

RESOLUCIÓN 2160 DE 2020

(octubre 23)

Diario Oficial No. 51.479 de 26 de octubre de 2020

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para el uso de estos

LA MINISTRA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES,

en ejercicio de sus facultades legales, en especial las que le confiere el artículo [2.2.17.4.1](#) del Decreto 2106 de 2015 y el artículo [90](#) del Decreto 2106 de 2019, y

CONSIDERANDO QUE:

Conforme al principio de “masificación del gobierno en línea” hoy Gobierno Digital, consagrado en el artículo 8 del artículo [20](#) 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 en el desarrollo de sus funciones.

De acuerdo con el artículo [2.2.9.1.2.1](#) del Decreto número 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (DUR-TIC), la Política de Gobierno Digital será definida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y se desarrollará a través de componentes y habilitadores transversales acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor por el entorno de confianza digital a partir del aprovechamiento de las TIC.

Según el mismo artículo [2.2.9.1.2.1](#) del DUR-TIC, los habilitadores transversales de la Política de Gobierno Digital, son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha Política.

El artículo [90](#) del Decreto número 2106 de 2019, por el cual se dictan normas para simplificar, suprimir, reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública”, las autoridades deberán integrarse y hacer uso del modelo de Servicios Ciudadanos Digitales y se irán por parte de las autoridades de conformidad con los estándares que establezca el MinTIC.

El numeral 13 del artículo [2.2.17.1.4](#) del DUR-TIC define los servicios ciudadanos digitales como soluciones y procesos transversales que brindan al Estado 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 especiales.

Los numerales 6 y 7 del mismo artículo [2.2.17.1.4](#) definen la Guía de lineamientos de los servicios ciudadanos digitales como “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 debe cumplir con el fin de garantizar la correcta prestación de los servicios ciudadanos digitales”; y, la Guía para vinculación de servicios ciudadanos digitales como “el documento expedido y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones destinado a las autoridades y que indica las condiciones necesarias y los pasos que éstas deben realizar para la preparación, adecuación, integración, uso y apropiación de los

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”.

El Artículo [2.2.17.4.1](#). del DUR-TIC señala como obligaciones del MinTIC, en concordancia con el literal a. del artículo [18](#) de la Ley 1341 de 2009, entre otras, la de expedir y publicar la Guía de lineamientos para los servicios ciudadanos digitales y la Guía para vinculación y uso de los servicios ciudadanos digitales. Dichas guías fueron publicadas para participación ciudadana entre los días 5 de junio y el 6 de julio de 2020.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1o. OBJETO. La presente resolución tiene por objeto 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 los servicios ciudadanos digitales.



ARTÍCULO 2o. ÁMBITO DE APLICACIÓN. Serán sujetos obligados a la aplicación del presente artículo todos los organismos y entidades que conforman las ramas del Poder Público en sus distintos órdenes de gobierno, los órganos autónomos e independientes del Estado, y los particulares, cuando cumplan funciones administrativas o públicas.



ARTÍCULO 3o. ESTÁNDARES DE IMPLEMENTACIÓN DE LOS SERVICIOS CIUDADANOS DIGITALES CONTENIDOS EN LA GUÍA DE LINEAMIENTOS DE LOS SERVICIOS CIUDADANOS DIGITALES. El articulador señalado en el numeral 3 del artículo [2.2.17.1.5](#). del Decreto número 1075 de 2015, deberá cumplir las condiciones y estándares establecidos en la Guía de lineamientos de los servicios ciudadanos digitales que se encuentran señaladas en el anexo 1 de la presente resolución, con el fin de garantizar la prestación de los servicios ofertados.



ARTÍCULO 4o. ESTÁNDARES DE IMPLEMENTACIÓN DE LOS SERVICIOS CIUDADANOS DIGITALES CONTENIDOS EN LA GUÍA PARA VINCULACIÓN Y USO DE LOS SERVICIOS CIUDADANOS DIGITALES. Las autoridades señaladas en el Artículo [2.2.17.1.2](#). del Decreto número 1075 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 en el anexo 2 de la presente resolución, con el fin de garantizar 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.



ARTÍCULO 5o. ACTUALIZACIÓN DE LA GUÍA DE LINEAMIENTOS DE LOS SERVICIOS CIUDADANOS DIGITALES Y LA GUÍA PARA VINCULACIÓN Y USO DE LOS SERVICIOS CIUDADANOS DIGITALES. 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 los servicios ciudadanos digitales serán actualizados cuando así lo determine la Dirección de Gobierno Digital del MinTIC, previo informe del equipo técnico encargado de liderar dicha política.



ARTÍCULO 6o. VIGENCIA. La presente resolución rige a partir de la fecha de su publicación en el Boletín Oficial.

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 23 de octubre de 2020.

La Ministra de Tecnologías de la Información y las Comunicaciones,

Karen Abudinen Abuchaibe.

<Anexos descargados de la web de la entidad>

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 Gob

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	Guía de Lineamientos de los Servicios Ciudadanos Digitales
Septiembre 2020	Dirigida al articulador de los Servicios Ciudadanos Digitales

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico:

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 A Internacional](https://creativecommons.org/licenses/by-sa/4.0/).

Tabla de Contenido

1 INTRODUCCIÓN	
----------------------	--

2 ALCANCE DE LA GUÍA	
3 DEFINICIONES	
4 MARCO JURÍDICO	
5 MODELO CONCEPTUAL DE LOS SERVICIOS CIUDADANOS DIGITALES	
6 MODELO DE INTENCIÓN DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD	
6.1 MODELO ESTRATÉGICO DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD	
7 MAPA DE CAPACIDADES DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD	
8 MODELO DEL SERVICIO DE INTEROPERABILIDAD	
8.1 ALINEACIÓN DEL SERVICIO DE INTEROPERABILIDAD Y EL MARCC INTEROPERABILIDAD	
8.2 OBJETIVOS DEL SERVICIO DE INTEROPERABILIDAD	
8.3 VISTA DE CONTEXTO DEL SERVICIO DE INTEROPERABILIDAD	
8.4 MAPA DE CAPACIDADES DEL SERVICIO DE INTEROPERABILIDAD	
8.5 MODELO DE DESPLIEGUE DEL SERVICIO DE INTEROPERABILIDAD	
8.6 SERVICIOS TECNOLÓGICOS DE LA PLATAFORMA DE INTEROPERABILIDAD	
8.6.1 CARACTERÍSTICAS DE LA PLATAFORMA DE INTEROPERABILIDAD	
8.6.2 REQUISITOS TÉCNICOS ASOCIADOS A LA PLATAFORMA	
8.6.3 SUMINISTRO, ADMINISTRACIÓN Y OPERACIÓN DE LA PLATAFORMA	
8.6.4 PROCEDIMIENTOS DE GESTIÓN DEL SERVICIO DE LA PLATAFORMA	
8.6.5 SOPORTE DE LA PLATAFORMA DE INTEROPERABILIDAD	
8.6.6 GESTIÓN DE LOS SERVICIOS DE INFORMACIÓN PUBLICADOS EN LA PLATAFO	
8.6.7 GOBIERNO DE LOS SERVICIOS DE INTERCAMBIO DE INFORMACIÓN	
8.6.8 PROCESO DE DESPLIEGUE DEL SERVICIO DE INTERCAMBIO DE INFORMA	
8.6.9 DISEÑO, DESARROLLO, IMPLEMENTACIÓN Y MANTENIMIENTO DE SERVICIO INTERCAMBIO DE INFORMACIÓN	
8.6.10 OPERACIÓN DE LA PLATAFORMA	
9 MODELO DEL SERVICIO DE AUTENTICACIÓN DIGITAL	
9.1 OBJETIVOS DEL SERVICIO	
9.2 CONTEXTO DEL SERVICIO	
9.3 MAPA DE CAPACIDADES DEL SERVICIO	
9.4 MODELO DE DESPLIEGUE DEL SERVICIO	
9.5 REQUISITOS OPERATIVOS DEL SERVICIO DE AUTENTICACIÓN DIGITAL	
9.5.1 CONDICIONES DE OPERACIÓN DEL SERVICIO DE AUTENTICACIÓN DIGITAL ..	
9.5.2 PROCESO DE REGISTRO Y VERIFICACIÓN DE ATRIBUTOS DIGITALES DEL USU	
9.5.3 REGISTRO DE PERSONAS NATURALES MAYORES DE EDAD	
9.5.4 REGISTRO DE PERSONAS NATURALES MENORES DE 18 AÑOS	
9.5.5 REGISTRO DE EXTRANJEROS	

9.5.6 REGISTRO DE PERSONAS JURÍDICAS	
9.5.7 REGISTRO DE FUNCIONARIOS PÚBLICOS Y PARTICULARES QUE DESEMPEÑAN FUNCIONES PÚBLICAS	
9.5.8 PROCESO DE EMISIÓN DE LAS CREDENCIALES DE AUTENTICACIÓN	
9.5.9 PROCESO DE AUTENTICACIÓN DIGITAL	
9.5.10 ENRUTAR SOLICITUDES DE AUTENTICACIÓN	
9.5.11 GESTIÓN DE LA BASE DE DATOS MAESTRA	
9.5.12 PROCESO DE FIRMADO ELECTRÓNICO CON LAS CREDENCIALES DE AUTENTICACIÓN DIGITAL	
9.5.13 DESVINCULACIÓN DEL USUARIO FRENTE AL SERVICIO DE AUTENTICACIÓN DIGITAL	
9.5.14 COMUNICACIÓN ENTRE PRESTADORES DE SERVICIO	
9.5.15 INTEGRACIÓN DE AUTENTICACIONES YA OFERTADAS POR OTRAS AUTORIDADES PÚBLICAS	
10 MODELO DEL SERVICIO DE CARPETA CIUDADANA	
10.1 OBJETIVOS DEL SERVICIO DE CARPETA CIUDADANA DIGITAL	
10.2 CONTEXTO DEL SERVICIO CARPETA CIUDADANA DIGITAL	
10.3 MODELO DE CAPACIDADES DEL SERVICIO CARPETA CIUDADANA DIGITAL	
10.4 MODELO DE DESPLIEGUE DEL SERVICIO CARPETA CIUDADANA DIGITAL	
11 REQUERIMIENTOS NO FUNCIONALES DE LOS SERVICIOS CIUDADANOS DIGITALES	
11.1 ATRIBUTO DE CALIDAD: FUNCIONAMIENTO	
11.2 ATRIBUTO DE CALIDAD: ESCALABILIDAD	
11.3 ATRIBUTO DE CALIDAD: MONITOREO	
11.4 ATRIBUTO DE CALIDAD: USABILIDAD	
11.5 ATRIBUTO DE CALIDAD: DISPONIBILIDAD	
11.6 ATRIBUTO DE CALIDAD: CONFIABILIDAD	
11.7 ATRIBUTO DE CALIDAD: PRIVACIDAD POR DEFECTO	
12 REQUISITOS TÉCNICOS DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD	
12.1 REQUISITOS TÉCNICOS DE LOS SCD	
12.2 SISTEMAS DE ADMINISTRACIÓN DE RIESGOS	
12.3 REQUISITOS DE INFRAESTRUCTURA	
12.4 REQUISITOS DE RED	
12.5 REQUISITOS A NIVEL DE APLICACIÓN	
12.6 ALMACENAMIENTO DE INFORMACIÓN	
13 SEGURIDAD Y PRIVACIDAD	
14 ANÁLISIS DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD	
14.1 SOBRE LAS REDES DE DATOS DE LOS SERVICIOS CIUDADANOS DIGITALES ...	
15 TÉRMINOS Y CONDICIONES DE USO	

Ilustración 1 - Modelo conceptual de los Servicios Ciudadanos Digitales	
Ilustración 2 - Lienzo del modelo de negocio SCD	
Ilustración 3 - Modelo estratégico de SCD	
Ilustración 4 - Mapa de capacidades SCD	
Ilustración 5 - Servicio de Intercambio de Información	
Ilustración 6 - Alineación modelo / Marco de Interoperabilidad	
Ilustración 7 - Modelo de contexto del servicio IO	
Ilustración 8 - Modelo de despliegue IO	
Ilustración 9 - Modelo de despliegue nivel 2 IO	
Ilustración 10 - Modelo de contexto del servicio de Autenticación Digital	
Ilustración 11 - Modelo de despliegue servicio de Autenticación Digital	
Ilustración 12 - Componente CORE del servicio de Autenticación Digital	
Ilustración 13 - Modelo de contexto del servicio de Carpeta Ciudadana Digital	
Ilustración 14 - Modelo de despliegue del servicio de Carpeta Ciudadana Digital base.	

Lista de Tablas

Tabla 1 - Descripción de las entidades del modelo conceptual	
Tabla 2 - Descripción de las capacidades de nivel 1 de los SCD	
Tabla 3 - Capacidades de Nivel 2 de los Servicios Ciudadanos Digitales	
Tabla 4 - Relaciones del Modelo de contexto servicio de Interoperabilidad (IO)	
Tabla 5 - Descripción de las relaciones del modelo de despliegue de IO	
Tabla 6 - Descripción de las relaciones del modelo de despliegue de IO Nivel 2	
Tabla 7 - Relaciones del modelo de contexto	
Tabla 8 - Descripción de las relaciones del modelo de despliegue	
Tabla 9- Relaciones del modelo de contexto de Carpeta Ciudadana Digital, CCD	
Tabla 10 - Descripción de las relaciones del modelo del servicio de CCD	
Tabla 11 - Descripción de los elementos del atributo de funcionamiento	
Tabla 12 - Descripción de los elementos del atributo de escalabilidad	
Tabla 13 - Descripción de los elementos del atributo de monitoreo	
Tabla 14 - Descripción de los componentes del atributo usabilidad	
Tabla 15 - Descripción de los elementos del atributo de disponibilidad	
Tabla 16 - Descripción elementos del atributo de confianza	
Tabla 17 - Descripción de los elementos del atributo de privacidad por defecto	
Tabla 18 - Requisitos técnicos para el Articulador	
Tabla 19 - ANS Asociados a los Servicios Ciudadanos Digitales	
Tabla 20 - Lineamientos de seguridad y requisitos mínimos	

1. INTRODUCCIÓN.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), de acuerdo con la 2009, desarrolla políticas y planes enfocados a las Tecnologías de la Información y las Comunicaci

constituyen un componente vital para el crecimiento y desarrollo del sector, con el fin de brindar a la población, en el marco de la expansión y diversificación de las TIC, y conforme al principio de "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 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 sus beneficios". En este sentido, MinTIC ha conceptualizado y diseñado un modelo integral que incorpora 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 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 el entorno colombiano para que funcione como una sola institución que le brinde a los ciudadanos información 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 documento determina los estándares de implementación de los Servicios Ciudadanos Digitales contenidos en los lineamientos de los servicios ciudadanos digitales⁽¹⁾

2. ALCANCE DE LA GUÍA.

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, modelos de procesos, obligatoriedad, requerimientos técnicos, lineamientos y estándares necesarios, buscando que el articulador de los Servicios Ciudadanos Digitales desarrolle las capacidades para adelantar las interacciones entre los distintos actores involucrados en la prestación de los Servicios Ciudadanos Digitales tanto en la implementación 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 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.

3. DEFINICIONES.

A los efectos de la presente guía se deberán seguir los conceptos señalados en el artículo [2.2.17.1.4](#) 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 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 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 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 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 por el Ministerio de Tecnologías de la Información y las Comunicaciones destinado a las autoridades en el artículo [2.2.17.1.2](#). del Decreto 1078 de 2015, que indica cuáles son las condiciones necesarias 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 interoperabilidad y carpeta ciudadana digital.
8. Firma digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, mediante 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 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 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 presentar por niveles más detallados.

14. Marco de interoperabilidad: Es la estructura de trabajo común donde se alinean los conceptos y 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⁽²⁾.

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 validez del mismo ante un notario.

16. Mecanismo de identificación de los colombianos: Es el proceso mediante el cual la Registraduría Nacional del Estado Civil le asigna un único atributo a un colombiano a través del documento de identidad (cédula de ciudadanía 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 permiten que los sistemas de información del Estado conversen entre sí mediante interfaces estándar de comunicación de procesos y sistemas de información.

19. Política de Gobierno Digital: establecida mediante Decreto [1008](#) del 14 de junio de 2018, cuyo propósito es incentivar el uso y aprovechamiento de las TIC para consolidar un Estado y ciudadanos competitivos e innovadores que generen valor público en un entorno de confianza digital⁽³⁾.

20. Prestadores de Servicios Ciudadanos Digitales: Entidades pertenecientes al sector público o privado que, mediante un esquema coordinado y administrado por el Articulador, pueden proveer los servicios digitales a ciudadanos y empresas, siempre bajo los lineamientos, políticas, guías, que emite 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 toda la 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 recolección de información y de las infraestructuras que lo soportan.

22. Servicios Ciudadanos Digitales: Es el conjunto de soluciones y procesos transversales que brindan 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. Los 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, Integridad, Privacidad y Seguridad.

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, a innovaciones que realizan los prestadores de servicio a partir de la autorización dada por el titular y de la integración a los servicios ciudadanos digitales base, bajo un esquema coordinado por el Ar

25. Usuario de los servicios ciudadanos digitales: Es la persona natural, nacional o extranjera, o la 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.

4. MARCO JURÍDICO.

La Constitución Política en su artículo [2](#) establece como uno de los fines esenciales del Estado "(...) 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, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se disponen", estableció el reconocimiento jurídico a los mensajes de datos, en las mismas condiciones que ha otorgado para los soportes que se encuentren en medios físicos. De la misma manera, el Decreto [1010](#) 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 [2](#) de julio de 2015 en concordancia con el Decreto Ley [2241](#) de 1986 y el Decreto Ley 1010 de 2000, a la Registraduría Nacional del Estado Civil ejercer, entre otras, la dirección y organización de las entidades del registro civil y la identificación de las personas.

Conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el artículo [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 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 (...)", 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 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 por un nuevo país", atribuye al Ministerio de Tecnologías de la Información y las Comunicaciones

coordinación con las entidades responsables de cada uno de los trámites y servicios, la función de expedir los estándares, modelos, lineamientos y normas técnicas para la incorporación de las TIC, y ser adoptados por las entidades estatales, incluyendo, entre otros, autenticación electrónica, integración de sistemas de información de trámites y servicios de las entidades estatales con el Portal del Estado. La interoperabilidad de datos como base para la estructuración de la estrategia. Según el mismo precepto 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 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 valoren el 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 [20](#) 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. Como "Bases del Plan Nacional de Desarrollo 2018 -2022": Pacto por Colombia, pacto por la equidad en "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 de trámites, a través de la implementación e integración de los servicios ciudadanos digitales, (carpeta electrónica, autenticación electrónica e interoperabilidad de los sistemas del Estado), de forma paralela a la definición 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 lo 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 e interacciones entre el ciudadano y el Estado a través del Portal Único del Estado colombiano, y en políticas de seguridad y confianza digital, para ello, las entidades públicas deberán implementar el componente 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 de la seguridad de la información, 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 la entidad que haga las veces de articulador de servicios ciudadanos digitales, o la que defina el MinTIC al final.

El artículo [9](#) del Decreto 2106 de 2019 "Por el cual se dictan normas para simplificar, suprimir y reorganizar trámites, procesos y procedimientos innecesarios existentes en la administración pública, señala que para lograr un mayor nivel de eficiencia en la administración pública y una adecuada interacción con los ciudadanos usuarios, garantizando el derecho a la utilización de medios electrónicos, las autoridades deberán implementar el uso del modelo de Servicios Ciudadanos Digitales. Este mismo artículo dispone que el Gobierno prestará gratuitamente los Servicios Ciudadanos Digitales base y se implementarán por parte de las

de conformidad con los estándares que establezca el MinTIC.

Por ello, surge la obligación de expedir los estándares de implementación de los Servicios Ciudadanos contenidos en la guía de lineamientos de los servicios ciudadanos digitales y la guía para vinculación de estos, según se desprende del artículo [2.2.17.4.1](#), del DURT-TIC, en concordancia con el numeral 2 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 la utilización de medios electrónicos ante la administración pública, reconocido en el artículo [54](#) de la Ley 1712 de 2011, se han desarrollado los Servicios Ciudadanos Digitales, entendidos como el conjunto de procesos transversales que brindan al Estado capacidades y eficiencias para su transformación digital. 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, elección y portabilidad, privacidad por diseño y por defecto, seguridad, privacidad y circulación responsable 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, para 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 por parte de 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, 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 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 la 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 gestión de documentos que el ciudadano ya ha presentado y la complejidad para autenticar digitalmente a las entidades 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 condiciones de calidad, seguridad, interoperabilidad, disponibilidad y acceso a la información que se establece en la normativa vigente, adoptando las medidas necesarias para garantizar los derechos de las personas con 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. Los 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, es la persona natural, nacional o extranjera, o la persona jurídica, de naturaleza pública o privada, que hace 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 y 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 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 los 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 funcionamiento 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 involucren la prestación de los SCD.

El modelo de los SCD se enfoca en lograr una adecuada interacción del ciudadano con el Estado, para 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 ciudadano 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 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 las 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 documento digital, 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 custodian las entidades señaladas en el artículo [2.2.17.1.2](#) del Decreto 1078 de 2015. Adicionalmente, el 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 representan 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 la integración a los servicios ciudadanos digitales base, bajo un esquema coordinado por el Artículo 10 del Decreto 1078 de 2015.

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 presente 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 las 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 de 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). Además de la ilustración que se expone a continuación, se indica en la Tabla No. 1 la descripción de cada uno de los componentes del modelo.

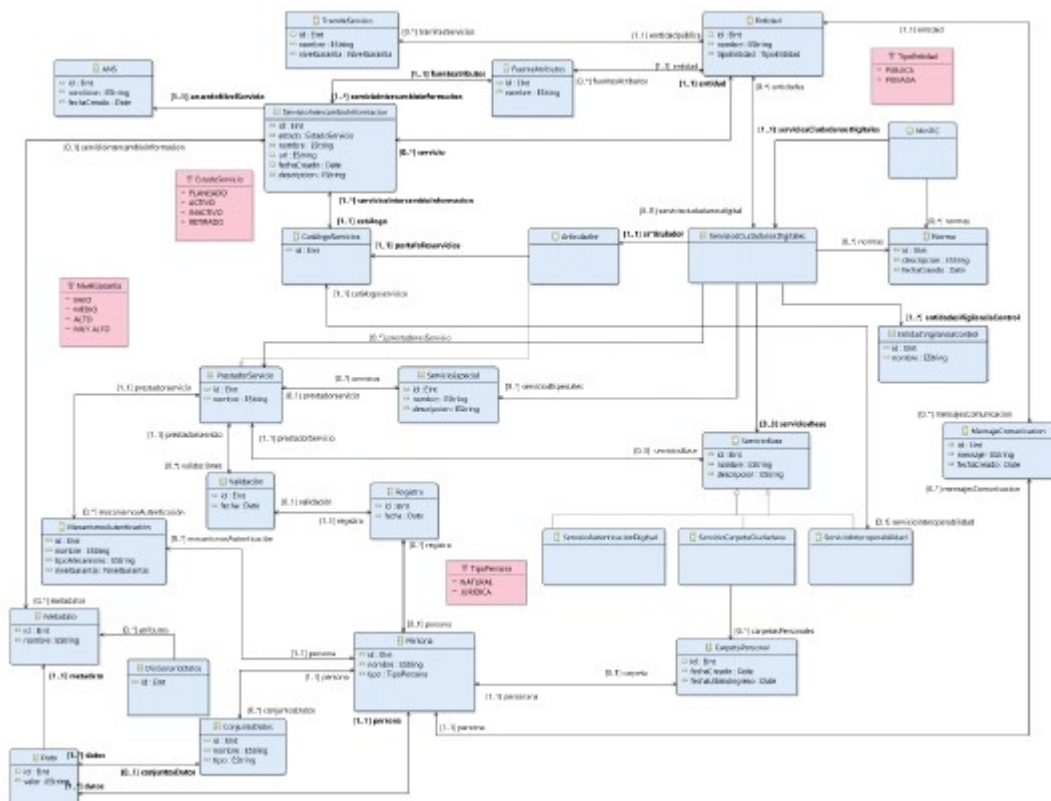


Ilustración 1 - Modelo conceptual de los Servicios Ciudadanos Digitales.

El modelo general de los SCD presentado en la anterior ilustración contempla que el articulador se encargará 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
Servicio Ciudadanos Digitales	Los Servicios Ciudadanos Digitales pueden ser servicios digitales especiales. Los servicios base son tres (Carpeta Ciudadana Digital, servicio Autenticación Digital y 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.
Carpeta Personal	Es el acceso a la consulta de un conjunto de datos que pertenecen a la administración pública de cada usuario.
Catálogo de Servicios	Es el catálogo de servicios de intercambio de información.
Conjunto de Datos	El conjunto de datos a intercambiar que genera un servicio de intercambio de información.
Dato	Identifica y define la unidad básica de información, a partir de la cual se realiza el intercambio de información de acuerdo con los requisitos funcionales definidos dentro del proceso o servicio de intercambio de información.
Diccionario de Datos	El diccionario de datos contiene todos los metadatos y define los elementos de datos, conceptualizados por las entidades del estándar de Lenguaje Común de Intercambio de Información.
Entidad	La entidad pública o privada.
Fuente de Atributos	La fuente de atributos contiene datos que permiten verificar la identidad digital asociada a la identidad de un usuario.
Mecanismo de Autenticación	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.
Mensaje de Comunicación	Los mensajes de comunicación generados por las entidades a través de los Servicios Ciudadanos Digitales.
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 reutilización de los mismos.
MinTIC	El Ministerio de Tecnologías de la Información y las Comunicaciones.
Nivel de Garantía	Es el grado de confianza en los procesos que conducen a la Adopción Digital, los cuales se clasifican en orden ascendente según el 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.
Prestador de Servicio	Personas jurídicas, pertenecientes al sector público o privado, que a través de un esquema coordinado y administrado por el articulador proveen los Servicios Ciudadanos Digitales a ciudadanos siempre bajo los lineamientos, políticas, guías, que expide 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.
Servicio de Autenticación Digital	Es el servicio de Autenticación Digital, que hace parte de los Servicios Ciudadanos Digitales base.
Servicio de Carpeta Ciudadana Digital	Es el servicio de Carpeta Ciudadana Digital, que hace parte de los Servicios Ciudadanos Digitales base.
Servicio Ciudadano Digital	Servicios Ciudadanos Digitales es el agrupador de los servicios ciudadanos digitales especiales.
Servicio Especial	Son los Servicios Ciudadanos Digitales Especiales que hacen parte de los Servicios Ciudadanos Digitales.

ServicioIntercambioInformacion	Recurso tecnológico que mediante el uso de un conjunto de estándares permite el intercambio de información.
ServicioInteroperabilidad	Es el servicio de Interoperabilidad, que hace parte de los t Ciudadanos Digitales base.
TramiteServicio	Los trámites o procesos o procedimientos de las entidades púb
Verificacion	La verificación que se hace al registro de un usuario contra l atributos.

Para que este modelo de SCD inicie su operación, MinTIC pone a disposición esta Guía de lineami Servicios Ciudadanos Digitales en la que se consignan las condiciones de carácter general y técnico 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 I presenta el modelo de intención utilizando el lienzo de modelo de negocio (Business Model Canva Este modelo permite documentar y comunicar la propuesta de valor y la relación con los segmentos 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 Cai Ciudadana Digital, Interoperabilidad, Autenticación Digital y para los elementos transversales.

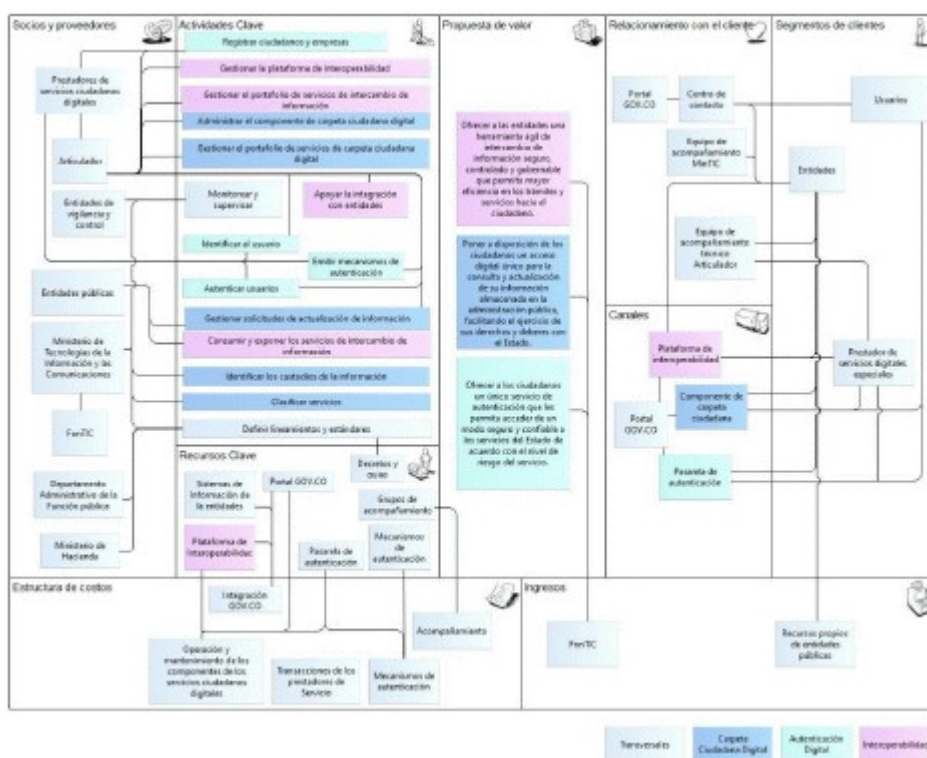


Ilustración 2 - Lienzo del modelo de negocio SCD

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 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

plataforma de interoperabilidad, gestionar el portafolio de servicios de intercambio de información, autoridades con la integración de sus servicios en la plataforma de interoperabilidad, así como cons 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 identifi único servicio de autenticación, que les permita acceder de un modo seguro y confiable a los trámit y procedimientos que ofrece el Estado de acuerdo con el nivel de riesgo del servicio o trámite. Para este servicio, los usuarios acceden a la pasarela de autenticación integrada al Portal Único del Estac Las funcionalidades que ofrece este servicio son: autenticar y registrar usuarios, emitir los mecanis 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 se un acceso digital único a comunicaciones e información que las entidades de la administración púb producen, recolectan o almacenan de ellos. Las funcionalidades claves que ofrece este servicio son el componente de Carpeta Ciudadana Digital, gestionar el portafolio de servicios de CCD, visualiza que las entidades públicas tienen de los usuarios y clasificar los servicios. Así mismo, este servicio los usuarios, solicitar la actualización y/o corrección de los datos ante la administración pública, po requiere generar la capacidad en el articulador de direccionar estas solicitudes a las entidades públi podrá entregar las comunicaciones o alertas que las entidades tienen para los usuarios, previa autori estos.

