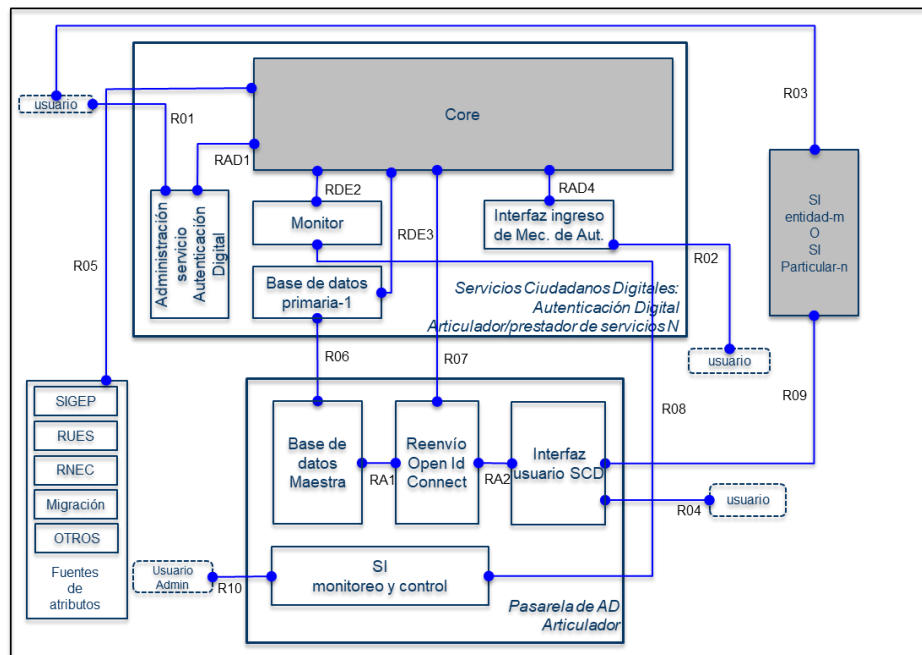


Ilustración 11 - Modelo de despliegue servicio de Autenticación Digital

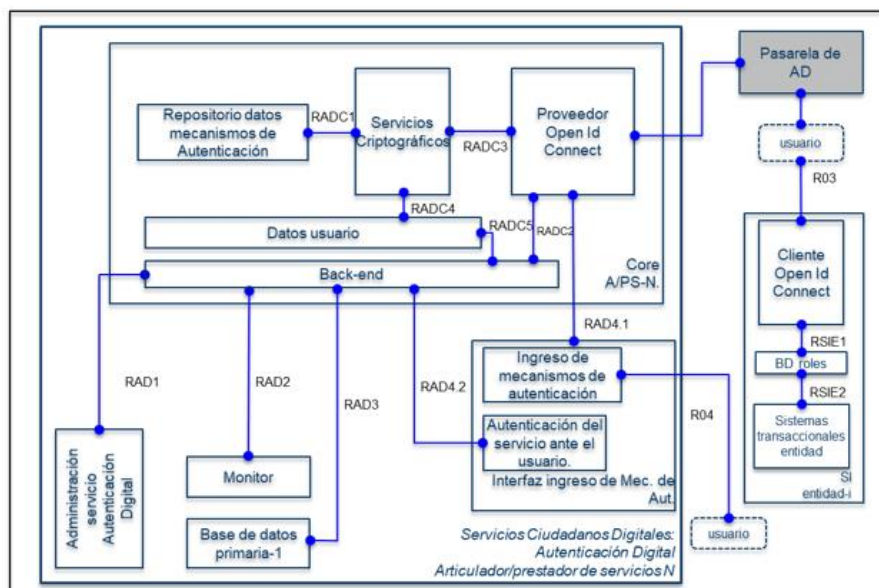


Ilustración 12 - Componente CORE del servicio de Autenticación Digital



Tabla 8 – Descripción de las relaciones del modelo de despliegue

Ítem	Origen	Destino	Descripción
<b>R0 1</b>	Usuario	Administración servicio Autenticación Digital	<p>Interacción entre el componente de administración del servicio de Autenticación Digital y el usuario para llevar a cabo la configuración del servicio y preferencias del usuario, el tratamiento de sus datos, permitiéndole al usuario que sea quien tenga la administración del servicio.</p> <p>Los usuarios podrán acceder, modificar y suprimir su información personal susceptible a ser modificada, así como permisos y autorizaciones.</p> <p>El prestador de servicios de Autenticación Digital deberá validar que los usuarios son quienes dicen ser, verificando la información contra las bases de datos que produzca y administre la entidad facultada para ello.</p>
<b>R0 2</b>	Usuario	Autenticación Digital: Ingreso de mecanismos de autenticación	<p>Interacción entre el formulario de ingreso de mecanismos de autenticación del articulador o un prestador de servicios de Autenticación Digital y los usuarios para el ingreso de los mecanismos de a</p> <p>Autenticación según el nivel de garantía solicitado por el sistema de información de la entidad o el particular.</p>
<b>R0 3</b>	Usuario	Sistema de información de entidad	<p>En esta interacción el usuario busca autenticarse para interactuar con el sistema transaccional de la entidad.</p> <p>En caso de que el usuario supere de modo satisfactorio el proceso de Autenticación Digital, el sistema de información de la entidad deberá emplear su propio proceso de autorización para determinar su rol en el</p>

Ítem	Origen	Destino	Descripción
			sistema otorgando derechos y privilegios al usuario.
<b>R04</b>	Usuario	Articulador: Interfaz Usuario SCD	Interacción entre articulador y el usuario, en el que este podrá ingresar los siguientes datos: o Tipo de documento o Id_user o Número de NIT (en caso de requerir acceso representando a una persona jurídica). Con base en esa información, la pasarela de Autenticación resolverá si la solicitud deberá ser atendida por el mismo articulador o si deberá resolverla un prestador de servicios, en ese caso el articulador deberá redirigir la solicitud de Autenticación Digital al prestador de servicios que le corresponda.
<b>R05</b>	Fuentes de atributos	Servicios Ciudadanos Digitales Autenticación Digital	Interacción entre el articulador/prestador de servicio de Autenticación Digital y las fuentes de atributos que pueden proveer atributos del ciudadano, tales como representación legal de una persona jurídica por medio del Registro Único Empresarial y Social (RUES) o vinculación con entidades públicas por medio del Sistema de Información y Gestión del Empleo Público (SIGEP) y la Registraduría Nacional del Estado Civil
<b>R06</b>	Pasarela de Autenticación: Base de datos maestra	Articulador/prestador de servicios Autenticación Digital: base de datos Primaria	Interacción entre la base de datos maestra del articulador y primaria del prestador de servicios. Para ello cada prestador de servicios deberá tener una base de datos de sus usuarios, denominada base de datos primaria, la cual será actualizada posterior a cada registro de usuario en el sistema, y compartida con la base de datos maestra del articulador en tiempo real, la base de datos primaria contendrá: (a) Id_user. Por su parte, la base

Ítem	Origen	Destino	Descripción
			de datos maestra contendrá: (a) Id_user, (b) Id_prestador de servicio. En caso de que la persona que desee ingresar al servicio no se encuentre registrada como usuario, el articulador le presentará un mensaje indicándole que no está registrado, así como el procedimiento para hacerlo.
<b>R07</b>	Pasarela de Autenticación: Reenvío Open Id Connect	Articulador/ prestador de servicios Autenticación Digital: Core	Interacción en la que, con base en la información de la base de datos maestra, el articulador atenderá o reenviará la solicitud de Autenticación Digital al prestador de servicios encargado de resolver la solicitud del servicio. Para ello deberán estar conectados por medio de Open Id Connect la pasarela de autenticación con el componente de Autenticación Digital del articulador y con cada prestador de servicios En la 'Guía de integración de los prestadores de Servicios Ciudadanos Digitales' se especificará el paso a paso de la integración.
<b>R08</b>	Articulador: Sistema de Información de monitoreo y control	Articulador/ prestador de servicios Autenticación Digital: Monitor	Interacción en la que a través de un servicio de monitoreo y control el prestador de servicios le envía información de su operación al articulador.
<b>R09</b>	Pasarela de autenticación: Interfaz usuario SCD	Sistema de información de la entidad	En esta interacción el sistema de información de entidad deberá embeber el formulario o las librerías de integración provistas por el articulador, para que la integración que le permita al usuario el ingreso de los siguientes datos. -Tipo de documento -Id_user -Número de NIT (en caso de requerir acceso representando a una persona jurídica).

Ítem	Origen	Destino	Descripción
			<p>Con esta información el articulador podrá consultar la base de datos maestra de usuarios para determinar qué Articulador/prestador de servicio deberá resolver la solicitud de Autenticación Digital. Para ello deberán estar conectados por medio de Open Id Connect a la pasarela de Autenticación con cada sistema de información de las entidades, incluyendo un cliente Open Id Connect.</p> <p>En la 'Guía para vinculación y uso de los Servicios Ciudadanos Digitales' se especificará el paso a paso de la integración.</p>
<b>R10</b>	Usuario administrador	Articulador	Interacción entre el usuario del articulador con perfil de administrador con el fin de verificar las métricas de monitoreo y generar acciones para mejorar la operación y la gobernabilidad del modelo.
<b>RA D1</b>	Autenticación Digital: administración servicio Autenticación Digital	Articulador/prestador de servicios de Autenticación Digital: Core	Interacción al interior de sistema de información del articulador o prestador de servicios de Autenticación Digital, en el que la administración del servicio de Autenticación Digital se conecta con el Core del sistema para hacer ajustes en las preferencias solicitadas por el usuario.
<b>RA D2</b>	Articulador/prestador de servicios de Autenticación Digital: Monitor	Articulador/prestador de servicios de Autenticación Digital: Core	Interacción al interior de sistema de información de articulador o prestador de servicios de Autenticación Digital, en el que el Core del sistema le envía información de su operación a su monitor para que esta la exponga a través de un servicio al articulador.
<b>RA D3</b>	Articulador/prestador de servicios de	Articulador/prestador de servicios de	Interacción al interior de sistema de información de articulador o prestador de servicios de Autenticación Digital, en el que el Core del sistema inserta, actualiza y consulta

Ítem	Origen	Destino	Descripción
	Autenticación Digital: Base de datos primaria	Autenticación Digital: Core	los registros de usuarios de la base de datos primaria. La base de datos primaria contendrá: (a) id_user.
<b>RA D4</b>	Articulador/prestador de servicios de Autenticación Digital: Interfaz ingreso mecanismos de Autenticación	Articulador/prestador de servicios de Autenticación Digital: Core	Interacción al interior de sistema de información del articulador o prestador de servicios de Autenticación Digital, en el que el Core del sistema consulta y verifica la información de los mecanismos de autenticación ingresados por los usuarios a través de la Interfaz de ingreso.
<b>RA 1</b>	Articulador: Base de datos maestra	Articulador: Reenvío Open Id Connect	Interacción al interior de sistema de información del articulador por medio de la cual este podrán reenviar las solicitudes de Autenticación Digital al prestador de servicios determinado, por medio de una consulta a la base de datos maestra de usuarios, la cual debe ser alimentada y actualizada con las bases de datos primarias de cada uno de los prestadores de servicios.
<b>RA 2</b>	Articulador: Interfaz usuario SCD	Articulador: Reenvío Open Id Connect	Interacción al interior de sistema de información del articulador en el que con base en la información ingresada por el usuario por medio de la interfaz de usuario SCD y comparada con la base de datos maestra, pueda reenviar las solicitudes de Autenticación Digital al prestador de servicios determinado. Para ello, a través de R10 el articulador deberá embeber un formulario que

Ítem	Origen	Destino	Descripción
			<p>le permita al usuario el ingreso de los siguientes datos.</p> <ul style="list-style-type: none"> <li>-Tipo de documento</li> <li>-Id_user.</li> <li>-Número de NIT (en caso de requerir acceso representando a una persona jurídica).</li> </ul>
<b>RA D4. 1</b>	Articulador/ prestador de servicios de Autenticación Digital: Core: Proveedor Open Id Connect	Articulador/ prestador de servicios de Autenticación Digital: Core: Proveedor Open Id Connect	<p>Interacción al interior de sistema de información de cada prestador de servicios de Autenticación Digital, en el que se produce un intercambio de mensajes de protocolo para la Autenticación Digital del usuario por parte del prestador de servicios.</p> <p>Para ello deberán implementarse el protocolo OpenID Connect 1.0.</p>
<b>RA D4. 2</b>	Articulador/ prestador de servicios de Autenticación Digital: Interfaz ingreso mecanismos de autenticación: Autenticación del servicio ante el usuario	Articulador/ prestador de servicios de Autenticación Digital: Core: Backend	<p>Interacción al interior de sistema de información del articulador o prestador de servicios de Autenticación Digital, en el que la interfaz de ingreso de mecanismos de autenticación deberá ofrecer componentes de autenticación del servicio ante el usuario, para que este pueda identificar que realmente está accediendo a la interfaz de ingreso de mecanismos de autenticación del prestador de servicios. Para ello podrá usar estrategias como frase e imagen de seguridad personalizadas por el usuario.</p>
<b>RA DC 1</b>	Articulador/ prestador de servicios de	Articulador/ prestador de servicios de Autenticación	<p>Interacción al interior de sistema de información del articulador o prestador de servicios de Autenticación Digital, en el que hace uso de servicios criptográficos para</p>

Ítem	Origen	Destino	Descripción
	Autenticación Digital: Core: Servicios criptográficos	Digital: Core: Repositorio de mecanismos de Autenticación	almacenar los datos de los mecanismos de Autenticación.
<b>RA DC 2</b>	Articulador/prestador de servicios de Autenticación Digital: Core: Proveedor Open Id Connect	Articulador/prestador de servicios de Autenticación Digital: Core: Backend	Interacción entre el backend y el proveedor Open Id Connect que le permite acceder a los datos de identidad y de configuración necesarios para ejecutar el proceso de Autenticación Digital.
<b>RA DC 3</b>	Articulador/prestador de servicios de Autenticación Digital: Core: Proveedor Open Id Connect	Articulador/prestador de servicios de Autenticación Digital: Core: Servicios criptográficos	Interacción al interior del sistema de información del articulador o prestador de servicios de Autenticación Digital, en el que se hace uso de servicios criptográficos para validar los mecanismos de autenticación ingresados por los usuarios dentro del proceso de intercambio de mensajes del protocolo Open Id Connect 1.0 para ejecutar los procesos de Autenticación Digital.
<b>RA DC 4</b>	Articulador/prestador de servicios de Autenticación Digital: Core: Datos de usuario	Articulador/prestador de servicios de Autenticación Digital: Core: Servicios criptográficos	Interacción al interior del sistema de información del articulador o prestador de servicios de Autenticación Digital, en el que hace uso de servicios criptográficos para proteger la información del usuario.

Ítem	Origen	Destino	Descripción
<b>RA DC 5</b>	Articulador/prestador de servicios de Autenticación Digital: Core: Datos de usuario	Articulador/prestador de servicios de Autenticación Digital: Core: Backend	Interacción al interior de sistema de información del articulador o prestador de servicios de Autenticación Digital, en el que el backend accede a los datos de usuario para proveer servicios como: <ul style="list-style-type: none"> <li>a. Configurar alertas y alarmas</li> <li>b. Configurar permisos</li> <li>c. Registrar personas jurídicas</li> <li>d. Visualizar registros de acceso</li> <li>e. Descargar registros de acceso</li> <li>f. Bloquear y desbloquear servicio</li> <li>g. Configurar alertas de acceso</li> <li>h. Visualizar registros de acceso</li> <li>i. Descargar registros de acceso</li> <li>j. Bloquear y desbloquear servicio</li> <li>k. Configurar mecanismos de autenticación del servicio ante el usuario.</li> <li>l. Entre otras.</li> </ul>
<b>RSI 1</b>	Sistema de información de entidad o particular: Cliente Open Id Connect	Sistema de Información de la entidad o particular: BD Roles	Interacción al interior del sistema de información de la entidad o particular en el que una vez superado de modo satisfactorio el proceso de Autenticación Digital, el sistema de información de la entidad consulte su base de datos de roles con el fin de validar las autorizaciones en el sistema, otorgando derechos y privilegios al usuario.
<b>RSI 2</b>	Sistema de información de la entidad o particular: BD Roles	Sistema de información de la entidad o particular: Sistemas transaccionales entidad	Interacción al interior del sistema de información de la entidad o particular en el que una vez superado de modo satisfactorio el proceso de Autenticación Digital y validadas las autorizaciones en el sistema otorgando derechos y privilegios al usuario, este le provea al usuario el acceso a los trámites y servicios ofrecidos por la entidad o particular.



## 9.5 Requisitos operativos del servicio de autenticación digital

El Articulador en su calidad de prestador del servicio de autenticación digital debe atender los siguientes lineamientos:

### 9.5.1 Condiciones de operación del servicio de autenticación digital

- a. El proceso de Autenticación Digital debe permitir implementar el protocolo *OpenID Connect* 1.0 a fin de permitir una integración estándar con los sistemas de información de las entidades.
- b. En caso de que se confirme un acceso desautorizado o el servicio de autenticación Digital este puesto parcialmente en peligro de una forma que afecte a la fiabilidad del servicio, el Articulador deberá escalar con MinTIC el incidente que permita valorar la criticidad conforme con lo establecido en los acuerdos de niveles de servicio-ANS de la operación y con ello proceder a suspender o interrumpir el servicio de manera inmediata.
- c. Cuando se haya subsanado y se tenga plena confirmación que el acceso desautorizado o puesta parcialmente en peligro violación de la plataforma provista por el Articulador para el servicio de Autenticación Digital ha sido mitigado y superado, el Articulador deberá restablecer las Credenciales a los usuarios sin dilaciones indebidas y sin generar costo alguno al usuario.
- d. Si existiera acceso desautorizado, o puesta parcialmente en peligro de violación, a las credenciales de autenticación digital el Articulador deberá corregir inmediatamente el incidente y proceder a suspender, revocar o cancelar dichas credenciales y establecer un plan de acción que permitan mitigar los riesgos asociados.
- e. Será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier usuario en caso de incumplimiento de sus obligaciones como Articulador o prestador de Autenticación Digital.

- f. Será responsable del procedimiento de autenticación del usuario, conforme a los lineamientos de esta guía, por lo anterior será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier usuario en caso de incumplimiento de sus obligaciones, es deber del Articulador mantener recursos financieros suficientes y las pólizas de responsabilidad civil, de conformidad con la normativa nacional que permita amparar perjuicios patrimoniales ocasionados a terceros.
- g. Debe contar con personal, que posean los conocimientos especializados, la fiabilidad, la experiencia y las competencias necesarias, deben recibir formación en seguridad, privacidad, normas de protección de datos personales.
- h. Debe informar de manera clara y comprensible al usuario acerca de las condiciones deberes y responsabilidades de la utilización del Servicio de Autenticación Digital, incluidas las limitaciones de su utilización.
- i. Debe contar con plataformas, sistemas, productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan.
- j. Debe garantizar el correcto almacenamiento de los datos que permitan una buena ejecución en la prestación del servicio de Autenticación Digital.
- k. Debe garantizar que solo las personas autorizadas puedan hacer, anotaciones y actualizaciones en los datos almacenados, siempre con una adecuada trazabilidad de sus acciones, además debe implementar procedimientos que permitan comprobar la autenticidad e integridad de los datos, trazabilidad en la anotaciones y modificaciones y garantizar el procedimiento a tomar contra la falsificación y el robo de datos.
- l. El Articulador, en caso de cesar actividades como prestador de servicio de autenticación deberá mantener accesible durante cinco (5) años la información referente a la operación prestada como prestador del Servicio de Autenticación Digital, como los registros y logs de auditoria, con el objeto de que sirvan de prueba en los procedimientos legales en donde se requiera información referente a las credenciales de un ciudadano. Debido a la neutralidad tecnológica, deberán estimar los mecanismos para poder garantizar durante este tiempo que la información sea accesible en caso de solicitudes. Esta actividad de conservación podrá realizarse por medios electrónicos.

## 9.5.2 Proceso de registro y verificación de atributos digitales del usuario

El registro de un usuario ya sea ciudadano colombiano, extranjero y las personas jurídicas al Servicio de Autenticación Digital puede llevarse de manera voluntaria y gratuita ante el Articulador (Agencia Nacional Digital), como prestador de servicios ciudadanos digitales, por los medios que este disponga, sean estos, digitales o presenciales. Adicionalmente, se debe llevar a cabo el proceso de validación de la identificación, para lo cual el usuario debe superar los procesos de demostración y verificación de su identidad.

El Articulador (Agencia Nacional Digital), como prestador de servicios ciudadanos digitales, registrará los atributos relacionados con la identidad del usuario. La recopilación de datos en el momento del registro deberá tener la plena aprobación del usuario a registrar y respetar la debida protección de datos personales, de conformidad y en los términos de la Ley 1581 de 2012.

En el registro del usuario, el articulador (Agencia Nacional Digital), deberá recopilar mínimo los siguientes datos en los grados de confianza medio, alto y muy alto:

- Datos obtenidos en la etapa de identificación.
- Correo electrónico
- Número telefónico o número de móvil
- Dirección y domicilio del suscriptor

En el registro del usuario, el articulador (Agencia Nacional Digital), deberá recopilar mínimo los siguientes datos en los grados de confianza bajo:

- Correo electrónico

Con base en los principios Privacidad por diseño y por defecto, el articulador (Agencia Nacional Digital), como prestador de servicios ciudadanos digitales, podrá solicitar información adicional. Los términos y condiciones deben indicar de manera clara que los únicos datos a recolectar serán los mínimos necesarios y descritos anteriormente, no obstante, con la previa justificación ante el Min TIC y con su correspondiente autorización, se podrán solicitar otros datos.

Los usuarios deberán tener el control sobre 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 conforme a lo establecido en la Ley 1581 de 2012.

El Articulador deberá ubicar en un lugar físico visible al público y en su portal Web el aviso de privacidad, así como de los términos, condiciones y operación del servicio que prestará al usuario. El Articulador deberá guardar la evidencia de la aceptación expresa de los usuarios de las condiciones informadas.

Una vez emitidas las credenciales, las evidencias recolectadas de aceptación de los términos y condiciones y tratamiento de datos personales deberán ser firmadas teniendo en cuenta las siguientes consideraciones:

- Electrónicamente, haciendo uso de las credenciales y mecanismos de autenticación entregados al usuario según el nivel de confianza bajo y medio. Esta información debe ser entregada al usuario en su carpeta ciudadana digital en caso de tenerla activa, en cualquier otro caso deberá ser entregada al usuario en formato PDF.
- Digitalmente, haciendo uso de las credenciales y mecanismos de autenticación entregados al usuario según el nivel de confianza alto y muy alto. Esta información debe ser entregada al usuario en su carpeta ciudadana digital en caso de tenerla activa, en cualquier otro caso deberá ser entregada al usuario en formato PADES-LTV.

Los datos personales y la información generada, producida, almacenada, enviada o compartida en relación con la prestación del Servicio de Autenticación Digital no podrán ser utilizados para un fin diferente al establecido, ni serán objeto de comercialización, ni de explotación económica de ningún tipo por parte del Articulador.

El Articulador deberá entregar a MinTIC el detalle del procedimiento a utilizar para el registro y verificación de la identidad de los usuarios, el cual deberá seguir los lineamientos aquí presentados.

El Articulador deberá llevar a cabo los siguientes procesos, para llevar a cabo el registro de los diferentes tipos de usuarios al Servicio de Autenticación Digital:

### 9.5.3 Registro de personas naturales mayores de edad

Se podrá efectuar de manera digital o presencial, previo al registro se deberá realizar la identificación de las personas naturales, por medio de sus datos biográficos o biométricos según corresponda al mecanismo de Autenticación Digital contra las bases de datos que administra la Registraduría Nacional del Estado Civil. Así mismo:

- Verificar la identidad contra el Archivo General de identificación de la Registraduría Nacional del Estado Civil.
- Validar la identidad del ciudadano por medio de preguntas cuyas respuestas sólo el usuario a registrar conozca y generadas de al menos tres (3) fuentes de información de diferentes contextos, lo suficiente fidedigna como para asegurar la identidad.
- Guardar la evidencia del resultado de los cotejos realizados.
- Estampa cronológica de la confirmación de la verificación realizada

### 9.5.4 Registro de personas naturales menores de 18 años

El registro de personas naturales menores de 18 años se realizará a través de los padres, el tutor o representante legal del menor, de manera digital o presencial y deberá tener mecanismos confiables que permitan emitir las credenciales del menor de edad, con la respectiva administración por parte de los padres, el tutor o representante legal.

En la operación de las credenciales el articulador deberá:

- Garantizar el tratamiento de datos personales de menores de edad.

- Validar y asegurar que quien otorga la autorización para el tratamiento es el padre, tutor o representante legal del menor, previo ejercicio del menor de su derecho a ser escuchado, conforme lo establecido en la ley 1581 de 2012 y sus decretos reglamentarios.
- El menor deberá estar acompañado por su padres, tutor o representante legal en los casos que aplique conforme a lo establecido en la sentencia C-748 de 2011 de la Corte constitucional.
- Solicitar certificaciones físicas o realizar consultas en línea con las bases de datos de entidades que tengan funciones a su cargo que permitan demostrar las condiciones de representación de los padres, tutor o representante legal.
- Emitir las credenciales de autenticación digital con las características de administración por parte de los padres, tutor o representante legal,
- Cuando la persona natural menor de 18 años cumpla la mayoría de edad deberá actualizar su condición con el Articulador de Autenticación Digital según el procedimiento que este establezca.
- Guardar la evidencia del resultado de los cotejos realizados.
- Estampa cronológica de la confirmación de la verificación realizada

### 9.5.5 Registro de extranjeros

El registro de extranjeros se efectuará por medio de las bases de datos de Migración Colombia.

### 9.5.6 Registro de personas jurídicas

El registro de las personas jurídicas deberá realizarlo su representante legal o apoderado, bajo los siguientes lineamientos:

- El representante legal o apoderado de la persona jurídica deberá registrarse conforme el procedimiento de “Registro de personas naturales” antes indicado.

- La persona jurídica realizará la solicitud de registro ante el mismo prestador de autenticación Digital de su representante legal o apoderado (Opción A), o en su defecto ante el Prestador de servicios de su elección (Opción B).
  - Opción A:
    - Se deberá validar que la persona natural cuenta con la facultad para representar legalmente a la persona jurídica, verificando la información contra las bases de datos que produzca y administre la entidad facultada para ello, según el tipo de persona jurídica.
    - Una vez el Articulador tenga una validación satisfactoria de la facultad de representación de la persona natural, se adicionará a los datos del usuario persona natural, el atributo de representante legal o apoderado de la persona jurídica.
  - Opción B:
    - Se deberá validar que la persona jurídica exista, verificando la información contra las bases de datos que produzca y administre la entidad facultada para ello, según el tipo de persona jurídica.
    - Se deberá registrar persona jurídica con los siguientes atributos básicos: NIT, nombre o razón social, dirección física y/o correo electrónico, teléfono.
    - Se deberá emitir credenciales de Autenticación Digital a la persona jurídica.
- La persona jurídica, a través del representante legal o apoderado, deberá efectuar la aceptación de los términos y condiciones del servicio.
- El representante legal o apoderado podrá autenticarse y firmar mensajes de datos ante los diferentes sistemas de información, en representación de la persona jurídica, de conformidad con las facultades conferidas en su mandato de representación o por los estatutos de la persona jurídica que representa.
- Los sistemas de información deberán incluir mecanismos que le permitan al representante legal o apoderado asignar y revocar roles y autorizaciones a otras personas naturales dentro de la organización de la persona jurídica, de acuerdo con su perfil.
- Guardar la evidencia del resultado de los cotejos realizados.
- Estampa cronológica de la confirmación de la verificación realizada

### 9.5.7 Registro de funcionarios públicos y particulares que desempeñen funciones publicas

Los funcionarios públicos y los particulares que desempeñen funciones públicas deberán registrarse para adquirir la calidad de usuario del Servicio de Autenticación Digital.

En relación con los atributos que relacionen a un usuario con el rol de funcionario público o particular que desempeñe función pública, se deberá complementar los datos de sus usuarios, verificando la información contra las bases de datos que produzca y administre la entidad facultada para ello o en su defecto el usuario deberá aportar actas o documentos que permitan verificar la información y competencias para firmar electrónicamente actos administrativos, expedientes y documentos en general, o accesos de administración a los sistemas de información de la entidad en el marco propio de sus funciones.

### 9.5.8 Proceso de emisión de las credenciales de autenticación

El Articulador deberá entregar a MinTIC el detalle del proceso de emisión de las credenciales de autenticación a utilizar, el cual deberá cumplir los siguientes requerimientos al momento de realizar el proceso de emisión de las credenciales a los usuarios que han superado el proceso de registro:

- a. Para los mecanismos de autenticación que incluyan certificados digitales acreditados, las credenciales entregadas al usuario deben estar conforme a lo dispuesto por el Organismo Nacional de Acreditación de Colombia (ONAC).
- b. Las credenciales entregadas al ciudadano deben corresponder a mecanismos de autenticación definidos, conforme a recomendaciones de la ITU X.1254 y en la ISO/IEC 29115:2013.



En ambos casos las credenciales de autenticación deben establecer de manera fehaciente que un usuario ingresó a un servicio y el usuario tenga control sobre el uso de sus credenciales electrónicas.

Las credenciales permitidas que deberán emplearse y ser provistas se listan a continuación:

a. La contraseña o secreto memorizado:

1. Una credencial correspondiente a secretos memorizados - comúnmente referido como una contraseña o, si es numérico, un PIN - es un valor secreto elegido y memorizado por el usuario u otorgado por el Articulador a partir de cadenas aleatorias. Las Contraseñas o secretos memorizados deben ser de suficiente complejidad y secreto para que un atacante no pueda adivinar o descubrir el valor secreto correcto. Un secreto memorizado es un factor de conocimiento.
2. La contraseña o secreto memorizado deberá tener al menos 8 caracteres de longitud si es elegido por el usuario. Las contraseñas o secretos memorizados que se provean por el Articulador deberán tener al menos 6 caracteres de longitud, deberán ser cadenas aleatorias y puede ser enteramente numérico. La contraseña o secreto memorizado deberá ser rechazado por el Articulador si llegará a estar incluido en una lista negra de valores comprometidos, en ese caso el usuario deberá elegir una contraseña o secreto memorizado. Ningunos otros requisitos de la complejidad para los secretos memorizados deben ser impuestos.
3. Los secretos memorizados que son elegidos al azar (por ejemplo, cuando un usuario se registra o solicita un nuevo PIN) deberá tener al menos 6 caracteres de longitud y será generado usando un generador de bit aleatorio aprobado y de acuerdo con la recomendación NIST *Special Publication* 800-90<sup>a</sup> o equivalentes.
4. Para el uso de contraseñas o secretos memorizados, se deberá usar estrategias que permitan frenar ataques tales como fuerza bruta (*brute-force attack*) o ataques a la tabla arcoíris (*rainbow table*), entre otros, para ello se deberán implementar mecanismos criptográficos de derivación de claves como el descrito en NIST

5. Para el uso de contraseñas, en el momento del registro el Articulador le deberá entregar al usuario una contraseña de un solo uso, con la cual este tendrá el primer acceso a la herramienta de administración con el fin de activar el servicio y crear la contraseña.
- b. Dispositivo de contraseña única de un solo factor (OTP)
1. Esta categoría incluye dispositivos de hardware y generadores OTP basados en software instalados en dispositivos como teléfonos móviles. Estos dispositivos tienen un secreto incrustado que se utiliza como la semilla para la generación de OTPs y no requiere la activación a través de un segundo factor.
  2. La OTP se muestra en el dispositivo y se introduce manualmente para su transmisión al Servicio de Autenticación digital, demostrando así la posesión y el control del dispositivo. Un dispositivo OTP puede, por ejemplo, mostrar 6 caracteres a la vez. Un dispositivo OTP de un solo factor, es un factor de conocimiento.
- c. Dispositivo OTP Multi Factor
1. Un dispositivo OTP multi-factor genera OTPs para su uso en la autenticación después de la activación a través de un factor de autenticación adicional. Esto incluye dispositivos de hardware y generadores OTP basados en software instalados en dispositivos como teléfonos móviles.
  2. El segundo factor de autenticación puede lograrse mediante algún tipo de mecanismo de entrada, un lector biométrico integral (por ejemplo, huella digital) o una interfaz de computadora directa (por ejemplo, puerto USB), los cuales deberán cumplir con estándares nacionales o internacionales verificables.
  3. El OTP se muestra en el dispositivo y se introduce manualmente para su transmisión al Servicio de Autenticación Digital. Por ejemplo, un dispositivo OTP puede mostrar 6 caracteres a la vez, demostrando así la posesión y el control del dispositivo. El dispositivo OTP multi-factor es un factor de posesión, y se debe activar por un factor de conocimiento o de inherencia.

#### d. Software Criptográfico de Un Solo Factor

Un autenticador criptográfico de software de un solo factor es una clave criptográfica almacenada en disco o en algún otro medio "blando". La autenticación se logra demostrando la posesión y el control de la llave. La salida del autenticador depende en gran medida del protocolo criptográfico específico, pero generalmente es un tipo de mensaje firmado. El autenticador criptográfico de software de factor único es un factor de posesión.

#### e. Dispositivo criptográfico de un solo factor

Un dispositivo criptográfico de un solo factor es un dispositivo de hardware que realiza operaciones criptográficas utilizando claves criptográficas protegidas y proporciona la salida del autenticador a través de la conexión directa al punto final del usuario. El dispositivo utiliza claves criptográficas simétricas o asimétricas incrustadas, y no requiere activación a través de un segundo factor de autenticación. La autenticación se logra demostrando la posesión del dispositivo a través del protocolo de autenticación. La salida del autenticador se proporciona mediante conexión directa al punto final del usuario y depende en gran medida del dispositivo criptográfico y del protocolo específicos, pero normalmente es un tipo de mensaje firmado. Un dispositivo criptográfico de un solo factor es un factor de posesión.

#### f. Software Criptográfico Multi Factor

Un autenticador criptográfico de software multi-factor es una clave criptográfica almacenada en disco o algún otro medio "blando" que requiere activación a través de un segundo factor de autenticación. La autenticación se logra demostrando la posesión y el control de la llave. La salida del autenticador depende en gran medida del protocolo criptográfico específico, pero generalmente es un tipo de mensaje firmado. El autenticador criptográfico de software multi-factor es un factor de posesión y se debe activar por un factor de conocimiento o inherencia.

#### g. Dispositivo criptográfico Multi Factor

Un dispositivo criptográfico multi-factor es un dispositivo de hardware que realiza operaciones criptográficas utilizando una o más claves criptográficas protegidas y requiere activación a través de un segundo factor de autenticación. La autenticación se logra demostrando la posesión del dispositivo y el control de la llave. La salida del autenticador se proporciona mediante conexión directa al punto final del usuario y depende en gran medida del dispositivo criptográfico y del protocolo específicos, pero normalmente es un tipo de mensaje firmado. El dispositivo criptográfico multi-factor es un factor de posesión y se debe activar por un factor de conocimiento o inherencia.

Para el servicio de Autenticación Digital, para los mecanismos de autenticación: Medio y muy alto.

El mecanismo de autenticación Medio da alguna confianza en que la identidad presentada sea precisa y es equivalente al nivel de Garantía 2 (NdG2) establecido en las recomendaciones de la ITU X.1254, ISO 29115

El mecanismo de autenticación muy alto tiene un nivel muy alto de confianza en la exactitud de la identidad presentada y se emplea para el acceso a datos muy restringidos y es equivalente al nivel de Garantía 4 (NdG4) establecido en las recomendaciones de la ITU X.1254, ISO 29115.

En el mecanismo de autenticación bajo: Se exigen mínimo un factor de autenticación y pueden emplearse los siguientes tipos de credenciales:

- Secreto memorizado
- Dispositivo de contraseña única de un solo factor (OTP)

En el mecanismo de autenticación medio: Se exigen mínimo un factor de autenticación y pueden emplearse los siguientes tipos de credenciales:

- Secreto memorizado
- Dispositivo de contraseña única de un solo factor (OTP)
- Dispositivo OTP Multi Factor
- Software Criptográfico de Un Solo Factor
- Dispositivo criptográfico de un solo factor

- Software Criptográfico Multi Factor
- Dispositivo criptográfico Multi Factor
- Mecanismos dispuestos en los anexos A, E y F del documento CEA-4.1-10 de la ONAC.

En el mecanismo de autenticación Alto: Se exigen mínimo dos factores de autenticación y pueden emplearse los siguientes tipos de credenciales:

- Dispositivo criptográfico Multi Factor
- Dispositivo criptográfico de un solo factor utilizado junto con Contraseña-Secreto memorizado
- Dispositivo OTP multi-factor utilizado junto con un Dispositivo Criptográfico de Un Factor
- Dispositivo OTP multi-factor (sólo hardware) utilizado junto con un software criptográfico de factor único
- Dispositivo OTP de factor único (sólo hardware) utilizado junto con un Software Criptográfico Multi-Factor
- Dispositivo OTP de factor único (sólo hardware) utilizado junto con un software criptográfico de un solo factor y una Contraseña-Secreto memorizados.
- Mecanismos dispuestos en los anexos A, E y F del documento CEA-4.1-10 de la ONAC utilizado junto con Contraseña-Secreto memorizado

En el mecanismo de autenticación muy Alto: Este mecanismo de autenticación, hará uso de la identificación por medios digitales de la cédula de ciudadanía digital y de la biometría que se registrará por las disposiciones que para tal efecto expida la Registraduría Nacional del Estado Civil, en el marco de sus competencias, el cual podrá se complementado con los siguientes tipos de credenciales:

- Dispositivo criptográfico Multi Factor
- Dispositivo criptográfico de un solo factor utilizado junto con Contraseña-Secreto memorizado
- Dispositivo OTP multi-factor utilizado junto con un Dispositivo Criptográfico de Un Factor
- Dispositivo OTP multi-factor (sólo hardware) utilizado junto con un software criptográfico de factor único

- Dispositivo OTP de factor único (sólo hardware) utilizado junto con un Software Criptográfico Multi-Factor
- Dispositivo OTP de factor único (sólo hardware) utilizado junto con un software criptográfico de un solo factor y una Contraseña-Secreto memorizados.
- Mecanismos dispuestos en los anexos A, E y F del documento CEA-4.1-10 de la ONAC utilizado junto con Contraseña-Secreto memorizado

Se podrán usar otros tipos de credenciales diferentes a los descritos anteriormente, en todo caso las credenciales deberán ser estudiadas y analizadas por MinTIC para determinar su nivel confianza y nivel de garantía según las recomendaciones de la ITU X.1254, ISO 29115. Antes de hacer la vinculación de una credencial a un usuario el Articulador debe tener la suficiente garantía de que la credencial está y sigue estando vinculada a la persona correcta. 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.

En caso de que el usuario que se registra en el en el servicio de Autenticación Digital quiera contar con credenciales de autenticación adicionales a las básicas ofrecidas, deberá asumir el costo.

**Nota:** Se debe informar a MinTIC los mecanismos adicionales ofrecidos, así como su costo. Cualquier modificación en costo o mecanismo deberá ser informado a MinTIC, por escrito, antes de su ofrecimiento a los usuarios.

## 9.5.9 Proceso de Autenticación Digital

En un proceso de autenticación digital, el usuario hace uso de sus credenciales con el objetivo de validar su identidad en relación con un mensaje de datos frente al sistema de información de una entidad pública o privada.

El Articulador deberá entregar a MinTIC el detalle del procedimiento a utilizar para la autenticación de usuarios, el cual deberá seguir los lineamientos aquí presentados.