Elementos Transversales

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

a) Bloque de relacionamiento: se incluye el centro de contacto de segundo nivel el cual será ofrecid articulador a los usuarios. Adicionalmente se identifican los equipos de trabajo de MinTIC y del A quienes estarán acompañando a las entidades públicas en la implementación de los Servicios Ciuda 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 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 vinculac servicio de Autenticación Digital y la Carpeta Ciudadana Digital proviene de los recursos propios c entidad.

c) Canales: la plataforma de interoperabilidad es para las entidades el principal medio para ofrecer l procesos y procedimientos a los usuarios, quienes a su vez acceden por el Portal Único del Estado (GOV.CO en donde adicionalmente encontraran integrado la pasarela de autenticación y el compon Carpeta Ciudadana Digital.

d) Bloque de recursos: Hacen parte del bloque de recursos, los sistemas de información de las entid productoras de información, para ofrecer servicios de intercambio de información a través de los cu realizar el intercambio de información entre las entidades públicas. El Portal Único del Estado Col

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 son 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 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 línea 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 Centro de Datos, la 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 servicios y la gestión de las solicitudes de los usuarios, entre otras. Adicionalmente, el articulador será el único 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 organismos de control y vigilancia realizarán las actividades de vigilancia y control a los SCD en el ámbito de sus competencias.

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:



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 sus procesos, 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 digital 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 la gestión pública y la generación de valor público.

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 los Servicios Ciudadanos Digitales. Cada capacidad cuenta con un identificador único, un nombre y un nivel que pueden ser consultados 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 que el Ministerio de Tecnologías de la Información y las Comunicaciones realiza apoyo de acuerdo con la 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
C01	Gestionar la estrategia de los SCD	Definir, mantener y hacer seguimiento a la estrategia Ciudadanos Digitales con el objetivo de definir la misión estratégica que genere valor a los ciudadanos.
C02	Gestionar las comunicaciones de los SCD	Generar las comunicaciones externas con el objetivo de conectar los Servicios Ciudadanos Digitales a los actores involucrados.
C03	Gestionar la normatividad de los SCD	Generar normatividad relacionada con los Servicios Digitales.
C04	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.
C05	Gestionar el Servicio de Autenticación Digital	Administrar integralmente el servicio de autenticación y verificación, registro, emisión de los mecanismos de autenticación de los usuarios, así como la administración de los mecanismos utilizados.
C06	Gestionar la atención al usuario	Administrar la atención al usuario gestionando las solicitudes y comunicaciones a los usuarios de los servicios ciudadanos.
C07	Gestionar el servicio de Carpeta Ciudadana Digital	Administrar y configurar el servicio de Carpeta Ciudadana Digital y los servicios que se incorporan en ella.

C08	Gestionar los prestadores de servicio	Integrar y administrar los prestadores de servicio que servicios ciudadanos digitales base y especiales.
C09	Gestionar la plataforma de interoperabilidad	Administrar, configurar y dar soporte de la pla Interoperabilidad.
C10	Gestionar tecnología e información	Planear, ejecutar y mantener los servicios de tecnología e en especial los incidentes de TI, problemas y requerimi Servicios Ciudadanos Digitales, así como el desarrollo servicios de intercambio de información.
C11	Gestionar los servicios administrativos y jurídicos	Gestionar los servicios jurídicos asociados a los SCD, talento humano que permite ofrecer los SCD, gestionar contractuales requeridos para la implementación de los SC
C12	Gestionar la seguridad de la información	Gestionar las políticas, controles, incidentes de seguridad de la información que permiten garantizar la disponibilidad y confidencialidad de los SCD.

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

COD	CAPACIDAD NIVEL 2	DESCRIPCIÓN
C01.01	Definir la estrategia de SCD	Construir la estrategia de los SCD.
C01.02	Hacer seguimiento a la estrategia de los SCD	Monitorear los indicadores asociados a la estrateg ejecutar las acciones de mejora en caso de ser neces
C02.01	Definir el plan de comunicaciones de los SCD	Construir el plan de comunicaciones de los SCD.
C02.02	Ejecutar el plan de comunicaciones de los SCD	Poner en marcha el plan de comunicaciones de los S
C02.03	Monitorear el plan de comunicaciones de los SCD	Realizar seguimiento y control a la ejecución comunicaciones de los SCD.
C03.01	Elaborar la normatividad de los SCD	Definir políticas y lineamientos asociados a los SCD
C03.02	Publicar la normatividad de los SCD	Publicar las políticas y lineamientos asociados a los
C03.03	Mantener actualizada la normatividad de los SCD	Actualizar de forma periódica la normatividad as SCD.
C04.01	Identificar los servicios de intercambio de información	Realizar la identificación de los servicios de int información realizando la definición de cada uno e de servicios.
C04.02	Gestionar los custodios de los datos	Identificar y definir la entidad que custodia los servicios de intercambio de información.
C04.03	Gestionar el diccionario de datos	Construir, publicar y mantener actualizado el di datos de los SCD.
C04.04	Gestionar los ANS	Definir y hacer seguimiento a la medición de los Niveles de Servicio (ANS) para garantizar las co calidad de los servicios de intercambio de utilizados para los SCD.
C05.01	Verificar identificación de usuarios	El prestador de servicios debe obtener del usuario relacionados con la identidad de la persona a verificar que estos sean los que le correspondan.E ciudadanos colombianos, la verificación de iden realiza con la Registraduría Nacional del Estado Ci
C05.02	Registrar usuarios	Si es superada satisfactoriamente la verificación de relacionados al usuario, el prestador de servicios el proceso de registro del usuario.

C05.03	Autenticar usuarios	Cuando el usuario requiere acceder a un servicio en sesión autenticándose en el sistema con los mecanismos de autenticación emitidos durante el registro.
C05.04	Administrar los mecanismos de autenticación	Administrar y configurar los mecanismos de Autenticación Digital para garantizar su seguridad.
C06.01	Gestionar las solicitudes	Recibir, analizar y remitir a las entidades las solicitudes de los usuarios de los SCD cuando corresponda atender las solicitudes que corresponda al prestador.
C06.02	Gestionar los mensajes al usuario	Generar los mensajes de comunicación para los usuarios de los Servicios Ciudadanos Digitales.
C06.03	Acompañar a las entidades públicas	Realizar el acompañamiento técnico a las entidades que lo requieran durante la implementación y operación de los SCD.
C07.01	Administrar los servicios de Carpeta Ciudadana	Configurar y clasificar los servicios de información disponibles en la Carpeta Ciudadana Digital.
C07.02	Gestionar componente de Carpeta Ciudadana	Configurar el componente de Carpeta Ciudadana Digital.
C08.03	Monitorear la prestación de servicio	Realizar el monitoreo de los servicios para garantizar la correcta prestación.
C08.04	Administrar los SCD especiales	Identificar, planear y coordinar los SCD especiales.
C09.01	Integrar nuevos servicios en la plataforma	Integrar los nuevos servicios de intercambio de información en la plataforma de Interoperabilidad.
C09.02	Administrar la seguridad de la plataforma de interoperabilidad	Administrar los mecanismos de seguridad en la plataforma de Interoperabilidad.
C09.03	Administrar la plataforma de interoperabilidad	Administrar y realizar mantenimiento a la plataforma de Interoperabilidad.
C09.04	Operar la plataforma de interoperabilidad	Operar la plataforma de Interoperabilidad.
C09.05	Gestionar reportes de información	Generar los reportes sobre el estado y uso de la plataforma de Interoperabilidad.
C10.01	Gestionar los requerimientos	Gestionar los requerimientos funcionales para nuevas soluciones tecnológicas que soportan los Servicios Ciudadanos Digitales.
C10.02	Gestionar los incidentes de TI	Gestionar los incidentes de las soluciones tecnológicas que soportan los Servicios Ciudadanos Digitales.
C10.03	Implementar Política De Gobierno Digital	Implementar el habilitador transversal de SCD de la Política De Gobierno Digital.
C10.04	Implementar las mejoras a los SCD	Implementar las mejoras de las soluciones tecnológicas que soportan los Servicios Ciudadanos Digitales.
C10.05	Gestionar infraestructura tecnológica	Gestionar la infraestructura tecnológica de las soluciones que soportan los Servicios Ciudadanos Digitales.
C10.06	Gestionar la Configuración	Gestionar la configuración de los servicios tecnológicos que soportan los Servicios Ciudadanos Digitales.
C10.07	Gestionar los cambios	Gestionar los cambios asociados a las soluciones tecnológicas e información que soportan los SCD.
C10.08	Desarrollar soluciones de tecnología e información	Gestionar el desarrollo de los requerimientos funcionales de las soluciones de tecnología e información que soportan los Servicios Ciudadanos Digitales y el proceso formal de desarrollo de software.
C11.01	Gestionar procesos contractuales	Ejecutar los procesos contractuales que permitan la adquisición de bienes y servicios asociados a los Servicios Ciudadanos Digitales.

C11.02	Gestionar servicios jurídicos	Prestar los servicios relacionados con la defec asociada a los Servicios Ciudadanos Digitales.
C11.03	Gestionar información financiera y contable	Gestionar los recursos financieros asociados con l Ciudadanos Digitales.
C12.01	Gestionar los riesgos	Gestionar los riesgos de seguridad de la informaci a la prestación de los SCD.
C12.02	Gestionar los controles de seguridad de la información	Realizar la definición de las políticas de segu información e implementación de controles aso Servicios Ciudadanos Digitales.
C12.03	Gestionar las políticas de seguridad de la información	Realizar la definición de las políticas de segu información e implementación de controles aso Servicios Ciudadanos Digitales.

8. MODELO DEL SERVICIO DE INTEROPERABILIDAD.

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

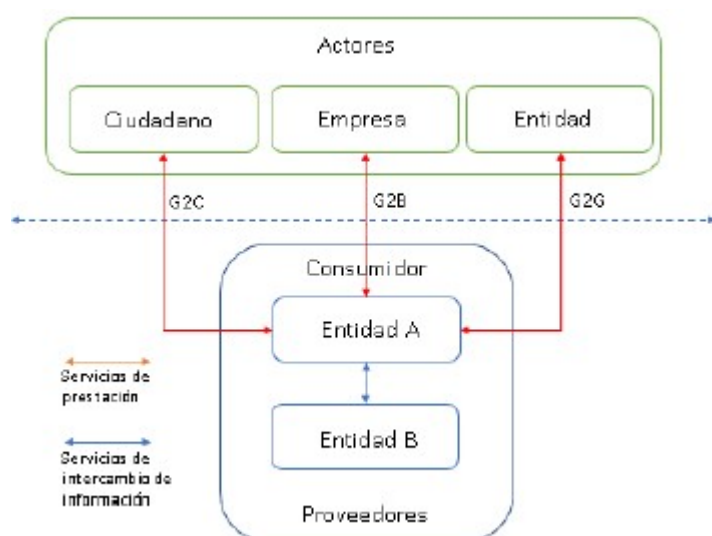


Ilustración 5 - Servicio de Intercambio de Información

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

Teniendo en cuenta lo anterior, la política de Gobierno Digital espera que el servicio de interoperat convierta en un instrumento que les permita a las entidades públicas poner en funcionamiento el int información desde el dominio técnico definido en el Marco de interoperabilidad para Gobierno Dig define el conjunto de elementos que orientan el intercambio de información a nivel público. Sin en 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 facilite la materialización de los servicios de intercambio de información entre las entidades, a la vez procure la máxima eficiencia y una fácil integración dentro de la dinámica de la administración pública, garantizar un desarrollo escalable, replicable y funcional, que también facilite la diversificación y un número de elementos entre los cuales elegir a la hora de desarrollar proyectos de Interoperabilidad entre 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 han alcanzado la interoperabilidad con los niveles de seguridad, confiabilidad, oportunidad, trazabilidad y valor público suficientes y ajustados a los lineamientos de la política de gobierno digital ni del marco de interoperabilidad por dificultades técnicas, operativas o de costos. Es aquí donde el servicio de interoperabilidad busca vincular 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 que los usuarios tengan que presentar los mismos datos y documentos en diferentes sistemas o entidades, agilizando así los trámites y servicios digitales ágiles aún aquellos que implican a diferentes entidades públicas. Con 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 expedientes completos de una entidad a otra en los diferentes escenarios administrativos en los que se producen. Esto permite minimizar el gasto en mensajería, agilizar los plazos y facilitar la interacción entre los diferentes órganos administrativos, lo que redundará en una mayor eficiencia administrativa y puede contribuir a una simplificación general de las relaciones del ciudadano con las diferentes administraciones.
- Intercambio de documentos. Envío de documentos individuales entre dos entidades (certificaciones, 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, 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 que permiten verificar la información necesaria. Este intercambio de datos es un servicio que beneficia a las partes: al usuario quien evita gastos y molestias por obtener algún documento; la entidad destinataria elimina la necesidad de gestionar el documento en papel; y la entidad emisora, que reduce la carga 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 a través de la provisión de una estructura tecnológica, para enviar y recibir información relevante, que 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⁽⁴⁾

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 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

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 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 a las entidades del Estado como un elemento transversal habilitador para interoperar con otras entidades, empresas y ciudadanos, como usuarios de los Servicios Ciudadanos Digitales.

- Interacción de usuarios con entidades públicas, desde la Carpeta Ciudadana Digital y la Auténtica para la verificación de atributos digitales.
- Intercambio de datos entre una o más entidades estatales para resolver trámites y dar respuesta al 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 c

servicios generados, evaluando la evolución de la gestión de dichos servicios en las entidades públi

b. Mejorar el modelo de gobernanza del Marco de Interoperabilidad, optimizando la gestión relac

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 us

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 p

f. Apoyar y mejorar la toma de decisiones por parte de los sujetos obligados de la política de Gobie

través de información en tiempo real.

g. Fomentar la innovación y el emprendimiento, favoreciendo con ello el desarrollo de nuevos nego

h. Mejorar la transparencia de la función pública y la participación ciudadana por medios digitales

los trámites de las entidades.

i. Medir los resultados de la gestión de la Interoperabilidad y su impacto en la administración públi

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 e

en servicios de intercambio de información.

k. Ofrecer una plataforma integral de Interoperabilidad como servicio que facilite la circulación de

entre las entidades, incorporar librerías para el intercambio de información, permitir la composició

orquestración y definición de reglas sobre los servicios de intercambio de información, proporcionar

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 prese

relacionan los actores, y muestra las interacciones que se realizan cuando se presenta un intercambi

información desde los Servicios Ciudadanos Digitales.

Los actores que participan en el modelo de contexto del servicio de Interoperabilidad y sus principa

obligaciones y roles, son:

Ministerio de Tecnologías de la Información y las Comunicaciones: define y señala la política a seg

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 platafo

de las entidades públicas.

Entidades: Encargadas de vincular a sus sistemas de información los servicios para interoperar con

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 responsa

la provisión de servicios de intercambio de información.

- Atender los procesos establecidos en los lineamientos del Marco de Interoperabilidad para la prov servicios de intercambio de información.
- Desarrollar las competencias y habilidades para usar y prestar los servicios de intercambio de info
- Proveer y consumir los servicios de intercambio de información a través de la plataforma de Inter
- Adecuar los procesos relacionados con trámites y servicios que ofrecen a usuarios y otras entidad para propiciar en el menor tiempo posible la utilización de servicios de intercambio de informaci
- Solicitar a MinTIC la incorporación de las definiciones semánticas o estándares internacionales al Común de Intercambio de Información.
- Asegurar que los servicios y sistemas de información a su cargo mantengan la capacidad de interco 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 q de información y que habilitan servicios para suministrar datos a otras entidades que lo requieran, e de su competencia.

a. Definir las autorizaciones de acceso a los servicios de intercambio de información que ofrece, es los protocolos y condiciones de acceso, los métodos de consulta permitidos, así como la informació 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 Interc

d. Establecer las condiciones técnicas de acceso y auditoría a los servicios de intercambio de inform ofrece.

e. Definir los controles y criterios de acceso a los datos necesarios para garantizar la confidencialid información según las políticas y procedimientos de gestión y control de acceso de usuarios y entid establezca.

f. Definir los Acuerdos de Nivel de Servicio (ANS) para regular las condiciones de prestación de lc mecanismos de respuesta a incidencias específicos acorde a la criticidad del servicio que se está pre

g. Facilitar la información para el directorio de servicios de intercambio de información, donde esta de sus servicios de intercambio disponibles, que están a disposición de otras entidades para su cons

- **Cliente:** hace referencia a aquellas entidades públicas o particulares autorizados para consultar o a servicios de información publicados en la PDI (Plataforma de Interoperabilidad) con el objeto de o procesos de negocio, automatizar los trámites y servicios al usuario.

a. Solicitar información en relación con los trámites y procedimientos autorizados por el proveedor 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

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 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 y 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 2011 y [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 sentido, la entidad encargada de adelantar las interacciones con los distintos actores involucrados en la prestación de los servicios, y quien provee este servicio a las entidades facilitando el intercambio de los datos desde una perspectiva tecnológica. Su función es proporcionar una plataforma de Interoperabilidad que garantice una 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 en 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 estándares 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 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 y salida de 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 presente el 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 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 prestando los servicios ciudadanos digitales, entre otros, comunicar el cumplimiento o incumplimiento de estándares de seguridad, privacidad, acceso, neutralidad tecnológica, o cualquier otra circunstancia que afecte la prestación del servicio de interoperabilidad al Ministerio de Tecnologías de la Información y las Comunicaciones, en el marco de la ejecución de los 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, dentro del 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 los requisitos para vinculación y uso de los servicios ciudadanos digitales.

p. Atender de manera oportuna los requerimientos que, en cualquier momento, le solicite MinTIC en relación con 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, así como 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 entre 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 la metodología 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 de control correspondientes.

y. Informar sobre la disponibilidad de cada servicio de intercambio bajo su responsabilidad, así como 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 el 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 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, en 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 Bases 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 que es el punto de acceso digital del usuario a los trámites, procesos y procedimientos, servicios, información y ejercicios de participación que ofrece a las entidades públicas un espacio cercano y ágil para desarrollar la Política de Gobierno Digital.

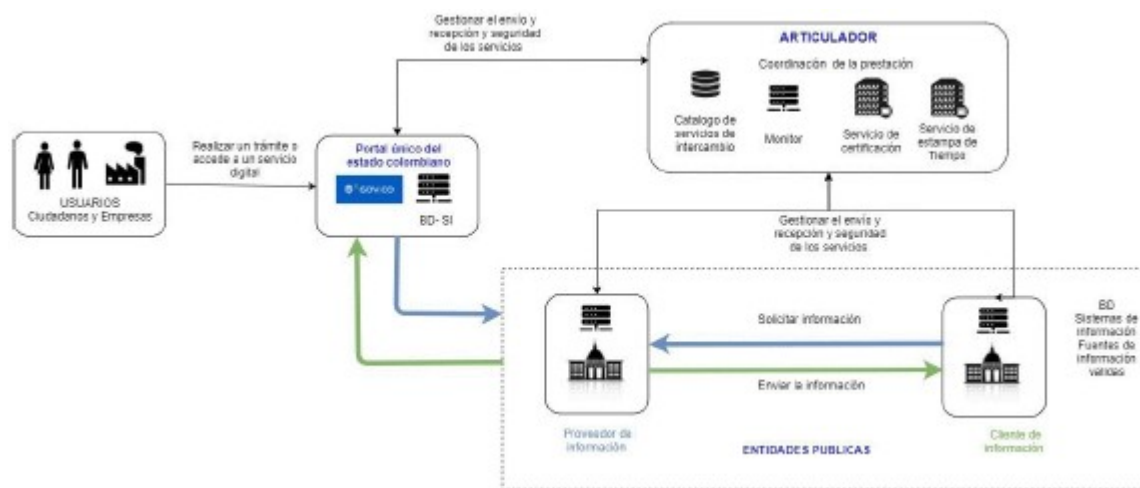


Ilustración 7 - Modelo de contexto del servicio IO

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

Relaciones del modelo de contexto			
Relación	Origen	Destino	Descripción
Realizar un trámite o acceder a un servicio digital	Usuarios	Portal Único del Estado colombiano (GOV.CO)	Permite utilizar los servicios de información a través del Portal Único colombiano (GOV.CO) o desde el información de la entidad pública para trámite o acceder a un servicio digital
Gestionar el envío y recepción de los servicios con	Portal Único del Estado colombiano (GOV.CO)	Articulador	Permite la administración de los servicios de interca información, garantiza la integridad de los mensajes de intercambio entre las entidades y monitoreo de la operación de la plataforma
características de seguridad	Prestadores de servicio	de Interoperabilidad, como por ejemplo cuántos servicios llamados, cuántas veces, cuál es el tiempo de respuesta por	
Solicitar información	Cliente de información	Proveedor de información	Permite usar el servicio de información enviando una solicitud para datos de interés al proveedor.
Enviar información	Proveedor de información	Cliente de información	Permite la provisión de los datos al 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 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 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, etc.).

8.5 MODELO DE DESPLIEGUE DEL SERVICIO DE INTEROPERABILIDAD.

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

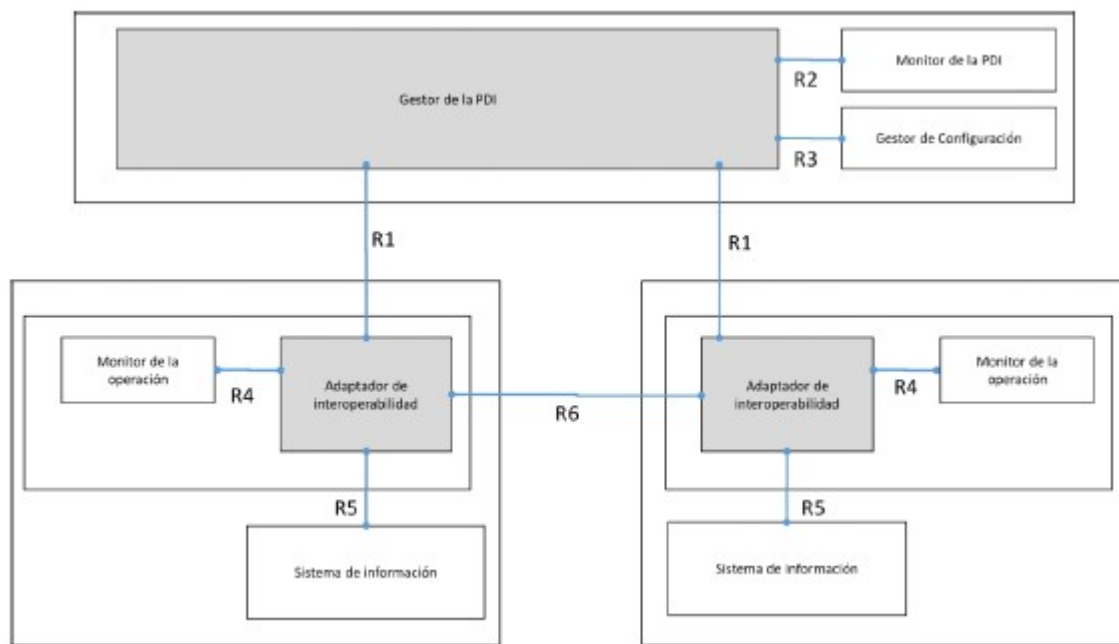


Ilustración 8 - Modelo de despliegue IO

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

a) Gestor de la plataforma de Interoperabilidad: administra la configuración global de la plataforma 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, 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 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 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 datos de la operación de los servicios de intercambio de información y hacerla disponible externamente al modelo de PDI.

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

Relación	Origen	Destino	Descripción
R1	Adaptador de Interoperabilidad	Gestor de la PDI	Interacción que permite comunicarse con el PDI para realizar tareas administrativas como: - Registrar o eliminar el proveedor involucrados en la Interoperabilidad. - Registrar o eliminar el servicio de intercambio de información invocado. - Administrar los servicios de certificación y tiempo.
R2	Gestor de la PDI	Monitor de la PDI	Interacción que permite almacenar los datos de monitoreo que se realiza a la PDI y de carácter operativo que realizan los adaptadores de interoperabilidad de las entidades.
R3	Gestor de la PDI	Gestor de configuración	Interacción que permite propagar la configuración de la PDI que se realiza a nivel central.
R4	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.
R5	Sistema de información	Adaptador de Interoperabilidad	Permite la llamada que hace el sistema transaccional de la entidad dentro de su flujo de trabajo para usar los servicios de Interoperabilidad para compartir, solicitar o intercambiar información con otras entidades, acceder a los servicios de Carpeta Electrónica, Autenticación Digital y de esta forma resolver las solicitudes de los ciudadanos u otras entidades.
R6	Adaptador de Interoperabilidad	Adaptador de Interoperabilidad	Interacción que realiza el intercambio de los datos de solicitud y respuesta, resultado de la ejecución de un servicio de intercambio de información.

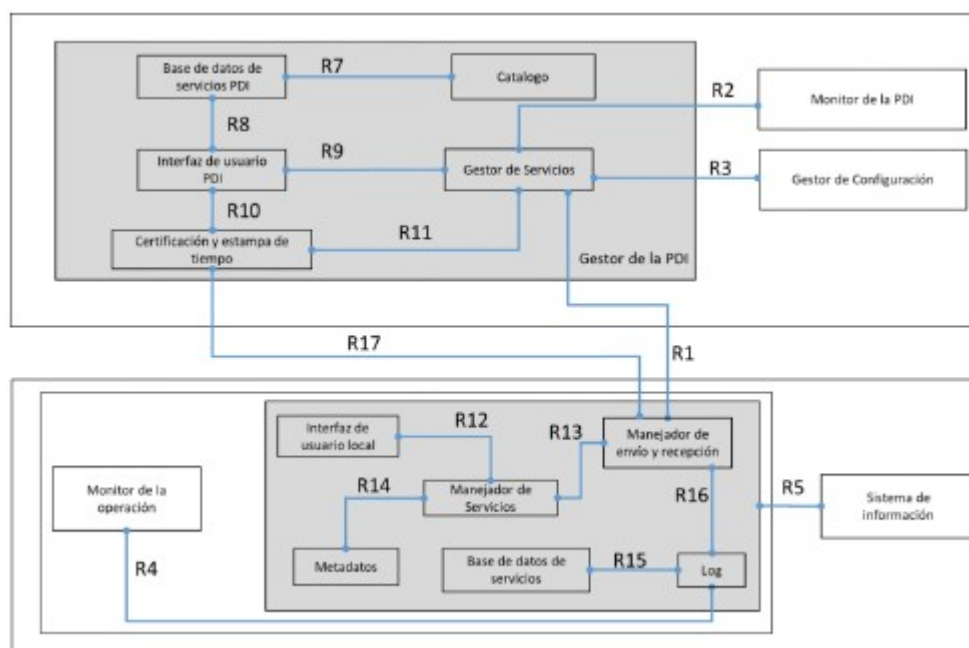


Ilustración 9 - Modelo de despliegue nivel 2 IO

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

a) Catálogo: registra la información sobre el directorio de servicios de intercambio de información que poseen las entidades para su consulta.

b) Gestor de servicios: administra y pone a disposición del adaptador de Interoperabilidad la política de seguridad de la PDI.

c) El servidor central: además de la distribución de la configuración, proporciona una interfaz para tareas de administración, como por ejemplo, agregar y eliminar clientes del servidor de seguridad. Los servicios de gestión se invocan desde la interfaz de usuario de los servidores de seguridad. Los servicios de gestión se invocan como servicios de X-Road estándar y se ofrecen a través del servidor de seguridad central.

d) Certificación y estampo de tiempo: el componente responsable de administrar el firmado y el estampo 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 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 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 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 disponibles a la plataforma de Interoperabilidad.

j) Log: registra todos los mensajes generados por los servicios de intercambio de información que p 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 me 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 inter información.