El trámite o servicio de una entidad pública o privada que desea validar la identidad de un usuario en relación con un mensaje de datos, debe integrar el componente de autenticación digital provisto por el Articulador, con el objetivo de direccionar el proceso de autenticación al prestador de servicio en donde el usuario se registró, de tal manera que las credenciales entregadas a los usuarios pueden ser empleadas para acceder a cualquier sistema de información de entidades públicas o privadas que integren los componentes de direccionamiento del Articulador.

Se debe implementar los siguientes mecanismos los cuales permiten delegar el proceso de autenticación digital:

- **Servicio Web:** Se deberá implementar un servicio web que informe el resultado del proceso de validación de las credenciales de autenticación, conforme a la descripción técnica informada por el Articulador.
- **OpenID Connect 1.0:** *OpenID Connect 1.0*, Permite a los sistemas de información verificar la identidad del usuario final en función de la autenticación realizada por un servidor de autenticación, así como también obtener información básica del perfil sobre el usuario final de una manera interoperable y similar a REST. Permite tecnologías de todo tipo, incluidas las aplicaciones basados en web, móviles y JavaScript, solicitar y recibir información sobre sesiones autenticadas y usuarios finales. El conjunto de especificaciones es extensible, lo que les permite a los participantes utilizar funciones opcionales como el cifrado de datos de identidad. Es un estándar abierto para intercambiar datos de autenticación y autorización entre diferentes dominios.

En los procesos de autenticación de personas naturales, se deberá actualizar cada vez que se genere una solicitud de Autenticación con mecanismos de autenticación medio, alto y muy alto, se deben definir periodos no mayores a 6 meses con el fin de verificar las condiciones del usuario, que permita verificar la validez y vigencia el documento de identificación a través la Registraduría Nacional del Estado Civil o a través de las bases de datos de Migración Colombia según corresponda.

Los procesos de autenticación de personas jurídicas se realizarán haciendo uso de las credenciales de autenticación otorgadas, como persona natural, por parte del representante legal o persona jurídica teniendo en cuenta la opción seleccionada (Ver Registro de personas jurídicas).

En caso de la opción A, el proceso de autenticación digital hará uso del atributo adicional generado en las credenciales del representante legal o apoderado de la persona jurídica, que le permita al representante legal autenticarse y firmar mensajes de datos ante los diferentes sistemas de información en representación de la persona jurídica.

En caso de la opción B, el proceso de autenticación digital hará uso de las credenciales de la persona jurídica, validando el representante legal ante la fuente de atributos que corresponda para que le permita autenticarse y firmar mensajes de datos ante los diferentes sistemas de información.

Para todo lo anterior, se deberá validar cada vez que se genere una solicitud de la persona jurídica, verificando la información contra las bases de datos que produzca y administre la entidad facultada para ello.

Los procesos de autenticación digital de funcionarios públicos y particulares que desempeñen funciones públicas se realizarán haciendo uso de las credenciales de autenticación otorgadas como personas naturales, para ello se hará uso del atributo adicional generado en el registro de los funcionarios públicos y particulares que desempeñen funciones públicas, que les permita autenticarse y firmar mensajes de datos ante los diferentes sistemas de información. Para ello, se deberá validar cada vez que se genere una solicitud de Autenticación Digital de los funcionarios públicos y particulares que desempeñen funciones públicas, que dicha persona natural cuenta con la facultad, verificando la información contra las bases de datos que produzca y administre la entidad facultada para ello.

**Nota:** Los atributos de representante legal, apoderado, funcionario público u otros que sean recolectados por medio de consultas a otros sistemas de información, serán usados única y exclusivamente en aquellos contextos donde se requiera realizar una transacción en representación de la persona jurídica, o como funcionario público, o en función de los atributos obtenidos, de conformidad con las facultades conferidas.



El servicio de Autenticación Digital debe asegurar que cumpla con las garantías y lineamientos acordes a los estándares como la NIST: 800-63-3 *Digital Identity Guidelines*, 800-63A *Enrollment and Identity Proofing* y 800-63B *Authentication and Lifecycle Management*; la ISO/IEC 29115:2013 *Entity Authentication Assurance Framework* y la ITU: X.1251 Marco para el control por el usuario de la identidad digital, X.1253 Directrices de seguridad para los sistemas de gestión de la identidad y X.1254 Marco de garantía de autenticación de entidad.

En el proceso de autenticación se deben asegurar los siguientes criterios:

Grado de confianza en el Mecanismos de autenticación.	Establecer el grado de confianza en los procesos de autenticación.
Fases de garantía de autenticación.	Verificar los requisitos para aplicación de los procesos de autenticación establecido en las recomendaciones de la ITU X.1254, ISO/IEC 29115:2013, en las fases de afiliación, gestión de credenciales y autenticación.
Amenazas, controles y estrategias de mitigación.	Implementar los criterios de garantía y los controles necesarios que se deben utilizar para mitigar las amenazas relativas a la autenticación (tales como: modificación, robo, duplicación, captura, <i>Phishing</i> , <i>Pharming</i> , ingeniería social, entre otras.) en cada una de las fases (afiliación, gestión de credenciales y autenticación).
Características de una credencial.	<p>Verificar la credencial, validando que este contenga, por lo menos las siguientes características:</p> <ul style="list-style-type: none"> <li>▪ Datos que demuestren una identidad y/o sus derechos como algo que se conoce, una característica biométrica o su representación y datos generados por algo que se posee.</li> <li>▪ Ir acompañada de otros datos que pueden ser de utilidad en los procesos de autenticación.</li> <li>▪ Sea una credencial derivada.</li> </ul>

		<ul style="list-style-type: none"> <li>▪ Ser auténtica pero no válida en todos los contextos.</li> <li>▪ Ser verificada antes de aceptarse como auténtica y fiable para la finalidad a la que está destinada.</li> <li>▪ Ser compleja y secreta.</li> <li>▪ Seguir lo indicado para la emisión de credenciales.</li> <li>▪ En caso del certificado digital se deben cumplir los requisitos de 10.5 del documento CEA-4.1-10 de ONAC, establecer las Políticas de Certificados que deben acoger las recomendaciones de RFC 3647 y la validez de un certificado digital para persona natural o jurídica no puede ser superior a 2 años.</li> <li>▪ Forzar el cambio de credencial si existe algún tipo de evidencia que la esté comprometiendo.</li> <li>▪ Establecer el periodo para el cambio y renovación de credencial.</li> </ul>
Repositorio de credenciales		<ul style="list-style-type: none"> <li>- Implementar un plan que garantice la protección de las credenciales estén protegidas con el más alto nivel de seguridad posible.</li> <li>- Realizar copias de seguridad con hardware seguro.</li> <li>- Dispositivos criptográficos para el almacenamiento de certificados digitales de firma electrónica con estándares vigentes simétricos y/o asimétricos.</li> </ul>
Capacidades de usuario.		Establecer las capacidades generales para usuario, funcionales y las directrices de seguridad establecido en las recomendaciones de la ITU X.1251Marco para el control por el usuario de la identidad digital.
Administración de riesgos.		Establecer los requisitos y niveles de seguridad para evitar la ocurrencia de riesgos como en la prueba de identidad donde un usuario malicioso solicita una identidad que nos es legítima, en la prueba de autenticación donde un usuario malicioso usa una credencial que nos legitima y prueba de una identidad cuando es comprometida.

Administración de sesiones.	<ul style="list-style-type: none"> <li>- Proporcionar las medidas necesarias para la protección e integridad de las sesiones y evitar ataques como XSS y CSRF (Falsificación de solicitudes entre sitios).</li> <li>- Las cookies de navegación deberán: <ul style="list-style-type: none"> <li>▪ Ser accesibles por sesiones seguras (HTTPS).</li> <li>▪ Ser inaccesibles a través de JavaScript.</li> <li>▪ Tener un periodo de validez de la sesión.</li> </ul> </li> </ul>
Tokens de acceso	Deberán ser validados durante periodos de tiempo.
Firma digital	<p>Cumpla con el artículo 28 ley 527 de 1999:</p> <ul style="list-style-type: none"> <li>▪ Es única a la persona que la usa.</li> <li>▪ Es susceptible de ser verificada.</li> <li>▪ Está bajo el control exclusivo de la persona que la usa.</li> <li>▪ Está ligada a la información o mensaje, de tal manera que, si éstos son cambiados, la firma digital es invalidada.</li> <li>▪ Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.</li> </ul>

## 9.5.10 Enrutar solicitudes de autenticación

En su función de articulación el Articulador debe enrutar las solicitudes de Autenticación digital al Prestador de servicio que le corresponda.

El Articulador deberá contar con una interfaz con un formulario que le permita al usuario el ingreso de los siguientes datos.

- o Tipo de documento
- o Número de documento de identificación.
- o Numero de NIT (en caso de requerir acceso representando a una persona jurídica)

Con esta información el Articulador podrá consultar la base de datos maestra de usuarios para determinar qué prestador de servicio deberá resolver la solicitud de Autenticación Digital.

Si el usuario se encuentra registrado en la Base de Datos Maestra se deberá enrutar la solicitud de Autenticación Digital al prestador de servicio correspondiente. En caso de que la persona no sea usuaria del servicio, se le deberá informar que para acceder al sistema deberá surtir el proceso de registro.

### 9.5.11 Gestión de la base de datos maestra

El articulador, deberá realizar la actualización de la base de datos Maestra de usuarios, a partir de la información de las bases de datos primarias dada por cada uno de los prestadores de servicio.

Cada prestador de servicio deberá tener una base de datos de sus usuarios, denominada base de datos primaria, la cual será actualizada posterior a cada registro de usuario en el sistema, y compartida con la base de datos maestra en tiempo real, la base de datos primaria contendrá únicamente: (a) número y tipo de documento de identificación del usuario.

A partir de la información enviada por cada prestador de servicio, el Articulador deberá construir la base de datos maestra que contendrá: (a) número y tipo de documento de identificación del usuario, (b) identificador del prestador de servicio que registró al ciudadano

### 9.5.12 Proceso de firmado electrónico con las credenciales de autenticación digital

El servicio de autenticación digital entrega los datos únicos de los usuarios (numeral 2, artículo 1 del decreto 2364 de 2012), de acuerdo con los mecanismos de autenticación para cada nivel de confianza descritos en el numeral 9, estos datos podrán ser utilizados por los diferentes sistemas de información de las entidades integrados al servicio, para firmar electrónicamente documentos.

La firma de documentos debe seguir los lineamientos estipulados en la Ley 527 de 1999, el Decreto 2364 de 2012 y garantizando la autenticidad, integridad y disponibilidad del documento firmado

Los diferentes sistemas de información de las entidades integrados al servicio de autenticación digital podrán usar una norma o estándar técnico que no se encuentre dentro de los mencionados a continuación. Para ello deberá enviar a MinTIC la información con la descripción de la norma o estándar técnico que se solicita implementar, para su estudio y análisis

Estándares que pueden utilizar:

- XAdEs
- PAdEs
- CAdEs o alguno que permita garantizar integridad y autenticidad o que se encuentre acreditado por ONAC.

### 9.5.13 Desvinculación del usuario frente al servicio de autenticación digital

Los usuarios podrán solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su desvinculación de los servicios ciudadanos digitales en cuyo caso se revocarán las credenciales y autorizaciones otorgadas a sistemas de información de entidades y particulares.

El proceso de desvinculación debe ejecutarse de inmediato a la solicitud del usuario y él se deberá contar con mecanismos que generen la revocación inmediata de las credenciales.

Se deberá conservar los registros y logs de auditoría por un plazo de 5 años.

## 9.5.14 Comunicación entre prestadores de servicio

Los prestadores de servicio de Autenticación Digital deben tener la capacidad de comunicarse entre ellos para realizar las siguientes actividades:

- i. Traslado de usuarios.
- ii. Conexión de *OpenID Connect* 1.0 entre prestadores de servicio.
- iii. Validación de credenciales de autenticación.

Por lo anterior, se debe disponer de la siguiente información debidamente documentada:

- I. Interfaces necesarias para cumplir las acciones de traslado de usuarios.
- II. APIS y protocolos normalizados para comunicación entre plataformas.

Todos los servicios web provistos por el Articulador, deben estar registrados en el directorio de servicios de intercambio de información y estar disponibles en la plataforma de interoperabilidad.

## 9.5.15 Integración de autenticaciones ya ofertadas por otras autoridades publicas

Las entidades públicas que cuente con implementaciones cuyas funcionalidades sean similares a las de los servicios ciudadanos digitales. éstas deberán elaborar un plan de migración o integración de acuerdo con los lineamientos establecidos para tal fin. El Articulador deberá entregar a MinTIC el detalle del procedimiento de integración, el cual deberá seguir los lineamientos aquí presentados.

# **10 Modelo del Servicio de Carpeta Ciudadana**

Es el servicio que les permite a las personas naturales o jurídicas, acceder y gestionar digitalmente el conjunto de datos almacenados o custodiados por la Administración Pública, de forma segura y confiable.

Este servicio se enmarca en lo definido en la Política de Gobierno Digital y en el cumplimiento de la normatividad vigente. En este escenario, el uso del servicio ciudadano digital de carpeta ciudadana es obligatorio para las entidades públicas, y optativo para las personas naturales y jurídicas.

El servicio de Carpeta Ciudadana cuenta con un carácter estratégico en el contexto de la Política de Gobierno Digital, tomando especial relevancia en la satisfacción de necesidades cotidianas de los ciudadanos y de las entidades, el uso masivo de nuevos servicios digitales, la masificación de trámites y procedimientos administrativos por medios electrónicos.

Como servicio compartido a las entidades públicas, el servicio de Carpeta Ciudadana trabaja de manera conjunta con los otros servicios digitales base. La autorización de acceso es canalizada por el servicio de Autenticación Digital, mientras que el servicio de Interoperabilidad permite realizar las consultas de los datos del usuario desde los custodios responsables en la administración pública.

Los servicios mínimos que deben ser provistos por el prestador de servicios de Carpeta Ciudadana, y a los cuáles tienen derecho de manera gratuita las personas naturales y jurídicas, tendrán las siguientes características:

- Sobre los datos:
  - a. Solicitar corrección a los custodios de responsables en la administración pública.
  - b. Solicitar actualización a los custodios de responsables en la administración pública.
  - c. Personalizar la presentación del conjunto de datos.
  - d. Autorizar el uso e intercambio de los datos que custodia la administración pública.
  - e. Recibir información de los derechos y obligaciones que tiene con el Estado.



- Sobre los trámites (integración con GOV.CO):
  - a. Ejecutar los trámites.
  - b. Acceder a historiales de la información generada en su relación con el Estado a nivel de trámites y servicios.
  - c. Recibir Comunicaciones sobre los actos administrativos emitidos por la Administración Pública.
- Sobre la gestión
  - a. Alertar: entregar mensajes de acceso y uso de su servicio de Carpeta.

## 10.1 Objetivos del servicio de carpeta ciudadana digital

Los objetivos del servicio de Carpeta Ciudadana Digital parten del desarrollo de una mejor relación entre el ciudadano y la empresa con el Estado, dándole al ciudadano y a la empresa facilidades para el conocimiento de los datos que posee el Estado, así como, acercándolos a la gestión de estos a través de un punto de acceso personal. Dichos objetivos se especifican de la siguiente forma:

- Permitir al usuario el acceso a sus datos almacenados en la Administración Pública de manera segura y confiable.
- Brindar un espacio personal para que el usuario conozca qué entidad tiene sus datos y qué tan veraces son.
- Entregar un medio para facilitar al usuario la solicitud de actualización o corrección de sus datos almacenados en la administración pública.
- Visualizar su información según las necesidades o preferencias (servicios públicos, salud, registro, etc.).
- Acceder a trámites y servicios determinados.
- Consultar la información generada en su relación con el Estado a nivel de trámites y servicios.
- Entregar las comunicaciones o alertas que las entidades tienen para los usuarios. previa autorización de estos.

## 10.2 Contexto del servicio carpeta ciudadana digital

En el servicio de Carpeta Ciudadana Digital se definen los actores de los Servicios Ciudadanos Digitales involucrados en el desarrollo de este servicio y los elementos que interactúan para el envío y recepción de la información necesaria para un correcto cumplimiento de los objetivos establecidos.

A continuación, se describen los roles relacionados con el Servicio de Carpeta Ciudadana Digital:

- **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC):** Encargado del desarrollo de la normatividad, lineamientos y requerimientos técnicos necesarios para que el servicio de Carpeta Ciudadana Digital se desarrolle de forma efectiva. Y para ello establece:
  - a. Los criterios técnicos que debe tener en cuenta el articulador en la oferta de la Carpeta Ciudadana Digital para registrar y vincular los usuarios al servicio.
  - b. La especificación de los servicios de la Carpeta Ciudadana Digital.
  - c. Hacer el seguimiento sobre el desarrollo operativo del servicio.
- **Articulador:** En cumplimiento de la prestación del servicio de Carpeta Ciudadana Digital, debe:
  - a. Integrar el servicio de Autenticación digital para que el usuario logre la autorización de ingreso a su carpeta.
  - b. Integrar el servicio de Interoperabilidad para lograr el intercambio de datos entre entidades del Estado
  - c. Generar la estructuración de los datos acorde a los requerimientos establecidos para los servicios de Carpeta Ciudadana Digital.
  - d. Diseñar el componente sobre el cual va a funcionar el servicio de Carpeta Ciudadana Digital, con las facilidades de personalización de los servicios establecidos, así como con el módulo habilitado de solicitud de actualización de datos y exposición de mensajes de las entidades.

- e. Administrar el componente destinado para prestar el servicio de Carpeta Ciudadana Digital.
  - f. Gestionar la operación propia, derivada de la prestación del servicio y los datos recolectados de esta, para generar reportes, estadísticas e informes.
  - g. Brindar acompañamiento a las entidades en cuanto al proceso de provisión de la Carpeta Ciudadana Digital, si es requerido de manera especial, así como dentro del acompañamiento general a la implementación de los servicios ciudadanos digitales base.
  - h. Las condiciones para gestionar la entrega de comunicaciones o mensajes electrónicos desde la entidad al usuario, derivados de las solicitudes de actualización o corrección de sus datos.
  - i. Cumplimiento de los lineamientos y mecanismos para el envío de información desde y hacia los diferentes sistemas y actores que hacen parte del ecosistema de los Servicios Ciudadanos Digitales.
  - j. Administrar la Información procedente de la prestación del servicio, teniendo en cuenta que los **prestadores del servicio de Carpeta Ciudadana** son responsables del tratamiento de los datos personales que los ciudadanos les suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen en la prestación del servicio, por lo que deben cumplir con los deberes legales establecidos en la Ley 1581 de 2012 y sus decretos reglamentarios o aquellas normas que la sustituyan, modifiquen o deroguen.
  - k. Garantizar las condiciones de seguridad y privacidad requeridas por el servicio, para garantizar aspectos como la integridad, la confidencialidad y la disponibilidad de la información, así como los niveles de acceso a la misma. Cumplimiento normativo, entre estos, el Modelo de Seguridad y Privacidad, así como de la Guía para la Administración del Riesgo y Diseño de controles del Departamento Administrativo de la Función Pública.
- **Usuarios:** representa a la persona natural, nacional o extranjera titular de cédula de extranjería, o la persona jurídica, de naturaleza pública o privada, que hace uso de los Servicios Ciudadanos Digitales.
  - **Portal Único del Estado GOV.CO:** teniendo en cuenta que el Portal Único del Estado es una herramienta de integración y punto de acceso digital del ciudadano,

será el medio a través del cual el usuario pueda ingresar para hacer uso del servicio de la Carpeta Ciudadana Digital.

- **Servicio de Autenticación Digital:** desde la perspectiva del servicio de Carpeta Ciudadana Digital, el servicio de Autenticación Digital es el encargado de proveer el mecanismo de autenticación para que el usuario obtenga las credenciales necesarias para lograr ingresar a su Carpeta.
- **Servicio de Interoperabilidad:** el servicio de Interoperabilidad es fundamental para una correcta prestación del servicio de Carpeta Ciudadana Digital, teniendo en cuenta que de esta integración dependerá el impacto que obtenga el ciudadano de la Carpeta, así como la utilidad de los datos que se logren exponer al usuario; por otro lado, también es el habilitador para la comunicación entre el usuario y la Administración Pública en cuanto a las solicitudes de actualización de sus datos.
- **Entidad:** es el actor encargado de suministrar los datos e información que posea del usuario para ser expuesta a través de la carpeta, de manera tal que deberá habilitar los servicios de información requeridos, bien sea desde sus sedes electrónicas o de sus sistemas de información. Así pues, es necesario para la correcta prestación del servicio de Carpeta:
  - a. Que cumpla con los requerimientos establecidos para la habilitación del servicio de Interoperabilidad.
  - b. Cumplir las directrices y lineamientos establecidos en el marco de interoperabilidad y del lenguaje común de intercambio de información, formulados por MinTIC.

Por otro lado, para el servicio de Carpeta Ciudadana Digital, las entidades deben tener en cuenta:

- a. Las condiciones de seguridad y privacidad, requeridas por el servicio para garantizar aspectos como la integridad, la confidencialidad y la disponibilidad de la información, así como los niveles de acceso a la misma.

b. El modelo de seguridad y privacidad y la Guía para la Administración del Riesgo y Diseño de controles de la Función Pública, con la normativa vigente sobre protección de datos personales.

- **Prestador de Servicios Ciudadanos Digitales:** Personas jurídicas, públicas o privadas, quienes, mediante un esquema coordinado y administrado por el articulador, pueden proveer los servicios Ciudadanos Digitales de Autenticación Digital y Carpeta Ciudadana Digital.

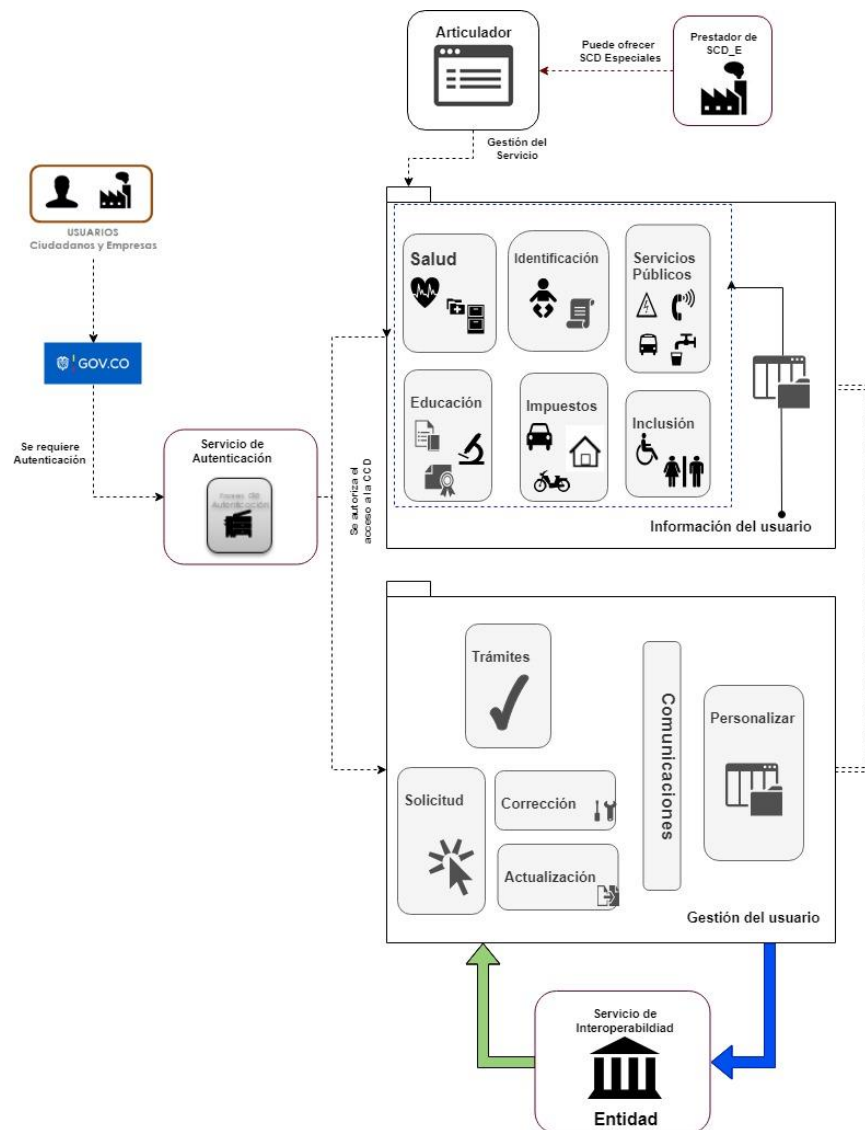


Ilustración 13 – Modelo de contexto del servicio de Carpeta Ciudadana Digital

Tabla 9- Relaciones del modelo de contexto de Carpeta Ciudadana Digital, CCD

Relación		Origen	Destino	Descripción
<b>Acceso al servicio de Carpeta Ciudadana Digital</b>		Usuario	Portal único del Estado GOV.CO	Se da cuando el usuario requiere hacer uso del servicio de la Carpeta Ciudadana Digital y para ello lo hace a través de GOV.CO
<b>Solicitud de autorización de ingreso</b>		Portal único del Estado GOV.CO	Pasarela de autenticación (servicio de Autenticación Digital)	Es este el momento en el cual se genera la solicitud de Autenticación para poder ingresar a la carpeta personal obteniendo las credenciales necesarias para esto.
<b>Ingreso a la Carpeta</b>		Pasarela de autenticación (servicio de Autenticación Digital)	Gov.co sección de Carpeta Ciudadana Digital	Una vez el usuario es autenticado, está autorizado para acceder a su espacio personal y es autorizado a gestionar su carpeta acorde a los privilegios dados por su nivel de autenticación establecido.
<b>Gestiones del usuario</b>		Usuario	Portal web del servicio de Carpeta Ciudadana Digital Portal Web del Servicio de Carpeta Ciudadana Digital	En este punto el Usuario logra acceder a los contenidos que expone el servicio de Carpeta Ciudadana Digital en el portal web. Dentro de las cuales encuentra:
<b>Gestiones del usuario</b>	Personalización			Personalización de la presentación de su información por sector, área de interés

Relación	Origen	Destino	Descripción
			o temáticas normativas.
	Solicitudes		Solicitudes: Corrección o actualización de datos.
	Comunicaciones		Visualización de comunicaciones sobre las gestiones realizadas.
	Autorizaciones		Habilitación para autorización de acciones sobre sus datos y las comunicaciones o envío de mensajes.
	Trámites		Realización de trámites (enlace con GOV.CO)
<b>Intercambio de datos e información</b>	Componente del servicio de Carpeta Ciudadana Digital	Entidades	Se da en el momento en que el usuario ingresa al portal a realizar las gestiones de su información desde los servicios habilitados para la Carpeta Ciudadana Digital.



## 10.3 Modelo de capacidades del servicio carpeta ciudadana digital

El mapa de capacidades del servicio de Carpeta Ciudadana Digital (CCD) corresponde al tercer nivel del modelo de capacidades de los Servicios Ciudadanos Digitales de la sección 16 de esta guía. Las capacidades de este nivel pueden ser consultadas en el siguiente anexo:

Anexo 4 Mapa de Capacidades SCD.xlsx.

Serán capacidades del servicio de Carpeta Ciudadana Digital aquellas que estén marcadas con "X" en la columna "CCD". Adicionalmente, dentro del mapa también se especifica qué actor es necesario para desarrollar la capacidad marcada con "X" en la columna con el nombre del actor (articulador, prestador de servicios, Entidad, MinTIC).

## 10.4 Modelo de despliegue del servicio carpeta ciudadana digital

A continuación, se presenta el modelo de despliegue de primer nivel del servicio de Carpeta Ciudadana Digital, a partir del cual se debe cumplir con la oferta del servicio a entregar:



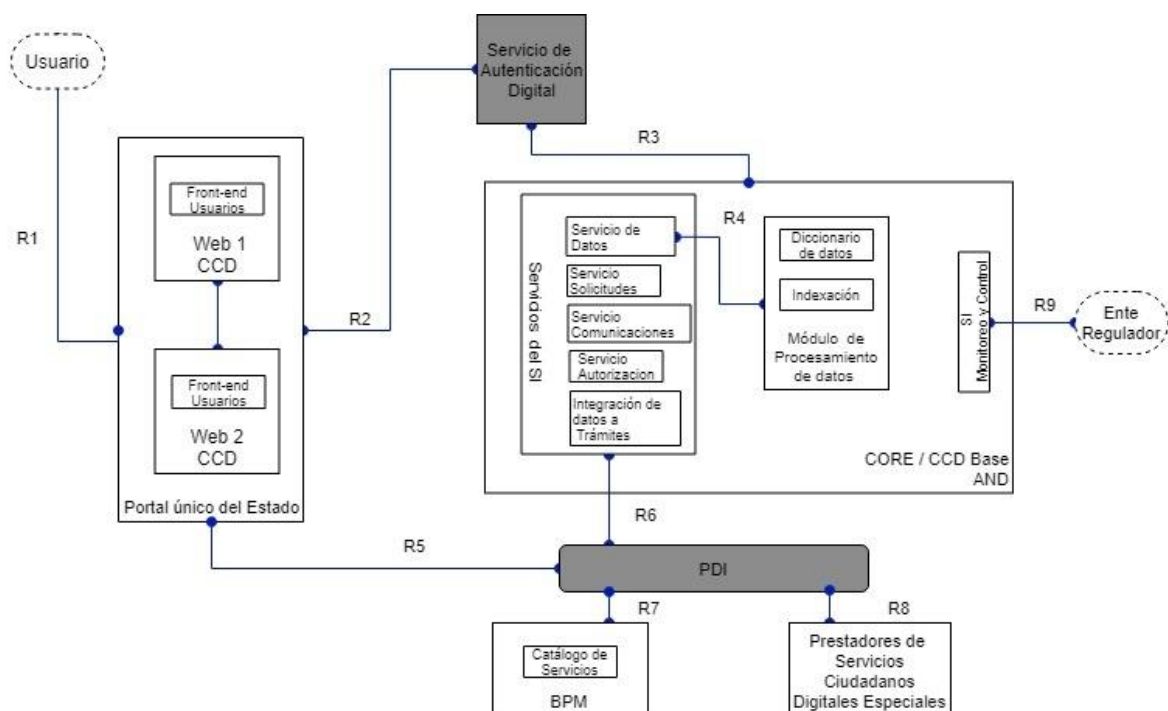


Ilustración 14 – Modelo de despliegue del servicio de Carpeta Ciudadana Digital base.

De esta manera, en la ilustración anterior se muestra cómo el usuario debe acceder a través del Portal Único del Estado Colombiano GOV.CO cuando quiere vincularse, y posteriormente ingresar para abrir su sesión en el componente de Carpeta Ciudadana Digital; esta acción se realiza a través de las credenciales entregadas por el servicio de Autenticación y generando la autorización de acceso.

Seguidamente, se muestran los servicios de Carpeta a través de los cuáles el usuario llega a la presentación predeterminada de sus datos, así como a las acciones que puede ejercer sobre ellos desde la Carpeta, a partir de los cuales se generan historiales, registros y posibles informes para el interés tanto del usuario, como de los entes de control.

Finalmente, todo lo anterior es soportado por el servicio de Interoperabilidad a través del cual se generan las solicitudes o peticiones y se obtienen los datos que nutren el servicio de Carpeta.

Tabla 10 – Descripción de las relaciones del modelo del servicio de CCD

ID	Origen	Destino	Descripción
R1	Usuario	Componente CCD	<p>Interacción directa entre el usuario y el sistema del Servicio de Carpeta Ciudadana Digital (CCD), incluyendo lo siguiente:</p> <p>Registrarse de manera voluntaria y gratuita al servicio de Carpeta Ciudadana, ingresar y administrar el servicio, configurar preferencias, gestionar sus datos, suscribir o cancelar servicios de comunicaciones electrónicas o mensajes, recibir comunicaciones electrónicas, cargar y/o descargar documentos, aportar o compartir documentos.</p> <p>Para acceder al servicio el usuario ingresa las credenciales emitidas por el Articulador / prestador de servicio de Autenticación Digital según el nivel de garantía solicitado por el sistema de Carpeta Ciudadana Digital.</p>
R2	Componente de CCD	Pasarela de Autenticación	<p>Interacción entre el Componente de Carpeta Ciudadana Digital y el servicio de Autenticación Digital para la validación de credenciales de usuarios en las operaciones y consumir los servicios del sistema de Autenticación.</p> <p>El servicio de Autenticación Digital deberá proveer un flujo de información con el sistema en el cual notifica el resultado de la validación, informando si su autenticación es satisfactoria o no, teniendo en cuenta que el nivel a partir del cual se podrá acceder a la Carpeta es el nivel 2, en el cual se mostrarán algunos trámites acorde sus permisos.</p> <p>El acceso a los conjuntos de datos definidos y demás funcionalidades se hará a partir de un nivel 3 de autenticación.</p>

ID	Origen	Destino	Descripción
R3	Servicio de Autenticación Digital	Core del Servicio de CCD	Interacción entre el CORE del servicio de Carpeta Ciudadana Digital y la pasarela de autenticación: Gestión de usuarios y el servicio de Autenticación Digital, con el fin de acceder a los principales componentes del servicio de Autenticación, tales como despliegue del protocolo de autenticación y repositorio de credenciales, para gestionar la autorización de acceso a los servicios de la Carpeta Ciudadana Digital
R4	Servicio de visualización de datos del usuario	Módulo de procesamiento	En este módulo se generarán la visualización de los datos acorde a las definiciones de casos de uso establecidos para cada conjunto de datos.
R5	PDI	GOV.CO	Interacción derivada de la necesidad de la integración de la visualización de los datos a la generación de trámites para que los usuarios logren efectuar trámites desde su carpeta.
R6	Servicios del SI	PDI	En esta interacción se soporta la oferta de servicios de la Carpeta Ciudadana Digital; a través de ella, se genera la interacción del usuario con el sistema de la PDI y así alcanzar los servicios de intercambio de información hacia y desde las entidades.
R7	PDI	BPM / Entidades	Es la interacción a través de los sistemas transaccionales de la entidad con la PDI, pues es la llamada que estos hacen dentro de su flujo para usar los servicios Ciudadanos Digitales y permitir al prestador de Carpeta Ciudadana Digital, presentar los datos necesarios para dar servicio al usuario.
R8	PDI	Prestadores de Servicios Ciudadanos Digitales Especiales	Punto en el que se genera la integración de los prestadores de Servicios Ciudadanos Especiales al ecosistema de los SCD base, y de esta forma añadir un mayor valor para los usuarios a través de su oferta sobre el servicio de Carpeta Ciudadana Digital base.

ID	Origen	Destino	Descripción
<b>R9</b>	Monitoreo y control	Entes reguladores	Interacción dada entre el Sistema de Monitoreo y Control, a través de la cual se generarán datos e información requerida por los entes de control, acorde a periodos y características definidas por estos.

# **11 Requerimientos no Funcionales de los Servicios Ciudadanos Digitales**

A continuación, se presentan los requerimientos no funcionales para los Servicios Ciudadanos Digitales.

## 11.1 Atributo de calidad: funcionamiento

### Atributo de calidad: funcionamiento

El funcionamiento se relaciona con la operación, tipo de respuesta, eficiencia, rendimiento y capacidad del sistema como un todo, teniendo en cuenta las condiciones normales de uso. Muchas de las características anteriores dependen de la infraestructura utilizada, el ancho de banda, la capacidad de procesamiento, la capacidad de memoria, la cantidad de espacio de almacenamiento del sistema y el espacio asignado a cada uno de los Servicios Ciudadanos Digitales, entre otros. Se deben establecer acuerdos de nivel de servicio sobre el funcionamiento que estimen, por ejemplo, el tiempo que debe tomar una consulta y retornar una respuesta.

Tabla 11 – Descripción de los elementos del atributo de funcionamiento

ID	Característica	Descripción	Metas
1	Precio por el uso	Gratuidad para el usuario	a. Los Servicios Ciudadanos Digitales base deberán ser gratuitos para los usuarios
2	Capacidad del sistema	Número de usuarios, entidades y servicios de intercambio de información	a. Número mínimo de usuarios concurrentes <1.000> b. Número máximo de entidades públicas concurrentes <100> c. Número mínimo de servicios de intercambio de información concurrentes <500> d. Número mínimo de transacciones concurrentes <100.000>
3	Rendimiento	Tiempo de respuesta de los Servicios Ciudadanos Digitales	a. El tiempo máximo para que el Articulador despliegue el componente de Autenticación y Carpeta Ciudadana Digital en el navegador de un usuario no supere <5 segundos>. b. El tiempo máximo de respuesta del proceso de Autenticación una vez el

ID	Característica	Descripción	Metas
			<p>usuario ha suministrado sus credenciales es de &lt;1 segundo&gt;.</p> <p>c. El tiempo máximo de respuesta de la Carpeta Ciudadana es de &lt;5 segundos&gt;.</p>
4	Soporte	Disponibilidad de documentación técnica	El sistema debe disponer de personal especializado y documentación técnica para dar un adecuado soporte en el funcionamiento del sistema.
5	Aseguramiento de la información	Copias de seguridad de la información	<p>a. El Articulador debe realizar copias de seguridad completas y copias de seguridad incrementales, con una periodicidad que garantice la adecuada recuperación en caso de falla del sistema.</p> <p>b. Las copias que contengan información clasificada y reservada deben estar cifradas y protegidas de cualquier acceso no autorizado</p> <p>c. Punto de Recuperación Objetivo (RPO). Tiempo entre una réplica de datos y la siguiente réplica, con el fin de mantener la continuidad de los servicios: 30 minutos.</p>
6	Capacidad del sistema	Ancho de banda del Articulador	El Articulador debe garantizar un ancho de banda suficiente para suplir la demanda que realizarán las entidades a los Servicios Ciudadanos Digitales en sistemas de información altamente transaccionales.
7	Mantenimiento	Actualización tecnológica permanente del sistema	<p>a. El Articulador dispondrá de un sistema de mantenimiento con nuevas versiones, paquetes de servicios o parches.</p> <p>b. En caso de que se incluyan nuevas características y funciones, el Articulador debe llevar a cabo nuevas capacitaciones de formación para los usuarios.</p>

ID	Característica	Descripción	Metas
8	Conformidad	Configuración de conformidad con los estándares de la industria y con las regulaciones nacionales	<ul style="list-style-type: none"> <li>a. Deben estar en conformidad con todas las disposiciones legislativas y regulatorias que apliquen a la naturaleza del Articulador y a la jurisdicción.</li> <li>b. Deben estar de conformidad con estándares industriales, generalmente aceptados en tecnología y en las plataformas en donde sea desplegado el sistema.</li> <li>c. Debe ajustarse a las normas locales aplicables para admisibilidad jurídica y valor probatorio de la información digital.</li> <li>d. El sistema no debe incluir funciones que sean incompatibles con la protección de datos a nivel nacional, la libertad de información u otra legislación.</li> </ul>
9	Aseguramiento de la información	Preservación a largo plazo y obsolescencia de la tecnología	El articulador debe considerar los riesgos tecnológicos de cara a la preservación de la información a largo plazo desde tres puntos de vista: (i) la degradación de los medios de comunicación, (ii) la obsolescencia del hardware, (iii) la obsolescencia del formato.
10	Soporte	Servicio de soporte a los usuarios	<ul style="list-style-type: none"> <li>a. Deben existir reglas claras de cómo acceder al servicio de soporte del articulador, de cómo reportar errores, problemas del software y qué tipo de nivel de ayuda in situ y asistencia remota puede esperar un usuario.</li> </ul>
11	Mantenimiento	Mantenimiento preventivo del sistema	<ul style="list-style-type: none"> <li>a. El articulador debe establecer el nivel de mantenimiento y soporte que le da al sistema (hardware, software y comunicaciones), frecuencias de actualización, fecha de la última versión liberada y la hoja de ruta del sistema.</li> </ul>



## 11.2 Atributo de calidad: escalabilidad

### Atributo de calidad: escalabilidad

La escalabilidad se relaciona con la capacidad de los Servicios Ciudadanos Digitales para soportar de manera adecuada el crecimiento en los requerimientos (aumento en el número de usuarios, aumento en el número de usuarios simultáneos conectados, aumento en el número de transacciones simultaneas, aumento en el tamaño de la emisión de credenciales, aumento en el número de entidades y servicios, etc.), sin afectar ninguno de los otros atributos de calidad del sistema (rendimiento, usabilidad, disponibilidad, etc.). El articulador debe asegurar el atributo de calidad de escalabilidad, usando la estrategia que estime conveniente, ya sea aumentando el tamaño y la capacidad de la infraestructura, o balanceando el aumento de carga entre diferentes sistemas o a través de servicios múltiples.