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

Relación	Origen	Destino	Descripción
R7	Catálogo	Base de datos de servicios PDI	Interacción que permite la consulta de datos de los intercambio de información disponibles en la PDI.
R8	Interfaz de usuario PDI	Base de datos de servicios PDI	Interacción que guarda en el repositorio la configu de la PDI.
R9	Interfaz de usuario PDI	Gestor de servicios	Interacción que permite la actualización y co configuración de la PDI.
R10	Interfaz de usuario PDI	Certificación y estampa de tiempo	Interacción que permite la actualización, administración de los servicios de firmado y es tiempo de los mensajes de datos que intercambian cliente.
R11	Gestor de servicios	Certificación y estampa de tiempo	Interacción que permite darle el valor probatorio de los mensajes intercambiados. Estos registros marca de tiempo para crear una prueba a largo plaz
R12	Interface de usuario local	Manejador de servicios	Interacción que permite la actualización, administración de los servicios de intercambio de que la entidad provee.
R13	Manejador de envío y recepción	Manejador de servicios	Interacción que permite gestionar la provisión de intercambio de información según la configuración reglas y seguridad determinadas.
R14	Manejador de servicios	Metadatos	Interacción que permite suministrar la informaci metadatos, reglas y políticas del servicio de int información.
R15	Log	Base de datos de servicios	Interacción que permite almacenar los datos re monitoreo a los servicios de intercambio de inform
R16	Manejador de envío y recepción	Log	Interacción que permite el registro sobre la rece mensaje de solicitud / respuesta, firmas y tiempo, e información operativa del adaptador de Interoperab
R17	Manejador de envío y recepción	Certificación y estampa de tiempo	Interacción que permite realizar el firmado y es tiempo de los mensajes de datos que intercambian 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 s tecnológicos que garanticen su disponibilidad y operación. De esta forma, el Articulador como pres servicio de interoperabilidad debe realizar la gestión de la tecnología como servicio permanente qu todas las entidades públicas, empresas y ciudadanos, permitiendo el suministro, administración y o infraestructura tecnológica, la disponibilidad de la plataforma para una operación continúa, el sopo 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 p 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 tráfico entrante y saliente y proporcionar las políticas y reglas en los recursos de seguridad de los ce datos para asegurar el aislamiento con otras entidades. Garantizar que la infraestructura tecnológica para prestar los servicios esté protegida, segmentada y separada tanto física como lógicamente, aseg no se produzcan accesos no autorizados por esta causa. En los casos de afectación a los servicios de 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 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 efectiviar entregado a cada Entidad pública, de forma que el Articulador y la entidad tengan acceso transparente 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 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 reutilización.
- d) Garantizar la escalabilidad, a medida que crezca el volumen de información y su modularidad pa extender sus funcionalidades en el futuro. Por tanto, ha de tratarse de una plataforma basada en esté 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 d 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 e sean desplegados sobre la Plataforma.
- h) Permitir reglar, componer u orquestar los servicios de intercambio de información a través de la 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 dife estructuras al interior de la entidad para exponerlas como un servicio de intercambio de informació 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 el 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 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 deben ser completos y exigentes:

- Rendimiento: habilidad del sistema para manejar en tiempo real un elevado número de servicios y de usuarios 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 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 Interacción e Información.
- Integral: la plataforma debe trabajar como un todo, no como piezas desacopladas que no están pre diseñadas 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 inicial (7x24x365) de la infraestructura tecnológica, almacenamiento de las configuraciones, copias de seguridad, plataforma, centro de datos, hosting dedicado, conectividad, seguridad física y lógica, monitoreo de la infraestructura, mesa de ayuda y servicios de operación y mantenimiento con sus propios recursos, entrega a las entidades públicas en forma integral como un servicio por demanda, que pueden ser rápidamente provisionados y liberados con un esfuerzo de gestión reducido o interacción mínima de las entidades 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 metodologías de gestión de servicios IT como es el caso de ITIL. El Articulador es responsable de 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 actividad se ajusta a las necesidades del servicio, de manera que se pueda distribuir y ajustar la dedicación de 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, procedimientos, 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 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. La 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 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 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 la ejecución de los procedimientos definidos.
- Procesos de soporte: El Articulador debe construir los procesos de soporte que garanticen la atención y resolución de los actores que interactúan con la plataforma.
- Elasticidad: Dependiendo de los servicios de intercambio de información ofrecidos por la Entidad, que existan períodos de alta o baja demanda, por lo que es conveniente que la plataforma cuente con capacidad y defina la estrategia particular de soporte, donde se tenga en cuenta la estructura y dimensión 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

servicio de Interoperabilidad se encarga de los elementos centrales y de seguridad en el transporte de datos. Es importante en este modelo definir desde el inicio el alcance de las tareas de administración a rea parte del Articulador que deberá entregar a MinTIC el detalle del procedimiento, herramientas y capacidad de soporte y gestión para solicitud de nuevos usuarios, autorizaciones, roles, perfiles, modificación de maestras o paramétricas, ejecución de scripts y cualquier otro tipo de operaciones de administración 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 servicios 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 cumpliendo 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 de los servicios de intercambio de información, flujos, procesos, políticas, reglas, controles de acceso 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 para el despliegue entre la entidad y el Articulador,
- Garantizar que los usuarios y personal de soporte estén entrenados y tengan la documentación correspondiente.

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

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 contará con la puesta en producción.

El Articulador cuando preste los servicios de diseño, desarrollo e implementación de servicios de información, debe realizar el proceso de cesión de derechos, conforme a la normativa vigente, a 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 tener la operación de la plataforma de interoperabilidad. Por ello, resulta conveniente que el Articulador de interoperabilidad establezca un Plan de Continuidad del Servicio en el que éste determinen todas las acciones para volver a proveer 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 definir 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 de interoperabilidad dimensionará 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 la planificación del consumo de capacidad del servicio con suficiente antelación y periodicidad como para que 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 modificaciones y mantenimientos de la plataforma de interoperabilidad o alguno de sus elementos base en infraestructura, 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 intervenciones con suficiente antelación informando a las entidades públicas.

Se debe generar un procedimiento específico para la publicación, despliegue y versionamiento de la

de intercambio de información de las entidades públicas que les permita contar con un entorno de interoperabilidad, preproducción y producción.

9. MODELO DEL SERVICIO DE AUTENTICACIÓN DIGITAL.

El Servicio de Autenticación Digital tiene como objetivo verificar los atributos digitales de una persona para que se adelanten trámites y servicios a través de medios digitales, afirmando que dicha persona es quien solicita el servicio. Este servicio permite generar un ambiente que habilita a los ciudadanos su acceso a los trámites y servicios de las 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 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 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 están 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 están 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, o 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 de los mecanismos que disponga la Registraduría Nacional del Estado Civil de sus funciones.

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

Tipo de tramite	Grado de confianza	Requiere previa identificación con Registraduría	Consulta req
Riesgo de autenticación errónea nulo o mínimo	Bajo	N/A	
Riesgo de autenticación errónea moderado	Medio	X	Consulta ANI y Información de Reg SIRC
Riesgo de autenticación errónea considerable	Alto	X	Consulta bases biométricas
Riesgo de autenticación errónea elevada	Muy Alto	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 identificación 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 los que se cuenta 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 establece 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 de manera segura 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 para la identificación.

el registro.

Posterior a la finalización de la prestación del servicio de Autenticación Digital, y si es superado de 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 autenticado. La entidad deberá emplear sus propios mecanismos para determinar los roles y autorizar los usuarios.

Nota: en la implementación del servicio de Autenticación Digital el articulador deberá tener en cuenta base de lineamientos y estándares internacionales como lo son la ITU: X.1251 Marco para el control de usuario de la identidad digital; X.1253 Directrices de seguridad para los sistemas de gestión de la identidad; 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; 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 conjunto de mecanismos de autenticación para acceder de un modo seguro y confiable a los servicios y que las entidades puedan confiar que quien accede a un servicio en línea es quien afirma ser, de acuerdo al 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:

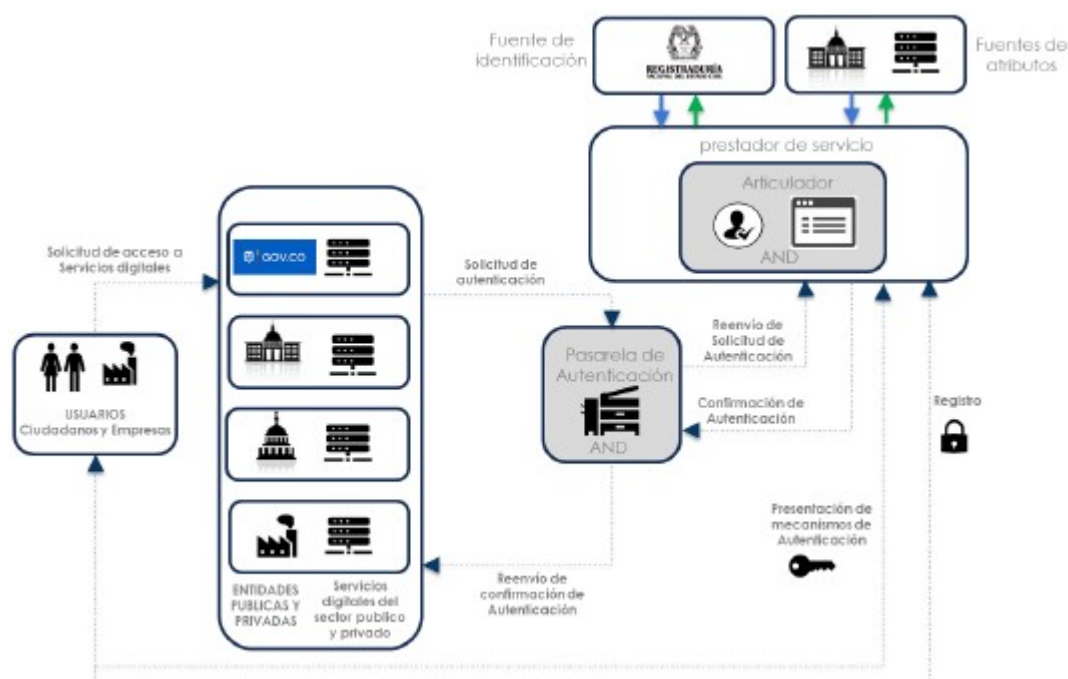


Ilustración 10 - Modelo de contexto del servicio de Autenticación Digital

Del modelo anterior se tienen los siguientes actores:

- Usuarios: son las personas naturales, nacionales o extranjeras titulares de cédula de extranjería, o 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 órdenes, sectores y niveles, los órganos autónomos e independientes del Estado, y los particulares que proveen de Servicios Ciudadanos Digitales para el uso de usuarios.
- Articulador: La Agencia Nacional Digital, que será la encargada de proveer y gestionar de manera servicios ciudadanos digitales, además de apoyar técnica y operativamente al Ministerio de Tecnología e Innovación 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 permite identificarlos en entornos digitales.
- Pasarela de autenticación: componente de software desarrollado por el articulador que servirá para conectar los servicios al prestador de servicios de Autenticación Digital con el que cuente el usuario y con el que 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 detallan en la siguiente tabla:

Relación	Origen	Destino	Descripción
	Usuario	Articulador/	Interacción entre el usuario y articulador o

Registro		prestadores de servicios	de servicio quien ingresará al sistema a las 10:00 AM o lo requieran. Para ello deberá llevar a cabo los procesos de: Identificación, inscripción y 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 servicios digitales para realizar un trámite o servicio digitales.
Solicitud de autenticación	Sistema de información de la entidad	Pasarela de autenticación	Interacción entre el Sistema de información de la entidad y la pasarela de Autenticación con el fin de solicitar autenticación de un usuario que solicita acceso a un servicio digital para un trámite o servicio por medios digitales. Para ello deberán estar conectados por medio de Connect a la pasarela de autenticación con el fin de obtener información de las entidades, incluyendo open id connect.
Reenvío de solicitud de autenticación	Pasarela de autenticación	Articulador o prestadores de servicios	Reenvío de la solicitud de Autenticación Digital a la pasarela de autenticación al prestador de servicios adecuado con el que se registró el usuario. Para ello deberán estar conectados por medio de Connect a la pasarela de Autenticación Digital al prestador de servicios, incluyendo un servicio de Connect.
Despliegue de Interoperabilidad	Articulador o prestadores de servicios	Fuentes de atributos	El articulador o prestadores de servicios de los atributos digitales de una persona a través de información externos, tales como Registraduría del Estado Civil, Migración Colombia, Eje Administrativo de la Función Pública, Comercio, etc., que en su conjunto permiten individualizar e identificar a una persona a través de los atributos digitales o hacer afirmaciones acerca de la validez de los valores de los atributos digitales Esta consulta y envío de información debe realizarse a través del servicio de Interoperabilidad. El transporte de esta información deberá estar cifrado.
Presentación de mecanismos de autenticación	Usuario	Articulador o prestadores de servicios	Interacción en la que se le solicita al usuario que seleccione uno de los mecanismos de Autenticación con el fin de autenticar a la persona que intenta acceder a un servicio digital, provisto por las entidades públicas. El transporte de esta información deberá estar cifrado.
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 satisfactorio se enviará la información de autenticación acompañada de los atributos del usuario de acuerdo al contexto. Esta información deberá estar cifrada y su validez deberá ser conocida 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 servicios a la entidad solicitante del Autenticación Digital.
--	---------------------------	--------------------------------------	--

9.3 MAPA DE CAPACIDADES DEL SERVICIO.

El mapa de capacidades del servicio de Autenticación Digital (AD) corresponde al tercer nivel del mapa de capacidades de los Servicios Ciudadanos Digitales de la sección 16 de esta guía. Las capacidades del servicio de Autenticación Digital 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 cada capacidad, marcada con "X" la columna con el nombre del actor (articulador, prestador de servicios o 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:

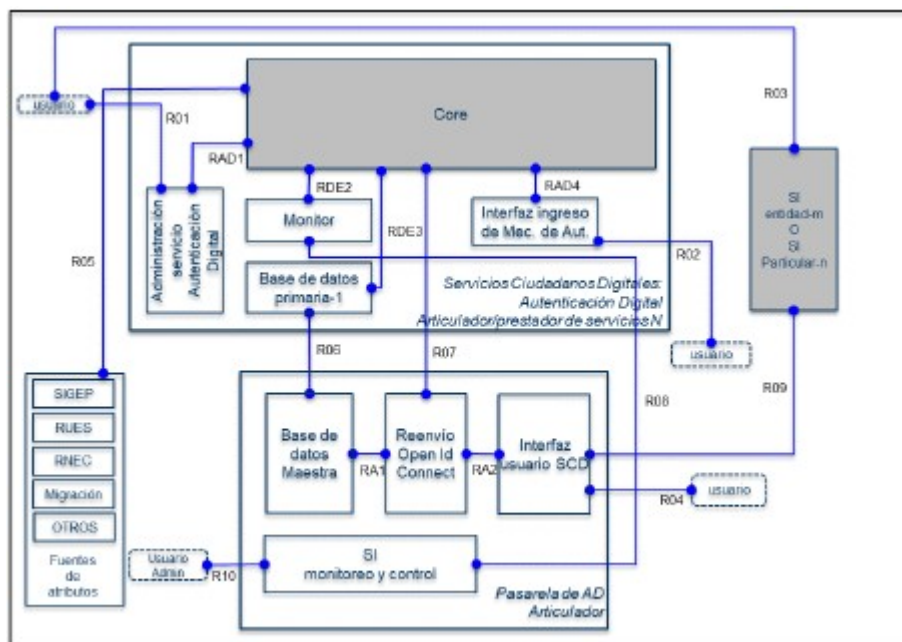


Ilustración 11 - Modelo de despliegue servicio de Autenticación Digital

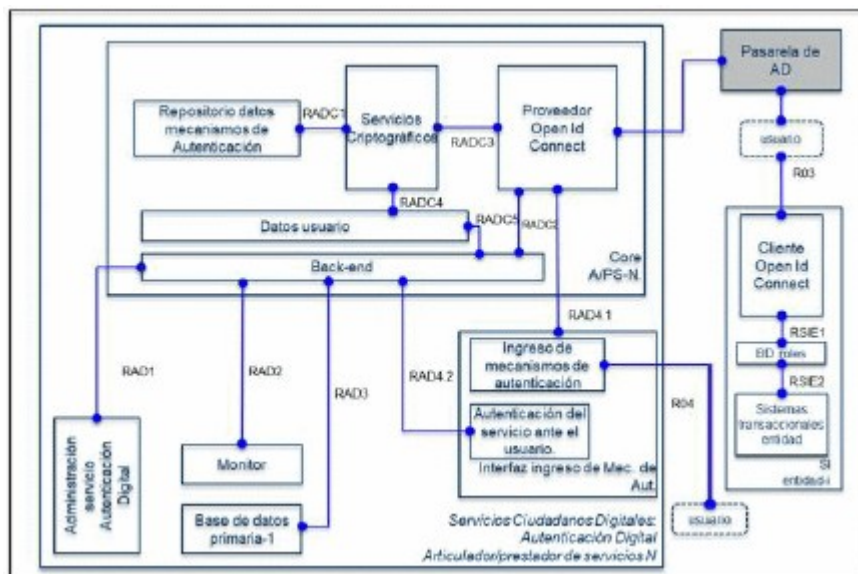


Ilustración 12 - Componente CORE del servicio de Autenticación Digital

Tabla 8 - Descripción de las relaciones del modelo de despliegue

Ítem	Origen	Destino	Descripción
R01	Usuario	Administración servicio Autenticación Digital	Interacción entre el componente de administración del servicio de Autenticación Digital para llevar a cabo la configuración de preferencias del usuario, el tratamiento de permisos, permitiéndole al usuario que sea quien administre el servicio. Los usuarios podrán acceder, modificar y gestionar información personal susceptible a ser controlada así como permisos y autorizaciones. El prestador de servicios de Autenticación deberá validar que los usuarios son quienes quieren acceder verificando la información contra las bases de datos que produzca y administre la entidad responsable.
R02	Usuario	Autenticación Digital: Ingreso de mecanismos de autenticación	Interacción entre el formulario de mecanismos de autenticación del articulo prestador de servicios de Autenticación Digital para el ingreso de los mecanismos de Autenticación según el nivel de garantía por el sistema de información de la entidad particular.
R03	Usuario	Sistema de información de entidad	En esta interacción el usuario busca autenticarse interactuando con el sistema transaccional de la entidad. En caso de que el usuario superara satisfactorio el proceso de Autenticación el sistema de información de la entidad deberá iniciar su propio proceso de autorización para controlar el sistema otorgando derechos y permisos al usuario.
	Usuario	Articulador: Interfaz Usuario SCD	Interacción entre articulador y el usuario donde este podrá ingresar los siguientes datos:

R04			documento o Id_user o Número de NIT requerir acceso representando a u jurídica). Con base en esa información, la Autenticación resolverá si la solicitud atendida por el mismo articulador o resolverla un prestador de servicios, el articulador deberá redirigir la s Autenticación Digital al prestador de ser corresponda.
R05	Fuentes de atributos	Servicios Ciudadanos Digitales Autenticación Digital	Interacción entre el articulador/prestado de Autenticación Digital y las fuentes que pueden proveer atributos del ciuc como representación legal de una pers por medio del Registro Único Empresa (RUES) o vinculación con entidades medio del Sistema de Información y Empleo Público (SIGEP) y la Registrad del Estado Civil
R06	Pasarela de Autenticación: Base de datos maestra	Articulador/prestador de servicios Autenticación Digital: base de datos Primaria	Interacción entre la base de datos articulador y primaria del prestador de se Para ello cada prestador de servicios deb base de datos de sus usuarios, denomin datos primaria, la cual será actualizada cada registro de usuario en el sistema, y con la base de datos maestra del ar tiempo real, la base de datos primaria c Id_user. Por su parte, la base de d contendrá: (a) Id_user, (b) Id_prestador c En caso de que la persona que dese servicio no se encuentre registrada com articulador le presentará un mensaje ind no está registrado, así como el proced hacerlo.
R07	Pasarela de Autenticación: Reenvío Open Id Connect	Articulador/prestador de servicios Autenticación Digital: Core	Interacción en la que, con base en la inf la base de datos maestra, el articulado reenviará la solicitud de Autenticació prestador de servicios encargado de solicitud del servicio. Para ello de conectados por medio de Open Id pasarela de autenticación con el con Autenticación Digital del articulador prestador de servicios En la 'Guía de integración de los pr Servicios Ciudadanos Digitales' se es paso a paso de la integración.
R08	Articulador: Sistema de Información de monitoreo y control	Articulador/prestador de servicios Autenticación Digital: Monitor	Interacción en la que a través de un monitoreo y control el prestador de servi información de su operación al articulad
			En esta interacción el sistema de inf entidad deberá embeber el formulario o de integración provistas por el articulac la integración que le permita al usuario

			los siguientes datos. -Tipo de documento -Id_user -Número de NIT (en caso de requ representando a una persona jurídica). Con esta información el articulador por la base de datos maestra de usuarios por qué Articulador/prestador de servicio de la solicitud de Autenticación Digital deberán estar conectados por medio Connect a la pasarela de Autenticación sistema de información de las entidades un cliente Open Id Connect. En la 'Guía para vinculación y uso de Ciudadanos Digitales' se especificará el de la integración.
R09	Pasarela de autenticación: Interfaz usuario SCD	Sistema de información de la entidad	
R10	Usuario administrador	Articulador	Interacción entre el usuario del articulador de administrador con el fin de verificar de monitoreo y generar acciones para operación y la gobernabilidad del modelo
RAD1	Autenticación Digital: administración servicio Autenticación Digital	Articulador/ prestador de servicios de Autenticación Digital: Core	Interacción al interior de sistema de información articulador o prestador de servicios de Autenticación Digital, en el que la administración de Autenticación Digital se conecta con sistema para hacer ajustes en las solicitadas por el usuario.
RAD2	Articulador/ prestador de servicios de Autenticación Digital: Monitor	Articulador/ prestador de servicios de Autenticación Digital: Core	Interacción al interior de sistema de información articulador o prestador de servicios de Autenticación Digital, en el que el Core del sistema información de su operación a su monitoreo esta la exponga a través de un servicio al
RAD3	Articulador/ prestador de servicios de Autenticación Digital: Base de datos primaria	Articulador/ prestador de servicios de Autenticación Digital: Core	Interacción al interior de sistema de información articulador o prestador de servicios de Autenticación Digital, en el que el Core del sistema actualiza y consulta los registros de usuario base de datos primaria. La base de datos primaria contendrá: (a)
RAD4	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 articulador o prestador de servicios de Autenticación Digital, en el que el Core del sistema verifica la información de los mecanismos de autenticación ingresados por los usuarios la Interfaz de ingreso.
RA1	Articulador: Base de datos maestra	Articulador: Reenvío Open Id Connect	Interacción al interior de sistema de información articulador por medio de la cual este por las solicitudes de Autenticación Digital de servicios determinado, por medio de a la base de datos maestra de usuarios, ser alimentada y actualizada con las bases primarias de cada uno de los prestadores de servicios.
	Articulador: Interfaz usuario SCD	Articulador: Reenvío Open Id Connect	Interacción al interior de sistema de información articulador en el que con base en la ingresada por el usuario por medio de la Interfaz de usuario SCD y comparada con la base

RA2			maestra, pueda reenviar las solicitudes de Autenticación Digital al prestador de servicios de Autenticación Digital determinado. Para ello, a través de R10 (Core: Datos de usuario) deberá embeber un formulario que le permita al usuario el ingreso de los siguientes datos: -Tipo de documento -Id user. -Número de NIT (en caso de requerir representación a una persona jurídica).
RAD4.1	Articulador/prestador de servicios de Autenticación Digital: Core: Proveedor Open Id Connect	Articulador/prestador de servicios de Autenticación Digital: Core: Proveedor Open Id Connect	Interacción al interior de sistema de información de cada prestador de servicios de Autenticación Digital, en el que se produce un intercambio de protocolo para la Autenticación Digital por parte del prestador de servicios de Autenticación Digital; deberán implementarse el protocolo Open Id Connect 1.0.
RAD4.2	Articulador/prestador de servicios de Autenticación Digital: Interfaz de ingreso mecanismos de autenticación: Autenticación del servicio ante el usuario	Articulador/prestador de servicios de Autenticación Digital: Core: Backend	Interacción al interior de sistema de información de articulador o prestador de servicios de Autenticación Digital, en el que la interfaz de usuario de los mecanismos de autenticación debe integrar los componentes de autenticación del servicio de Autenticación Digital, para que este pueda identificar si realmente está accediendo a la interfaz de usuario de los mecanismos de autenticación del proveedor de servicios. Para ello podrá usar estrategia de autenticación e imagen de seguridad personalizadas por el proveedor de servicios.
RADC1	Articulador/prestador de servicios de Autenticación Digital: Core: Servicios criptográficos	Articulador/prestador de servicios de Autenticación Digital: Core: Repositorio de mecanismos de Autenticación	Interacción al interior de sistema de información de articulador o prestador de servicios de Autenticación Digital, en el que hace uso de servicios de Autenticación Digital para almacenar los datos de los mecanismos de Autenticación.
RADC2	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 de servicios de Open Id Connect que le permite acceder a la información de identidad y de configuración necesarios para el proceso de Autenticación Digital.
RADC3	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 de articulador o prestador de servicios de Autenticación Digital, en el que se hace uso de servicios de Autenticación Digital y de servicios criptográficos para validar los mecanismos de autenticación ingresados por los usuarios de Autenticación Digital; proceso de intercambio de mensajes de Autenticación Digital por Open Id Connect 1.0 para ejecutar los servicios de Autenticación Digital.
RADC4	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 de articulador o prestador de servicios de Autenticación Digital, en el que hace uso de servicios de Autenticación Digital para proteger la información del usuario.
RADC5	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 de articulador o prestador de servicios de Autenticación Digital, en el que el backend accede a la información de usuario para proveer servicios como: a. Configurar alertas y alarmas

			b. Configurar permisos c. Registrar personas jurídicas d. Visualizar registros de acceso e. Descargar registros de acceso f. Bloquear y desbloquear servicio g. Configurar alertas de acceso h. Visualizar registros de acceso i. Descargar registros de acceso j. Bloquear y desbloquear servicio k. Configurar mecanismos de auten servicio ante el usuario. l. Entre otras.
RSI1	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 inf la entidad o particular en el que una vez modo satisfactorio el proceso de A Digital, el sistema de información de consulte su base de datos de roles co validar las autorizaciones en el sistem derechos y privilegios al usuario.
RSI 2	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 inf la entidad o particular en el que una vez modo satisfactorio el proceso de A Digital y validadas las autorizaciones e otorgando derechos y privilegios al usu provea al usuario el acceso a los trámite 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 sigui lineamientos:

9.5.1 CONDICIONES DE OPERACIÓN DEL SERVICIO DE AUTENTICACIÓN DIGITAL.

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

por lo anterior será responsable de los perjuicios causados de forma deliberada o por negligencia al usuario en caso de incumplimiento de sus obligaciones, es deber del Articulador mantener recursos 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 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 utilización.

i. Debe contar con plataformas, sistemas, productos fiables que estén protegidos contra toda alteración y 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 las 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 de Servicio de Autenticación Digital, como los registros y logs de auditoría, con el objeto de que sirvan de prueba en procedimientos legales en donde se requiera información referente a las credenciales de un ciudadano. La neutralidad tecnológica, deberán estimar los mecanismos para poder garantizar durante este tiempo 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 digitales o presenciales. Adicionalmente, se debe llevar a cabo el proceso de validación de la identidad, 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, registra atributos relacionados con la identidad del usuario. La recopilación de datos en el momento del registro debe 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) 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, podrán solicitar otros datos.

Los usuarios deberán tener el control sobre el tratamiento de sus datos, permitiéndole al usuario que defina sus preferencias. Los usuarios tienen el derecho de acceder, modificar y suprimir su información 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 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 de 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 en 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 o LTV.
- Digitalmente, haciendo uso de las credenciales y mecanismos de autenticación entregados al usuario en 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 PDF o 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 que fue recolectado, 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.

- Verificar la identidad contra el Archivo General de identificación de la Registraduría Nacional del Estado Civil.

Civil.

- Validar la identidad del ciudadano por medio de preguntas cuyas respuestas sólo el usuario a registrar y generadas de al menos tres (3) fuentes de información de diferentes contextos, lo suficiente fidedigna 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 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 1712 de 2012 y sus decretos reglamentarios.
- El menor deberá estar acompañado por su padres, tutor o representante legal en los casos que aplica 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 cumplan 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 de 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 "Registro de personas naturales" antes indicado.

La persona jurídica realizará la solicitud de registro ante el mismo prestador de autenticación Digital 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 jurídica, 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 por el 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 PÚBLICAS.

Los funcionarios públicos y los particulares que desempeñen funciones públicas deberán registrarse y 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 desempeña 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 Articulador 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 de 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, el cual deberá cumplir los siguientes requerimientos al momento de realizar el proceso de entrega 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 Colombia (ONAC).

b. Las credenciales entregadas al ciudadano deben corresponder a mecanismos de autenticación del tipo físico, 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 tiene acceso 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 numérica, 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 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 8 caracteres de longitud, deberán ser cadenas aleatorias y puede ser enteramente numérico. La contraseña memorizada deberá ser rechazada por el Articulador si llegará a estar incluido en una lista negra de contraseñas comprometidas, en ese caso el usuario deberá elegir una contraseña o secreto memorizado. Ninguno de los 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 genera un nuevo PIN) deberá tener al menos 6 caracteres de longitud y será generado usando un generador de números aleatorios aprobado y de acuerdo con la recomendación NIST Special Publication 800-90^a 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, deberán implementar mecanismos criptográficos de derivación de claves como el descrito en NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation o RFC 7914 The script-based Key Derivation Function o equivalentes.

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 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 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.

Autenticación digital, demostrando así la posesión y el control del dispositivo. Un dispositivo OTP 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 en software instalados en dispositivos como teléfonos móviles.
2. El segundo factor de autenticación puede lograrse mediante algún tipo de mecanismo de entrada, biométrico integral (por ejemplo, huella digital) o una interfaz de computadora directa (por ejemplo, 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 posesión y el control del dispositivo. El dispositivo OTP multi-factor es un factor de posesión, y se requiere 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 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 y control.

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 una conexión directa al punto final del usuario. El dispositivo utiliza claves criptográficas simétricas o asimétricas, 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 proporciona una 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 y control.

f. Software Criptográfico Multi Factor

Un autenticador criptográfico de software multi-factor es una clave criptográfica almacenada en 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 de 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.

firmado. El dispositivo criptográfico multi-factor es un factor de posesión y se debe activar por un 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 3 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 de posesión
- 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 factor de posesión y una Contraseña-Secreto memorizados.
- Mecanismos dispuestos en los anexos A, E y F del documento CEA-4.1-10 de la ONAC utilizados

Contraseña-Secreto memorizado

En el mecanismo de autenticación muy Alto: Este mecanismo de autenticación, hará uso de la identidad digital de la cédula de ciudadanía digital y de la biometría que se registrará por las disposiciones de la Ley 1712 de 2014, en el marco de sus competencias, el cual será 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 factor y una Contraseña-Secreto memorizados.
- Mecanismos dispuestos en los anexos A, E y F del documento CEA-4.1-10 de la ONAC utilizados con Contraseña-Secreto memorizado

Se podrán usar otros tipos de credenciales diferentes a los descritos anteriormente, en todo caso las mismas deberán ser estudiadas y analizadas por MinTIC para determinar su nivel de confianza y nivel de garantía. 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 identidad 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 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.

El Articulador deberá entregar a MinTIC el detalle del procedimiento a utilizar para la autenticación digital, 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 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 registra, de manera que las credenciales entregadas a los usuarios pueden ser empleadas para acceder a cualquier información de entidades públicas o privadas que integren los componentes de direccionamiento de la entidad.

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

- **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. Las tecnologías de todo tipo, incluidas las aplicaciones basadas en web, móviles y JavaScript, solicitan información sobre sesiones autenticadas y usuarios finales. El conjunto de especificaciones es extensible y permite a los participantes utilizar funciones opcionales como el cifrado de datos de identidad. El 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 credencial de Autenticación con mecanismos de autenticación medio, alto y muy alto, se deben definir periodos de validez mayores a 6 meses con el fin de verificar las condiciones del usuario, que permita verificar la validez del 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 que tenga la 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, 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. En 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 jurídica o 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 a través de consultas a otros sistemas de información, serán usados única y exclusivamente en aquellos casos 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 acordados como estándares como la NIST: 800-63-3 Digital Identity Guidelines, 800-63A Enrollment and Identity Proofing, 800-63B Authentication and Lifecycle Management; la ISO/IEC 29115:2013 Entity Authentication Framework y la ITU: X.1251 Marco para el control por el usuario de la identidad digital, X.1253 Di

seguridad para los sistemas de gestión de la identidad y X.1254 Marco de garantía de autenticación

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, 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 utilizarán para mitigar las amenazas relativas a la autenticación (modificación, robo, duplicación, captura, Phishing, Pharming, ingeniería social, entre otras.) en cada una de las fases (afiliación, gestión de credenciales y autenticación).
Características de una credencial.	Verificar la credencial, validando que este contenga, por lo menos las siguientes características: - Datos que demuestren una identidad y/o sus derechos como algo que es único y no puede ser replicado o su representación y datos generados por el usuario. - Ir acompañada de otros datos que pueden ser de utilidad en los procesos de autenticación. - Sea una credencial derivada.
	- Ser auténtica pero no válida en todos los contextos. - Ser verificada antes de aceptarse como auténtica y fiable para la finalidad a la que está destinada. - Ser compleja y secreta. - Seguir lo indicado para la emisión de credenciales. - En caso del certificado digital se deben cumplir los requisitos del documento CEA-4.1-10 de ONAC, establecer las Políticas de Certificados, 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. - Forzar el cambio de credencial si existe algún tipo de evidencia de compromiso. - Establecer el periodo para el cambio y renovación de credencial.
Repositorio de credenciales	- Implementar un plan que garantice la protección de las credenciales protegidas con el más alto nivel de seguridad posible. - Realizar copias de seguridad con hardware seguro. - Dispositivos criptográficos para el almacenamiento de certificados de firma electrónica con estándares vigentes simétricos y/o asimétricos.
Capacidades de usuario.	Establecer las capacidades generales para usuario, funcionales y las capacidades de seguridad establecido en las recomendaciones de la ITU X.1251 y 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 credencial que nos es legítima, en la prueba de autenticación donde un usuario no puede probar una credencial que nos es legítima y prueba de una identidad comprometida.
Administración de sesiones.	- Proporcionar las medidas necesarias para la protección e integridad de las sesiones y evitar ataques como XSS y CSRF (Falsificación de sitios). - Las cookies de navegación deberán: - Ser accesibles por sesiones seguras (HTTPS). - Ser inaccesibles a través de JavaScript. - Tener un periodo de validez de la sesión.
Tokens de acceso	Deberán ser validados durante periodos de tiempo.

Firma digital	Cumpla con el artículo 28 ley 527 de 1999: - Es única a la persona que la usa. - Es susceptible de ser verificada. - Está bajo el control exclusivo de la persona que la usa. - Está ligada a la información o mensaje, de tal manera que, si cambiados, la firma digital es invalidada. - Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional
---------------	--

9.5.10. ENRUTAR SOLICITUDES DE AUTENTICACIÓN.

En su función de articulación el Articulador debe enrutar las solicitudes de Autenticación digital al 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.

- Tipo de documento
- Número de documento de identificación.
- 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 si el 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 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 los datos 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) identificación 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 de la Ley 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 integradas al servicio, para firmar electrónicamente documentos.

La firma de documentos debe seguir los lineamientos estipulados en la Ley [527](#) de 1999, el Decreto 2121 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 deben usar una norma o estándar técnico que no se encuentre dentro de los mencionados a continuación. El Articulador deberá enviar a MinTIC la información con la descripción de la norma o estándar técnico que se va a 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 el Articulador.

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 el Articulador deberá implementar 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 sí 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 PÚBLICAS.

Las entidades públicas que cuenten 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 proceso 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 los 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 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 ciudadano desde los custodios responsables en la administración pública.

Los servicios mínimos que deben ser provistos por el prestador de servicios de Carpeta Ciudadana, los cuales 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.
- 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 control de los datos que posee el Estado, así como, acercándolos a la gestión de estos a través de un punto de contacto único y 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 verificados están.
- Entregar un medio para facilitar al usuario la solicitud de actualización o corrección de sus datos en la administración pública.
- Visualizar su información según las necesidades o preferencias (servicios públicos, salud, registro civil, 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.

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 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 los servicios.
 - 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 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 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 los usuarios, para generar reportes, estadísticas e informes.
 - g. Brindar acompañamiento a las entidades en cuanto al proceso de provisión de la Carpeta Ciudadana Digital, 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 er 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 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 p del servicio de Carpeta Ciudadana son responsables del tratamiento de los datos personales que los les suministren directamente y encargados del tratamiento respecto de los datos que otras entidades proporcionen en la prestación del servicio, por lo que deben cumplir con los deberes legales estable Ley [1581](#) de 2012 y sus decretos reglamentarios o aquellas normas que la sustituyan, modifiquen o

k. Garantizar las condiciones de seguridad y privacidad requeridas por el servicio, para garantizar a la integridad, la confidencialidad y la disponibilidad de la información, así como los niveles de acc misma. Cumplimiento normativo, entre estos, el Modelo de Seguridad y Privacidad, así como de la Administración del Riesgo y Diseño de controles del Departamento Administrativo de la Función I

- Usuarios: representa a la persona natural, nacional o extranjera titular de cédula de extranjería, o l 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 herra integración y punto de acceso digital del ciudadano,

- Servicio de Autenticación Digital: desde la perspectiva del servicio de Carpeta Ciudadana Digital de Autenticación Digital es el encargado de proveer el mecanismo de autenticación para que el usu las credenciales necesarias para lograr ingresar a su Carpeta.

- Servicio de Interoperabilidad: el servicio de Interoperabilidad es fundamental para una correcta p servicio de Carpeta Ciudadana Digital, teniendo en cuenta que de esta integración dependerá el imp obtenga el ciudadano de la Carpeta, así como la utilidad de los datos que se logren exponer al usuar lado, también es el habilitador para la comunicación entre el usuario y la Administración Pública e solicitudes de actualización de sus datos.

- Entidad: es el actor encargado de suministrar los datos e información que posea del usuario para s través de la carpeta, de manera tal que deberá habilitar los servicios de información requeridos, bien sus sedes electrónicas o de sus sistemas de información. Así pues, es necesario para la correcta pres servicio de Carpeta:

a. Que cumpla con los requerimientos establecidos para la habilitación del servicio de Interoperabil

b. Cumplir las directrices y lineamientos establecidos en el marco de interoperabilidad y del lengua 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 co integridad, la confidencialidad y la disponibilidad de la información, así como los niveles de acceso

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

- Prestador de Servicios Ciudadanos Digitales: Personas jurídicas, públicas o privadas, quienes, me

esquema coordinado y administrado por el articulador, pueden proveer los servicios Ciudadanos Di Autenticación Digital y Carpeta Ciudadana Digital.

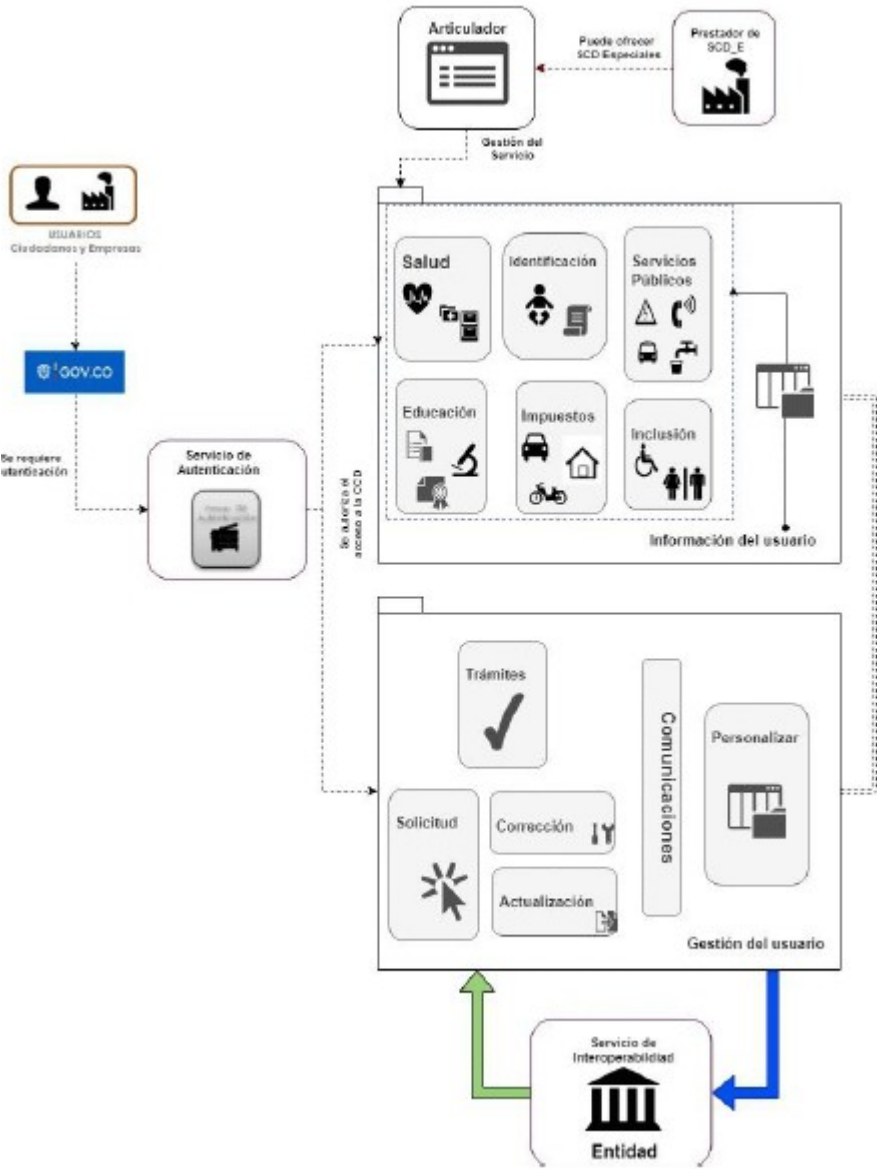


Ilustración 13 - Modelo de contexto del servicio de Carpeta Ciudadana Digital

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

Relación	Origen	Destino	Descripción
Acceso al servicio de Carpeta Ciudadana Digital	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
Solicitud de autorización de ingreso	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.
Ingreso a la Carpeta	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.
Gestiones del usuario	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:
Gestiones del usuario	Personalización		Personalización de presentación de información sector, área o normativa
Solicitudes			Solicitud de Corrección o actualización de datos.
Comunicaciones			Visualización de comunicaciones realizadas
Autorizaciones			Habilitación de acciones de datos comunicados envío de
Trámites			Realización de trámites GOV.CC
Intercambio de datos e información			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 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 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:

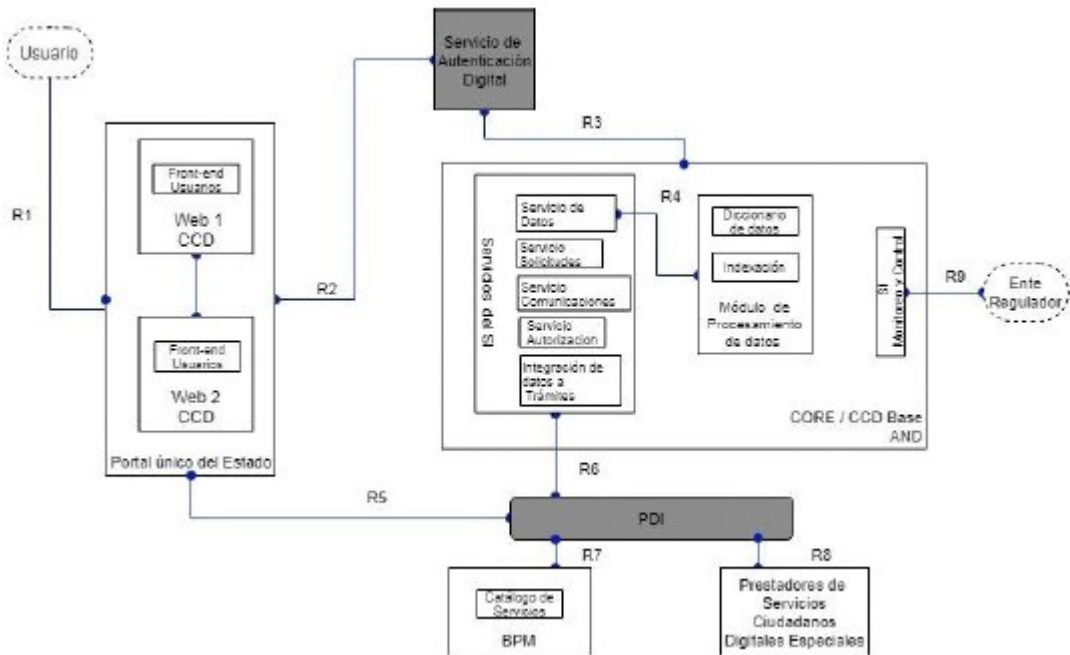


Ilustración 14 - Modelo de despliegue del servicio de Carpeta Ciudadana Digital base.

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

Finalmente, todo lo anterior es soportado por el servicio de Interoperabilidad a través del cual se gestionan 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	Interacción directa entre el usuario y el sistema de Carpeta Ciudadana Digital (CCD), incluyendo Registrarse de manera voluntaria y gratuita al Carpeta Ciudadana, ingresar y administrar configurar preferencias, gestionar sus datos, cancelar servicios de comunicaciones electrónicas, recibir comunicaciones electrónicas, cargar y documentos, aportar o compartir documentos. Para acceder al servicio el usuario ingresa las emitidas por el Articulador / prestador de Autenticación Digital según el nivel de garantía s el sistema de Carpeta Ciudadana Digital.
R2	Componente de CCD	Pasarela de Autenticación	Interacción entre el Componente de Carpeta Digital y el servicio de Autenticación Digital validación de credenciales de usuarios en las o consumir los servicios del sistema de Autenticación El servicio de Autenticación Digital deberá prove de información con el sistema en el cual notifica de la validación, informando si su auter satisfactoria o no, teniendo en cuenta que el nivel cual se podrá acceder a la Carpeta es el nivel 2, mostrarán algunos trámites acorde sus permisos. El acceso a los conjuntos de datos definidos funcionalidades se hará a partir de un nivel 3 de a
R3	Servicio de Autenticación Digital	Core del Servicio de CCD	Interacción entre el CORE del servicio de Carpeta Digital y la pasarela de autenticación: Gestión de servicio de Autenticación Digital, con el fin de a principales componentes del servicio de Autenticación como despliegue del protocolo de autenticación de credenciales, para gestionar la autorización de servicios de la Carpeta Ciudadana Digital.
R4	Servicio de visualización de datos del usuario.	Módulo de procesamiento	En este módulo se generarán la visualización acorde a las definiciones de casos de uso establecida cada conjunto de datos.
R5	PDI	GOV.CO	Interacción derivada de la necesidad de la integración visualización de los datos a la generación de trámites los usuarios logren efectuar trámites desde su carpeta
R6	Servicios del SI	PDI	En esta interacción se soporta la oferta de servicios Carpeta Ciudadana Digital; a través de ella, se soporta la interacción del usuario con el sistema de la PDI y los servicios de intercambio de información hacia las entidades.
R7	PDI	BPM / Entidades	Es la interacción a través de los sistemas transaccionales entidad con la PDI, pues es la llamada que estos sistemas de su flujo para usar los servicios Ciudadanos permitir al prestador de Carpeta Ciudadana Digital a 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 base, y de esta forma añadir un mayor valor para a través de su oferta sobre el servicio de Carpeta Ciudadana Digital base.

R9	Monitoreo y control	Entes reguladores	Interacción dada entre el Sistema de Monitoreo a través de la cual se generarán datos e información por los entes de control, acorde a periodos y condiciones 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, capacidad de memoria, la cantidad de espacio de almacenamiento del sistema y el espacio asignado a los Servicios Ciudadanos Digitales, entre otros. Se deben establecer acuerdos de nivel de servicio de 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 gratuitos para los usuarios
2	Capacidad del sistema	Número de usuarios, entidades y servicios de intercambio de información	a. Número mínimo de usuarios concurrente Número máximo de entidades públicas <100> c. Número mínimo de servicios de intercambio de información concurrentes <500> d. Número de transacciones concurrentes <100.000>
3	Rendimiento	Tiempo de respuesta de los Servicios Ciudadanos Digitales	a. El tiempo máximo para que el Articulador de Componentes de Autenticación y Carpeta Ciudadana en el navegador de un usuario no supere <5 segundos> b. El tiempo máximo de respuesta del Articulador una vez el usuario ha sumistrado credenciales es de <1 segundo>. c. El tiempo de respuesta de la Carpeta Ciudadana es de <5 segundos>
4	Soporte	Disponibilidad de documentación técnica	El sistema debe disponer de personal especializado en documentación técnica para dar un adecuado soporte al funcionamiento del sistema.
5	Aseguramiento de la información	Copias de seguridad de la información	a. El Articulador debe realizar copias de seguridad completas y copias de seguridad incremental con periodicidad que garantice la adecuada recuperación de falla del sistema. b. Las copias de seguridad de información clasificada y reservada deben estar protegidas de cualquier acceso no autorizado. c. Recuperación Objetivo (RPO). Tiempo entre una copia de datos y la siguiente réplica, con el fin de garantizar la continuidad de los servicios: 30 minutos.
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 de Servicios Ciudadanos Digitales en sistemas de alta transaccionalidad.

7	Mantenimiento	Actualización tecnológica permanente del sistema	a. El Articulador dispondrá de un sistema de m con nuevas versiones, paquetes de servicios o p caso de que se incluyan nuevas características el Articulador debe llevar a cabo nuevas capa formación para los usuarios.
8	Conformidad	Configuración de conformidad con los estándares de la industria y con las regulaciones nacionales	a. Deben estar en conformidad con todas las c legislativas y regulatorias que apliquen a la n Articulador y a la jurisdicción.b. Debe conformidad con estándares industriales, g aceptados en tecnología y en las plataformas e desplegado el sistema.c. Debe ajustarse a las nc aplicables para admisibilidad jurídica y valor p la información digital.d. El sistema no c funciones que sean incompatibles con la p datos a nivel nacional, la libertad de inform legislación.
9	Aseguramiento de la información	Preservación a largo plazo y obsolescencia de la tecnología	El articulador debe considerar los riesgos tec cara a la preservación de la información a largo tres puntos de vista: (i) la degradación de lo comunicación, (ii) la obsolescencia del hardv obsolescencia del formato.
10	Soporte	Servicio de soporte a los usuarios	a. Deben existir reglas claras de cómo acceder a soporte del articulador, de cómo reportar errore del software y qué tipo de nivel de ayuda in situ remota puede esperar un usuario.
11	Mantenimiento	Mantenimiento preventivo del sistema	a. El articulador debe establecer el nivel de m y soporte que le da al sistema (hardware, comunicaciones), frecuencias de actualización última versión liberada y la hoja de ruta del sist

11.2 ATRIBUTO DE CALIDAD: ESCALABILIDAD.

Atributo de calidad: escalabilidad

La escalabilidad se relaciona con la capacidad de los Servicios Ciudadanos Digitales para soportar adecuada el crecimiento en los requerimientos (aumento en el número de usuarios, aumento en el n usuarios simultáneos conectados, aumento en el número de transacciones simultaneas, aumento en la emisión de credenciales, aumento en el número de entidades y servicios, etc.), sin afectar ningún atributos de calidad del sistema (rendimiento, usabilidad, disponibilidad, etc.). El articulador debe a atributo de calidad de escalabilidad, usando la estrategia que estime conveniente, ya sea aumentand la capacidad de la infraestructura, o balanceando el aumento de carga entre diferentes sistemas o a t 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 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 la capacidad de procesamiento y almacenamiento que migra a un nuevo ambiente.
4	Crecimiento del sistema	Crecimiento de la funcionalidad	El articulador deberá estar en la capacidad de mejorar el sistema con nuevas funcionalidades que realizar cambios importantes a la infraestructura del sistema, en particular la introducción de funcionalidad adicional al sistema no debe requerir cambios ya en operación que no tienen relación con la funcionalidad.
5	Rendimiento al escalar	Al escalar, el sistema no deberá verse afectado en el rendimiento de cada una de sus funciones	a. Debe mantener el rendimiento específico de mantener el tiempo máximo de búsqueda es de 10 segundos. b. Debe mantener la periodicidad de los reportes de eliminación especificada.

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 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 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	El sistema debe estar en capacidad de garantizar información confiable para los procesos de auditoría debe verificar los siguientes aspectos: a. Solo los usuarios autorizados tienen acceso al sistema. b. Todos los usuarios autorizados tienen acceso al sistema. c. Los controles de seguridad y acceso del sistema están funcionando correctamente. d. Los usuarios no están accediendo a información, funciones, servicios, etc. a los que no le ha sido permitido el acceso. e. Los usuarios cuentan con los mecanismos de configuración. f. Los documentos de monitoreo están siendo producidos en agrupaciones apropiadas.

			g. Los documentos de monitoreo están siendo correctamente. h. Ningún documento de monitoreo está siendo eliminado del sistema, fuera del proceso de desecho de documentos. i. Los períodos de desecho están siendo monitoreados y las fechas límite están siendo cumplidas. j. Las confirmaciones ocurren dentro de las fechas límite de desecho y no hay atraso en los documentos que deben eliminarse. k. El contenido de los documentos está siendo monitoreado correctamente. l. Las copias de los contenidos de los documentos de monitoreo están siendo eliminadas de fuentes secundarias como: Articulador / prestador de servicio inmediatamente o al tiempo con la eliminación formal del archivo. m. Garantizar la trazabilidad mediante el uso de acciones sobre el sistema tales como: estampado, autor, estado, entre otras.
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 las Entidades y Ciudadanos todo tipo de alertas.
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.	a. Monitorear el número de usuarios, tipos de servicios de intercambio de información, a qué hora y en qué lugar tienen acceso al sistema, a qué hora y en qué lugar. b. Monitorear la cantidad de almacenamiento que se está usando y el ritmo de aumento. c. Monitorear el tiempo de búsqueda y ritmo en incremento o disminución. d. Monitorear el tiempo de respuesta promedio de las funciones. e. Monitorear la utilización de procesamiento de memoria.
5	Reportes comparados	El sistema debe estar en capacidad de monitorear y advertir acerca del uso de recursos, comparando reportes estadísticos en el tiempo.	a. Estos informes deberán ser remitidos de forma periódica al MinTIC.

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

minimizar el impacto de los errores del usuario, (c) el sistema facilita el uso a los 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 la 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, formas de minimizar el número de decisiones que los usuarios deben tomar, personalización y localización de facilidades de ayuda, documentación de usuario, preguntas frecuentes, videos y tutoriales en línea, y 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 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 niveles de capacitación para usar los Ciudadanos Digitales base eficientemente, cursos de entrenamiento, tutoriales y otros de educación y aprendizaje. b. Debe haber capacitación dirigida a usuarios generales (ciudadanos) y especializados (administradores técnicos y otros de las entidades, auditores, etc.).
2	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 al recibirlos puedan tomar las medidas adecuadas. c. El sistema debe ser capaz de mostrar múltiples documentos de forma simultánea. d. El sistema debe permitir que, cuando sea necesario, existan valores por defecto persistentes para la introducción de datos, entre los que conviene incluir (i) valores definidos por el usuario y (ii) idénticos a los del elemento anterior, derivados del contexto, como la fecha, el identificador del usuario, entre otros. e. Las transacciones más habituales del sistema deben diseñarse de forma que puedan realizarse con el menor número de interacciones
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 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	a. El sistema deberá permitir que los usuarios configuren la interfaz de usuario a su gusto, incluyendo

		visualización y de la interacción con el usuario, de acuerdo con sus preferencias	(i) el contenido de los menús, (ii) la disposición de las pantallas, (iii) la utilización de teclas de función, (iv) los colores, las fuentes y el tamaño de las fuentes, (v) las alarmas sonoras. b. Cuando el sistema recurra a la visualización en forma de ventanas, conviene que el usuario pueda configurar cada una de ellas.
6	Accesibilidad	El sistema debe ser accesible a todo tipo de usuario, con diferentes capacidades, incluyendo aquellos con discapacidades específicas.	a. La interfaz de usuario del sistema debe ser compatible con los usuarios con necesidades especiales, esto significa que el software especializado pueda utilizar y con las directrices pertinentes para ese tipo de usuarios. b. El sistema deberá proveer la opción de alto contraste en la interfaz web para facilitar la presentación a usuarios con problemas de visión. c. El sistema debe cumplir con los requisitos establecidos en la Norma Técnica Colombiana NTC 5854, la cual establece los requisitos de accesibilidad para las páginas web, como mínimo conformidad AA. La norma fue desarrollada como documento de referencia 'Las Directrices de Accesibilidad para el Contenido web (WCAG 2.0) de diciembre de 2008'. d. Uno de los principales referentes para la evaluación de los requerimientos no funcionales de accesibilidad es el World Wide Web Consortium (W3C) Web Accessibility Initiative (WAI). El W3C publica las guías para el acceso al contenido en la red, las cuales cubren recomendaciones para hacer el contenido más accesible. e. El sistema debe cumplir con los requisitos establecidos en la WCAG (Web Content Accessibility Guidelines). Estas guías proveen una clasificación de los niveles de accesibilidad (la más baja) o AAA (la más alta).

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 y las consecuencias asociadas a los ANS. Una falla del sistema ocurre cuando por alguna razón este no cumple 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 del sistema puede proporcionar debe estar claramente establecido por el Articulador/prestador de servicios. 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 (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 recursos de disponibilidad brindados por el alojamiento del sistema sean establecidos o mejores condiciones que las del Articulador.
4	Monitoreo de la disponibilidad	El articulador debe contar (directamente o por medio de un tercero) con las herramientas que permitan medir los porcentajes de disponibilidad del sistema.	a. El sistema debe contar con herramientas para medir su disponibilidad y la disponibilidad de cada uno de sus componentes. b. La medición de la disponibilidad del sistema debe realizarse en tiempo real. c. Los resultados del monitoreo deben ser mantenidos por el articulador y deben poder ser consultados por el MinTIC en cualquier momento. d. La información de monitoreo mantenida por el articulador le debe permitir al MinTIC verificar la disponibilidad del servicio en los meses anteriores y el mes en curso. e. El articulador debe entregar mensualmente un reporte de la disponibilidad del sistema, incluyendo el número de caídas: fecha, hora de la caída, hora de restablecimiento del sistema, componente, duración de la caída, componentes afectados, causas de la caída y afectados (número y quiénes).
5.	Cálculo de disponibilidad	La disponibilidad se mide usando la siguiente ecuación: $(1 - (\text{Número total de minutos en que el servicio no está disponible} / (\text{Número de días en el mes} \times 24 \text{ horas} \times 60 \text{ minutos}))) \times 100\%$ 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.	Disponibilidad exigida $\geq 99.982\%$

		facturado.	
		La medición la hace el Articulador /prestador de servicio monitoreando permanentemente el servicio durante el mes.	

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 resistencia a los defectos, problemas de funcionamiento o inesperadas condiciones de operación. 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 permitir que la información consignada, transmitida en un mensaje de datos sea íntegra, completa e inalterable.	Para determinar el grado de requerido se seguirán las recomendaciones de ITU e ISO dispuestas en sus documentos 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 que permitan garantizar que la información no sea alterada.
4	Recuperación ante fallas	El sistema debe poseer mecanismos de recuperación ante fallas.	a. Si el sistema se cae o no responde, se debe identificar las fallas y automáticamente iniciar la recuperación o redireccionar a sistemas de respaldo o sistemas alternos. b. En caso de fallas, el sistema debe proporcionar un detalle de las fallas a sistemas externos para la información en bitácoras de eventos, de trazabilidad, u otros similares y no de la Agencia Nacional Digital (AND). c. Tiempo Objetivo de Recuperación: Tiempo máximo que puede estar fuera de servicio una vez se ha producido una Interrupción de servicio en minutos.
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 cumplen con 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 demás normativa aplicable a la protección de los datos personales.	El tratamiento de datos personales debe realizarse de acuerdo con la ley vigente.
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 trámite el usuario en los Servicios Ciudadanos debe ser informado de la finalidad 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 solicita los datos estrictamente necesarios para la prestación del SCD al cual el usuario está registrado.
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.	a. El Articulador solamente almacena las credenciales del usuario mientras este encuentre registrado a sus servicios. b. Si el usuario realiza cambio de servicio, el prestador de servicio debe eliminar toda la información de las credenciales del usuario de todos los dispositivos y las copias de seguridad de las mismas.
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 ley 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 información.
7	Transparencia	El ciudadano tiene el derecho a obtener información sobre la existencia de sus datos personales.	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 conciernen e) del Artículo 4 de la Ley 1581 de 2012. b. El Articulador debe ofrecer al usuario la siguiente información cualificada y comprensible cuando procese datos personales, el Articulador debe ofrecer, como mínimo, la siguiente información: (i) información sobre la existencia de los datos y el controlador de datos, (ii) el propósito del procesamiento de los datos personales, (iii) a quien se podrán revelar los datos personales, (iv) cómo el usuario puede ejercer su derecho que le otorgue la ley de protección de datos, y (v) toda otra información necesaria para el justo procesamiento de los datos. [C-748 de 2011].
	Acceso, uso y circulación		a. El Articulador debe proveer los mecanismos necesarios para garantizar que sus bases de datos sean accesibles y seguras.