Tabla 12 – Descripción de los elementos del atributo de escalabilidad

ID	Característica	Descripción	Metas
1	Crecimiento del sistema	Crecimiento del número de usuarios	El sistema debe estar diseñado suponiendo que el número de usuarios se duplica en un período de tres años.
2	Crecimiento del sistema	Crecimiento de la infraestructura	El sistema deberá proveer los medios para adicionar capacidad de procesamiento y almacenamiento, sin tener que migrar a un nuevo ambiente.
4	Crecimiento del sistema	Crecimiento de la funcionalidad	El articulador deberá estar en la capacidad de expandir y mejorar el sistema con nuevas funcionalidades 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.
5	Rendimiento al escalar	Al escalar, el sistema no deberá verse afectado en el rendimiento de cada una de sus funciones	<ul style="list-style-type: none"> <li>a. Debe mantener el rendimiento especificado.</li> <li>b. Debe mantener el tiempo máximo de búsqueda especificado.</li> <li>c. Debe mantener la periodicidad de los procesos de eliminación especificada.</li> </ul>

## 11.3 Atributo de calidad: monitoreo

### Atributo de calidad: monitoreo

El atributo de calidad de monitoreo se refiere a la capacidad de los Servicios Ciudadanos Digitales de permitir ser observado desde múltiples puntos de vista, con el fin de garantizar una comprensión exacta de su funcionamiento y de la manera como los distintos actores participan en la operación. Esta capacidad de observación incluye la capacidad de mantener en el tiempo lo observado, almacenando los registros de toda la operación, con el fin de poder ejecutar procesos de auditoría, seguimiento, diagnóstico y mejora del sistema. Debe ser capaz de utilizar la información recolectada para generar indicadores de tipo estratégico, táctico y operativo, incluyendo diversos reportes y análisis estadístico. En particular, debe mantener trazabilidad de los errores, del uso inadecuado del sistema y de toda situación considerada como anormal.

Tabla 13 – Descripción de los elementos del atributo de monitoreo

ID	Característica	Descripción	Metas
1	Auditoría	El sistema debe estar en capacidad de garantizar y facilitar información confiable para los procesos de auditoría	<p>La auditoría debe verificar los siguientes aspectos:</p> <ul style="list-style-type: none"> <li>a. Solo los usuarios autorizados tienen acceso al sistema.</li> <li>b. Todos los usuarios autorizados tienen acceso al sistema.</li> <li>c. Los controles de seguridad y acceso del sistema están funcionando correctamente.</li> <li>d. Los usuarios no están accediendo a activos de información, funciones, servicios, etc. a los que no tienen permitido el acceso.</li> <li>e. Los usuarios cuentan con los mecanismos adecuados de configuración.</li> <li>f. Los documentos de monitoreo están siendo puestos en las agrupaciones apropiadas.</li> </ul>

ID	Característica	Descripción	Metas
			<ul style="list-style-type: none"> <li>g. Los documentos de monitoreo están siendo clasificados correctamente.</li> <li>h. Ningún documento de monitoreo está siendo eliminado del sistema, fuera del proceso de desecho de documentos.</li> <li>i. Los períodos de desecho están siendo monitoreados y las fechas límite están siendo cumplidas.</li> <li>j. Las confirmaciones ocurren dentro de las fechas límite de desecho y no hay atraso en los documentos que deben eliminarse.</li> <li>k. El contenido de los documentos está siendo eliminado correctamente.</li> <li>l. Las copias de los contenidos de los documentos están siendo eliminadas de fuentes secundarias dentro del Articulador / prestador de servicio inmediatamente después o al tiempo con la eliminación formal del archivo.</li> <li>m. Garantizar la trazabilidad mediante el uso de metadatos de acciones sobre el sistema tales como: estampa de tiempo, autor, estado, entre otras.</li> </ul>
2	Registro de errores	El sistema debe permitir el acceso y uso del registro de error	Bitácora y los detallados de los registros de errores.
3	Alertas	El sistema debe permitir la utilización de mecanismos de alerta y consolidación de alertas a los usuarios cuando el sistema realice funciones determinadas	El sistema debe permitir notificar a al articulador, MinTIC, Entidades y Ciudadanos todo tipo de alertas.

ID	Característica	Descripción	Metas
4	Monitoreo del uso de recursos	El sistema debe estar en capacidad de monitorear el uso de recursos para asegurar que el sistema tenga las reservas adecuadas	<ul style="list-style-type: none"> <li>a. Monitorear el número de usuarios, transacciones, servicios de intercambio de información, carpetas que tienen acceso al sistema, a qué hora y en qué días.</li> <li>b. Monitorear la cantidad de almacenamiento que está siendo usada y el ritmo de aumento.</li> <li>c. Monitorear el promedio de tiempo de búsqueda y ritmo en incremento o disminución.</li> <li>d. Monitorear el tiempo de respuesta promedio de todas las funciones.</li> <li>e. Monitorear la utilización de procesamiento y memoria.</li> </ul>
5	Reportes comparados	El sistema debe estar en capacidad de monitorear y advertir acerca del uso de recursos, comparando reportes estadísticos en el tiempo	<ul style="list-style-type: none"> <li>a. Estos informes deberán ser remitidos de forma mensual a MinTIC.</li> </ul>

## 11.4 Atributo de calidad: usabilidad

### Atributo de calidad: usabilidad

El atributo de calidad de usabilidad tiene que ver con qué tan fácil es para el usuario lograr una determinada tarea y el tipo de soporte al usuario que el sistema provee. Esta capacidad tiene que ver principalmente con: (a) el sistema ayuda a que el usuario pueda hacer sus tareas de manera eficiente, (b) el sistema es capaz de minimizar el impacto de los errores del usuario, (c) el sistema facilita el uso a las usuarios sin experiencia, (d) el sistema facilita el uso a usuarios con alguna disminución en sus capacidades, (e) el sistema permite que el usuario haga las adaptaciones y configuraciones que faciliten le ejecución de sus tareas. La facilidad de uso es

una consideración importante en el sistema, especialmente por la aceptación del usuario. Algunas de las características que deben ser consideradas en el diseño incluyen:

- Interfaces limpias, consistencia, capacidad de respuesta, mensajes de error, procesamiento automático y otras formas de minimizar el número de decisiones que los usuarios deben tomar, personalización y localización, facilidades de ayuda, documentación de usuario, preguntas frecuentes, videos y tutoriales en línea, etc.
- Programas de capacitación y formación

Tabla 14 – Descripción de los componentes del atributo usabilidad

ID	Característica	Descripción	Metas
1	Capacitación a los usuarios	Dentro del modelo de gestión del sistema debe estar explícita la manera en que el Articulador/ prestador de servicio garantizará el adecuado uso del sistema por parte de los usuarios	a. El Articulador debe brindar a los usuarios diferentes niveles de capacitación para usar los Servicios Ciudadanos Digitales base eficientemente, incluyendo cursos de entrenamiento, tutoriales y otros recursos de educación y aprendizaje. b. Debe haber capacitación dirigida a usuarios generales (ciudadanos) y especializados (administradores técnicos y de seguridad de las entidades, auditores, etc.).
2	Interacción con el usuario	El sistema debe garantizar que la interacción con el usuario sea simple, ajustada a las necesidades e intuitiva	a. El sistema debe ser diseñado para minimizar la introducción de errores por parte del usuario. b. 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. c. El sistema debe ser capaz de mostrar varios documentos de forma simultánea. d. El sistema debe permitir que, cuando sea conveniente, existan valores por defecto persistentes para la introducción de datos, entre los que convendría que se incluyeran (i) valores

ID	Característica	Descripción	Metas
			<p>definidos por el usuario, (ii) valores idénticos a los del elemento anterior, (iii) valores derivados del contexto, como la fecha, el identificador del usuario, entre otros.</p> <p>e. Las transacciones más habituales del sistema se deben diseñar de forma que puedan realizarse con un pequeño número de interacciones</p>
3	Uniformidad de la interacción	El sistema debe garantizar uniformidad en la manera como presenta la información e interactúa con el usuario	El sistema debe utilizar un conjunto único o un pequeño número de conjuntos, de normas de interfaz de usuario.
4	Ayuda en línea al usuario	El sistema debe ofrecer ayuda en línea al usuario	El sistema debe proporcionar asistencia en línea al usuario en todo momento. Es deseable que la ayuda en línea del sistema sea sensible al contexto.
5	Configuración de la interacción	El sistema debe permitir la configuración de la visualización y de la interacción con el usuario, de acuerdo con sus preferencias	<p>a. El sistema deberá permitir que los usuarios configuren la interfaz de usuario a su gusto, incluyendo entre otros: (i) el contenido de los menús, (ii) la disposición de las pantallas, (iii) la utilización de teclas de funciones, (iv) los colores, las fuentes y el tamaño de las fuentes que se muestran en pantalla, (v) las alarmas sonoras.</p> <p>b. Cuando el sistema recurra a la visualización en pantalla en forma de ventanas, conviene que el usuario pueda configurar cada una de ellas.</p>
6	Accesibilidad	El sistema debe ser accesible a todo tipo de usuario, con	<p>a. La interfaz de usuario del sistema debe ser adecuada a usuarios con necesidades especiales, esto significa</p>

ID	Característica	Descripción	Metas
		diferentes capacidades, incluyendo aquellos con discapacidades específicas.	<p>que ha de ser compatible con el software especializado que se pueda utilizar y con las directrices pertinentes sobre interfaces para ese tipo de usuarios.</p> <p>b. El sistema deberá proveer la opción de alto contraste en la interfaz web para facilitar la presentación a personas con problemas de visión.</p> <p>c. El sistema debe cumplir con los requerimientos establecidos en la Norma Técnica Colombiana NTC 5854, la cual establece los requisitos de accesibilidad que son aplicables a las páginas web, como mínimo Nivel de conformidad AA. La norma fue desarrollada empleando como documento de referencia 'Las Pautas de Accesibilidad para el Contenido web (WCAG) 2.0 del 11 de diciembre de 2008'.</p> <p>d. 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.</p> <p>e. El sistema debe cumplir con los requerimientos establecidos en la WCAG (Web Content Accessibility Guidelines). Estas guías proveen una clasificación de A (la más baja) o AAA (la más alta).</p>

## 11.5 Atributo de calidad: disponibilidad

### Atributo de calidad: disponibilidad

El atributo de calidad de disponibilidad cubre todos los aspectos relacionados con las posibles fallas del sistema y las consecuencias asociadas a los ANS. Una falla del sistema ocurre cuando por alguna razón este deja de cumplir con las solicitudes hechas por el usuario. Este atributo de calidad hace referencia a los siguientes puntos, entre otros: (a) qué sucede cuando una falla ocurre, (b) qué tan frecuentes pueden ser las fallas, (c) cuánto tiempo puede estar el sistema fuera de operación debido a una falla, (d) cómo pueden ser prevenidas las fallas, (e) cómo se deben informar las fallas y a quiénes, (f) cómo se debe recuperar el sistema después de una falla, (g) a través de qué indicadores se deben medir los niveles de servicio. El nivel de disponibilidad que el sistema puede proporcionar debe estar claramente establecido por el Articulador/prestador de servicio. La disponibilidad del sistema deberá estar constantemente monitoreada para observar si las metas del servicio están siendo alcanzadas o si han sido sobrepasadas.

Tabla 15 – Descripción de los elementos del atributo de disponibilidad

ID	Característica	Descripción	Metas
1	Horarios de indisponibilidad	El articulador debe declarar con anticipación 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.	Se requiere acceso y soporte al sistema 24/7 (24 horas al día 7 días de la semana).
2	Traslado de responsabilidad	Si el sistema está alojado por cuenta de un tercero, no deben existir limitaciones adicionales de disponibilidad y las garantías deben ser proporcionadas por el sistema anfitrión.	Se requiere que los requisitos de disponibilidad brindados por el tercero que aloja el sistema sean establecidos en iguales o mejores condiciones que las solicitadas al Articulador.
4	Monitoreo de la disponibilidad	El articulador debe contar (directamente o por medio de un tercero) con las	a. El sistema debe contar con herramientas para medir su disponibilidad total, y la



ID	Característica	Descripción	Metas
		herramientas que permitan medir los porcentajes de disponibilidad del sistema.	<p>disponibilidad de cada uno de sus componentes.</p> <p>b. La medición de la disponibilidad del sistema debe realizarse en tiempo real.</p> <p>c. Los resultados del monitoreo son mantenidos por el articulador para que puedan ser consultados por la entidad o MinTIC en cualquier momento.</p> <p>d. La información mantenida por el articulador le debe permitir a la entidad o a MinTIC verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.</p> <p>e. El articulador debe entregar a MinTIC mensualmente un reporte de la disponibilidad del sistema, incluyendo el detalle de las caídas: fecha, hora de la caída, fecha y hora de restablecimiento del sistema o del componente, duración de la caída, componentes afectados, causas, usuarios afectados (número y quiénes).</p>
5	Cálculo de la disponibilidad	<p>Los requerimientos de disponibilidad del sistema son usualmente expresados como un porcentaje o ratio del tiempo de actividad comparado con el tiempo de inactividad.</p> <p>La disponibilidad se mide usando la siguiente ecuación:</p>	Disponibilidad exigida $\geq 99.982\%$ mensual

ID	Característica	Descripción	Metas
		<p>(1 - (Número total de minutos en que el servicio no está disponible/ Número de días en el mes x 24 horas x 60 minutos)) x 100%</p> <p>La indisponibilidad es el número total de minutos, durante el mes facturado, en los que el servicio no está disponible, dividido en el número total de minutos en el mes facturado.</p> <p>La medición la hace el Articulador / prestador de servicio monitoreando permanentemente el servicio durante el mes.</p>	

## 11.6 Atributo de calidad: confiabilidad

### Atributo de calidad: confiabilidad

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. El sistema deberá ser capaz de manejar condiciones de error, sin quiebra o falla repentina.

Tabla 16 – Descripción elementos del atributo de confianza

ID	Característica	Descripción	Metas
1	Integridad	Los Servicios Ciudadanos Digitales base provistos deben	Para determinar el grado de confiabilidad requerido se seguirán las recomendaciones de la ITU e ISO

ID	Característica	Descripción	Metas
		permitir que la información consignada, transmitida en un mensaje de datos sea íntegra, completa e inalterable.	dispuestas en sus documentos ITU X.1254 e ISO/IEC 29115:2013
3	Inmutabilidad de la 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.	El sistema debe tener herramientas y mecanismos que permitan garantizar que la información no sea alterada.
4	Recuperación ante fallas	El sistema debe poseer mecanismos de recuperación ante fallas.	<ul style="list-style-type: none"> <li>a. Si el sistema se cae o no responde, se deben identificar las fallas y automáticamente iniciar la recuperación o redireccionar a sistemas de respaldo o sistemas alternos.</li> <li>b. En caso de fallas, el sistema debe enviar el detalle de las fallas a sistemas externos y mostrar la información en bitácoras de eventos, archivos de trazabilidad, u otros similares y notificarlos a la Agencia Nacional Digital (AND).</li> <li>c. Tiempo Objetivo de Recuperación (RTO). Tiempo máximo que puede estar fuera de servicio una vez se ha producido una Interrupción: <math>\leq 8</math> minutos.</li> </ul>

ID	Característica	Descripción	Metas
5	Sustitución de medios de almacenamiento	El sistema debe permitir el seguimiento y la sustitución de medios de almacenamiento para protegerse contra la degradación de los medios de comunicación.	
6	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.	

## 11.7 Atributo de calidad: privacidad por defecto

Tabla 17 – Descripción de los elementos del atributo de privacidad por defecto.

ID	Característica	Descripción	Metas
1	Legalidad y lealtad	El tratamiento de datos personales debe cumplir en su totalidad con la Ley 1581 de 2012, sus decretos reglamentarios y	El tratamiento de datos personales debe realizarse de acuerdo con la normatividad vigente.

ID	Característica	Descripción	Metas
		demás normativa aplicable a la protección de los datos personales.	
2	Finalidad	El usuario debe ser informado de la finalidad legítima para la cual se tratarán sus datos personales.	En el momento de realizar el registro de usuario en los Servicios Ciudadanos Digitales, debe ser informado de la finalidad de los datos que le son solicitados.
3	Pertinencia y proporcionalidad	No se deben recolectar o tratar datos más allá de los estrictamente necesarios para cumplir la finalidad del tratamiento.	El Articulador solamente solicitará al usuario los datos estrictamente necesarios para la prestación del SCD al cual el usuario se está registrando.
4	Limitación temporal del tratamiento de datos personales	Los datos no deben ser usados por un período superior al necesario para cumplir los fines para los cuales fueron recogidos.	<ul style="list-style-type: none"> <li>a. El Articulador solamente almacenará las credenciales del usuario mientras éste se encuentre registrado a sus servicios.</li> <li>b. Si el usuario realiza cambio de prestador de servicio, el prestador de servicio saliente debe eliminar toda la información de las credenciales del usuario de todos sus sistemas y las copias de seguridad de las mismas.</li> </ul>
5	Autorización del titular del dato	El tratamiento de datos debe estar precedido de la autorización previa, expresa e informada de la persona.	El usuario debe autorizar el uso de sus datos personales, de acuerdo con la normatividad vigente.
6	Veracidad o calidad	La información debe ser veraz, completa, exacta, actualizada comprobable y comprensible.	El Articulador debe proveer mecanismos de rectificación, actualización o supresión de la información.

ID	Característica	Descripción	Metas
7	Transparencia	El ciudadano tiene el derecho a obtener información sobre la existencia de sus datos personales.	<p>a. En el tratamiento de datos personales el Articulador debe garantizar el derecho del titular a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. [Literal e) del Artículo 4 de la Ley 1581 de 2012].</p> <p>b. El Articulador debe ofrecer al titular de los datos información cualificada y por tanto, cuando procese datos personales, el articulador debe ofrecer, como mínimo, la siguiente información: (i) información sobre la identidad del controlador de datos, (ii) el propósito del procesamiento de los datos personales, (iii) a quien se podrán revelar los datos, (iv) cómo el usuario puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos, y (v) toda otra información necesaria para el justo procesamiento de los datos. [C-748 de 2011].</p>
8	Acceso, uso y circulación restringida	El tratamiento de los datos personales solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley 1581 de 2012.	<p>a. El Articulador debe proveer los mecanismos para garantizar que sus bases de datos son accedidas solamente por personas autorizadas conforme lo establecido en la Ley 1581 de 2012.</p> <p>b. El Articulador no puede circular, dar a conocer o enviar la información de</p>

ID	Característica	Descripción	Metas
			<p>los usuarios, salvo autorización expresa de éstos.</p> <p>c. El Articulador no puede realizar cruce de bases de datos o de los servicios de intercambio de información que contengan datos de los usuarios.</p> <p>d. El Articulador debe proveer controles de acceso y envío de información.</p>
9	Seguridad	<p>La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.</p> <p>[<a href="https://www.law.cornell.edu/uscode/text/44/3542">https://www.law.cornell.edu/uscode/text/44/3542</a>]</p>	<p>a. El Articulador debe proveer las medidas técnicas, humanas y administrativas para garantizar la seguridad de la información.</p> <p>b. El Articulador debe proveer las medidas técnicas, humanas y administrativas para evitar la adulteración o modificación de la información.</p> <p>c. El Articulador debe proveer las medidas técnicas, humanas y administrativas para evitar la pérdida de información.</p> <p>d. El Articulador debe proveer las medidas técnicas, humanas y administrativas para evitar la destrucción o eliminación de la información.</p> <p>e. El Articulador debe proveer las medidas técnicas, humanas y administrativas para evitar la consulta, acceso o uso no autorizados de la información.</p> <p>f. El Articulador debe proveer las medidas técnicas, humanas y administrativas para evitar el acceso fraudulento a la información.</p> <p>g. El Articulador debe proveer las medidas técnicas, humanas y</p>

ID	Característica	Descripción	Metas
			<p>administrativas para evitar la divulgación no autorizada de la información.</p> <p>h. El Articulador debe proveer las medidas técnicas, humanas y administrativas para evitar la utilización encubierta de datos.</p> <p>i. El Articulador debe proveer las medidas técnicas, humanas y administrativas para evitar la contaminación de datos por virus informáticos u otros.</p> <p>j. El Articulador debe proveer las medidas técnicas, humanas y administrativas para garantizar la revisión periódica de las herramientas de seguridad y la evaluación de su efectividad.</p>
10	Confidencialidad	<p>Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento</p> <p>[Literal h) del artículo 4 de la Ley 1581 de 2012].</p>	El articulador debe garantizar la reserva de la información, inclusive después de finalizada su relación con el usuario.