8	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.	accedidas solamente por personas conforme lo establecido en la Ley 1581 de 2012. b. El Articulador no puede conocer o enviar la información de los usuarios, salvo autorización expresa. c. El Articulador no puede realizar bases de datos o de los sistemas de intercambio de información que contengan datos de los usuarios. d. El Articulador debe proveer acceso y envío de información. e. El Articulador debe proveer técnicas, humanas y administrativas para la consulta, acceso o uso no autorizado de la información. f. El Articulador debe proveer técnicas, humanas y administrativas para prevenir el acceso fraudulento a la información. g. El Articulador debe proveer técnicas, humanas y administrativas para prevenir la divulgación no autorizada de la información. h. El Articulador debe proveer técnicas, humanas y administrativas para prevenir la utilización encubierta de datos. i. El Articulador debe proveer técnicas, humanas y administrativas para prevenir la contaminación de datos informáticos u otros. j. El Articulador debe proveer técnicas, humanas y administrativas para garantizar la revisión periódica de las herramientas de seguridad y la evaluación de su efectividad.
10	Confidencialidad	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 [Literal h) del artículo 4 de la Ley 1581 de 2012].	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

adecuada prestación del servicio, facilitando la entrega de servicios en línea a los ciudadanos, empresas y 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 que puedan dar cumplimiento a los requisitos que se encuentran relacionados a continuación, estos propios o tercerizados:

Tabla 18 - Requisitos técnicos para el Articulador

Componente o Capacidad	Requisitos mínimos
Servicios de Centro de Operaciones de Seguridad	El Articulador debe contar con un servicio de Centro de Operaciones de 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, asegure las condiciones de servicio. La gestión incluye la notificación de incidentes de seguridad a las entidades, una vez sucedido el evento.
Centro de Procesamiento de Datos (CPD)	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 I o mínimo Nivel III, en todos los aspectos entre ellos los de telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico: Centro de datos Concursos Públicos Mantenibles: disponibilidad del al menos 99.982%. Los centros de datos podrán estar alojados en un esquema de nube pública o híbrida siempre y cuando cumplan con lo establecido en el Capítulo IV Título V de la Circular Única de la SIC, sobre estándares de nivel de protección de datos personales para transferencia de datos personales a terceros y países que cuentan con un nivel adecuado de protección de datos personales.
Centro de Monitoreo de Red (CMR/NOC)	El Articulador deberá cumplir con las siguientes condiciones mínimas para el Centro de Monitoreo de Red: - Operación 7/24. - Construcción o refuerzo sísmico resistente. - Seguridad de acceso con guardia 7/24. - Sistemas de detección inteligente de incendio. - Seguridad física certificada. - CCTV digital. - Acceso de visitantes con cita previa y control de listas de acceso. - Operación, CAC (Centro de Atención a Clientes) y Monitoreo 7/24. - Sistemas de UPS configurados en redundancia. - Autonomía eléctrica de mínimo 24 horas en caso de interrupción del flujo de energía. - Control ambiental: sistemas de aire acondicionado redundantes. - Alimentación segura a los sistemas de control ambiental. Herramientas de monitoreo para la infraestructura de los diversos países utilizados. El Articulador debe proporcionar las herramientas y acceso necesario, para que la Agencia Nacional Digital (AND) pueda consultar el monitoreo de la infraestructura con gráficas en tiempo real, y puedan enviar mensajes de alerta al gestor.

Canal de conexión	El Articulador debe contar con doble canal de conexión al ofrecer los serv
Mesa de servicio/centro soporte	El Articulador debe disponer de un conjunto de recursos tecnológicos de para prestar servicios de soporte incluyendo un canal de atención p usuarios puedan reportar inconvenientes con el servicio y abrir tickets o fallas, así como peticiones, quejas, requerimientos y solicitudes. La mesa centro de soporte debe estar disponible 24 horas al día, 7 días a la se posibilidad de gestionar y solucionar todas las incidencias de mane efectuar el seguimiento a los tickets llevándolos a los niveles adecua cierre. El Articulador debe realizar y detallar el diseño de la solución de Mesa bajo mejores prácticas, como por ejemplo ITIL, para recibir, atender y casos de solicitud de servicio o incidentes que se reporten incluyendo soporte, monitoreo y seguimiento, trazabilidad, solución y cierre de to reportados por los usuarios. Todas las herramientas para la gestión de deben permitir una integración a diferentes tecnologías de soporte de serv Se debe asignar prioridad de solución a los tickets de acuerdo con la Ti Usuarios y la afectación del servicio, así: - Prioridad Alta - Emergencia, tiempo máximo de solución 4 horas: infraestructura atribuibles al Articulador y problemas operacionales de (Red, virtualización y configuración) entregados por el Articulador y que indisponibilidad crítica del negocio de la Entidad. - Prioridad Media - Degradación del servicio, tiempo máximo de soluci Fallas en la infraestructura y problemas operacionales de los servicios ; Articulador (Red, virtualización y configuración) entregados por el Arti afectan el desempeño o confiabilidad de los procesos de negocio de Solicitudes de asesoramiento para la configuración, implementación y ad de servicios. - Prioridad Baja - Solicitudes, tiempo máximo de solución 48 horas: S soporte menores o de información que no tienen impacto en los proceso de la Entidad, solicitud de información técnica de los servicios, se documentación de servicios, solicitudes de información y aclaraciones a y operación de los servicios.
Roles	El Articulador de los Servicios Ciudadanos Digitales deberán disponer o de trabajo idóneo que garantice la adecuada prestación de los se cumplimiento de los niveles de servicio acordados (ANS). Dentro de trabajo, el Articulador designará los siguientes roles, los cuales debe experiencia y conocimientos especializados en la materia, tales como: - Gerente/Director de Proyectos: gestión de proyectos. - Oficial/Delegado de protección de datos personales: Ley 1581 de decretos reglamentarios. - Oficial de Seguridad de la Información: ciberseguridad, ciberdefensa, la información y seguridad informática.

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 contempl

métodos lógicos y sistemáticos adecuados y efectivos para tal fin. El SARO debe ser implementado el número de usuarios y/o transacciones proyectados para los tres (3) primeros años de prestación 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 momento de prestación de sus servicios.

Para los anteriores efectos el Articulador deberán acreditar junto con la documentación el Manual de 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 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 sus grupos de interés sea oportuna y transparente.
- c. Objetivos de cumplimiento: se refiere a la observancia y acatamiento de los lineamientos de esta Ley 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 planea tener dentro de los tres (3) primeros años de actividad. Para lo anterior deberán contar con un plan 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 27001:2012 en Continuidad del negocio, ITIL v3 en Administración de los servicios TIC, ISO 24762 en Lineamientos sobre servicios de tecnología de la información y comunicación para recuperación ante desastres, National Institute of Standards and Technology - Special Publication NIST 800-53 Revision 4 en Seguridad y Privacidad de la Información, el estándar interamericano ISO/IEC 27001:2017 en Seguridad y Privacidad de la Información, el estándar internacional OWASP Top 10 Application Security Risks - 2017 y del Modelo de Seguridad y privacidad de la información definido por MinTIC. Además, los 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 de dos años en auditoría 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 y parches omitidos.

- Cadena de custodia de la evidencia recolectada que se solicite para los procesos de análisis forense lo establecido en la Norma ISO/IEC 27037:2012.

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

Capa de seguridad	Requisitos mínimos
Datos	- ACL (Lista de control de acceso para establecer privilegios de acceso a recursos) - Cifrado de la información con criptografía simétrica y/o asimétrica de acuerdo como lo establece la NIST) de longitud no inferior a 2048. - Asegurar las claves de acceso con almacenamiento por medio de dispositivos especialmente diseñado para protegerlas.
Aplicación	- WAF (Web Application Firewall) - Antivirus de nueva generación NGAV
Host	- HIDS (Host Intrusion Detection System) - Virtualización de host
Red interna	- Segmentación - Protocolo de accesos a un directorio. - IPSec - TLS/SSL
Perímetro	VPN (Virtual Private Network)
Seguridad física	- Seguridad en los accesos físicos al edificio. - Seguridad interna de salas. - Seguridad en los Racks de comunicaciones. - Control y filtrado de accesos. - Control medioambiental. - Control de energía.
Seguridad perimetral	- Sistema Anti DDoS (Distributed denial of service) - IDS (Intrusion Detection System) - IPS (Intrusion Prevention System) - Firewall de nueva generación NGFW - Balanceador de carga. - DMZ (demilitarized zone)
	- El Centro de Operaciones de Seguridad SOC debe tener la especificaciones: * Suministrar características UBA (User Behavior Analytics) para detectar indicadores de compromiso. * Realizar el monitoreo 7x24, y la gestión de incidentes y la administración de los componentes 7x24. * El triage de eventos e incidentes sean táctico y estratégico con cada una de las categorizaciones, informes, correlaciones, priorizaciones, clasificaciones, valoraciones y asignaciones. * Cubrir la respuesta técnica con: investigación, contención, recuperación y prevención a eventos e incidentes. - Deberá cumplir con las condiciones mínimas para el Centro de Operaciones de Seguridad

NOC establecidas en la Tabla Requisitos Técnicos.

- La plataforma de gestión de eventos e información de seguridad SIE (Information and Event Management) puede ser reconocida en el mercado como el encuentro líder en el cuadrante de Gartner.
- Servidor de registros (Syslog).
- Supervisión, Monitorización y Alarmas.
- Plataformas de mitigación.
- Metodología de evaluación, auditoría y acción de mejora sobre el incidente de ciberseguridad.
- Herramientas para el trabajo con logs, centralización y explotación de I.
- Sincronización de relojes con la Hora Legal Colombiana.
- Todos los servicios deben generar logs de las transacciones realizadas.
- Auditar toda actividad de los administradores de ESB- Habilitar la auditoría en el manejo de usuarios y grupos.
- Crear listas blancas y negras para realizar la validación de entradas.
- Habilitar auditoría en los procesos de reinicio y apagado.
- Copias de seguridad de los logs de transacción.
- Sistemas actualizados y parches de seguridad al día.

El Articulador debe proporcionar las herramientas y acceso web que se requiere para que MinTIC pueda consultar los canales e infraestructura con gráficas en tiempo real y con los siguientes indicadores de monitoreo:

- Accesos a Bases de Datos.
- Acceso a los logs.
- Reportes de los incidentes.
- Respuesta de incidentes.
- Los perfiles de los usuarios.
- Los roles de los administradores del sistema.
- Calidad del servicio.
- Privilegios del sistema.
- Estado de los recursos.
- Estado y nivel de respuesta de los Servicios.
- Informes de desempeño.
- Estado de las aplicaciones del sistema.
- Utilización de red.
- Espacio en disco.
- Métricas ANS.
- Métricas ITIL (KPIS).
- Reportes de ataques informáticos y de malware.

Se podrán contar con las siguientes características adicionales:

- Puede ser miembro de la organización global FIRST (Forum of Incident and Security Teams).
- Contar con la certificación en sistema de gestión de seguridad de la

12.4 REQUISITOS DE RED.

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

Lineamiento de seguridad	Requisitos mínimos
Confidencialidad	- Garantizar que los accesos a los servicios ciudadanos digitales estén autorizados. - Cifrar los canales de comunicación, para lo cual podrá usar los medios como HTTPS, establecer VPN o similares siempre y cuando se garanticen el cifrado
Integridad	- Garantizar la integridad de los mensajes utilizando mecanismos con valor probatorio que salvaguarden la completitud y precisión de la información - Garantizar el cifrado y la integridad de la información. - Canales Cifrados punto a punto.
Disponibilidad	- Garantizar el acceso a los Servicios Ciudadanos Digitales en el momento que y a los usuarios autorizados. - Mantener conexiones redundantes para alta disponibilidad. - Establecer los puertos abiertos necesarios para los servicios. - Proveer servicios de DNS redundantes con doble autenticación, control limitando y cifrando el tráfico y protegiendo la cache.
Autenticación	- Garantizar el manejo y validación de usuarios por medio de un protocolo de directorio que asegure la alta transaccionalidad de los usuarios. - Configurar el TCP Session Timeout en 900 segundos.
Autorización	- Determinar los grupos/roles que el usuario tiene asignado poseen el p consumir el servicio solicitado. - Establecer permisos a roles específicos para acceder a cada funcional servicios.
No repudio	- Asignar un usuario plenamente identificado a la entidad al momento de servicio para ser autenticado junto con el código de la entidad.
	- Establecer canales de comunicación cifrados. - Firmar el mensaje enviado con un certificado digital de propiedad de cada entidad.
Auditoría	- Proveen servicios para realizar operaciones Crear y actualizar transaccion eventos de la transacción, Registrar errores de la transacción. - Registro de transacciones del origen, el destino y quien hizo de transacción. - Centro de Operaciones de Red NOC - Planos de segmentación de las redes de Gestión y Servicio. - Virtualización de red - 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.

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 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 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 de acuerdo con los lineamientos de seguridad:

Lineamiento de seguridad	Requisitos mínimos
Confidencialidad	- Implementar criptografía simétrica y/o asimétrica (vigente de acuerdo como 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 posible. - Soportar W3C XML Encryption. - Implementar criptografía simétrica y/o asimétrica (vigente de acuerdo como 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 seguridad a los Servicios Web con estándar vigente en el mercado y previa vta MinTIC
Autenticación	- Hay que asegurar que todas las páginas y recursos por defecto, requieren un 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 seguridad a los Servicios Web con estándar vigente en el mercado y previa vta 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 función. - Solicitar usuario y contraseñas únicos e irrepetibles, para todos los sistemas.
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 de Application Security Verification Standard (ASVS) de OWASP. - Comprobación de control de acceso para asegurar que el usuario está autorizado para acceder. - Realizar mínimo dos pruebas de análisis y detección de vulnerabilidades respectivo Re-test cada año. - Plan de mitigación de vulnerabilidades.
No repudio	- Soportar W3C XML Digital Signature como posible opción de estándar de firma electrónica. - Soportar Web SSO Metadata Exchange protocol

12.6 ALMACENAMIENTO DE INFORMACIÓN.

Los Servicios Ciudadanos Digitales, en especial el Servicio de Interoperabilidad y Carpeta Ciudadana realizará almacenamiento de los datos que se intercambian entre usuarios. El servicio de Autenticación y Carpeta Ciudadana Digital, realizará el almacenamiento de la información de los usuarios registrados 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, auditoría del sistema, entre otros, deberán mantenerse accesibles durante la prestación del servicio y 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 servicios que presta el Articulador, debe ser seguro y garantizar la privacidad de los datos de los ciudadanos. En este sentido, el Articulador debe recibir la máxima atención por parte del Articulador en el sentido, el tratamiento de datos personales, incluido el tratamiento de datos sensibles, de los diferentes servicios que presta el Articulador.

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 Articulador 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 y las normas que la modifiquen, deroguen o subroguen, sin perjuicio de las obligaciones que establece el artículo [1078](#) de 2015. La prestación de servicios ciudadanos digitales se encuentra sometida al cumplimiento de las normas 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
Evaluación de Impacto Decreto o Privacidad prestación	Se debe cumplir con lo definido en el Artículo 2.2.17.5.2 (PIA) 1078 de 2012, en la 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 (Privacy Assessment), realizando el análisis de riesgos que los SCD puede presentar en el ejercicio del 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 prestación del servicio y deberá contener como mínimo: - Análisis en profundidad de cada uno de los SCD, adoptando medidas de mitigación internacionalmente, identificando los tipos de datos personales objeto de tratamiento de los titulares de los mismos, los flujos de información desde su recolección hasta su disposición final y las tecnologías utilizadas. - Una descripción detallada de las operaciones de tratamiento de datos personales que involucra la prestación de los SCD y de los fines del tratamiento. - Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad. - Una identificación y evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales, valoración de la probabilidad de que ocurran y el daño que causarían si se materializaran. - Determinación de los controles y las medidas previstas para afrontar los riesgos, mitigar, transferir o aceptar los riesgos, incluidas garantías, medidas de control y monitoreo de los riesgos, tecnologías y mecanismos que garanticen la protección de datos personales, pudiendo realizar diseño de software, políticas de privacidad, cuenta los derechos e intereses legítimos de los titulares de los datos, personas eventualmente afectadas, y responsables de implementar dichas medidas. - Verificación de que el servicio cumple con la Ley 1581 de 2012, los reglamentos y demás normativa aplicable a la protección de datos personales. Por otro lado, el Articulador deberá presentar a MinTIC, los resultados de la evaluación junto con los controles y las medidas para eliminar o mitigar los riesgos. Una vez se haya iniciado la prestación efectiva del servicio de Interacción Ciudadana digital y carpeta ciudadana digital, el Articulador deberá realizar la revisión y actualización periódica, durante toda la prestación del servicio, de los resultados de la evaluación. En el momento en el que el Articulador considere pertinente adelantar la correspondiente revisión y actualización de la evaluación, deberá considerar los siguientes dos años de la prestación del servicio contados

	momento de realización de dicha revisión, verificando si se han creado nuevos riesgos o se han detectado otros que habían pasado desapercibidos. Estos riesgos serán utilizados para actualizar la Evaluación de Impacto en la Privacidad cuando sea necesario.
Privacidad desde el Diseño y por Defecto (PbD)	Se debe cumplir con lo definido en el Artículo 2.2.17.5.5 del decreto 107 de 2015. Así mismo, el Articulador está en la obligación de cumplir con las actividades relativas a la privacidad por diseño y por defecto: - 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. - Toma de medidas proactivas, anticipándose y previniendo la pérdida de información antes que suceda. - Aplicar las medidas técnicas, humanas y organizativas apropiadas para el tratamiento de los datos personales que solo sean necesarios para las finalidades específicas del tratamiento (minimización de los datos). - Seudonimización de los datos a través de técnicas de cifrado de acuerdo con la clasificación de la información. - 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. - Incorporar las prácticas y los procesos de desarrollo necesarios, para garantizar la salvaguarda de la información personal de los actores y usuarios, proporcional a la naturaleza jurídica, tamaño empresarial, la naturaleza de los datos, el tipo de tratamiento, el tipo de tratamiento, los riesgos potenciales, etc., durante la prestación de los servicios y durante cinco (5) años luego de haber finalizado las actividades como Articulador / prestador del servicio, conforme lo establece la sección "Almacenamiento de Información" de este Manual. Mantener las prácticas y procesos de gestión adecuados durante el ciclo de vida de los datos que son diseñados para asegurar que los sistemas de información cumplan con los requisitos, políticas y preferencias de privacidad de los actores. - Uso de los máximos medios posibles necesarios para garantizar la 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. - Asegurar la infraestructura, sistemas TI, y prácticas de negocios que impliquen el uso de cualquier información personal siendo razonablemente segura y sujeta a verificación independiente por parte de todas las partes involucradas incluyendo usuarios y entidades públicas.
Responsabilidad Demostrada (accountability) Tratamiento de datos personales (Ley 1581 de 2012)	Se debe cumplir con lo definido en el Artículo 2.2.17.5.3 del decreto 107 de 2015. Responsabilidad demostrada y programa integral de gestión de datos personales. Los prestadores de servicios ciudadanos digitales deberán adoptar medidas efectivas y verificables que les permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deberán implementar un Programa Integral de Gestión de Datos Personales. En la prestación de los Servicios Ciudadanos Digitales, el Articulador debe: - El Programa Integral de Gestión de Datos Personales PIGDP debe estar alineado a los lineamientos de la Superintendencia de Industria y Comercio, en particular en la implementación de la responsabilidad demostrada (accountability) de acuerdo con 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 lo

	constitucionales, legales y reglamentarias de cada autoridad pública y/o p cumpla funciones públicas, y los límites que impone la Ley de Transpa Derecho de Acceso a la Información Pública Nacional, Ley 1712 de 2014, que la modifiquen, deroguen o subroguen - Garantizar el cumplimiento de los derechos consagrados en los artículos. Constitución Política y de la normatividad colombiana vigente y aplicabl los principios, derechos y obligaciones de la Ley 1581 de 2012 de Protecc Personales, del Capítulo 25 del Decreto único reglamentario del secto industria y turismo - 1074 de 2015- y de la Guía para la implemen Responsabilidad Demostrada de la SIC. - Diseñar, implementar y promulgar un manual interno de políticas y pro basado en el ciclo interno de la gestión de los datos personales, que conter e indicadores que arrojen resultados medibles sobre el grado de cumplimiento de la normativa, así como los mecanismos para la atención de las peticiones y reclamos presentados por los titulares en ejercicio de s hábeas data. - Diseñar y aprobar una Política de Tratamiento de la Información Personal tratamiento y finalidades de la información personal en el servicio de Inter autenticación digital y carpeta ciudadana digital, que contenga como establecido en el Artículo 2.2.2.25.3.1. del Decreto 1074 de 2015. - Publicar, socializar a los actores involucrados establecidos en el Artícul del DUR-TIC y garantizar el entendimiento y apropiación de la Política de de la Información Personal por parte de los usuarios, en el interoperabilidad. Realizar una revisión periódica de la Política de Tratamiento de la Personal y efectuar los cambios y actualizaciones pertinentes conforme del servicio de Interoperabilidad, Autenticación Digital y Carpeta Ciudadana informar a los usuarios y actores sobre los cambios sustanciales - rea Política. - Utilizar Avisos de privacidad, en los casos que no sea posible poner a di los usuarios la Política de Tratamiento de la Información, cumpliendo con mínimo establecido en el Artículo 2.2.2.25.3.3. del Decreto 1074 de 2015. - Realizar el proceso de debida diligencia para el diseño, revisión e implem un Programa Integral de Gestión de Datos Personales, a la luz de la (Implementación del Principio de Responsabilidad Demostrada (Account Superintendencia de Industria y Comercio y de las Evaluaciones de In Privacidad o en la Protección de Datos. - Establecer reglas de conducta, perfiles de acceso y confidencialidad para involucradas en el diseño, desarrollo, operación o mantenimiento de cualc de archivos, o en mantener algún registro.
Oficial de Protección de datos	Se debe cumplir con lo definido en el Artículo 2.2.17.5.4. Oficial de p datos. De conformidad con el artículo 2.2.2.25.4.4. del Decreto 1074 de responsable y encargado del tratamiento de datos deberá designar a una p que asuma la función de protección de datos personales, quien dará t solicitudes de los Titulares para el ejercicio de los derechos a que se refiere de 2012 y del capítulo 25 del Decreto 1074 de 2015; y quien deberá cumplir los lineamientos de la Superintendencia de Industria y Comercio, la guía para la implementación de la responsabilidad demostrada (accou dicha entidad, realizar las siguientes actividades en cuanto a los datos de de los servicios ciudadanos digitales: 1. Velar por el respeto de los der titulares de los datos personales respecto del tratamiento de datos q prestador de servicios ciudadanos digitales. 2. Informar y asesorar al

	servicios ciudadanos digitales en relación con las obligaciones que les virtud de la regulación colombiana sobre privacidad y tratamiento de dato 3. Supervisar el cumplimiento de lo dispuesto en la citada regulación y en de tratamiento de información del prestador de demostrada. 4. Prestar el as que se le solicite acerca de la evaluación de impacto relativa a la protecció Atender los lineamientos y requerimientos que le haga la Delegatura de F Datos Personales de la Superintendencia de Industria y Comercio o qu veces. Todo lo anterior de conformidad a los límites que impone Transparencia y del Derecho de Acceso a la Información Pública Nacion de 2014.
Roles asignados, responsabilidades, y rendición de cuentas	El Articulador identificará las funciones generales y específicas y las resp para la gestión y uso de información personal, además de garantizar la cuentas para cumplir estas responsabilidades. Para esto deberá: - Designar un Oficial de Privacidad o Protección de Datos responsable de cumplimiento de la Política de Tratamiento de la Información, el Manu políticas y procedimientos, de las medidas legislativas, reglamentarias, y o propuestas, las evaluaciones de impacto en la privacidad, del imp tecnologías de información personal, y tecnologías que permiten la audito de conformidad con las políticas y prácticas de privacidad establecidas. - Identificar las personas que diariamente tienen la responsabilidad en la del Articulador de la ejecución de los procedimientos y políticas de pri cumplimiento normativo; designar un funcionario de alto nivel apropiado (C CIO) para servir como contacto principal del Articulador para asuntos c /web y las políticas de privacidad de la información. - Establecer un Comité de Privacidad o Protección de Datos que apoye Oficial de Privacidad o protección de datos, para supervisar y co componentes y la aplicación de los programas, así como las evaluaciones de cuentas. Todos los empleados y contratistas del Articulador deben tener conocimie normativa de protección de datos personales, el Programa Integral de Gest Personales, la Política de Tratamiento de la Información Personal tratamiento de los datos personales y el seguimiento de las medidas c pertinentes, además de ser conscientes de la privacidad y su obligación pa información en forma identificable.
Sensibilización y programas de capacitación basado en funciones	El Articulador deberá garantizar que los administradores y usuarios de la personal de su organización sean conscientes de los riesgos de privacidad con sus actividades y de las leyes aplicables, políticas y procedimientos con la privacidad, para lo cual tendrá que: - Crear una cultura organizacional entorno a la privacidad y la protecc personales. - Capacitar regularmente en la normativa a cada persona implicada, sol tratamiento de datos personales, medidas de seguridad, las reglas de sanciones en caso de incumplimiento. - Informar y educar a los empleados y contratistas sobre su responsa proteger información en forma identificable. - Asegurarse de que todo el personal está familiarizado con las leyes de p datos personales y privacidad de la información, reglamentos y políticas y implicaciones que conlleva el acceso inadecuado, revelación y/o u personales sin estar autorizado para ello, conforme lo establecido por el A de la Ley 1273 de 2009. - Impartir una formación adaptada específicamente a las funciones del

	maneja datos personales. Esta formación debe ser permanente e incluir la actualización periódica en el contenido del Programa Integral de Gestión de Datos Personales y los resultados de las Evaluaciones de Impacto en la Privacidad. Conservar el debido soporte de todas las capacitaciones.
Publicación	El Articulador, en la prestación de los Servicios Ciudadanos Digitales deberá publicar: - La Política de Tratamiento de la Información Personal. - Avisos de Privacidad que informen la existencia de la Política de Tratamiento de la Información Personal. - El canal establecido para atender las consultas y reclamos de los titulares de datos personales. - El procedimiento para la recepción, atención y respuesta a las consultas por datos personales.
Derechos individuales. Participación individual	El Articulador deberá garantizar a los actores el pleno y efectivo ejercicio de sus derechos, estableciendo un canal de atención de consultas y reclamos de datos personales, además de dar respuesta a los mismos en los plazos establecidos en la Ley 1581 de 2012.
Notificación	El Articulador deberá - Notificar a MinTIC cualquier dato o registro de un actor sea solicitud de información, entidad pública o administrativa en ejercicio de sus funciones legales o judiciales. - Adoptar tecnologías que permitan alertar a las entidades de forma automática sobre cambios en las prácticas de privacidad y seguridad. - Garantizar confidencialidad, integridad y autenticidad, teniendo las medidas de seguridad necesarias.
Suministro de información	El Articulador solo podrá suministrar información a: - Los titulares de datos personales, sus causahabientes o representante legal. - A las entidades públicas o administrativas en ejercicio de sus funciones legales o judiciales. - A terceros autorizados por el titular o por la ley. - Garantizar confidencialidad, integridad y autenticidad, teniendo las medidas de seguridad necesarias.
Autorización y Finalidad	El Articulador deberá solicitar la autorización previa e informada para el tratamiento de datos personales a todos los titulares de los cuales recolecte información cuando en la prestación del servicio se requiera, conforme los requisitos establecidos en la Ley 1581 de 2012 y sus decretos reglamentarios. De igual forma, deberá almacenar copia de la autorización otorgada por los titulares en los casos en los que solicitan autorización. El Articulador debe garantizar que utilizará la información personal solo para las finalidades autorizadas por el titular, las cuales deben ser pertinentes y adecuadas al caso de requerir el tratamiento de la información para finalidad diferente a la que solicitó una nueva autorización al titular.
	El Articulador deberá garantizar que la información personal se utilice solo para las finalidades previstas en la autorización del tratamiento de datos personales y para las finalidades pertinentes de la prestación del servicio de interoperabilidad, Autenticación y

Uso aceptable	carpeta ciudadana digital. Los datos personales y los datos enviados a través del servicio de interoperabilidad serán tratados en los servicios de Autenticación Digital y Carpeta Ciudadana Digital. En general la información generada, producida, enviada o compartida en la prestación del servicio no podrán ser objeto de comercialización ni de explotación económica en ningún tipo.
Cadena de confianza	Todo subcontratista o proveedor del Articulador, que actúe en su calidad de proveedor para desarrollar servicios sobre un sistema de registros, debe cumplir con los requisitos enumerados en esta sección sobre privacidad y protección de datos personales.
Monitoreo y medición	El Articulador debe llevar a cabo y estar preparado para informar de los resultados de las evaluaciones y auditorías de las actividades encomendadas por la Ley 1712 de 2014 sobre Protección de datos personales y aplicaciones de buenas prácticas de gestión, incluyendo contratos, registros, los usos de rutina, exenciones, excepciones, violaciones y sistemas de registros.
Notificación y respuesta ante incidentes	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 competente de datos personales, y deberá: - Informar a MinTIC sobre cualquier incidente de seguridad que afecte la confidencialidad, disponibilidad e integridad de la información personal con el servicio de interoperabilidad, Autenticación Digital y Carpeta Ciudadana Digital, las acciones de mitigación o solución del incidente, acciones implementadas. - Documentar los resultados de las auditorías de cumplimiento, acciones implementadas para remediar las deficiencias identificadas de cumplimiento. - Reportar los incidentes a los usuarios titulares de la información afectada 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. - Realizar las acciones de mejora para eliminar y prevenir futuros incidentes. - 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 y las normas que la modifiquen, deroguen o subroguen.
Registro Nacional de Bases de Datos - RNDB	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 Datos - RNBD-, conforme lo establecido en el Capítulo 26 del título 2 del Decreto Único Reglamentario del sector Comercio, Industria y Turismo -1074 de 2018, deberá actualizar sus bases de datos personales y la información contenida en el Registro Nacional de Bases de Datos -RNBD-, con la información personal sujeta a tratamiento por la prestación de los SCD y las bases de datos creadas o que se puedan crear o modificar por la prestación del servicio 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.

14. ANS DE LOS SERVICIOS CIUDADANOS DIGITALES, SCD.

Con el objetivo de articular las condiciones y términos que regularán la prestación de los Servicios Digitales, El Articulador informará a MinTIC los niveles de servicio (Acuerdos de Nivel de Servicio). 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 el servicio prestado, siguiendo el lineamiento LI.ST.08. Acuerdos de Nivel de Servicios del Marco 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 fiabilidad 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 acuerdo 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 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 disponible 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	Medida
1	Disponibilidad	La disponibilidad se mide usando la siguiente ecuación: $(1 - (\text{Número total de minutos en que el servicio no está disponible} / \text{Número de días en el mes} \times 24 \text{ horas} \times 60 \text{ minutos})) \times 100\%$. 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.	Disponibilidad $\geq 99.98\%$
2	RTO	El RTO por sus siglas en inglés es Recovery Time Objective o en español Tiempo Objetivo de Recuperación. 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.	RTO ≤ 8
3	Interrupciones máximas	El ANS de Interrupciones máximas hace referencia al número máximo de interrupciones durante el período observado (mensual). 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.	Interrupciones máximas ≤ 1
4	MTBF	El MTBF por sus siglas en inglés es Mean Time Between Failures o en español Tiempo Medio Entre Fallas. El MTBF es un indicador de confiabilidad definido como el promedio aritmético acumulado del tiempo entre fallas, asumiendo que los Servicios Ciudadanos Digitales se	MTBF > 4320 horas

		recuperan de forma inmediata cuando se produce la falla. Una falla se define como una degradación los Servicios Ciudadanos Digitales con respecto a las condiciones pactadas para la prestación del servicio 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.	
5	Latencia	Mide el tiempo promedio en el mes, por servicio, que tarda una transacción en ir y volver entre los siguientes puntos: - Desde la Entidad, hasta el Articulador. - Desde el Articulador, hasta la Entidad. 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.	Latencia m
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 d ser mayor ancho 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 me comunicación garanticen la confidencialidad, integridad, disponibilidad, autenticación, autorización repudio y auditoria que se requieren para el intercambio seguro de datos que viajan a través de los s asociados. A continuación, se muestra el lineamiento de seguridad y el requisito mínimo que debe c

Tabla 20 - Lineamientos de seguridad y requisitos mínimos

Lineamiento de seguridad	Requisitos mínimos
Confidencialidad	- Garantizar que los accesos a los Servicios Ciudadanos Digitales estén autorizados. - Cifrar los canales de comunicación entre las entidades y el articulador.
Integridad	- Garantizar la integridad de los mensajes utilizando mecanismos con v probatorio que salvaguarden la completitud y precisión de la intercambiada. - Garantizar el cifrado y la integridad de la información en todas las realizadas a los Servicios Ciudadanos Digitales
Disponibilidad	- Garantizar el acceso a los Servicios Ciudadanos Digitales en el mon requiera y a los usuarios autorizados. - Mantener conexiones redundantes para alta disponibilidad de lo Ciudadanos Digitales. - Establecer los puertos abiertos necesarios para los Servicios Ciudadanos l - Proveer servicios de DNS redundantes con doble Autenticación, control limitando y cifrando el tráfico y protegiendo la memoria caché.
Autenticación	- Garantizar el manejo y validación de usuarios por medio de un protocolo un directorio que asegure la alta transaccionalidad de los usuarios. - Configurar el TCP Session Timeout en 900 segundos.
Autorización	- Determinar los grupos/roles que el usuario tiene asignado poseen el p acceder a los Servicios Ciudadanos Digitales. - Establecer permisos a roles específicos para acceder a cada funciona Servicios Ciudadanos Digitales.
No repudio	- Asignar un usuario plenamente identificado a la entidad al momento de i Servicios Ciudadanos Digitales para ser autenticado junto con el código de - Firmar el mensaje enviado con un certificado digital de propiedad de cada

Auditoría	- Proveer servicios para realizar operaciones crear y actualizar transacciones, eventos de la transacción, registrar errores de la transacción. - Registro de transacciones del origen, el destino y quién hizo de transacción. - Centro de Operaciones de Red NOC. - Planos de segmentación de las redes de Gestión y Servicio. - Virtualización de red. - 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 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 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 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 tarifas que no hayan sido expresamente aceptados por los usuarios y autorizados por el Ministerio de Tecnología e 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 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 será realizada por cada uno de los organismos del Estado que en el marco de sus competencias tengan que ver con 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.

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, incluyen 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 f para su tratamiento.
- d. Las medidas técnicas, humanas y administrativas que se emplearán para garantizar su custodia y 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 general y de aquellos específicos para la formulación de peticiones, quejas y reclamos, incluyendo consultas y reclamos por datos personales.
- f. Adicionalmente, el Articulador deberá indicar las condiciones para la prestación del Servicio para edad y dependientes, estableciendo los requisitos para el registro, los derechos, obligaciones y proh

2. Condiciones de uso de las credenciales de autenticación:

Descripción de las condiciones de uso de las credenciales de autenticación que el operador entregue 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 p dichos derechos.
- b. Opción de seleccionar, conforme al catálogo de entidades con sus servicios o trámites, aquellas c desea interactuar.
- c. Opción de gestionar y revocar sus autorizaciones, para recibir información y comunicaciones des entidades públicas.
- d. Opción de compartir información con otros usuarios del servicio, con entidades públicas o tercer

4. Condiciones para el tratamiento de datos personales:

- a. El Articulador deberá indicar que cuenta con una política de tratamiento de la información perso dónde puede ser consultada.
- a. Que realiza evaluaciones de impacto sobre el tratamiento de datos personales y que cuenta con u integral de gestión de datos personales.
- b. El Articulador deberá indicar el tratamiento al que se encuentran sujetos los datos personales sen menores de edad.

5. Política de seguridad de la información: el Articulador debe garantizar que toda la información q el marco de los Servicios Ciudadanos Digitales está protegida y custodiada bajo los más estrictos e seguridad y privacidad, para ello deberá indicar que cuenta con una Política de Seguridad de la Info

indicando dónde puede ser consultada.

6. Referencias de las políticas: pueden especificarse las referencias a políticas de calidad y servicio definidas frente al servicio.

7. Supresión de la información: el Articulador debe especificar las condiciones y los procedimientos para la supresión de la información del usuario. Estos procedimientos deben estar acordes con los r asociados al tratamiento de datos personales en cada una de las etapas e incluir controles coherente la supresión (borrado seguro) de la información.

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

<NOTAS DE PIE DE PÁGINA>

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

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

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

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

ANEXO 2. GUÍA PARA LA VINCULACIÓN Y USO DE LOS SERVICIOS CIUDADANOS DIGITALES
<Anexo modificado por el Anexo 2 versión de mayo 2023. El nuevo texto es el siguiente:>

Notas de Vigencia

- Guía para vinculación y uso de los servicios ciudadanos digitales, actualizado.

Legislación Anterior

Texto original de la Resolución 2160 de 2020:

Consulte [aquí el anexo original](#).

Mayo de 2023

Ministerio de Tecnologías de la Información y las Comunicaciones

Viceministerio de Transformación Digital

Dirección de Gobierno Digital

Equipo de trabajo

Mauricio Lizcano - Ministro de Tecnologías de la Información y las Comunicaciones

Sindey Carolina Bernal Villamarín – Viceministra de Transformación Digital

Ana María Sterling Bastidas - Directora de Gobierno Digital

José Ricardo Aponte Oviedo – Equipo Servicios Ciudadanos Digitales

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

Equipo Subdirección de Estándares y Arquitectura de TI

Subdirección de Servicios Ciudadanos Digitales - Agencia Nacional Digital

Versión	Observaciones
Versión 1 Septiembre 2020	Guía para vinculación y uso de los servicios ciudadanos digitales
Versión 2 Mayo de 2022	Actualización de la vinculación a cada servicio

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico:
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 A Internacional.

Tabla de Contenido

1	INTRODUCCIÓN
2	ALCANCE DE LA GUIA
	DEFINICIONES
4	MARCO NORMATIVO
5	SERVICIOS CIUDADANOS DIGITALES
6	PROCESO DE VINCULACIÓN AL SERVICIO DE INTEROPERABILIDAD
6.1	INTEROPERABILIDAD
6.2	MARCO DE INTEROPERABILIDAD PARA GOBIERNO DIGITAL
6.2.1	PRINCIPIOS DE INTEROPERABILIDAD
6.2.2	DOMINIOS DEL MARCO DE INTEROPERABILIDAD
6.2.2.1	DOMINIO POLÍTICO – LEGAL
6.2.2.2	DOMINIO ORGANIZACIONAL
6.2.2.3	DOMINIO SEMÁNTICO
6.2.2.4	DOMINIO TÉCNICO

6.3.	SERVICIO DE INTERCAMBIO DE INFORMACIÓN	
.....		
6.4.	PLATAFORMA DE INTEROPERABILIDAD - PDI	
.....		
6.5.	X-ROAD	
.....		
6.5.1.	DESCRIPCIÓN GENERAL DE X-ROAD	
6.5.2.	DESCRIPCIÓN DE LA ARQUITECTURA DE X-ROAD	
6.6.	VINCULACIÓN AL SERVICIO DE INTEROPERABILIDAD	
.....		
6.6.1.	METODOLOGÍA	
6.6.2.	REQUERIMIENTOS	
6.6.3.	RIESGOS DE NO CONTAR CON LOS AMBIENTES DEFINIDOS DE X-ROAD	
6.6.4.	PROCESO DE INSTALACIÓN Y CONFIGURACIÓN DE X-ROAD	
6.6.5.	CARACTERÍSTICAS DE LOS CERTIFICADOS	
6.6.6.	PROCESO DE SOLICITUD DE CERTIFICADOS DIGITALES (FIRMA, AUTENTIC PARA ENTIDADES PÚBLICAS	
6.6.7.	PROCESO DE SOLICITUD DE CERTIFICADOS DIGITALES PARA ENTIDADES PRI	
6.6.8.	CONDICIONES TÉCNICAS DE LOS CERTIFICADOS QUE DEBEN PROPORCION, ENTIDADES PRIVADAS	
6.7.	INTERVENCIÓN DE LOS SERVICIOS Y ADAPTADOR DE TRANSFORMACIÓN DE SERVICIOS	
.....		
6.7.1	COMPONENTE ADAPTADOR DE TRANSFORMACIÓN PARA EL CONSU EXPOSICIÓN DE SERVICIOS WEB EN X-ROAD	
6.8.	ACUERDO DE VINCULACIÓN	
.....		
6.9.	USO Y APROPIACIÓN	
.....		
7	PROCESO DE VINCULACIÓN AL SERVICIO DE AUTENTICACIÓN DIGITAL	
7.1	OBJETIVOS DEL SERVICIO	
.....		
7.2	REQUERIMIENTOS	
.....		
7.3	PREPARACIÓN	
.....		
7.4	ADECUACIÓN	
.....		
7.5	INTEGRACIÓN	
.....		

-	7.5.1 EMPLEO DE LIBRERÍAS (CONNECT)
-	7.5.2 EMPLEANDO SERVIDOR INTEGRACIÓN (CONNECT)
-	7.5.3 IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD
7.6	INTEGRACIÓN DE LA ENTIDAD COMO FUENTE DE ATRIBUTOS
7.7	INTEGRACIÓN DE ENTIDADES PÚBLICAS COMO PRESTADORAS DEL SERVICIO
7.8	RECOMENDACIONES DE SEGURIDAD
7.9	USO Y APROPIACIÓN
8	PROCESO DE VINCULACIÓN AL SERVICIO DE CARPETA CIUDADANA DIGITAL
8.1	REQUERIMIENTOS
8.2	PREPARACIÓN
8.3	ADECUACIÓN
8.4	INTEGRACIÓN
9	MESA DE SERVICIO DE LOS SERVICIOS CIUDADANOS DIGITALES

Lista de Ilustraciones

Figura 1	Problemática a resolver
Figura 2	Marco de interoperabilidad
Figura 3	Componentes de la PDI
Figura 4	Modelo Conceptual de la PDI operada con X-ROAD
Figura 5	Arquitectura de componentes de la PDI
Figura 6	Metodología para la instalación y configuración de los ambientes requeridos para el servicio de seguridad
Figura 7	Proceso de solicitud de certificados
Figura 8	Proceso de firma de certificados
Figura 9	Proceso de solicitud de certificados privados
Figura 10	Proceso de firma de certificados privados
Figura 11	Arquitectura de referencia con Adaptador de Transformación de Servicio
Figura 12	Diagrama de despliegue del Adaptador de integración

Figura 13 Componente del servicio de Autenticación Digital	
Figura 14 Road Map para la integración como fuente de atributo	
Figura 15 Diagrama de componentes carpeta ciudadana digital.....	

1. INTRODUCCIÓN.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), de acuerdo con la Ley 1712 de 2014, desarrolla políticas y planes enfocados a las Tecnologías de la Información y las Comunicaciones. Estas políticas y planes constituyen un componente vital para el crecimiento y desarrollo del sector, con el fin de brindar acceso a la población, en el marco de la expansión y diversificación de las TIC.

Con base en lo anterior, MinTIC tiene establecido dentro de sus funciones: “1. Diseñar, adoptar y promover 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 sus beneficios”. En este sentido, MinTIC ha conceptualizado y diseñado un modelo integral que incorpora 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 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 el modelo colombiano para que funcione como una sola institución que le brinde a los ciudadanos información 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, presentar a las entidades públicas la información del modelo y cómo debe preparar la vinculación para hacer uso de ellos en su proceso de transformación digital, se determinan los estándares, modelos, lineamientos y requisitos técnicos específicos de vinculación de los Servicios Ciudadanos Digitales.

2. ALCANCE DE LA GUÍA.

El presente documento presenta el modelo de los Servicios Ciudadanos Digitales (SCD), destinado a las autoridades referidas en el artículo [2.2.17.1.2](#) del Decreto 1078 de 2015, indicando las condiciones 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 integrar a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad, carpeta ciudadana digital.

En esta guía se dan algunas indicaciones para permitir la compatibilidad de aplicaciones, así como la operación y desarrollo de los servicios que las entidades públicas deben ofrecer. Sin embargo, está fuera del alcance la definición de los protocolos de comunicación, los tipos de bases de datos, y las soluciones tecnológicas concretas de los componentes de la plataforma.

3. DEFINICIONES.

A los efectos de la presente guía se deberán seguir los conceptos señalados en el artículo [2.2.17.1.4](#) 1078 de 2015 que define los lineamientos generales en el uso y operación de los servicios ciudadanos en especial los siguientes:

1. Autenticidad: Es el atributo generado en un mensaje de datos, cuando existe certeza sobre la persona que ha elaborado, emitido, firmado, o cuando exista certeza respecto de la persona a quién se atribuya los datos.
2. Articulador: Es la Agencia Nacional Digital, que será encargada de proveer y gestionar de manera 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.
3. Disponibilidad: Es la propiedad de la información que permite que ésta sea accesible y utilizable cuando se requiera.
4. 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 que el Articulador de los SCD debe cumplir con el fin de garantizar la correcta prestación de los servicios a los ciudadanos digitales.
5. Guía para la vinculación y uso de los Servicios Ciudadanos Digitales: Es el documento expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones destinado a las autoridades en el artículo [2.2.17.1.2](#) del Decreto 1078 de 2015, que indica cuáles son las condiciones necesarias que deben realizar para la preparación, adecuación, integración, uso y apropiación de los servicios digitales, a través de los cuales podrán vincular a sus sistemas de información los mecanismos de interoperabilidad digital, interoperabilidad y carpeta ciudadana digital.
6. Integridad: es la condición que garantiza que la información consignada en un mensaje de datos sea completa e inalterada, salvo la adición autorizada de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.
7. 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 presentar por niveles más detallados.
8. Marco de interoperabilidad: Es la estructura de trabajo común donde se alinean los conceptos y conceptos 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⁽¹⁾
9. Mecanismos de autenticación: 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.
10. Modelo: representación de una realidad, definida de forma correcta y suficiente mediante conceptos, instancias, atributos, valores y relaciones.
11. La Plataforma De Interoperabilidad – PDI: son el conjunto de herramientas necesarias que permiten que los sistemas de información del Estado conversen entre sí mediante interfaces estándar de comunicación y procesos y sistemas de información.

12. Prestadores de Servicios Ciudadanos Digitales: Entidades pertenecientes al sector público o privado, 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 el Ministerio de Tecnologías de la Información y las Comunicaciones.

13. Privacidad por diseño y por defecto: Desde antes que se recolecte información y durante toda la 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 recolección de información y de las infraestructuras que lo soportan.

14. Servicios Ciudadanos Digitales: Es el conjunto de soluciones y procesos transversales que brindan 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. Los servicios se clasifican en servicios base y servicios especiales.

15. 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.

16. 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, se refieren a innovaciones que realizan los prestadores de servicio a partir de la autorización dada por el titular y de la integración a los servicios ciudadanos digitales base, bajo un esquema coordinado por el Articulador.

17. Single Sign-On (SSO): Ocurre cuando un usuario inicia sesión en una aplicación y luego inicia sesión en otras aplicaciones automáticamente, independientemente de la plataforma, la tecnología o el dominio, utilizando el usuario.

18. Single Log-Out (SLO): Permite que un usuario cierre sesión en todos los sitios y aplicaciones al finalizar la sesión creada.

19. 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.

20. 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.

4. MARCO NORMATIVO.

La Constitución Política en su artículo [2](#) establece como uno de los fines esenciales del Estado “(…) 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, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se disponen” y el Decreto 2364 de 2012, por medio del cual se reglamenta el artículo [7](#) de la Ley 527 de 1999 sobre la firma electrónica, 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...

Que de conformidad con el artículo [266](#) de la Constitución Política modificado por el Acto Legislativo

de julio de 2015, en concordancia con el Decreto Ley [2241](#) de 1986 y el Decreto Ley 1010 de 2000, a la Registraduría Nacional del Estado Civil ejercer, entre otras, la dirección y organización de las entidades del registro civil y la identificación de las personas.

Conforme al principio de “masificación del gobierno en línea” hoy Gobierno Digital, consagrado en el artículo 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 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 (...),” 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 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 por un nuevo país”, atribuye al Ministerio de Tecnologías de la Información y las Comunicaciones la coordinación con las entidades responsables de cada uno de los trámites y servicios, la función de expedir los estándares, modelos, lineamientos y normas técnicas para la incorporación de las TIC, que serán adoptados por las entidades estatales, incluyendo, entre otros, autenticación electrónica, integración de sistemas de información de trámites y servicios de las entidades estatales con el Portal del Estado Civil, 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 (DUR-TIC), “Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”, el Gobierno Digital se desarrolla a través de un esquema que articula los elementos que la componen, como son: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, para lograr su objetivo.

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 esa ley. Queda establecido en el Plan Nacional de Desarrollo 2018 -2022” 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 de los servicios ciudadanos digitales, (carpeta ciudadana, autenticación electrónica e interoperabilidad de sistemas del Estado), de forma paralela a la definición y adopción de estándares tecnológicos, al mejoramiento de la arquitectura TI, a la articulación del uso de la tecnología, y todo lo anterior en el marco de la seguridad.

El artículo [147](#) de la Ley 1955 de 2019, señala la obligación de las entidades estatales del orden nacional incorporar en sus respectivos planes de acción el componente de transformación digital, siguiendo lo establecido en el artículo [147](#) de la Ley 1955 de 2019, que para este propósito defina el MinTIC. De acuerdo con el mismo precepto, los proyectos estratégicos

transformación digital se orientarán entre otros, por los principios de interoperabilidad, vinculación interacciones entre el ciudadano y el Estado a través del Portal Único del Estado colombiano, y en políticas de seguridad y confianza digital, para ello, las entidades públicas deberán implementar el principio de seguridad y privacidad como habilitador de la política de Gobierno Digital y las acciones contenidas en el Decreto 3995 de 2020, cuyo fin es desarrollar la confianza digital a través de la mejora de la seguridad de la información 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 la entidad que haga las veces de articulador de servicios ciudadanos digitales, o la que defina el MinTIC.

El artículo [9](#) del Decreto 2106 de 2019 “Por el cual se dictan normas para simplificar, suprimir y reorganizar 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, garantizando el derecho a la utilización de medios electrónicos, las autoridades deberán implementar el uso del modelo de Servicios Ciudadanos Digitales. Este mismo artículo dispone que el Gobierno prestará gratuitamente los Servicios Ciudadanos Digitales base y se implementarán por parte de las entidades 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 de estos, según se desprende del artículo [2.2.17.4.1](#). del DUR-TIC, en concordancia con el numeral 2, artículo [18](#) de la Ley 1341 de 2009.

En ese mismo sentido, con el fin de lograr una adecuada interacción con el ciudadano, garantizando la utilización de medios electrónicos ante la administración pública, reconocido en el artículo [54](#) de la Ley 1712 de 2011, se han desarrollado los Servicios Ciudadanos Digitales, entendidos como el conjunto de servicios y procesos transversales que brindan al Estado capacidades y eficiencias para su transformación digital. 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, elección y portabilidad, privacidad por diseño y por defecto, seguridad, privacidad y circulación responsable 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.

digitales. Esto incluye en el articulado las mejoras funcionales del modelo de los Servicios Ciudadanos que permitan al Articulador tener el rol de prestador de servicios para las entidades públicas, así como 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 la transformación digital.

5. SERVICIOS CIUDADANOS DIGITALES.

Para entender los Servicios Ciudadanos Digitales debemos inicialmente identificar las dificultades que los usuarios al acceder a los trámites, procesos y procedimientos de las entidades públicas.

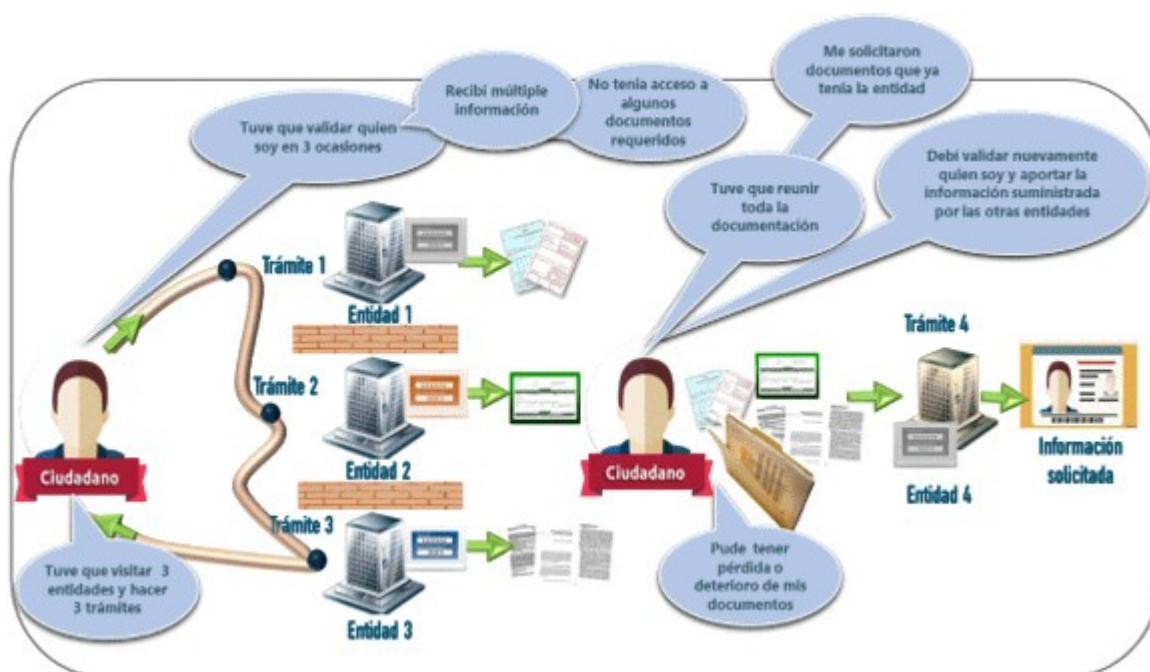


Figura 1 Problemática a resolver

La Figura 1, muestra varias de las situaciones a las que cotidianamente se ven enfrentados los usuarios cuando se acercan a las entidades para adelantar un trámite o solicitar un servicio. Tienen que dirigirse físicamente a varias entidades, cada una de ellas le solicita tener un usuario y contraseña para autenticarse, pero cada una recibe múltiple información de manera dispersa o no tienen acceso a todos los documentos que necesitan. Además, solicitan siempre los mismos documentos y termina siendo un mensajero para recolectar toda la información. Finalmente, contar que el usuario al tener estos documentos en formatos físicos los puede perder o deteriorar o pierden vigencia o validez.

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, para resolver la dificultad en el intercambio de información entre las entidades, la necesidad de presentar documentos que el ciudadano ya ha presentado previamente y la complejidad para identificar a las entidades en el mundo digital.

En este sentido, los Servicios Ciudadanos Digitales se definen como el conjunto de soluciones y procesos transversales que brindan al Estado capacidades y eficiencias para su transformación digital y para una adecuada interacción con el ciudadano, garantizando el derecho a la utilización de medios electrónicos en la administración pública.

Los Servicios Ciudadanos Digitales se han dividido en tres servicios base:

1. Servicio de Interoperabilidad: Es el servicio que brinda las capacidades necesarias para garantizar el 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 funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad.

2. 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 documento digital, 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.

3. Servicio de Carpeta Ciudadana Digital: Es el servicio que le permite a los usuarios de servicios digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que custodian las entidades. Adicionalmente, este servicio podrá entregar las comunicaciones o alertas que las entidades tienen para los usuarios, previa autorización de estos.

Estos tres servicios proporcionan las herramientas para mejorar la interacción digital de los usuarios y garantizando las condiciones de calidad, seguridad, interoperabilidad, disponibilidad y acceso a la información y así:

1. Permitir que el estado funcione como una sola institución que le brinde a los ciudadanos información oportuna, trámites ágiles y mejores servicios.

2. Mejorar las condiciones de intercambio de información entre entidades (Interoperabilidad).

3. Garantizar la igualdad en el acceso a la administración pública por medios digitales, transformando digitalmente y masificando la prestación de trámites, procesos y procedimientos del Estado.

4. Evitar desplazamientos y costos para reunir y aportar información que ya reposa en las entidades que puede ser intercambiada e integrada a los trámites por parte de estas sin convertir al ciudadano en un trámite del Estado.

5. Crear las condiciones de confianza en el uso de los medios digitales con medidas para la preservación e integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos y las comunicaciones.

6. Mitigar los riesgos en la suplantación de la identidad de los ciudadanos creando un entorno de confianza digital con las entidades.

7. Permitir a los usuarios de forma segura y confiable, acceder y conocer las informaciones que se han recogido sobre ellas en las entidades públicas.

El modelo de los Servicios Ciudadanos Digitales considera los siguientes actores cuyos roles se describen en la continuación:

1. Usuarios: Son los principales beneficiarios de los Servicios Ciudadanos Digitales quienes usan los medios digitales para acceder a los trámites y servicios de las entidades. Los usuarios son personas naturales o extranjeras, o las personas jurídicas, de naturaleza pública o privada, que hacen uso de los Servicios Ciudadanos Digitales.

2. Organismos y entidades: Son los encargados de ofrecer los trámites y servicios, custodiar datos de usuarios y que colaborarán armónicamente con otras entidades para intercambiar información en el desempeño de sus funciones.

3. Articulador: Es la entidad encargada de proveer y gestionar de manera integral los servicios 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. Este actor podrá prestar servicios de Carpeta Ciudadana Digital y Autenticación Digital, al igual que los prestadores de servicios. El único actor que podrá ofrecer el servicio de Interoperabilidad. Todo esto siguiendo los lineamientos que defina MinTIC. El rol es desarrollado por la Agencia Nacional Digital.

4. Prestadores de SCD: Son personas jurídicas, pertenecientes al sector público o privado, quienes, en un esquema coordinado y administrado por el Articulador, pueden proveer los servicios ciudadanos digitales de acuerdo a los lineamientos, políticas, guías, que expida el Ministerio de Tecnologías de la Información y las Comunicaciones. Los servicios ciudadanos digitales de autenticación digital y carpeta ciudadana digital son prestados por el Articulador y por los prestadores.

5. El Ministerio de las 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 funcionamiento de los SCD. Vigila el cumplimiento de funciones del Articulador y los Prestadores de Servicios

6. Entidades de vigilancia y control: son las autoridades que en el marco de sus funciones constitucionales ejercerán vigilancia y control sobre las actividades que involucren la prestación de los SCD

6. PROCESO DE VINCULACIÓN AL SERVICIO DE INTEROPERABILIDAD.

Para entender la importancia y beneficios de que todas las entidades adopten recomendaciones para poder intercambiar información haciendo uso de la interoperabilidad, es fundamental unificar los principales conceptos a los que hace referencia esta guía, entre los que se resaltan: interoperabilidad, marco de interoperabilidad para Gobierno en digital, servicio de intercambio de información, Plataforma De Interoperabilidad – PDI y X-ROAD.

6.1. INTEROPERABILIDAD.

Si bien la interoperabilidad ha sido entendida como la habilidad de dos o más sistemas o componentes para poder intercambiar y utilizar información, dentro del Gobierno Digital su interpretación se extiende más allá de lo puramente técnico. Involucra retos de diversos tipos para el intercambio efectivo de información, bajo un enfoque sistémico que redunde en mejores servicios hacia la ciudadanía, retos relacionados con la voluntad política, la formación y apropiación al interior de las entidades, con la necesidad de integrar procesos interinstitucionales o con la ausencia de un marco legal adecuado que le otorgue las facultades a una entidad para intercambiar su información. Es por esto por lo que para el desarrollo de la estrategia de Gobierno Digital la definición de interoperabilidad es acogida como la “Capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia objetivos mutuamente beneficiosos, con el propósito de facilitar la entrega de servicios en línea a ciudadanos y a otras entidades, mediante el intercambio de datos entre sus sistemas”.

La interoperabilidad tiene como propósito hacer que el Estado funcione como una sola entidad eficaz y brinde a sus ciudadanos información oportuna, trámites y servicios en línea ágiles. Las entidades deben ser conscientes del impacto de la interoperabilidad en la sociedad, asumir con compromiso y dar el primer paso para estar digitalmente conectados y articulados. ¡Ser un solo Sistema!

La sociedad y la tecnología se encuentran en constante evolución. Las relaciones entre entidades y el ciudadano deben estar a la par del sector público, garantizando el aprovechamiento de las TIC. Un gobierno digital debe contar con un Gobierno Digital.