# **12 Requisitos Técnicos de los Servicios Ciudadanos Digitales, SCD**

## 12.1 Requisitos técnicos de los SCD

A continuación, se describen los requisitos técnicos mínimos que deben ser cumplidos en los diferentes procesos y componentes de los Servicios Ciudadanos Digitales por parte del Articulador para garantizar la adecuada prestación del servicio, facilitando la entrega de servicios en línea a los ciudadanos, empresas y las entidades públicas.

La determinación de los requisitos, por su naturaleza fundamentalmente tecnológica, puede estar sujeta a cambios como consecuencia del desarrollo e innovación de la tecnología. Para su definición se ha tenido en cuenta la información en materia de normas, estándares y reglamentaciones técnicas internacionales.

El Articulador deben contar con una infraestructura física, tecnológica, procedimientos y sistemas de seguridad que puedan dar cumplimiento a los requisitos que se encuentran relacionados a continuación, estos pueden ser propios o tercerizados:

Tabla 18 - Requisitos técnicos para el Articulador

Componente	o Requisitos mínimos
<b>Capacidad</b>	
Servicios de Centro de Operaciones de Seguridad	<p>El Articulador debe contar con un servicio de Centro de Operaciones de Seguridad o Security Operations Center (SOC) 7/24 para la gestión de seguridad de los servicios ofertados, que cuente con un centro de monitoreo de los incidentes de seguridad que se puedan presentar de manera proactiva y que gestione los riesgos, asegurando así las condiciones de servicio.</p> <p>La gestión incluye la notificación de incidentes de seguridad a los usuarios y entidades, una vez sucedido el evento.</p>
Centro de Procesamiento de Datos (CPD)	<p>El Articulador debe garantizar que está en la capacidad de contar con Centros de Datos que cumplan como mínimo las características de construcción requeridas para la certificación en el estándar ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers, en el nivel de fiabilidad como mínimo Tier III, o ICREA mínimo Nivel III, en todos los aspectos entre ellos los de telecomunicaciones,</p>

Componente	o Requisitos mínimos
Capacidad	<p>arquitectura, sistema eléctrico y sistema mecánico: Centro de datos Concurrentemente Mantenibles: disponibilidad del al menos 99.982%.</p> <p>Los centros de datos podrán estar alojados en un esquema de nube pública, privada o híbrida siempre y cuando cumplan con lo establecido en el Capítulo Tercero del Título V de la Circular Única de la SIC, sobre estándares de nivel adecuado de protección de datos personales para transferencia de datos personales a terceros países y países que cuentan con un nivel adecuado de protección de datos personales.</p>
Centro de Monitoreo de Red (CMR/NOC)	<p>El Articulador deberá cumplir con las siguientes condiciones mínimas para el NOC:</p> <ul style="list-style-type: none"> <li>• Operación 7/24.</li> <li>• Construcción o refuerzo sismo resistente.</li> <li>• Seguridad de acceso con guardia 7/24.</li> <li>• Sistemas de detección inteligente de incendio.</li> <li>• Seguridad física certificada.</li> <li>• CCTV digital.</li> <li>• Acceso de visitantes con cita previa y control de listas de acceso.</li> <li>• Operación, CAC (Centro de Atención a Clientes) y Monitoreo 7/24.</li> <li>• Sistemas de UPS configurados en redundancia.</li> <li>• Autonomía eléctrica de mínimo 24 horas en caso de interrupción del fluido eléctrico.</li> <li>• Control ambiental: sistemas de aire acondicionado redundantes.</li> <li>• Alimentación segura a los sistemas de control ambiental.</li> <li>• Herramientas de monitoreo para la infraestructura de los diversos fabricantes utilizados.</li> </ul> <p>El Articulador debe proporcionar las herramientas y acceso necesario, para que la Agencia Nacional Digital (AND) pueda consultar el monitoreo de los canales e infraestructura con gráficas en tiempo real, y puedan enviar mensajes de alerta a un gestor.</p>
Canal de conexión	El Articulador debe contar con doble canal de conexión al ofrecer los servicios

Componente	o Requisitos mínimos
Capacidad	
Mesa de servicio/centro de soporte	<p>de de El Articulador debe disponer de un conjunto de recursos tecnológicos y humanos, para prestar servicios de soporte incluyendo un canal de atención para que los usuarios puedan reportar inconvenientes con el servicio y abrir tiquetes de reporte de fallas, así como peticiones, quejas, requerimientos y solicitudes. La mesa de servicio o centro de soporte debe estar disponible 24 horas al día, 7 días a la semana, con la posibilidad de gestionar y solucionar todas las incidencias de manera integral, y efectuar el seguimiento a los tiquetes llevándolos a los niveles adecuados hasta su cierre.</p> <p>El Articulador debe realizar y detallar el diseño de la solución de Mesa de Servicio bajo mejores prácticas, como por ejemplo ITIL, para recibir, atender y clasificar los casos de solicitud de servicio o incidentes que se reporten incluyendo la gestión, soporte, monitoreo y seguimiento, trazabilidad, solución y cierre de todos los casos reportados por los usuarios. Todas las herramientas para la gestión de la operación deben permitir una integración a diferentes tecnologías de soporte de servicios.</p> <p>Se debe asignar prioridad de solución a los tiquetes de acuerdo con la Tipificación de Usuarios y la afectación del servicio, así:</p> <ul style="list-style-type: none"> <li>• Prioridad Alta – Emergencia, tiempo máximo de solución 4 horas: Fallas en la infraestructura atribuibles al Articulador y problemas operacionales de los servicios (Red, virtualización y configuración) entregados por el Articulador y que generen una indisponibilidad crítica del negocio de la Entidad.</li> <li>• Prioridad Media – Degradación del servicio, tiempo máximo de solución 24 horas: Fallas en la infraestructura y problemas operacionales de los servicios atribuibles al Articulador (Red, virtualización y configuración) entregados por el Articulador, que afectan el desempeño o confiabilidad de los procesos de negocio de la Entidad. Solicitudes de asesoramiento para la configuración, implementación y administración de servicios.</li> </ul>

Componente	o Requisitos mínimos
Capacidad	<ul style="list-style-type: none"> <li>• Prioridad Baja – Solicitudes, tiempo máximo de solución 48 horas: Solicitudes de soporte menores o de información que no tienen impacto en los procesos de negocio de la Entidad, solicitud de información técnica de los servicios, solicitudes de documentación de servicios, solicitudes de información y aclaraciones acerca del uso y operación de los servicios.</li> </ul>
Roles	<p>El Articulador de los Servicios Ciudadanos Digitales deberán disponer de un equipo de trabajo idóneo que garantice la adecuada prestación de los servicios y el cumplimiento de los niveles de servicio acordados (ANS). Dentro del equipo de trabajo, el Articulador designará los siguientes roles, los cuales deberán acreditar experiencia y conocimientos especializados en la materia, tales como:</p> <ul style="list-style-type: none"> <li>• Gerente/Director de Proyectos: gestión de proyectos.</li> <li>• Oficial/Delegado de protección de datos personales: Ley 1581 de 2012 y sus decretos reglamentarios.</li> <li>• Oficial de Seguridad de la Información: ciberseguridad, ciberdefensa, seguridad de la información y seguridad informática.</li> </ul>

## 12.2 Sistemas de administración de riesgos

El Articulador debe acreditar que cuentan con los siguientes sistemas de administración de riesgo:

- Sistema de Administración de Riesgo Operativo (SARO)

Para la administración del riesgo operativo el Articulador debe desarrollar un sistema que contemple los métodos lógicos y sistemáticos adecuados y efectivos para tal fin. El SARO debe ser implementado acorde con el número de usuarios y/o transacciones proyectados para los tres (3) primeros años de prestación del servicio, de forma tal que le permita identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan

incidir en la debida administración del riesgo operativo a que puede estar expuesto en el marco de la prestación de sus servicios.

Para los anteriores efectos el Articulador deberán acreditar junto con la documentación el Manual de Riesgo Operativo que contenga los siguientes elementos:

- a. Políticas
  - b. Procedimientos
  - c. Documentación
  - d. Estructura administrativa
  - e. Registro de eventos de riesgo operativo
  - f. Órganos de Control sobre el Sistema
  - g. Políticas de divulgación de información
  - h. Programa de capacitación
  - i. Plan de continuidad del negocio
  - j. Cubrimiento del Sistema a los terceros en los que se apoye para prestar uno o alguno de los servicios
- Sistema de Control Interno

El Articulador como deberán contar con un sistema de control interno (SCI) que les permita cumplir con los objetivos operativos, de reporte y de cumplimiento que se describen a continuación:

- a. Objetivos Operativos: se refiere a la eficacia y eficiencia en los procesos relacionados con la prestación del servicio.
- b. Objetivos de información o de reporte: apuntan a que la información generada por el Articulador a nivel de sus grupos de interés sea oportuna y transparente.
- c. Objetivos de cumplimiento: se refiere a la observancia y acatamiento de los lineamientos de esta guía, así como de todas las normas relacionadas con la prestación de los servicios ciudadanos digitales para los cuales haya sido inscrito.

## Alcance del sistema de control interno

El SCI debe responder tanto a la estructura del Articulador como al monto de los usuarios/transacciones que éste planea tener dentro de los tres (3) primeros años de actividad. Para lo anterior deberán contar con un Manual en el cual se desarrollen todos los aspectos aquí establecidos a saber:

1. Principios: son principios generales de un SCI
  - i. Autocontrol
  - ii. Autorregulación
  - iii. Autogestión
  - iv. Responsabilidad
2. Elementos del SCI
  - ii. Ambiente de control
  - iii. Valoración y gestión de riesgos
  - iv. Actividades de control
  - v. Información y Comunicación
  - vi. Actividades de monitoreo
3. Roles y responsabilidades dentro del SCI: deben establecerse roles y responsabilidades al interior de la entidad relacionados con el SCI en al menos los siguientes órganos
  - i. Junta directiva u órgano equivalente
  - ii. Comité de auditoría
  - iii. Representante Legal
  - iv. Revisor Fiscal

## 12.3 Requisitos de infraestructura

El articulador debe asegurar que su infraestructura cumpla con las garantías y los lineamientos de seguridad necesarios acordes a los estándares de seguridad de la información como la norma técnica ISO/IEC 27001:2013, la ISO 22301:2012 en

Continuidad del negocio, ITIL v3 en Administración de los servicios TIC, ISO/IEC 24762 en Lineamientos sobre servicios de tecnología de la información y comunicación para recuperación de desastres, National Institute of Standards and Technology - Special Publication NIST 800-53 Revisión 5, Security and Privacy Controls for Federal Information Systems and Organizations, el estándar internacional OWASP Top 10 Application Security Risks - 2017 y del Modelo de Seguridad y privacidad de la información definido por MinTIC. Además, el Articuladores deberán presentar informe de cumplimiento de un sistema de gestión de seguridad de la información SGSI emitido por un tercero imparcial que tenga experiencia mínima de dos años en auditoria de sistema de gestión de seguridad de la información SGSI, que evidencie lo siguiente:

- Plan estratégico de seguridad de la información.
- Políticas de seguridad necesarias para la gestión y administración de seguridad de la información.
- Inventario de activos de información y el análisis de riesgos.
- Controles adecuados para garantizar la confidencialidad, integridad y disponibilidad mitigando los riesgos identificados.
- Declaración de aplicabilidad.
- Plan de Recuperación de Desastres, el Plan de contingencia y el Plan de continuidad de negocio.
- Pruebas de seguridad periódicas, ejecutando escaneos para detectar vulnerabilidades, fallos de configuración o parches omitidos.
- Cadena de custodia de la evidencia recolectada que se solicite para los procesos de análisis forense conforme a lo establecido en la Norma ISO/IEC 27037:2012.

Del mismo modo, se debe evaluar dichas garantías y articular las medidas de protección necesarias y correspondientes. Para esto deberá contar con un modelo de defensa en profundidad aplicando controles en seguridad, resiliencia, directivas, procedimientos y concienciación, para proteger los datos en diferentes capas, cumpliendo con los siguientes requerimientos:

Capa de seguridad	Requisitos mínimos
Datos	- ACL (Lista de control de acceso para establecer privilegios de acceso a los datos).



	<ul style="list-style-type: none"> <li>- Cifrado de la información con criptografía simétrica y/o asimétrica (vigente de acuerdo como lo establece la NIST) de longitud no inferior a 2048.</li> <li>- Asegurar las claves de acceso con almacenamiento por medio de un algoritmo especialmente diseñado para protegerlas.</li> </ul>
Aplicación	<ul style="list-style-type: none"> <li>- WAF (Web Application Firewall)</li> <li>- Antivirus de nueva generación NGAV</li> </ul>
Host	<ul style="list-style-type: none"> <li>- HIDS (Host Intrusion Detection System)</li> <li>- Virtualización de host</li> </ul>
Red interna	<ul style="list-style-type: none"> <li>- Segmentación</li> <li>- Protocolo de accesos a un directorio.</li> <li>- IPSec</li> <li>- TLS/SSL</li> </ul>
Perímetro	VPN (Virtual Private Network)
Seguridad física	<ul style="list-style-type: none"> <li>- Seguridad en los accesos físicos al edificio.</li> <li>- Seguridad interna de salas.</li> <li>- Seguridad en los Racks de comunicaciones.</li> <li>- Control y filtrado de accesos.</li> <li>- Control medioambiental.</li> <li>- Control de energía.</li> </ul>
Seguridad perimetral	<ul style="list-style-type: none"> <li>- Sistema Anti DDoS (Distributed denial of service)</li> <li>- IDS (Intrusion Detection System)</li> <li>- IPS (Intrusion Prevention System)</li> <li>- Firewall de nueva generación NGFW</li> <li>- Balanceador de carga.</li> <li>- DMZ (demilitarized zone)</li> </ul>
Monitoreo y auditoría	<ul style="list-style-type: none"> <li>- El Centro de Operaciones de Seguridad SOC debe tener las siguientes especificaciones: <ul style="list-style-type: none"> <li>▪ Suministrar características UBA (User Behavior Analytics) para implementar indicadores de compromiso.</li> <li>▪ Realizar el monitoreo 7x24, y la gestión de incidentes y la administración de todos los componentes 7x24.</li> <li>▪ El triage de eventos e incidentes sean táctico y estratégico con cada una de las categorizaciones, informes,</li> </ul> </li> </ul>

	<p>correlaciones, priorizaciones, clasificaciones, valoraciones y asignaciones.</p> <ul style="list-style-type: none"> <li>▪ Cubrir la respuesta técnica con: investigación, contención, erradicación, recuperación y prevención a eventos e incidentes.</li> </ul> <ul style="list-style-type: none"> <li>- Deberá cumplir con las condiciones mínimas para el Centro de Operaciones de Red NOC establecidas en la Tabla Requisitos Técnicos.</li> <li>- La plataforma de gestión de eventos e información de seguridad SIEM (Security Information and Event Management) puede ser reconocida en el mercado y que se encuentre líder en el cuadrante de Gartner.</li> <li>- Servidor de registros (Syslog).</li> <li>- Supervisión, Monitorización y Alarmas.</li> <li>- Plataformas de mitigación.</li> <li>- Metodología de evaluación, auditoría y acción de mejora sobre un potencial incidente de ciberseguridad.</li> <li>- Herramientas para el trabajo con logs, centralización y explotación de Logs.</li> <li>- Sincronización de relojes con la Hora Legal Colombiana.</li> <li>- Todos los servicios deben generar logs de las transacciones realizadas.</li> <li>- Auditar toda actividad de los administradores de ESB</li> <li>- Habilitar la auditoria sobre el manejo de usuarios y grupos.</li> <li>- Crear listas blancas y negras para realizar la validación de entradas.</li> <li>- Habilitar auditoria en los procesos de reinicio y apagado.</li> <li>- Copias de seguridad de los logs de transacción.</li> <li>- Sistemas actualizados y parches de seguridad al día.</li> </ul> <p>El Articulador debe proporcionar las herramientas y acceso web que se requiera, para que MinTIC pueda consultar los canales e infraestructura con gráficas en tiempo real con los siguientes indicadores de monitoreo:</p>
--	---

	<ul style="list-style-type: none"> <li>▪ Accesos a Bases de Datos.</li> <li>▪ Acceso a los logs.</li> <li>▪ Reportes de los incidentes.</li> <li>▪ Respuesta de incidentes.</li> <li>▪ Los perfiles de los usuarios.</li> <li>▪ Los roles de los administradores del sistema.</li> <li>▪ Calidad del servicio.</li> <li>▪ Privilegios del sistema.</li> <li>▪ Estado de los recursos.</li> <li>▪ Estado y nivel de respuesta de los Servicios.</li> <li>▪ Informes de desempeño.</li> <li>▪ Estado de las aplicaciones del sistema.</li> <li>▪ Utilización de red.</li> <li>▪ Espacio en disco.</li> <li>▪ Métricas ANS.</li> <li>▪ Métricas ITIL (KPIS).</li> <li>▪ Reportes de ataques informáticos y de malware.</li> </ul> <p>Se podrán contar con las siguientes características adicionales:</p> <ul style="list-style-type: none"> <li>▪ Puede ser miembro de la organización global FIRST (Fórum of Incident Response and Security Teams).</li> <li>▪ Contar con la certificación en sistema de gestión de seguridad de la información ISO 27001.</li> </ul>
--	--

## 12.4 Requisitos de red

Se debe satisfacer los lineamientos de seguridad para que los mecanismos de comunicación garanticen la confidencialidad, integridad, disponibilidad, autenticación, autorización, el no repudio y auditoria, que se requieren para en los Servicios Ciudadanos Digitales. A continuación, se muestra el lineamiento de seguridad y el requisito mínimo que debe cumplir:

Lineamiento de seguridad	Requisitos mínimos
Confidencialidad	<ul style="list-style-type: none"> <li>- Garantizar que los accesos a los servicios ciudadanos digitales estén debidamente autorizados.</li> <li>- Cifrar los canales de comunicación, para lo cual podrá usar los medios como el protocolo HTTPs, establecer VPN o similares siempre y cuando se garanticen el cifrado</li> </ul>
Integridad	<ul style="list-style-type: none"> <li>- Garantizar la integridad de los mensajes utilizando mecanismos con valor jurídico probatorio que salvaguarden la completitud y precisión de la información intercambiada.</li> <li>- Garantizar el cifrado y la integridad de la información.</li> <li>- Canales Cifrados punto a punto.</li> </ul>
Disponibilidad	<ul style="list-style-type: none"> <li>- Garantizar el acceso a los Servicios Ciudadanos Digitales en el momento que se requiera y a los usuarios autorizados.</li> <li>- Mantener conexiones redundantes para alta disponibilidad.</li> <li>- Establecer los puertos abiertos necesarios para los servicios.</li> <li>- Proveer servicios de DNS redundantes con doble autenticación, control de interfaces limitando y cifrando el tráfico y protegiendo la cache.</li> </ul>
Autenticación	<ul style="list-style-type: none"> <li>- Garantizar el manejo y validación de usuarios por medio de un protocolo de accesos a un directorio que asegure la alta transaccionalidad de los usuarios.</li> <li>- Configurar el TCP Session Timeout en 900 segundos.</li> </ul>
Autorización	<ul style="list-style-type: none"> <li>- Determinar los grupos/roles que el usuario tiene asignado poseen el permiso para consumir el servicio solicitado.</li> <li>- Establecer permisos a roles específicos para acceder a cada funcionalidad de los servicios.</li> </ul>
No repudio	<ul style="list-style-type: none"> <li>- Asignar un usuario plenamente identificado a la entidad al momento de consumir un servicio para ser autenticado junto con el código de la entidad.</li> </ul>

	<ul style="list-style-type: none"> <li>- Establecer canales de comunicación cifrados.</li> <li>- Firmar el mensaje enviado con un certificado digital de propiedad de cada entidad.</li> </ul>
Auditoría	<ul style="list-style-type: none"> <li>- Proveen servicios para realizar operaciones Crear y actualizar transacciones, Registrar eventos de la transacción, Registrar errores de la transacción.</li> <li>- Registro de transacciones del origen, el destino y quien hizo de transacción.</li> <li>- Centro de Operaciones de Red NOC</li> <li>- Planos de segmentación de las redes de Gestión y Servicio.</li> <li>- Virtualización de red</li> <li>- Plataformas de sincronización de tiempo.</li> </ul>

Los Servicios Ciudadanos Digitales deben contar con procesos de seguridad en redes como:

- Gestión de cambios
- Gestión de accesos
- Configuraciones e inventario
- Gestión de copias de seguridad
- Gestión de incidencias
- Supervisión y Monitorización
- Gestión de logs
- ACLs en routers.

La información de los servicios debe ser conocida por las entidades públicas para evaluar la conveniencia de utilizar el servicio de intercambio de información, es importante aplicar los lineamientos del ámbito de la Gestión de la calidad y seguridad de los Servicios Tecnológicos del Marco de referencia de Arquitectura Empresarial para la Gestión de TI del MinTIC.

Las principales garantías para considerar son:

- Seguridad integral, coordinando todos los elementos técnicos, humanos, materiales y organizativos relacionados con el servicio.

- Gestión de riesgos.
- Prevención, reacción y recuperación, para reducir la posibilidad de amenazas, deteniendo los incidentes de seguridad a tiempo.
- Reevaluación periódica, de cara a adecuar la eficacia a la constante evolución de los riesgos y sistemas de protección.
- Función diferenciada, distinguiendo entre el responsable de la información, responsable del servicio y responsable de la seguridad.

Se debe informar inmediatamente a MinTIC sobre la ocurrencia de incidentes de seguridad que afecten a los Servicios Ciudadanos, así como de las medidas de mitigación que deban ser adoptadas para la resolución del incidente y evitar los daños que puedan producirse.

Las entidades públicas deben establecer las medidas de seguridad cuya aplicación es su responsabilidad y que se encuentre ajustadas al Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.

## 12.5 Requisitos a nivel de aplicación

El nivel de aplicación los Servicios Ciudadanos Digitales debe satisfacer los siguientes requerimientos mínimos de acuerdo con los lineamientos de seguridad:

Lineamiento de seguridad	Requisitos mínimos
Confidencialidad	- Implementar criptografía simétrica y/o asimétrica (vigente de acuerdo como lo establece la NIST) de longitud no inferior a 2048.
Integridad	- Soportar el manejo de certificados digitales (X509 y rutas de certificados). - Uso de directorios en donde se autenticuen los servicios en la forma más granular posible. - Soportar W3C XML Encryption.

Lineamiento de seguridad	Requisitos mínimos
	- Implementar criptografía simétrica y/o asimétrica (vigente de acuerdo como lo establece la NIST) de longitud no inferior a 2048.
Disponibilidad	- WS-Security o JWT (JSON web token) - o cualquier otro protocolo de comunicación que suministre un medio para aplicar seguridad a los Servicios Web con estándar vigente en el mercado y previa validación por MinTIC
Autenticación	- Hay que asegurar que todas las páginas y recursos por defecto, requieren autenticación proceso para gestión de accesos y permisos. - Cifrar los datos de autenticación. - Soportar WS-Federation o JWT (JSON web token) - o cualquier otro protocolo de comunicación que suministre un medio para aplicar seguridad a los Servicios Web con estándar vigente en el mercado y previa validación por MinTIC. - Establecimiento, mantenimiento y cierre de sesiones. - Crear un túnel SSH (Secure SHell) para asegurar la conexión remoto.
Autorización	- Establecer explícito de permisos a roles específicos para acceder a cada funcionalidad. - Solicitar usuario y contraseñas únicos e irrepetibles, para todos los sistemas de acceso.
Auditoría	- Realizar monitoreo y auditoria de las cuentas y accesos a los servicios establecidos. - Monitoreo a los intentos fallidos de acceso. - Verificar la identidad de quien envía la comunicación. - Cumplir con todos los requisitos de autenticación y gestión de sesiones definidos en el Application Security Verification Standard (ASVS) de OWASP. - Comprobación de control de acceso para asegurar que el usuario está autorizado para acceder.

Lineamiento de seguridad	Requisitos mínimos
	<ul style="list-style-type: none"> <li>- Realizar mínimo dos pruebas de análisis y detección de vulnerabilidades con su respectivo Re-test cada año.</li> <li>- Plan de mitigación de vulnerabilidades.</li> </ul>
No repudio	<ul style="list-style-type: none"> <li>- Soportar W3C XML Digital Signature como posible opción de estándar para firmado electrónico.</li> <li>- Soportar Web SSO Metadata Exchange protocol</li> </ul>

## 12.6 Almacenamiento de información

Los Servicios Ciudadanos Digitales, en especial el Servicio de Interoperabilidad y Carpeta Ciudadana Digital no realizará almacenamiento de los datos que se intercambian entre usuarios. El servicio de Autenticación Digital y Carpeta Ciudadana Digital, realizará el almacenamiento de la información de los usuarios registrados respetando siempre la seguridad de la información y los principios de privacidad por diseño y por defecto.

La información técnica como la configuración, datos de la operación prestada, estadísticas del servicio, logs, auditoría del sistema, entre otros, deberán mantenerse accesibles durante la prestación del servicio y durante cinco (5) años más. Esta actividad podrá realizarse por medios electrónicos.

Se debe contar con una política de respaldo de la información que garantice su accesibilidad, integridad y disponibilidad.



## **13 Seguridad y Privacidad**

La seguridad y la privacidad son factores que deben recibir la máxima atención por parte del Articulador, en este sentido, el tratamiento de datos personales, incluido el tratamiento de datos sensibles, de los diferentes actores del servicio.

En este sentido el Articulador como prestadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente. Asimismo, será el encargado del tratamiento de los datos que otras entidades les proporcionen. En cada caso, se deberán cumplir los deberes que les corresponden como responsables o encargados, establecidos en la Ley 1581 de 2012 o las normas que la modifiquen, deroguen o subroguen, sin perjuicio de las obligaciones que establece el Decreto 1078 de 2015 La prestación de servicios ciudadanos digitales se encuentra sometida al cumplimiento de los establecido en la Ley 1581 de 2012 o las normas que la modifiquen, deroguen o subroguen.

El Articulador deberá cumplir los siguientes requisitos:

Componente o Capacidad	Requisitos mínimos exigidos
<b>Evaluación de Impacto en la Privacidad (PIA)</b>	<p>Se debe cumplir con lo definido en el Artículo 2.2.17.5.2 Decreto 1078 de 2015. De esta forma, antes de dar inicio a la prestación del servicio, el Articulador deberá efectuar la Evaluación de Impacto en la Privacidad - PIA por sus siglas en inglés (<i>Privacy Impact Assessment</i>), realizando el análisis de riesgos que los SCD puede presentar para el derecho a la protección de los datos personales de los usuarios de los servicios. La evaluación deberá realizarse sobre la expectativa de los primeros dos años de la prestación del servicio y deberá contener como mínimo:</p> <ul style="list-style-type: none"> <li>• Análisis en profundidad de cada uno de los SCD, adoptando medidas reconocidas internacionalmente, identificando los tipos de datos personales objeto de tratamiento, los titulares de los mismos, los flujos de información desde su recolección hasta su disposición final y las tecnologías utilizadas.</li> <li>• Una descripción detallada de las operaciones de tratamiento de datos personales que involucra la prestación de los SCD y de los fines del tratamiento.</li> </ul>

Componente o Capacidad	Requisitos mínimos exigidos
	<ul style="list-style-type: none"> <li>• Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.</li> <li>• Una identificación y evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales, valoración de la probabilidad que sucedan y el daño que causarían si se materializaran.</li> <li>• Determinación de los controles y las medidas previstas para afrontar, eliminar, mitigar, transferir o aceptar los riesgos, incluidas garantías, medidas de seguridad, control y monitoreo de los riesgos, tecnologías y mecanismos que garanticen la protección de datos personales, pudiendo realizar diseño de software, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas, y responsables de implementar dichos controles y medidas.</li> <li>• Verificación de que el servicio cumple con la Ley 1581 de 2012, sus decretos reglamentarios y demás normativa aplicable a la protección de datos personales.</li> </ul> <p>Por otro lado, el Articulador deberá presentar a MinTIC, los resultados de esta evaluación junto con los controles y las medidas para eliminar o mitigar los riesgos.</p> <p>Una vez se haya iniciado la prestación efectiva del servicio de Interoperabilidad, autenticación digital y carpeta ciudadana digital, el Articulador deberá realizar una revisión y actualización periódica, durante toda la prestación del servicio, sobre el análisis de los resultados de la evaluación. En el momento en el que el Articulador considere pertinente adelantar la correspondiente revisión y actualización, deberá considerar los siguientes dos años de la prestación del servicio contados a partir del momento de realización de dicha revisión, verificando si se han creado nuevos riesgos o se han detectado otros que habían pasado desapercibidos. Estos resultados se utilizarán para actualizar la Evaluación de Impacto en la Privacidad cuando sea necesario.</p>

Componente o Capacidad	Requisitos mínimos exigidos
<b>Privacidad desde el Diseño y por Defecto (PbD)</b>	<p>Se debe cumplir con lo definido en el Artículo 2.2.17.5.5 del decreto 1078 de 2015. Así mismo, el Articulador está en la obligación de cumplir con las siguientes actividades relativas a la privacidad por diseño y por defecto:</p> <ul style="list-style-type: none"> <li>• Implementar los principios para el tratamiento de datos personales establecidos en la Ley 1581 de 2012, aportando a MinTIC documento que detalle las medidas técnicas, humanas y/o administrativas implementadas para la aplicación de cada principio.</li> <li>• Toma de medidas proactivas, anticipándose y previniendo la pérdida de privacidad de la información antes que suceda.</li> <li>• Aplicar las medidas técnicas, humanas y organizativas apropiadas para garantizar el tratamiento de los datos personales que solo sean necesarios para las finalidades específicas del tratamiento (minimización de los datos).</li> <li>• Seudonimización de los datos a través de técnicas de cifrado de acuerdo con la clasificación de la información.</li> <li>• Realizar y actualizar las Evaluaciones de Impacto en la Privacidad y el Programa Integral de Gestión de Datos Personales, cuando cambios de los Servicios Ciudadanos Digitales creen nuevos riesgos a la privacidad.</li> <li>• Incorporar las prácticas y los procesos de desarrollo necesarios, destinados a salvaguardar la información personal de los actores y usuarios, proporcionales a su naturaleza jurídica, tamaño empresarial, la naturaleza de los datos objeto de tratamiento, el tipo de tratamiento, los riesgos potenciales, etc., durante toda la prestación de los servicios y durante cinco (5) años luego que hayan cesado las actividades como Articulador / prestador del servicio, conforme lo establecido en la sección “Almacenamiento de Información” de este Manual.</li> <li>• 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</li> </ul>

Componente o Capacidad	Requisitos mínimos exigidos
	<p>los requisitos, políticas y preferencias de privacidad de los actores.</p> <ul style="list-style-type: none"> <li>• Uso de los máximos medios posibles necesarios para garantizar la seguridad, confidencialidad e integridad de información personal durante el ciclo de vida del tratamiento que realicen sobre los datos personales en la prestación de los Servicios Ciudadanos Digitales.</li> <li>• 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 usuarios y entidades públicas.</li> </ul>
<b>Responsabilidad Demostrada</b> <i>(Accountability)</i>	<p>Se debe cumplir con lo definido en el Artículo 2.2.17.5.3. del decreto 1074 de 2015 de Responsabilidad demostrada y programa integral de gestión de datos personales. Los prestadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos Personales</p>
<b>Tratamiento de datos personales (Ley 1581 de 2012)</b>	<p>En la prestación de los Servicios Ciudadanos Digitales, el Articulador deberá:</p> <ul style="list-style-type: none"> <li>▪ El Programa Integral de Gestión de Datos Personales PIGDP debe cumplir los lineamientos de la Superintendencia de Industria y Comercio, en particular, la guía para la implementación de la responsabilidad demostrada (accountability) de dicha entidad. Todo lo anterior de conformidad a los límites que impone la Ley de Protección de Datos de Carácter Personal, Ley 1581 de 2012, el cumplimiento de las funciones constitucionales, legales y reglamentarias de cada autoridad pública y/o particular que cumpla funciones públicas, y los límites que impone la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, Ley 1712 de 2014, o las normas que la modifiquen, deroguen o subroguen</li> </ul>

Componente o Capacidad	Requisitos mínimos exigidos
	<ul style="list-style-type: none"> <li>• Garantizar el cumplimiento de los derechos consagrados en los artículos 15 y 20 de la Constitución Política y de la normatividad colombiana vigente y aplicable en especial los principios, derechos y obligaciones de la Ley 1581 de 2012 de Protección de Datos Personales, del Capítulo 25 del Decreto único reglamentario del sector comercio, industria y turismo - 1074 de 2015- y de la Guía para la implementación de la Responsabilidad Demostrada de la SIC.</li> <li>• Diseñar, implementar y promulgar un manual interno de políticas y procedimientos, basado en el ciclo interno de la gestión de los datos personales, que contenga controles e indicadores que arrojen resultados medibles sobre el grado de diligencia y cumplimiento de la normativa, así como los mecanismos para la atención y respuesta de las peticiones y reclamos presentados por los titulares en ejercicio de su derecho de hábeas data.</li> <li>• Diseñar y aprobar una Política de Tratamiento de la Información Personal, adaptada al tratamiento y finalidades de la información personal en el servicio de Interoperabilidad, autenticación digital y carpeta ciudadana digital, que contenga como mínimo lo establecido en el Artículo 2.2.25.3.1. del Decreto 1074 de 2015.</li> <li>• Publicar, socializar a los actores involucrados establecidos en el Artículo 2.2.17.1.5. del DUR-TIC y garantizar el entendimiento y apropiación de la Política de Tratamiento de la Información Personal por parte de los usuarios, en el servicio de interoperabilidad.</li> <li>• Realizar una revisión periódica de la Política de Tratamiento de la Información Personal y efectuar los cambios y actualizaciones pertinentes conforme el desarrollo del servicio de Interoperabilidad, Autenticación Digital y Carpeta Ciudadana Digital, e informar a los usuarios y actores sobre los cambios sustanciales realizados a la Política.</li> <li>• Utilizar Avisos de privacidad, en los casos que no sea posible poner a disposición de los usuarios la Política de Tratamiento</li> </ul>

Componente o Capacidad	Requisitos mínimos exigidos
	<p>de la Información, cumpliendo con el contenido mínimo establecido en el Artículo 2.2.2.25.3.3. del Decreto 1074 de 2015.</p> <ul style="list-style-type: none"> <li>• Realizar el proceso de debida diligencia para el diseño, revisión e implementación de un Programa Integral de Gestión de Datos Personales, a la luz de la Guía para la Implementación del Principio de Responsabilidad Demostrada (<i>Accountability</i>) de la Superintendencia de Industria y Comercio y de las Evaluaciones de Impacto en la Privacidad o en la Protección de Datos.</li> <li>• Establecer reglas de conducta, perfiles de acceso y confidencialidad para las personas involucradas en el diseño, desarrollo, operación o mantenimiento de cualquier sistema de archivos, o en mantener algún registro.</li> </ul>
<b>Oficial de protección de datos</b>	<p>Se debe cumplir con lo definido en el Artículo 2.2.17.5.4. Oficial de protección de datos. De conformidad con el artículo 2.2.2.25.4.4. del Decreto 1074 de 2015, todo responsable y encargado del tratamiento de datos deberá designar a una persona o área que asuma la función de protección de datos personales, quien dará trámite a las solicitudes de los Titulares para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y del capítulo 25 del Decreto 1074 de 2015; y quien deberá, además de cumplir los lineamientos de la Superintendencia de Industria y Comercio, en particular, la guía para la implementación de la responsabilidad demostrada (<i>accountability</i>) de dicha entidad, realizar las siguientes actividades en cuanto a los datos de los usuarios de los servicios ciudadanos digitales: 1. Velar por el respeto de los derechos de los titulares de los datos personales respecto del tratamiento de datos que realice el prestador de servicios ciudadanos digitales. 2. Informar y asesorar al prestador de servicios ciudadanos digitales en relación con las obligaciones que les competen en virtud de la regulación colombiana sobre privacidad y tratamiento de datos personales. 3. Supervisar el cumplimiento de lo dispuesto en la citada regulación y en las políticas de tratamiento de información del prestador de servicios ciudadanos digitales, así como del principio de responsabilidad</p>

Componente o Capacidad	Requisitos mínimos exigidos
	<p>demostrada. 4. Prestar el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos. 5. Atender los lineamientos y requerimientos que le haga la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio o quien haga sus veces. Todo lo anterior de conformidad a los límites que impone la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, Ley 1712 de 2014.</p>
<b>Roles asignados, responsabilidades, y rendición de cuentas</b>	<p>El Articulador identificará las funciones generales y específicas y las responsabilidades para la gestión y uso de información personal, además de garantizar la rendición de cuentas para cumplir estas responsabilidades. Para esto deberá:</p> <ul style="list-style-type: none"> <li>• Designar un <i>Oficial de Privacidad o Protección de Datos</i> responsable de velar por el cumplimiento de la Política de Tratamiento de la Información, el Manual interno de políticas y procedimientos, de las medidas legislativas, reglamentarias, y otras políticas propuestas, las evaluaciones de impacto en la privacidad, del impacto de las tecnologías de información personal, y tecnologías que permiten la auditoría continua de conformidad con las políticas y prácticas de privacidad establecidas.</li> <li>• Identificar las personas que diariamente tienen la responsabilidad en la organización del Articulador de la ejecución de los procedimientos y políticas de privacidad y el cumplimiento normativo; designar un funcionario de alto nivel apropiado (por ejemplo, CIO) para servir como contacto principal del Articulador para asuntos de tecnología /web y las políticas de privacidad de la información.</li> <li>• Establecer un <i>Comité de Privacidad o Protección de Datos</i> que apoye la labor del Oficial de Privacidad o protección de datos, para supervisar y coordinar los componentes y la aplicación de los programas, así como las evaluaciones y rendición de cuentas.</li> </ul> <p>Todos los empleados y contratistas del Articulador deben tener conocimiento sobre la normativa de protección de datos personales, el Programa Integral de Gestión de Datos</p>