El Marco de Interoperabilidad es genérico y aplicable a todas las entidades públicas y privadas en Colombia. Este marco establece las condiciones básicas que se deben considerar para alcanzar la interoperabilidad local, interinstitucional, sectorial, nacional o internacional y orientado a todos los involucrados en el diseño, desarrollar y entregar servicios de intercambio de información, como son:

- Entidades públicas responsables de planear servicios que requieran colaboración interinstitucional.
- Entidades públicas que para mejorar su funcionamiento y relacionamiento con otras entidades a través de las TIC.
- Organizaciones privadas involucradas en la ejecución y/o evolución de la estrategia de Gobierno Digital.
- Miembros de gobiernos extranjeros interesados en la interoperabilidad con entidades del Estado colombiano.
- Miembros de la comunidad académica interesados en la interoperabilidad del Gobierno Digital.

6.2. MARCO DE INTEROPERABILIDAD PARA GOBIERNO DIGITAL.

El Marco de Interoperabilidad proporciona la orientación necesaria a las entidades públicas y en general a aquellos que quieran intercambiar información, mediante un conjunto de lineamientos sobre cómo gestionar la gobernanza de las actividades relacionadas a la interoperabilidad, permitiendo establecer relaciones entre proveedores y consumidores de información y racionalizar los procesos que dan soporte a los trámites y servicios o cualquier servicio digital prestado por las entidades, de conformidad con el marco normativo y con garantía de hacerlo en un entorno de confianza digital.

El Marco de Interoperabilidad para Gobierno digital, se presenta bajo una estructura de trabajo donde se definen los conceptos y criterios que guían el intercambio de información. Este marco cuenta con nueve (9) dominios: cuatro (4) dominios con veinte (20) lineamientos distribuidos a lo largo de cada uno de los dominios en el dominio político - legal; cinco (5) en el dominio organizacional; siete (7) en el dominio semántico y cinco (5) en el dominio técnico.



Figura 2 Marco de Inoperabilidad

El marco define el conjunto de principios, recomendaciones y lineamientos que orientan los esfuerzos legales, organizacionales, semánticos y técnicos de las entidades con el fin de facilitar el intercambio eficiente de información. Además ofrece un modelo de madurez, un conjunto de actividades que pueden usarse como referente por las entidades para compartir datos a través de servicios de intercambio de información vinculados a los Servicios Ciudadanos Digitales.

6.2.1. PRINCIPIOS DE INTEROPERABILIDAD.

- Enfoque en el ciudadano
- Cobertura y proporcionalidad
- Seguridad, protección y preservación de la Información
- Colaboración y participación
- Simplicidad
- Neutralidad, tecnológica y adaptabilidad
- Reutilización
- Confianza
- Costo-efectividad

6.2.2. DOMINIOS DEL MARCO DE INTEROPERABILIDAD.

El Marco de Interoperabilidad para Gobierno Digital contempla múltiples interacciones, denominadas dominios de interoperabilidad. Estos dominios, mediante un conjunto de lineamientos permiten mejorar la gobernanza digital.

las actividades relacionadas a la interoperabilidad, permitiendo establecer relaciones entre proveedores y consumidores de información y racionalizar los procesos que dan soporte a los trámites y servicios de las entidades para los ciudadanos.

6.2.2.1. DOMINIO POLÍTICO – LEGAL.

Este dominio corresponde a la disposición de un conjunto de políticas y normas que permiten el intercambio de información. La interoperabilidad político - legal consiste en garantizar que las entidades públicas puedan intercambiar información ajustado al marco jurídico vigente, las políticas y estrategias pueden tener impacto y no se obstaculiza o impide la interoperabilidad.

6.2.2.2. DOMINIO ORGANIZACIONAL.

Este dominio de la interoperabilidad se refiere al modo en que las misiones, políticas, procesos y procedimientos interactúan con aquellos de otras entidades para alcanzar las metas adoptadas de común acuerdo y de manera beneficiosa, a través del intercambio de información. Para lograrlo es necesario la integración, además de la eliminación o definición de nuevos procesos, trámites, servicios y otros procedimientos administrativos, así como realizar la identificación de los conjuntos de datos que son pertinentes y susceptibles de ser intercambiados.

6.2.2.3. DOMINIO SEMÁNTICO.

El dominio semántico permite garantizar que, en el momento de intercambiar datos, el significado de la información sea exacto y el mismo para todas las partes interesadas. De igual manera, permite que las entidades del Estado colombiano puedan estandarizar, gestionar y administrar su información.

6.2.2.4. DOMINIO TÉCNICO.

El dominio técnico de la interoperabilidad hace referencia a las aplicaciones e infraestructuras que soportan los sistemas de información, las aplicaciones con los servicios de intercambio de información. Incluye como especificaciones de interfaz, protocolos de interconexión, servicios de integración de datos, protocolos de intercambio de datos y protocolos de comunicación seguros.

6.3. SERVICIO DE INTERCAMBIO DE INFORMACIÓN.

Por su parte el concepto de servicio de intercambio de información está ligado al recurso tecnológico. Mediante el uso de un conjunto de protocolos y estándares permite el intercambio de información. El servicio de intercambio de información debe responder a una interfaz común y cumplir con el Lenguaje Común de Intercambio de Información.

6.4. PLATAFORMA DE INTEROPERABILIDAD - PDI.

La Plataforma De Interoperabilidad – PDI son el conjunto de herramientas necesarias que permiten que los sistemas de información del Estado interactúen entre sí mediante interfaces estándar de comunicación de procesos y sistemas de información.

La PDI cuenta con varios componentes como se muestra en la Figura 3 Componentes de la PDI, el núcleo de la plataforma es X-ROAD que es el encargado de habilitar las capacidades para realizar el intercambio de datos de manera distribuida con un tráfico de datos cifrados con estampa cronológica de tiempo.

El componente Adaptador para el consumo y Exposición de servicios WEB (REST - SOAP) es un componente opcional que las entidades pueden utilizar de manera independiente con el propósito de servir como

intermediario en la exposición y consumo de servicios entre los sistemas de información de las entidades servidor X-ROAD instalado.

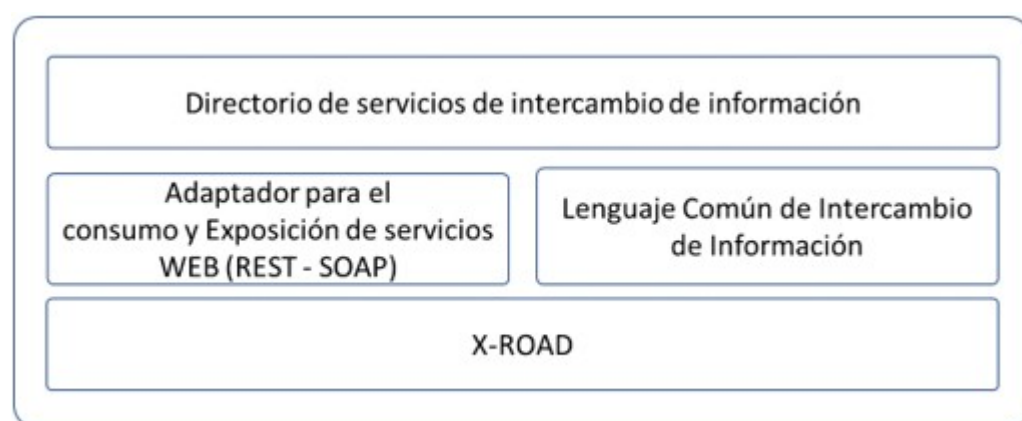


Figura 3 Componentes de la PDI

El Directorio de Servicios de Intercambio de Información es una herramienta que permite la publicación de información general, semántica y técnica de servicios de intercambio de información dispuestos por autoridades y disponibles en la PDI que cumplen con los lineamientos del Marco de Interoperabilidad del Gobierno Digital. Por su parte, el Lenguaje Común de Intercambio de Información es el estándar nacional definido y administrado por MinTIC en el cual se describen los conceptos y sintaxis de los elementos que componen el conjunto de datos a intercambiar entre las autoridades.

Con la entrada del servicio de la plataforma de interoperabilidad, se estima que las entidades públicas sostenibles (social, económica y medioambientalmente), más eficientes y efectivos en la contribución a la mejora de la calidad de los servicios que se prestan a los ciudadanos, mediante el uso de la tecnología. Los objetivos que persigue el servicio de interoperabilidad son los siguientes.

- a) Mejorar la calidad de los servicios de intercambio de información prestados, el control de los costos de los servicios generados y la evolución de la gestión de los servicios en las entidades públicas.
- b) Mejorar el modelo de gobierno del marco de interoperabilidad, la gestión de relaciones entre las entidades públicas y la participación de entidades, empresas y ciudadanos.
- c) Aumentar la información disponible y los servicios adicionales que de ella se deriven para los ciudadanos, empresas, mediante difusión a través de la plataforma de interoperabilidad.
- d) Aportar a un gobierno abierto, ofreciendo transparencia mediante la apertura de datos de forma constante, consistente, unificada e integral.
- e) Reducir el gasto público y mejorar la coordinación entre diferentes servicios y administraciones.
- f) Apoyar y mejorar la toma de decisiones por parte del gestor público a través de información en tiempo real.
- g) Mejorar la transparencia de la función pública y la participación ciudadana por medios digitales en los trámites de las entidades.
- h) Medir los resultados de la gestión de la interoperabilidad y su impacto en la administración pública y su relacionamiento con las empresas y la calidad de vida del ciudadano.
- i) Evolucionar hacia un modelo auto gestionado y sostenible tanto en consumo de recursos como en la prestación de servicios de intercambio de información.

6.5. X-ROAD.

El Ministerio como parte de la estrategia de implementación del Servicio Ciudadano Digital de Interoperabilidad, definió la utilización de X-ROAD (<https://X-ROAD.global/>) como la herramienta que sustenta la plataforma de interoperabilidad del estado y es usada como el componente tecnológico de intercambio de datos. X-ROAD fue seleccionada luego de un análisis detallado de diferentes herramientas tecnológicas en los frentes técnicos y funcionales, así como de una revisión de las mejores prácticas aprendidas de diferentes gobiernos en términos de Interoperabilidad. X-ROAD es una capa de intercambio de datos distribuidos que proporciona una forma estandarizada y segura de producir y consumir servicios. Adicionalmente, garantiza la confidencialidad, integridad e interoperabilidad entre las partes de intercambio de datos.

X-ROAD le aporta a la Plataforma de Interoperabilidad del Estado las siguientes características:

1. El intercambio de datos se produce directamente entre las entidades sin intermediarios.
2. Las entidades son las que autorizan el acceso a los servicios de intercambio de información expuestos.
3. La propiedad de los datos no cambia, la autoridad propietaria de los datos controla quién puede acceder al servicio de intercambio de información.
4. Cada miembro es autenticado a través de certificados digitales para el acceso a la plataforma.
5. El intercambio de datos se realiza con protocolos criptográficos seguros a través HTTPS con TLS, los mensajes cifrados aplicando el algoritmo RSA con la función Hash SHA512.
6. Todos los mensajes intercambiados a través de X-ROAD son estampados cronológicamente, se genera un sello para estampar todas las solicitudes salientes, solicitudes entrantes, respuestas salientes y respuestas entrantes en los servidores de seguridad.
7. Los mensajes intercambiados en la PDI tienen valor jurídico y pueden ser usados como evidencia en el envío y recepción del mensaje intercambiado.
8. No hay roles predeterminados, una vez que una entidad se ha unido al ecosistema de X-ROAD, puede actuar como cliente y proveedor de servicios web sin tener que realizar ningún registro adicional.
9. Log y auditoria sobre los mensajes intercambiados.

6.5.1. DESCRIPCIÓN GENERAL DE X-ROAD.

La siguiente figura ilustra el modelo conceptual de la plataforma de interoperabilidad.

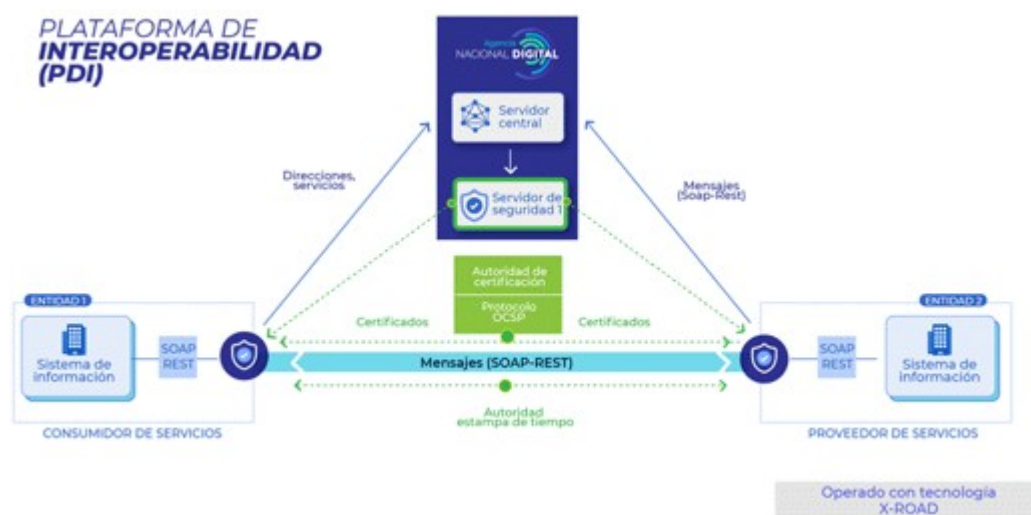


Figura 4 Modelo Conceptual de la PDI operada con X-ROAD

El Articulador de los SCD administrará los componentes centrales de la plataforma de interoperabilidad y prestará a través de las Entidades de Certificación Digital acreditadas ante la ONAC, los servicios de Certificación Digital (Certificados Digitales, Estampa Cronológica de tiempo y validación del estado de un certificado), lo cual en el momento en que se selecciona la o las entidades que prestan dichos servicios, estas deben cumplir los requisitos técnicos de integración de la plataforma de X-ROAD. Las entidades actuarán dentro del ecosistema como proveedores y consumidores de servicios de intercambio de datos a través de los canales de X-ROAD instalados y las conexiones que realice al interior con los sistemas de información. El intercambio de datos se realiza entre cada entidad a través de internet estableciendo canales seguros y usando mensajes cifrados. Los componentes de X-ROAD dentro del ecosistema se comunican a través de servicios de sincronización de la configuración y auditoría.

Cada uno de los miembros, servidores de seguridad y servicios dentro del ecosistema de X-ROAD se identifican de acuerdo con la siguiente estructura:

- Instancia: Es un entorno organizativo que agrupa a todos los participantes del ecosistema X-ROAD permitiendo el intercambio seguro de datos entre ellos y administrados por una autoridad de gobierno. Se definen 3 instancias relacionadas al ambiente de QA, Preproducción y Producción para Colombia.
- Clase Miembro: Es un identificador dado por la autoridad de gobierno de X-ROAD para clasificar a los miembros que poseen características similares dentro del ecosistema. Las clases de miembro serán utilizadas para identificar a entidades públicas y PRIV para identificar a entidades privadas.
- Nombre del Miembro: Nombre que se le dará a cada miembro dentro del ecosistema, este será el nombre de cada entidad.
- Código de Miembro: Es el identificador único de cada miembro dentro de su Clase Miembro, este permanece sin modificarse durante todo el tiempo de permanencia dentro del ecosistema. Este código es generado de acuerdo con el código definido en la base de datos del SIGEP para las entidades.
- Código del servidor de seguridad: Código que identifica un servidor de seguridad de los demás servidores dentro del ecosistema. Este consta del código del miembro y el código del servidor de seguridad.
- Código del subsistema: Código que identifica de forma exclusiva el subsistema en todos los subsistemas de un miembro. Se establecerá de acuerdo con los nombres de los sistemas de información de la entidad.

· Código del servicio: Código que identifica de forma exclusiva el servicio expuesto por un miembro del ecosistema X-ROAD. El código es el nombre que haya establecido la entidad al servicio en estilo C

6.5.2. DESCRIPCIÓN DE LA ARQUITECTURA DE X-ROAD.

A continuación, se detalla el funcionamiento de los componentes de la herramienta X-ROAD de la interoperabilidad de acuerdo con la arquitectura de componentes de la Figura 5.

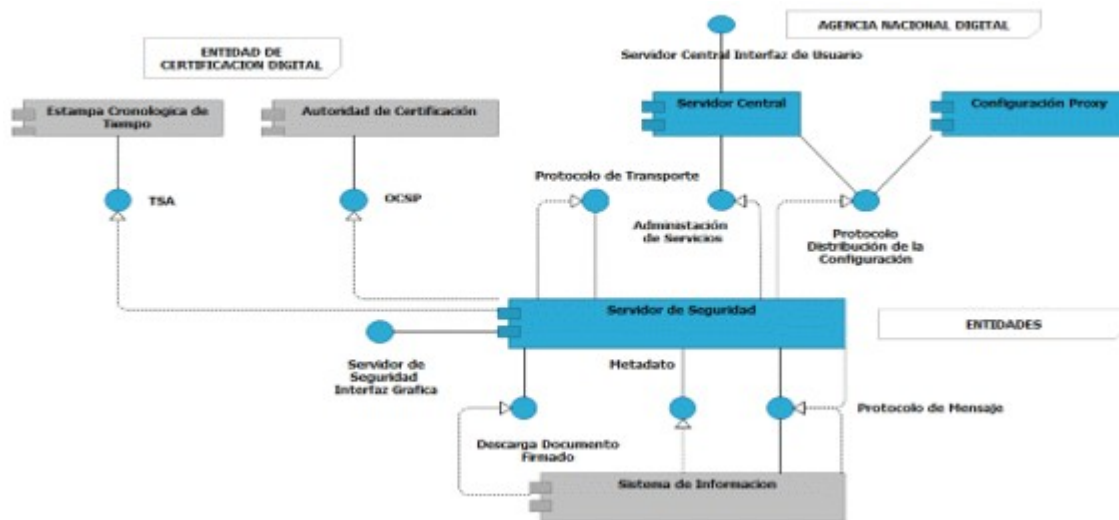


Figura 5 Arquitectura de componentes de la PDI

6.5.2.1. SERVIDOR CENTRAL DESCRIPCIÓN DETALLADA DE COMPONENTES DE LA PLATAFORMA DE INTEROPERABILIDAD.

El servidor central gestiona la base de datos de miembros de X-ROAD y servidores de seguridad. El servidor central contiene la política de seguridad de la instalación de X-ROAD. La política de seguridad incluye los siguientes elementos:

- Lista de autoridades de Certificación Digital confiables.
- Lista de entidades confiables de Estampado Cronológico de Tiempo.
- Parámetros ajustables de configuración de los servicios de administración.

El servidor central sirve de vehículo para la gestión y distribución de la configuración compartida entre los servidores de seguridad. La configuración que se comparte entre los servidores de seguridad incluye parámetros de configuración de red necesarios para la comunicación entre servidores de seguridad, información relacionada con la Entidad de Certificación Digital y el listado de miembros y subsistemas del ecosistema.

Ninguna comunicación pasa a través del servidor central; este podría no estar presente en la red durante un tiempo sin ningún impacto en la disponibilidad del servicio de la plataforma de interoperabilidad.

Adicional a la distribución de configuración, el servidor central proporciona una interfaz para realizar la administración, como agregar y quitar miembros o subsistemas. Los servicios de gestión se implementan como servicios estándares de X-ROAD y se ofrecen a través del servidor de seguridad central.

6.5.2.2. PROXY DE CONFIGURACIÓN.

El proxy de configuración implementa el protocolo de distribución de configuración administrada por la Agencia Nacional Digital. El proxy de configuración descarga la configuración, la almacena y la pone a disposición para su descarga. Por lo tanto, el proxy de configuración se puede utilizar para aumentar la disponibilidad del sistema mediante la creación de un origen de configuración adicional y reducir la carga del servidor central.

6.5.2.3. SERVICIO ESTAMPA CRONOLÓGICA DE TIEMPO-TSA.

La entidad de sellado de tiempo emite estampas cronológicas de tiempo que certifican la existencia de elementos de datos en un determinado momento. La entidad de estampado de tiempo debe proveer de sellado de tiempo.

Los servidores de seguridad utilizan el sellado de tiempo por lotes. Esto reduce la carga del servicio de tiempo. La carga no depende del número de mensajes intercambiados a través de la PDI, en su lugar depende del número de servidores de seguridad en el sistema.

6.5.2.4. ENTIDAD DE CERTIFICACIÓN DIGITAL.

La Entidad de Certificación (CA)⁽²⁾ emite certificados digitales a los servidores de seguridad (certificados de autenticación) y a las entidades miembro de X-ROAD (certificados de firma). Todos los certificados se almacenan en los servidores de seguridad.

La CA debe distribuir la información de validez del certificado vía el protocolo OCSP, los servidores de seguridad guardan en caché las respuestas OCSP⁽³⁾ para reducir la carga en el servicio OCSP y para aumentar la disponibilidad. La carga en el servicio OCSP depende del número de certificados emitidos.

6.5.2.5. SERVIDORES DE SEGURIDAD.

El Servidor de Seguridad se requiere para producir y consumir servicios a través de X-ROAD. Este canal de llamadas de servicio y las respuestas de servicio entre los sistemas de información de las entidades de Seguridad encapsula los aspectos de seguridad involucrados En el intercambio de datos: gestión de claves para la firma y autenticación, envío de mensajes a través de un canal seguro, creación del valor de firma y mensajes con firmas digitales y sellado de tiempo. Para los sistemas de información que proveen o consumen servicios, el servidor de seguridad ofrece un protocolo de mensajes basado en REST y SOAP. El mismo protocolo se utiliza tanto para el cliente y el proveedor de servicios, lo que hace que el servidor de seguridad sea transparente para las aplicaciones.

El servidor de seguridad administra dos tipos de claves (certificados digitales). Las claves de autenticación se asignan a un servidor de seguridad y se utilizan para establecer canales de comunicación criptográficos seguros con los otros servidores de seguridad. Las claves de firma se asignan a los clientes del servicio de seguridad y se usan para firmar los mensajes intercambiados.

El servidor de seguridad descarga y almacena en caché la configuración global actualizada y la información de validez del certificado. El almacenamiento en caché permite que el servidor de seguridad funcione cuando las fuentes de información no están disponibles.

6.5.2.6. SISTEMA DE INFORMACIÓN.

El Sistema de información expone y/o consume servicios a través de X-ROAD y es propiedad de un miembro de X-ROAD. X-ROAD admite el consumo y exposición de servicios REST y SOAP. Sin embargo, X-ROAD no proporciona conversiones automáticas entre diferentes tipos de mensajes y servicios.

Para un Sistema de información que consume servicios, el servidor de seguridad actúa como un puente de entrada a todos los servicios de X-ROAD. El consumidor puede descubrir miembros registrados de sus servicios disponibles utilizando el protocolo de metadatos de X-ROAD.

Para un sistema de información que expone servicios y lo pone a disposición en X-ROAD, los servidores no requieren ningún cambio o intervención. De otra parte, los servicios SOAP deben implementar el protocolo de mensajes X-ROAD para SOAP. La descripción de los servicios REST se definen usando la especificación OpenAPI3 y superiores, y las descripciones de servicio de los servicios SOAP se definen usando WSDL.

6.5.2.7. PROTOCOLO DE MENSAJES X-ROAD.

Es utilizado por los sistemas de información de la entidad para comunicarse con el servidor de seguridad.

El protocolo es un protocolo de estilo RPC sincrónico, iniciado por el sistema de Información de la entidad que expone y consume servicios a través de X-ROAD.

El protocolo de mensajes se basa en SOAP o REST a través de HTTP (S) y agrega campos de encabezado adicionales para identificar el cliente de servicio y el servicio invocado.

6.5.2.8. PROTOCOLO DISTRIBUCIÓN DE LA CONFIGURACIÓN.

El protocolo de descarga de la configuración es un protocolo sincrónico que es ofrecido por el servidor de seguridad. Lo utilizan los clientes de configuración, como los servidores de seguridad y los proxys de configuración.

El protocolo se basa en la mensajería multiparte HTTP y MIME. La configuración está firmada digitalmente por el servidor central para protegerla contra modificaciones. Por lo general, la configuración consta de varias partes. El protocolo permite a los clientes de configuración comprobar si la configuración ha cambiado desde la última descarga de partes modificadas.

Los servidores de seguridad de la PDI mantienen una copia local de la configuración global, que actualizan periódicamente desde su respectivo origen de configuración. Esta configuración global almacenada tiene un período de validez, los servidores de seguridad siguen estando totalmente operativos mientras la configuración global almacenada en caché sigue siendo válida.

6.5.2.9. PROTOCOLO DE TRANSPORTE DE MENSAJES.

El servidor de seguridad utiliza el protocolo de transporte de mensajes para intercambiar solicitudes y respuestas de servicio entre entidades. El protocolo es un protocolo de estilo RPC sincrónico iniciado por el servidor de seguridad del cliente de servicio.

El protocolo se basa en HTTPS y utiliza la autenticación TLS basada en certificados mutuos. Los mensajes SOAP o REST recibidos del cliente y el proveedor de servicios se ajustan en un mensaje MIME de transporte junto con datos adicionales relacionados con la seguridad, como firmas y respuestas OCSP. Este protocolo (junto con el protocolo de mensajes) forma el núcleo del intercambio de datos.

6.5.2.10. PROTOCOLO METADATOS DE SERVICIO.

Los sistemas de información del cliente del servicio pueden utilizar el protocolo de metadatos de X-ROAD para recopilar información sobre la instalación de X-ROAD, en particular, el protocolo puede ser utilizado para encontrar miembros de X-ROAD, servicios ofrecidos por estos miembros y WSDL de cada servicio.

El protocolo de metadatos de servicio se utiliza para la configuración del sistema de información de la entidad.

entidades, por lo tanto, la disponibilidad, el rendimiento y la latencia de sus componentes de implementación son críticos para el funcionamiento de X-ROAD.

6.5.2.11. DESCARGA DOCUMENTO FIRMADO.

El servicio de descarga de documentos firmados puede ser utilizado por los sistemas de información para descargar los contenedores firmados desde el registro de mensajes del servidor de seguridad. Además, el servicio proporciona un método de verificación para descargar la configuración global que se puede utilizar para validar los contenedores firmados.

El protocolo es un protocolo síncrono de estilo RPC Iniciado por el sistema de información. El servicio se implementa como solicitudes HTTP (S) GET.

El protocolo Descarga documento firmado es utilizado por el sistema de información para descargar documentos almacenados en el servidor de seguridad y, por lo tanto, la disponibilidad, el rendimiento y la latencia de sus componentes de implementación no son críticos para el funcionamiento de X-ROAD.

6.5.2.12. PROTOCOLO DE SERVICIOS DE ADMINISTRACIÓN.

Los servidores de seguridad hacen uso de los servicios de administración para realizar tareas de administración, como registrar un cliente de servidor de seguridad o eliminar un certificado de autenticación. El protocolo de administración es un protocolo síncrono de estilo RPC que ofrece el servidor central.

6.5.2.13. PROTOCOLO OCSP.

Los servidores de seguridad utilizan el protocolo OCSP (Protocolo de comprobación del Estado de Certificado En línea) que permite consultar la información de validez sobre los certificados de firma de autenticación.

El protocolo OCSP es un protocolo síncrono que será ofrecido por una Entidad de Certificación Intermedia acreditada. Cada servidor de seguridad es responsable de descargar y almacenar en caché la información de validez sobre sus certificados. Las respuestas OCSP se envían a los otros servidores de seguridad a través del Protocolo de transporte de mensajes. Esto garantiza que los servidores de seguridad no necesiten del servicio OCSP utilizado por la otra parte.

Debido a que las respuestas OCSP se utilizan en el proceso de validación de certificados, el error del protocolo OCSP deshabilita eficazmente el intercambio de mensajes de X-ROAD. Cuando las respuestas OCSP almacenadas en caché no se pueden actualizar, los servidores de seguridad no son capaces de comunicarse. Por lo tanto, la duración de las respuestas OCSP determina la cantidad máxima de tiempo que el servicio puede no estar disponible.

6.5.2.14. PROTOCOLO DE ESTAMPA CRONOLÓGICA DE TIEMPO-TSA.

Los servidores de seguridad utilizan el protocolo de Estampa de Tiempo (TSA) para garantizar la integridad y autenticidad a largo plazo de los mensajes intercambiados. Los servidores de seguridad registran los mensajes y sus firmas. Estos registros se marcan para crear evidencias a largo plazo. Es un protocolo síncrono proporcionado por la Entidad Certificadora. Sin embargo, los servidores de seguridad tienen la capacidad de utilizar el protocolo de sellado de tiempo de forma asincrónica, mediante el sellado de lotes. Esto se hace para desacoplar la disponibilidad del intercambio de mensajes con la disponibilidad de la autoridad certificadora, para disminuir la latencia del intercambio de mensajes y para reducir la carga de la autoridad de certificación en el servicio de sellado de tiempo.

6.6. VINCULACIÓN AL SERVICIO DE INTEROPERABILIDAD.

El Marco de Interoperabilidad proporciona la orientación necesaria a las entidades y en general toda entidad que quiera intercambiar información, mediante un conjunto de lineamientos sobre cómo mejorar la interoperabilidad de las actividades relacionadas a la interoperabilidad, permitiendo establecer relaciones entre proveedores de información y racionalizar los procesos que dan soporte a los trámites y servicios digitales prestados por las entidades, de conformidad con el marco normativo vigente y con el objetivo de hacerlo en un entorno de confianza digital.

6.6.1. METODOLOGÍA.

La siguiente gráfica muestra la metodología que se llevará a cabo para la instalación y configuración del Servidor de Seguridad de X-Road en los diferentes ambientes requeridos para cada entidad en su interacción con la Plataforma de Interoperabilidad.