Componente o Capacidad	Requisitos mínimos exigidos
	<p>Personales, la Política de Tratamiento de la Información Personal, el debido tratamiento de los datos personales y el seguimiento de las medidas de seguridad pertinentes, además de ser conscientes de la privacidad y su obligación para proteger la información en forma identificable.</p>
<p><b>Sensibilización y programas de capacitación basado en funciones</b></p>	<p>El Articulador deberá garantizar que los administradores y usuarios de la información personal de su organización sean conscientes de los riesgos de privacidad asociados con sus actividades y de las leyes aplicables, políticas y procedimientos relacionados con la privacidad, para lo cual tendrá que:</p> <ul style="list-style-type: none"> <li>• Crear una cultura organizacional entorno a la privacidad y la protección de datos personales.</li> <li>• Capacitar regularmente en la normativa a cada persona implicada, sobre el debido tratamiento de datos personales, medidas de seguridad, las reglas de conducta y sanciones en caso de incumplimiento.</li> <li>• Informar y educar a los empleados y contratistas sobre su responsabilidad para proteger información en forma identificable.</li> <li>• Asegurarse de que todo el personal está familiarizado con las leyes de protección de datos personales y privacidad de la información, reglamentos y políticas y entender las implicaciones que conlleva el acceso inadecuado, revelación y/o uso de datos personales sin estar autorizado para ello, conforme lo establecido por el Artículo 269F de la Ley 1273 de 2009.</li> <li>• 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 en la Privacidad</i>.</li> <li>• Conservar el debido soporte de todas las capacitaciones.</li> </ul>

Componente o Capacidad	Requisitos mínimos exigidos
<b>Publicación</b>	<p>El Articulador, en la prestación de los Servicios Ciudadanos Digitales, tendrá que publicar:</p> <ul style="list-style-type: none"> <li>• La Política de Tratamiento de la Información Personal.</li> <li>• Avisos de Privacidad que informen la existencia de la Política de Tratamiento de la Información Personal.</li> <li>• El canal establecido para atender las consultas y reclamos de los titulares por datos personales.</li> <li>• El procedimiento para la recepción, atención y respuesta a las consultas y reclamos por datos personales.</li> </ul>
<b>Derechos individuales. Participación individual</b>	<p>El Articulador deberá garantizar a los actores el pleno y efectivo ejercicio de sus derechos, estableciendo un canal de atención de consultas y reclamos por datos personales, además de dar respuesta a los mismos en los plazos establecidos por la Ley 1581 de 2012.</p>
<b>Notificación</b>	<p>El Articulador deberá</p> <ul style="list-style-type: none"> <li>• Notificar a MinTIC cualquier dato o registro de un actor sea solicitado por alguna entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.</li> <li>• Adoptar tecnologías que permitan alertar a las entidades de forma automática sobre cambios en las prácticas de privacidad y seguridad.</li> <li>• Garantizar confidencialidad, integridad y autenticidad, teniendo las medidas de seguridad necesarias.</li> </ul>
<b>Suministro de información</b>	<p>El Articulador solo podrá suministrar información a:</p> <ul style="list-style-type: none"> <li>• Los titulares de datos personales, sus causahabientes o representante legales.</li> <li>• A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.</li> <li>• A terceros autorizados por el titular o por la ley.</li> <li>• Garantizar confidencialidad, integridad y autenticidad, teniendo las medidas de seguridad necesarias.</li> </ul>
<b>Autorización Finalidad</b>	<p>y El Articulador deberá solicitar la autorización previa e informada para el tratamiento de datos personales a todos los titulares de los cuales recolecte información personal, cuando en la prestación del servicio se requiera, conforme los requisitos establecidos en la</p>

Componente o Capacidad	Requisitos mínimos exigidos
	<p>Ley 1581 de 2012 y sus decretos reglamentarios. De igual forma, deberá almacenar copia de la autorización otorgada por los titulares en los casos que deba solicitar autorización.</p> <p>El Articulador debe garantizar que utilizará la información personal solo para las finalidades autorizadas por el titular, las cuales deben ser pertinentes y adecuadas. En caso de requerir el tratamiento de la información para finalidad diferente, deberá solicitar una nueva autorización al titular.</p>
<b>Uso</b> <b>aceptable</b>	<p>El Articulador deberá garantizar que la información personal se utilice sólo en la forma prevista en la autorización del tratamiento de datos personales y para los fines pertinentes de la prestación del servicio de interoperabilidad, Autenticación Digital y carpeta ciudadana digital.</p> <p>Los datos personales y los datos enviados a través del servicio de interoperabilidad y/o tratados en los servicios de Autenticación Digital y Carpeta Ciudadana Digital, y en general la información generada, producida, enviada o compartida en la prestación del servicio no podrán ser objeto de comercialización ni de explotación económica de ningún tipo.</p>
<b>Cadena de confianza</b>	<p>Todo subcontratista o proveedor del Articulador, que actúe en su nombre para desarrollar servicios sobre un sistema de registros, debe cumplir con los requisitos enumerados en esta sección sobre privacidad y protección de datos personales.</p>
<b>Monitoreo y medición</b>	<p>El Articulador debe llevar a cabo y estar preparado para informar de los resultados de evaluaciones y auditorias 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, capacitación, violaciones y sistemas de registros.</p>
<b>Notificación y respuesta ante incidentes</b>	<p>El Articulador deberá diseñar e implementar un procedimiento de gestión de incidentes y de reporte de incidentes que afecten los datos personales a la autoridad de vigilancia de datos personales, y deberá:</p>

Componente o Capacidad	Requisitos mínimos exigidos
	<ul style="list-style-type: none"> <li>• Informar a MinTIC sobre cualquier incidente de seguridad que afecte la confidencialidad, disponibilidad e integridad de la información personal relacionada con el servicio de interoperabilidad, Autenticación Digital y Carpeta Ciudadana Digital, las acciones de mitigación o solución del incidente, acciones de mejora realizadas.</li> <li>• Documentar los resultados de las auditorías de cumplimiento, acciones correctivas implementadas para remediar las deficiencias identificadas de cumplimiento.</li> <li>• Reportar los incidentes a los usuarios titulares de la información afectada y a la Superintendencia de Industria y Comercio-SIC, conforme a lo establecido en el Capítulo Segundo del Título V de la Circular única de la SIC.</li> <li>• Realizar las acciones de mejora para eliminar y prevenir futuros incidentes.</li> <li>• En caso de incidentes de seguridad en el marco del servicio de Autenticación Digital dar cumplimiento a lo dispuesto en Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen.</li> </ul>
<b>Registro Nacional de Bases de Datos - RNDB</b>	<p>El Articulador, cuando actúe como responsable de tratamiento de datos personales en la prestación de los Servicios Ciudadanos Digitales, y en cumplimiento de la obligación de registrar sus bases de datos personales en el Registro Nacional de Bases de Datos - RNBD-, conforme lo establecido en el Capítulo 26 del título 2 del Decreto Único Reglamentario del sector Comercio, Industria y Turismo -1074 de 2015- y el Decreto 90 de 2018, deberá actualizar sus bases de datos personales y la información contenida en el Registro Nacional de Bases de Datos -RNBD-, conforme a la información personal sujeta a tratamiento por la prestación de los SCD y las nuevas bases de datos creadas o que se puedan crear o modificar por la prestación de los SCD, y realizar los reportes de novedades, según lo estipulado en el Título V de la Circular Única de la Superintendencia de Industria y Comercio - SIC-, cuando aplique.</p>

# **14 ANS de los Servicios Ciudadanos Digitales, SCD**

Con el objetivo de articular las condiciones y términos que regularán la prestación de los Servicios Ciudadanos Digitales, El Articulador informará a MinTIC los niveles de servicio (Acuerdos de Nivel de Servicio – ANS). Estas condiciones se definirán a través de indicadores que permitirán cuantificar la calidad del servicio en términos de capacidad, disponibilidad, continuidad, gestión de incidentes y cualquier otro ámbito que afecte al servicio prestado, siguiendo el lineamiento LI.ST.08. Acuerdos de Nivel de Servicios del Marco de referencia de Arquitectura Empresarial para la Gestión de TI.

Los indicadores deberán contener los siguientes atributos para cada acuerdo:

- **Descripción del Indicador:** detalle del indicador, qué mide, cómo y con qué fuente de datos y la finalidad del indicador definido.
- **Responsabilidades:** quién recoge y facilita los datos necesarios para realizar los cálculos.
- **Fórmula:** para el cálculo y obtención del nivel de servicio periódico de cara a poder identificar si se ha cumplido o no el acuerdo.
- **Umbrales:** valores mínimos en la prestación del servicio que disparan situación de aviso y de alarma. los umbrales son consensuados entre ambas partes, aunque el proveedor podría definir otros umbrales de cara al aseguramiento de la calidad en el servicio.
- **Periodicidad:** momentos de la captura de datos para el cálculo de las métricas y de la verificación de umbrales de aviso. Se debe determinar además la periodicidad de los informes de cumplimiento de los ANS.

La medición de los acuerdos de niveles de servicio (ANS) se realizan con base en la información de monitoreo permanentemente de los Servicios Ciudadanos Digitales. Los resultados del monitoreo son mantenidos por el Articulador para que puedan ser consultados por la Entidad o MinTIC en cualquier momento durante la duración de los servicios. La información mantenida por el articulador debe permitir verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.

Tabla 19 – ANS Asociados a los Servicios Ciudadanos Digitales

ANS ASOCIADOS A LOS SERVICIOS CIUDADANOS DIGITALES				
ID	ANS	Descripción	Medición	
1	Disponibilidad	<p>La disponibilidad se mide usando la siguiente ecuación:</p> $\left(1 - \frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes} \times 24 \text{ horas} \times 60 \text{ minutos}}\right) \times 100\%$ <p>La indisponibilidad es el número total de minutos, durante el período observado (mensual), en los que los servicios Ciudadanos Digitales no está disponible, dividido en el número total de minutos del período observado.</p>	Disponibilidad	exigida mensual. ≥99.98%
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 los Servicios Ciudadanos Digitales 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, Autenticación Digital, ni acceso a la Carpeta Ciudadana Digital.</p>	RTO	≤ 8 minutos

ANS ASOCIADOS A LOS SERVICIOS CIUDADANOS DIGITALES			
ID	ANS	Descripción	Medición
3	Interrupciones máximas	<p>El ANS de Interrupciones máximas hace referencia al número máximo de interrupciones durante el período observado (mensual).</p> <p>Una interrupción se define como una pérdida total del servicio que implica que no hay intercambio de datos sobre la PDI, Autenticación Digital, ni acceso a la Carpeta Ciudadana Digital.</p>	Interrupciones máximas en un mes 1 Interrupción.
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 los Servicios Ciudadanos Digitales se recuperan de forma inmediata cuando se produce la falla.</p> <p>Una falla se define como una degradación los Servicios Ciudadanos Digitales con respecto a las condiciones pactadas para la prestación del servicio</p> <p>Nota aclaratoria: una falla es diferente a una interrupción. La falla está asociada a la confiabilidad del servicio y la interrupción está asociada a la disponibilidad del servicio.</p>	MTBF >4320 horas
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"> <li>- Desde la Entidad, hasta el Articulador.</li> </ul>	Latencia máxima < 3 s



ANS ASOCIADOS A LOS SERVICIOS CIUDADANOS DIGITALES			
ID	ANS	Descripción	Medición
		<ul style="list-style-type: none"> <li>- Desde el Articulador, hasta la Entidad.</li> </ul> <p>En los casos de sospecha de una falla, el Articulador debe medir y reportar la latencia en el momento y con la frecuencia que la Entidad o el MinTIC lo requiera.</p>	
6	Ancho de banda	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.	El ancho de banda debe ser mayor o igual al ancho de banda contratado.

## 14.1 SOBRE LA REDES DE DATOS DE LOS SERVICIOS CIUDADANOS DIGITALES

Los Servicios Ciudadanos Digitales deben satisfacer los lineamientos de seguridad para que los mecanismos de comunicación garanticen la confidencialidad, integridad, disponibilidad, autenticación, autorización, el no repudio y auditoría que se requieren para el intercambio seguro de datos que viajan a través de los servicios asociados. A continuación, se muestra el lineamiento de seguridad y el requisito mínimo que debe cumplir:

Tabla 20 – Lineamientos de seguridad y requisitos mínimos

Lineamiento de seguridad	Requisitos mínimos
<b>Confidencialidad</b>	<ul style="list-style-type: none"> <li>- Garantizar que los accesos a los Servicios Ciudadanos Digitales estén debidamente autorizados.</li> <li>- Cifrar los canales de comunicación entre las entidades y el articulador.</li> </ul>

Lineamiento de seguridad	Requisitos mínimos
<b>Integridad</b>	<ul style="list-style-type: none"> <li>- Garantizar la integridad de los mensajes utilizando mecanismos con valor jurídico probatorio que salvaguarden la completitud y precisión de la información intercambiada.</li> <li>- Garantizar el cifrado y la integridad de la información en todas las conexiones realizadas a los Servicios Ciudadanos Digitales</li> </ul>
<b>Disponibilidad</b>	<ul style="list-style-type: none"> <li>- Garantizar el acceso a los Servicios Ciudadanos Digitales en el momento que se requiera y a los usuarios autorizados.</li> <li>- Mantener conexiones redundantes para alta disponibilidad de los Servicios Ciudadanos Digitales.</li> <li>- Establecer los puertos abiertos necesarios para los Servicios Ciudadanos Digitales.</li> <li>- Proveer servicios de DNS redundantes con doble Autenticación, control de interfaces limitando y cifrando el tráfico y protegiendo la memoria caché.</li> </ul>
<b>Autenticación</b>	<ul style="list-style-type: none"> <li>- Garantizar el manejo y validación de usuarios por medio de un protocolo de accesos a un directorio que asegure la alta transaccionalidad de los usuarios.</li> <li>- Configurar el TCP Session Timeout en 900 segundos.</li> </ul>
<b>Autorización</b>	<ul style="list-style-type: none"> <li>- Determinar los grupos/roles que el usuario tiene asignado poseen el permiso para acceder a los Servicios Ciudadanos Digitales.</li> <li>- Establecer permisos a roles específicos para acceder a cada funcionalidad de los Servicios Ciudadanos Digitales.</li> </ul>
<b>No repudio</b>	<ul style="list-style-type: none"> <li>- Asignar un usuario plenamente identificado a la entidad al momento de acceder a los Servicios Ciudadanos Digitales para ser autenticado junto con el código de la entidad.</li> <li>- Firmar el mensaje enviado con un certificado digital de propiedad de cada entidad.</li> </ul>
<b>Auditoría</b>	<ul style="list-style-type: none"> <li>- Proveer servicios para realizar operaciones crear y actualizar transacciones, registrar eventos de la transacción, registrar errores de la transacción.</li> <li>- Registro de transacciones del origen, el destino y quién hizo de transacción.</li> <li>- Centro de Operaciones de Red NOC.</li> <li>- Planos de segmentación de las redes de Gestión y Servicio.</li> <li>- Virtualización de red.</li> </ul>

Lineamiento de seguridad	Requisitos mínimos
	- Plataformas de sincronización de tiempo.

Los Servicios Ciudadanos Digitales deben contar con procesos de seguridad en redes como:

- Gestión de cambios
- Gestión de accesos
- Configuraciones e inventario
- Gestión de copias de seguridad
- Gestión de incidencias
- Supervisión y monitorización
- Gestión de logs
- ACLs en routers.

Así mismo, el articulador y los prestadores de servicio deberán establecer las medidas de seguridad, cuya aplicación es su responsabilidad, las que, además, deberán encontrarse ajustadas al Modelo de Seguridad y Privacidad de la Información de MinTIC.

## **15 Términos y Condiciones de Uso**

El Articulador deberá ofrecer a sus usuarios un documento de Términos y Condiciones de los Servicios Ciudadanos Digitales, el cual deberá ser previamente aprobado por MinTIC.

Los usuarios de los SCD a su vez tendrán la obligación de informarse acerca de las condiciones de cada uno de los servicios, hacer un manejo adecuado del mismo, custodiar sus mecanismos de autenticación e informar a las autoridades competentes cuando ocurra un evento de seguridad que pueda afectar la identidad y datos personales del titular, así como la integridad de la operación de los SCD.

El Articulador no podrá modificar de forma unilateral los términos y condiciones, ni imponer o cobrar servicios que no hayan sido expresamente aceptados por los usuarios y autorizados por el Ministerio de Tecnologías de la Información y las Comunicaciones.

En los casos de los servicios de Autenticación Digital y Carpeta Ciudadana Digital, los términos y condiciones deberán estar asociados con el formulario de registro, el cual a su vez deberá contar con la autorización, en caso de requerirse, para el tratamiento de datos personales, según lo establecido en la Ley 1581 de 2012.

La vigilancia y control de las actividades involucradas en la prestación de los Servicios Ciudadanos Digitales se realizará por cada uno de los organismos del Estado que en el marco de sus competencias tengan que conocer de una o varias de las actividades involucradas en la prestación de tales servicios, de conformidad con lo establecido en el artículo 2.2.17.3.3. del Decreto 1074 de 2015.

Los términos y condiciones deben ser aceptados de forma libre, expresa e informada por el usuario, y deberán contener como mínimo la siguiente información:

**1. Condiciones generales de uso con:**

- a. Descripción de los Servicios Ciudadanos Digitales, sus condiciones de uso y operación, incluyendo que el servicio de Carpeta Ciudadana Digital y Autenticación Digital es personal e intransferible.
- b. Las características básicas de las credenciales o mecanismos entregados.

- c. Una descripción de los campos de registro destinados para recolectar información, así como las finalidades para su tratamiento.
- d. Las medidas técnicas, humanas y administrativas que se emplearán para garantizar su custodia y seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- e. Una descripción de los compromisos de calidad del servicio y la identificación de los canales de atención general y de aquellos específicos para la formulación de peticiones, quejas y reclamos, incluyendo atención de consultas y reclamos por datos personales.
- f. Adicionalmente, el Articulador deberá indicar las condiciones para la prestación del Servicio para menores de edad y dependientes, estableciendo los requisitos para el registro, los derechos, obligaciones y prohibiciones.

## 2. Condiciones de uso de las credenciales de autenticación:

Descripción de las condiciones de uso de las credenciales de autenticación que el operador entregue a los usuarios, incluyendo que las credenciales son personales e intransferibles.

## 3. Derechos y obligaciones de los usuarios con:

- a. Descripción de los derechos de los usuarios, así como la forma y medios a través de los cuales podrán ejercer dichos derechos.
- b. Opción de seleccionar, conforme al catálogo de entidades con sus servicios o trámites, aquellas con las cuales desea interactuar.
- c. Opción de gestionar y revocar sus autorizaciones, para recibir información y comunicaciones desde las entidades públicas.
- d. Opción de compartir información con otros usuarios del servicio, con entidades públicas o terceros, etc.

## 4. Condiciones para el tratamiento de datos personales:

- a. El Articulador deberá indicar que cuenta con una política de tratamiento de la información personal indicando dónde puede ser consultada.

- b. Que realiza evaluaciones de impacto sobre el tratamiento de datos personales y que cuenta con un programa integral de gestión de datos personales.
  - c. El Articulador deberá indicar el tratamiento al que se encuentran sujetos los datos personales sensibles y de menores de edad.
- 5. **Política de seguridad de la información:** el Articulador debe garantizar que toda la información que se trate en el marco de los Servicios Ciudadanos Digitales está protegida y custodiada bajo los más estrictos esquemas de seguridad y privacidad, para ello deberá indicar que cuenta con una Política de Seguridad de la Información, indicando dónde puede ser consultada.
- 6. **Referencias de las políticas:** pueden especificarse las referencias a políticas de calidad y servicio u otras definidas frente al servicio.
- 7. **Supresión de la información:** el Articulador debe especificar las condiciones y los procedimientos empleados para la supresión de la información del usuario. Estos procedimientos deben estar acordes con los riesgos asociados al tratamiento de datos personales en cada una de las etapas e incluir controles coherentes en cuanto a la supresión (borrado seguro) de la información.

Todos los documentos y políticas asociados a los términos y condiciones formarán parte integral de los mismos y deberán estar disponibles para consulta de los usuarios. Cualquier ajuste, modificación o actualización deberá ser notificado con anticipación a los usuarios.

El Articulador deberá entregar una copia al usuario de los términos y condiciones y guardar constancia de la fecha y hora en que el usuario manifiesta su aceptación. Para garantizar la validez e integridad del consentimiento es necesario que el documento sea leído y firmado por el usuario.



**El futuro digital  
es de todos**

**Gobierno  
de Colombia  
MinTIC**