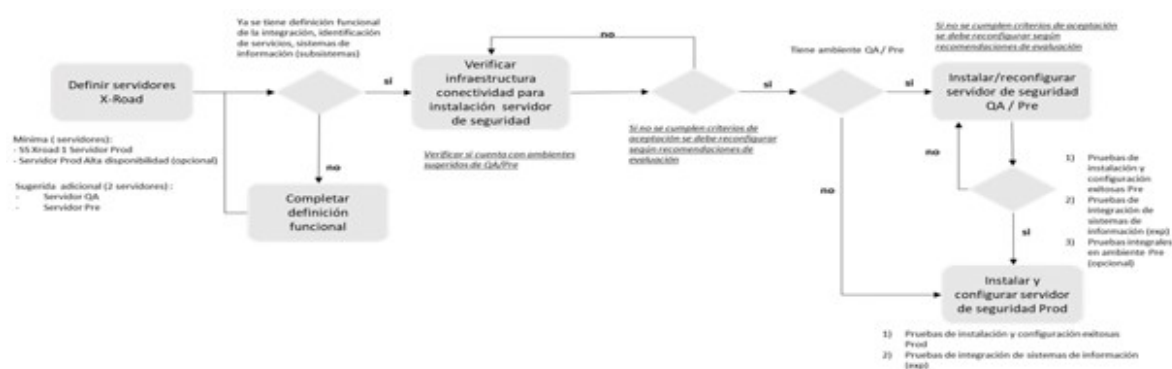


Figura 6 Metodología para la instalación y configuración de los ambientes requeridos para el servicio de seguridad

Por medio de la siguiente tabla se describen cada uno de los pasos, validaciones de la metodología.

Ítem	Requisito	Explicación
1	Definir servidores X-ROAD	Previo a cualquier instalación del Servidor de Seguridad de X-ROAD, definir la disponibilidad y aprovisionamiento por parte de la entidad de los servidores (Ambiente QA, ambiente preproducción, producción, producción alta disponibilidad). Como caso excepcional y luego de haber validado la carga transaccional de los servicios de consumo y exposición, la entidad podría definir un ambiente de alta disponibilidad (Ambiente QA, ambiente preproducción y producción sin alta disponibilidad). Las características del sistema operativo base para cada uno de los ambientes se describen más adelante.
2	Validación funcional previo a despliegue en servidor QA	Previo a la instalación, despliegue y configuración del Servidor de Seguridad de X-Road en el ambiente de producción, QA o preproducción según corresponda, se debe validar: - Formato de pruebas de conectividad y configuración diligenciado. - Diseño funcional y técnico con la información de los subsistemas que participan en el intercambio de información. Si cumple con los criterios de aceptación antes mencionados, se debe proceder a la ejecución del ítem 4. De lo contrario, se deberá complementar por la ejecución del ítem 3.

3	Completar definición funcional	Completar la información funcional, técnica contemplando la información: Contrato de servicios Definición de las variables: código miembro y subsistema del ec ROAD. Si no se ha diligenciado el formato de conectividad por parte de la entidad, se deberá completar el formato de conectividad haciendo uso de la plantilla compartida por el enlace.
4	Instalar/reconfigurar servidor de seguridad QA	Una vez validado el diseño funcional, técnico y el formato de conectividad, se deberá realizar la instalación de la versión Colombia del servidor de seguridad X-ROAD. En este ítem se deben realizar las siguientes tareas: 1. Instalación del servidor según la descripción en el punto 6.6.4 del documento. 2. Anclaje del servidor de seguridad al nodo central. 3. Configuración de los subsistemas definidos para el miembro del ecosistema. Si los pasos 1) y 2) ya se han realizado, se deberá entonces trabajar únicamente en el paso 3). Luego de realizar los pasos antes mencionados, se deberán generar las siguientes evidencias: - Formato de pruebas de instalación y configuración X-ROAD en ambiente de QA. - Formato de pruebas de integración de sistemas de información (aplicación y servicio es de exposición). Formato de pruebas integrales en ambiente de QA.
5	Validación previa al despliegue en Pre Producción	Esta validación revisa que los siguientes formatos estén completos: - Formato de pruebas de instalación y configuración X-ROAD en ambiente de QA. - Formato de pruebas de integración de sistemas de información (aplicación y servicio es de exposición) - Formato de pruebas integrales en ambiente de QA Adicionalmente, las pruebas integrales hayan sido ejecutadas de manera satisfactoria. Si la validación es satisfactoria, se realiza la instalación en ambiente de producción (ítem 6). De lo contrario, se deberá volver a la tarea anterior para completar los criterios que hagan falta.
6	Instalar/reconfigurar servidor de seguridad Pre Producción	Una vez validados los criterios de aceptación descritos en el ítem 5, se deberá realizar la instalación/configuración de la versión Colombia del servidor de seguridad X-ROAD. En este ítem se deben realizar las siguientes tareas: 1. Instalación del servidor según la descripción en el punto 6.6.4 del documento. 2. Anclaje del servidor de seguridad al nodo central pre productivo. 3. Configuración de los subsistemas definidos para el miembro del ecosistema. Si los pasos 1) y 2) ya se han realizado, se deberá entonces trabajar únicamente en el paso 3). Luego de realizar los pasos antes mencionados, se deberán generar las siguientes evidencias: - Formato de pruebas de instalación y configuración X-ROAD en ambiente de Preproducción.

		- Formato de pruebas de integración de sistemas de información (apli servicio es de exposición). Formato de pruebas integrales en ambiente de Pre producción.
7	Validación previa al despliegue en Producción	Esta validación revisa que los siguientes formatos estén completos: - Formato de pruebas de instalación y configuración X-Road en aml aplica - Formato de pruebas de integración de sistemas de información (apli servicio es de exposición) - Formato de pruebas integrales en ambiente de Preproducción, si aplic Si la validación es satisfactoria, se realiza la instalación/configuración productivo (ítem 8). De lo contrario, se deberá volver a la tarea anteri completar los criterios que hagan falta.
8	Instalar/reconfigurar servidor de seguridad Producción	Una vez validados los criterios de aceptación descritos en el ítem realizar la instalación/configuración de la versión Colombia del Seguridad de X-Road. En este ítem se deben realizar las siguientes tare 1. Instalación del servidor según la descripción en el titulo 6.6.4 documento. 2. Anclaje del Servidor de Seguridad al nodo central productivo. 3. Configuración de los subsistemas definidos para el miembro del eco Si los pasos 1) y 2) ya se han realizado, se deberá entonces trabajar e únicamente. Luego de realizar los pasos antes mencionados, se deberán generar l evidencias: - Formato de pruebas de instalación y configuración X-Road (Preproducción. Formato de pruebas de integración de sistemas de información (apli servicio es de exposición).

6.6.2. REQUERIMIENTOS.

A continuación, se describen las características mínimas que deben tener los servidores de seguridad en el punto **6.6.1 Metodología** del presente documento para el ambiente de QA:

Tabla 2 Requerimientos mínimos para la integración en ambiente de QA

Ítem	Requisito	Explicación
1	Sistema Operativo Ubuntu 18.04 Long-Term Support (LTS), 64 bits, Red Hat RHEL7 o Red Hat RHEL8. Nota: Los servidores de seguridad puede ser físicos o virtuales.	X-Road soporta estas versiones operativos.
2	1 CPU Intel o AMD o compatible de doble núcleo de 64 bits; El soporte del conjunto de instrucciones AES es altamente recomendado.	El hardware del servidor base, CPU, tarjeta de red, sistema de almacenamiento) compatible con Ubuntu en general.
3	4 GB de RAM.	Memoria RAM requerida. de acuerdo a la transaccionalidad puede aumentar la RAM.
4	20 GB de espacio libre en disco (partición del sistema operativo) 20-40 GB de espacio libre en disco (/var/partición);	Almacenamiento requerido.
5	Para la instalación del Servidor de Seguridad, se requiere que el servidor instalado tenga conectividad a Internet para acceder a los repositorios de instalación.	Acceso a repositorio de instalación.
6	Una tarjeta de interfaz de red de 1000 Mbps.	Red mínima requerida.
7	El Servidor de Seguridad puede estar separado de otras redes por un firewall y / o NAT y se deben permitir las conexiones necesarias hacia y desde el servidor de seguridad. La habilitación de los servicios auxiliares que son necesarios para el funcionamiento y la administración del sistema operativo (como DNS, NTP y SSH) se encuentran fuera del alcance de esta guía. Nota: Si el servidor de seguridad tiene una dirección IP privada, se debe crear un registro NAT correspondiente en el firewall.	Segmentación de red para Seguridad.

A continuación, las características para el ambiente Pre producción:

Tabla 3 Requerimientos mínimos para la integración en ambiente de Pre producción

Ítem	Requisito	Explicación
1	Sistema Operativo Ubuntu 18.04 Long-Term Support (LTS), 64 bits, Red Hat RHEL7 o Red Hat RHEL8. Nota: Los servidores de seguridad puede ser físicos o virtuales.	X-Road soporta únicamente estas versiones en sistemas operativos.
2	2 CPU Intel o AMD o compatible de doble núcleo de 64 bits; El soporte del conjunto de instrucciones AES es altamente recomendado.	El hardware del servidor base, CPU, tarjetas de red, sistema de almacenamiento debe ser compatible con Ubuntu en general.
3	6 GB de RAM	Memoria RAM mínima requerida de acuerdo con la transaccionalidad de la entidad puede aumentar la memoria RAM.
4	20 GB de espacio libre en disco (partición del sistema operativo) 20-40 GB de espacio libre en disco (/var/partición);	Almacenamiento requerido.
5	Para la instalación del Servidor de Seguridad, se requiere que el servidor instalado tenga conectividad a Internet para acceder a los repositorios de instalación.	Acceso a repositorio de instalación.

6	Una tarjeta de interfaz de red de 1000 Mbps.	Red mínima requerida.
7	El Servidor de Seguridad puede estar separado de otras redes por un firewall y / o NAT y se deben permitir las conexiones necesarias hacia y desde el servidor de seguridad. La habilitación de los servicios auxiliares que son necesarios para el funcionamiento y la administración del sistema operativo (como DNS, NTP y SSH) se encuentran fuera del alcance de esta guía. Nota: Si el servidor de seguridad tiene una dirección IP privada, se debe crear un registro NAT correspondiente en el firewall.	Segmentación de Red y

Por medio de la siguiente tabla se describen los requerimientos en el ambiente productivo:

Tabla 4 Requerimientos mínimos para la integración en ambiente de Producción

Ítem	Requisito	Explicación
1	Sistema Operativo Ubuntu 18.04 Long-Term Support (LTS), 64 bits, Red Hat RHEL7 o Red Hat RHEL8. Nota: Los servidores de seguridad puede ser físicos o virtuales.	X-Road soporta únicas versiones en sistemas operativ
2	4 CPU Intel o AMD o compatible de doble núcleo de 64 bits; El soporte del conjunto de instrucciones AES es altamente recomendado.	El hardware del servidor (plac tarjetas de interfaz de red, almacenamiento) debe ser con RHEL7 o Ubuntu en general.
3	16 GB de RAM	Memoria RAM mínima re acuerdo con la transacción entidad puede aumentar la mem
4	20 GB de espacio libre en disco (partición del sistema operativo) 20-40 GB de espacio libre en disco (/var/partición);	Almacenamiento mínimo requ
5	Para la instalación del Servidor de Seguridad, se requiere que el servidor instalado tenga conectividad a Internet para acceder a los repositorios de instalación.	Acceso a repositorios de instal
6	Una tarjeta de interfaz de red de 1000 Mbps.	Red mínima requerida.
7	El Servidor de Seguridad puede estar separado de otras redes por un firewall y / o NAT y se deben permitir las conexiones necesarias hacia y desde el servidor de seguridad. La habilitación de los servicios auxiliares que son necesarios para el funcionamiento y la administración del sistema operativo (como DNS, NTP y SSH) se encuentran fuera del alcance de esta guía. Nota: Si el servidor de seguridad tiene una dirección IP privada, se debe crear un registro NAT correspondiente en el firewall.	Segmentación de Red y Seguri
8	Alta disponibilidad	Hacer uso de un balanceado Round-robin como recomenda

NOTA: Los recursos establecidos en ambiente productivo podrán ser cambiados según el diseño técnico de la solución. Se deberá tener en cuenta la influencia de variables como:

I. El volumen de datos intercambiados.

II. La demanda de uso en el consumo y exposición de servicios (conurrencia).

III. Cantidad de servicios de intercambio de información expuestos o consumidos, entre otros.

6.6.3. RIESGOS DE NO CONTAR CON LOS AMBIENTES DEFINIDOS DE X-ROAD.

A continuación, se listan los riesgos que se materializarían al no contar con los tres ambientes (QA, Producción) antes mencionados:

- Cada ambiente de X-ROAD tiene variables diferentes de instancia, miembro clase, código de miembro, subsistemas que se deberán garantizar en las configuraciones de adaptadores/transformadores en cada ambiente. El hacer esta configuración y pruebas en QA y luego en ambiente productivo, sin una transición gradual, generará posibles inconsistencias/errores en producción ya haciendo uso de certificados, servicio O TSA oficiales. Se tendría un uso no eficiente de los recursos.
- Desarrollar los componentes de integración (buses, APIs, adaptadores, demás), en ambientes productivos directamente, no es recomendado bajo ningún estándar de buenas prácticas. Esto genera entregas sin consistencia en los datos, logs de evidencias innecesarias, errores en el intercambio, uso de datos en transacciones no oficiales.
- Desarrollar, probar o ajustar servicios en un ambiente productivo resultará en la no prestación del servicio en cierto momento, debido a los diferentes despliegues, modificaciones que se deberán hacer en ambientes productivos.
- Las entidades pueden tener ambientes de Desarrollo, QA, Pre producción y Producción para sus sistemas de información. De llegar a realizar despliegues internos apuntando a un único Servidor de Seguridad, garantizar la validación de las diferentes variables de los ecosistemas QA, Pre de X-ROAD, se conlleva a dicho Servidor de Seguridad en un único punto de acceso a todos los ambientes. Este escenario genera riesgos en seguridad y operación para los diferentes ambientes de los sistemas de información internos.
- Una vez existan servicios operando, no será posible realizar reinstalaciones en el servidor. De lo contrario, afectaría la operación. No se podría utilizar este ambiente para reinstalaciones de QA o Pre producción para próximas integraciones.
- Cuando una entidad no tiene servicios operando, enfrentarse a la reinstalación del Servidor de Seguridad es la única opción para garantizar ambientes. De cara a migrar de QA a PRE debería reinstalarse el servidor en QA o PRE pero esto generaría un desgaste operativo no recomendado, inconsistencias en el Nodo Central de X-Road, entregas sin calidad, procesos operativos, costos altos de mantenibilidad, no escalabilidad y riesgos para futuras integraciones.
- En el Nodo Central, en el ambiente productivo de la AND, se tendrían miembros, subsistemas que se configuran en ambiente QA y/o Pre, y no los productivos. Se tendría un ambiente productivo en Nodo Central para cada entidad con diferentes miembros, subsistemas. Según las buenas prácticas establecidas para el ecosistema X-ROAD, esto generará inconsistencias en la validez jurídica, errores en el monitoreo, datos sin calidad, catálogos de servicios, entre otros.

6.6.4. PROCESO DE INSTALACIÓN Y CONFIGURACIÓN DE X-ROAD.

Para la instalación del servidor de seguridad la entidad deberá configurar los siguientes requerimientos:

Los servidores de seguridad se comunican entre sí utilizando servicios REST y SOAP. Los servicios REST requieren ajustes para ser implementados. Por el contrario, los servicios SOAP requieren de ajustes en las cabeceras para cumplir con el protocolo de mensajes X-Road para SOAP. A su vez, cada servidor de seguridad establece comunicación directa con los servicios de confianza (CA y Autoridad de Estampa de Tier 1).

Actualmente, los servidores de seguridad se instalan en el Sistema Operativo Linux Ubuntu 18.04 y

la comunicación entre ellos se lleva a cabo a través de los Puertos 80, 443 y 5500. Varios servidores se pueden instalar en una misma máquina a través de contenedores o máquinas virtuales, por ejemplo ambientes de prueba, sin embargo, se debe considerar el impacto en el rendimiento.

A continuación, se relacionan los manuales técnicos de instalación y configuración de los servidores de seguridad:

- Manual de instalación de servidor de seguridad de X-Road 6.25 en Ubuntu 18.04.

Nombre del archivo: Instalación X-Road 6.25 servidor de seguridad entidades Ubuntu 18.04. Haga clic aquí para acceder al documento (Ambiente QA)

- Manual de instalación y configuración de X-Road 6.25 en Red Hat 7.

Nombre del archivo: Instalación y Configuración de X-Road 6.25 servidor de seguridad Red Hat 7.

Haga clic aquí para acceder al documento (Ambiente QA)

- Manual de instalación y configuración de X-Road 6.25 en Red Hat 8.

Nombre del archivo: Instalación y configuración de X-Road 6.25 servidor de seguridad Red Hat 8.

Haga clic aquí para acceder al documento (ambiente QA)

- Manual de Usuario X-Road 6.25

Haga clic aquí para acceder al documento (ambiente QA)

6.6.5. CARACTERÍSTICAS DE LOS CERTIFICADOS.

El Organismo Nacional de Acreditación de Colombia - ONAC acredita la confiabilidad de las Entidades de Certificación Digital. Los certificados se caracterizan por tener vigencia y estar firmados usando el algoritmo de firma con la función hash SHA-256 y el sistema criptográfico de llave pública RSA. En Colombia las entidades acreditadas se pueden consultar en el Directorio Oficial del Organismo de Evaluación de la Conformidad (ONAC, 2020). Sólo se reconocerán certificaciones emitidas por las entidades autorizadas por la ONAC.

La Agencia Nacional Digital registra en el servidor central tantas entidades de certificación como hay autorizadas en el entorno nacional. El servidor central supervisa cuáles son las autoridades de certificación. El servidor que consume el servicio debe firmar cada petición. El servidor que ofrece el servicio recibe la petición y verifica la autenticidad.

Los servidores de seguridad deben configurar un OCSP Responder y proveer a la Agencia Nacional Digital la dirección del OCSP. También se debe configurar un certificado de estampa de tiempo. Para el caso de las Entidades de Certificación Digital acreditadas en Colombia, estas tienen una subordinación, por lo que es necesario configurar el servicio OCSP subordinado. El subordinado genera dos certificados: Uno de autenticación digital y uno de firma digital. Las peticiones se firman con el certificado de firma digital.

6.6.6. PROCESO DE SOLICITUD DE CERTIFICADOS DIGITALES (FIRMA, AUTENTICACIÓN) PARA ENTIDADES PÚBLICAS.

Para realizar la conexión de los servidores de seguridad de las entidades públicas y sus servicios al servicio de producción de X-Road, la Agencia Nacional Digital a través de la Entidad de Certificación Digital debe generar un certificado de autenticación y un certificado de firma para que estos sean importados en el servicio.

seguridad al momento de la configuración.

La Entidad de Certificación Digital dispondrá de 2 portales web para que la entidad pueda realizar de los certificados y realizar la solicitud de firma de los certificados.

El proceso general de la solicitud de certificados se describe a continuación:

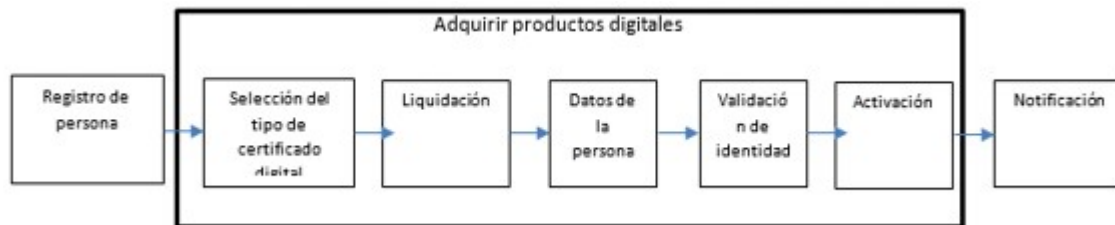


Figura 7 Proceso de solicitud de certificados

Registro de persona: el CIO, director o jefe del área de tecnologías de la información de la entidad deberá hacer el registro y la solicitud de los certificados digitales en el portal de la Entidad de Certificación Digital.

Selección de tipo de certificado digital: El producto que se debe seleccionar es el tipo de certificado perteneciente a empresa.

Liquidación: Los certificados digitales son entregados a la entidad pública sin ningún costo. En esta entidad deberá seleccionar el paquete “Convenio AND – perteneciente a empresa”.

Datos de la persona: el CIO, director o jefe del área de tecnologías de la información deberá diligenciar el formulario con datos de la entidad y personales.

Validación de identidad: el CIO, director o jefe del área de tecnologías de la información deberá cargar documentos que acrediten la relación laboral con la entidad.

Activación: La entidad de certificación digital revisará y aprobará la solicitud.

Notificación: el CIO, director o jefe del área de tecnologías de la información recibirá una notificación electrónica registrada con el estado de la solicitud.

Para detallar el proceso, consultar el manual de usuario de solicitud de certificado digital anexo a la guía.

El proceso general para la solicitud de la firma de los certificados digitales que se generan desde el portal de seguridad es el siguiente:



Figura 8 Proceso de firma de certificados

Inicio de sesión: el CIO, director o jefe del área de tecnologías de la información deberá ingresar la información de los usuarios creados en el proceso anterior.

Buscar solicitud: Ingresar y buscar el ID de la solicitud enviado al correo electrónico registrado.

Generar certificados: Generar desde el Servidor de Seguridad en formato. PEM las solicitudes de firma de certificados y cargarlos en el portal. En la siguiente sección se detallará el proceso de generación de certificados.

Solicitudes finalizadas: Buscar en la opción de solicitudes finalizadas y descargar los certificados firmados por la autoridad de certificación digital. La entidad deberá almacenar estos certificados de manera segura de acuerdo con su política de seguridad y privacidad de la información.

Cerrar Sesión: Salir del portal de firma de certificados de la entidad de certificación digital.

6.6.7. PROCESO DE SOLICITUD DE CERTIFICADOS DIGITALES PARA ENTIDADES PRIVADAS

Para realizar la conexión de los servidores de seguridad de entidades privadas y sus servicios al entorno de producción de X-Road, la Entidad Privada deberá adquirir un certificado de autenticación digital y un certificado de firma a una de las Entidades de Certificación Digital con acreditación vigente del Organismo Nacional de Acreditación Nacional - ONAC, para que estos sean importados en el servidor de seguridad en el momento de la configuración.

La Entidad de Certificación Digital dispondrá de un mecanismo para que la entidad privada pueda solicitar los certificados y la solicitud de firma de los certificados.

El proceso general de la solicitud de certificados que se describe a continuación es un ejemplo del proceso que puede diferir dependiendo de las Entidades de Certificación Digital:



Figura 9 Proceso de solicitud de certificados privados

Registro de persona: El representante legal de la entidad privada o quien haga sus veces deberá hacer el registro y la solicitud de los certificados digitales en el portal de la Entidad de Certificación Digital.

Selección de tipo de certificado digital: El producto que se debe seleccionar es el tipo de certificado digital perteneciente a persona jurídica.

Datos de la persona: El representante legal de la entidad privada o quien haga sus veces deberá diligenciar el formulario con datos del Prestador Privado y personales.

Validación de identidad: El representante legal de la entidad privada o quien haga sus veces deberá presentar documentos que acrediten la relación laboral con el Prestador privado.

Activación: La Entidad de Certificación Digital revisará y aprobará la solicitud.

Notificación: El CIO, director o jefe del área de tecnologías de la información recibirá una notificación por correo electrónico registrado con el estado de la solicitud.

El proceso general para la solicitud de la firma de los certificados digitales que se generan desde el servidor de seguridad es el siguiente.

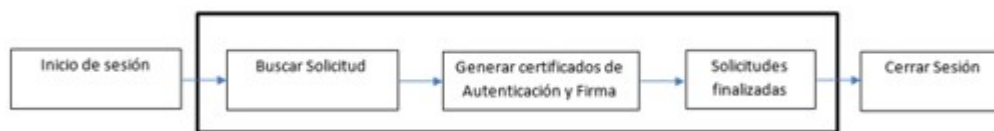


Figura 10 Proceso de firma de certificados privados

Inicio de sesión: El representante legal de la entidad privada o quien haga sus veces deberá ingresar credenciales creadas en el proceso anterior.

Buscar solicitud: Ingresar y buscar el ID de la solicitud enviado al correo electrónico registrado.

Generar certificados: Generar desde el Servidor de Seguridad en formato (.PEM) las solicitudes de certificados y proceder a firmarlos a través de la entidad certificadora correspondiente. En la siguiente se detallará el proceso de generación de los certificados.

Solicitudes finalizadas: Buscar en la opción de solicitudes finalizadas y descargar los certificados de la Entidad de Certificación Digital. La entidad deberá almacenar estos certificados de manera segura con su política de seguridad y privacidad de la información.

Cerrar Sesión: Salir del portal de firma de certificados de la Autoridad de Certificación Digital.

6.6.8. CONDICIONES TÉCNICAS DE LOS CERTIFICADOS QUE DEBEN PROPORCIONAR LAS ENTIDADES PRIVADAS.

Si bien las entidades públicas reciben los certificados de manera gratuita por parte de la Agencia Nacional de Seguridad Digital a través de la Entidad de Certificación Digital, en el caso de las entidades privadas no sucederá, deberán entregar a la Agencia Nacional Digital la siguiente configuración: Certificados de autenticación y firma, URL, Autoridad de Estampa de Tiempo y OCSP, con el propósito de realizar las respectivas configuraciones a nivel central.

Los certificados CA, deberán cumplir con las siguientes especificaciones técnicas:

1. Los certificados emitidos deben permitir la compatibilidad e integración con el sistema X-Road y el intercambio de información con la versión 6.25 Colombia.
2. Estructura del certificado de la CA-Subordinada:
 - a. La estructura del certificado subordinado se genera a partir de certificado Raíz de la Entidad de Certificación Digital.
 - b. Algoritmo de firma: SHA256.
 - c. Uso de Claves: contener el uso de firma de certificados y firma de lista de revocación de certificados.
 - d. Usos Mejorados: contener el uso de firma de OCSP.
3. Estructura de los certificados de firma y autenticación digital.

Los certificados de firma y autenticación digital emitidos son firmados por la Subordinada de la Entidad de Certificación Digital, las solicitudes de estos certificados se generan desde los servidores de seguridad de X-Road bajo la extensión (.PEM) y bajo el formato X509 para dos (2) usos: Firma y Autenticación de seguridad.

Al recibir la petición, la Entidad de Certificación Digital, construye un certificado X.509 con base en la clave privada y la llave pública que está en la petición del certificado y datos propios del mismo con extensión (1.3.6.1.5.5.7.48.1).

Los certificados de firma digital de persona jurídica deben tener las siguientes características:

Emitido por: Certificado subordinado de la Entidad de Certificación Digital.

1. Algoritmo de firma: SHA256.
2. Uso de Claves: Sin repudio
3. Acceso a información de autoridad:
 - a. Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
 - b. Nombre alternativo: URL=https:// Url del servicio para OCSP
 - c. Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)
 - d. Nombre alternativo: URL=https:// Url nombre alternativo

La Entidad de Certificación Digital debe estar acreditada por el Organismo Nacional de Acreditación Colombia – ONAC, dando cumplimiento al artículo [30](#) de la Ley 527 de 1999, modificado mediante el artículo [161](#) del Decreto Ley 019 de 2012, en las siguientes actividades:

- a. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.
- b. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje y de documentos electrónicos transferibles.
- c. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

El servicio de Estampa Cronológica de Tiempo debe cumplir las siguientes características:

1. El servicio de Estampa cronológica de tiempo debe permitir la compatibilidad e integración con Road versión 6.25 Colombia para el intercambio de información.
2. Prestar el Servicio de Estampado Cronológico (Timestamping) como mecanismo on-line que permita demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. La implementación debe cumplir con el protocolo definido en la norma RFC 3161 “Internet X.509 Infrastructure Time-Stamp Protocol (TSP)” o posteriores.
3. El servicio no deberá leer el contenido de los mensajes de datos para estampar la transacción.
4. La Autoridad de Certificación mantendrá un registro de las estampas emitidas para su futura verificación.
5. El servicio de estampa cronológica deberá soportar un rendimiento de mínimo 1000 transacciones criptográficas por segundo de las operaciones de firma.
6. Una solicitud a la Autoridad de Estampa de Tiempo que utiliza el método POST se construye de la siguiente manera: El encabezado Content-Type tiene el valor “application/timestamp-query”, mientras que el cuerpo del mensaje es el valor binario Time-Stamp Request Message.

7. Una respuesta Autoridad de Estampa de Tiempo basada en HTTP se compone del valor binario (codificación del Time-Stamp Response Message. El encabezado Content-Type tiene el valor "application/timestamp-reply".

URL: url del servicio de Autoridad de Estampa de Tiempo

Método: Post

Parámetro: Header = Content – Type (application/timestamp-query)

Body = TimeStampRequest

Returns: Header = Content – Type (application/timestamp-reply)

Body = TimeStampResponse.

8. El servicio de Autoridad de Estampa de Tiempo debe ser provisto haciendo uso de las librerías de Bouncy Castle (OpenSource), bajo el RFC 3161. La solicitud (request) al servicio de Autoridad de Tiempo se realiza haciendo uso del algoritmo de cifrado 2.16.840.1.101.3.4.2.3 de la librería Bouncy Castle correspondiente al algoritmo SHA512. El response del servicio se realiza haciendo uso del algoritmo 1.3.14.3.2.26, el cual corresponde al algoritmo SHA1.

9. La entidad privada deberá en conjunto con la entidad certificadora que presta el servicio de Autoridad de Estampa de Tiempo, llevar el control / filtro de consumo de las estampas, utilizando los mecanismos que considere adecuados.

El protocolo de comprobación del estado de un certificado en línea debe cumplir las siguientes características:

1. El protocolo de comprobación del estado de un certificado en línea debe permitir la compatibilidad e integración con el sistema X-Road para el intercambio de información.

2. Integrar a la plataforma de X-Road el servicio de OCSP que permita por medio de una URL verificar el estado de los certificados vigentes o revocados dando pleno cumplimiento al RFC 6960 - X.509 Internet Key Infrastructure Online Certificate Status Protocol – OCSP.

3. Una solicitud OCSP que utiliza el método POST y se debe construir de la siguiente manera: El encabezado Content-Type tiene el valor "application/ocsp-request", mientras que el cuerpo del mensaje es el valor de la OCSPRequest.

4. Una respuesta OCSP basada en HTTP se debe componer del valor binario de la codificación del OCSPResponse. El encabezado Content-Type tiene el valor "application/ocsp-response" este encabezado especifica la longitud de la respuesta.

URL: Url del servicio de OCSP

Método: Post

Parámetro: Header = Content-Type (application/ocsp-request)

Body = {

TBSRequest

}

Respuesta: Header = Content-Type (application/ocsp-response)

Body = {

OCSPResponseStatus,

OCSPCertificado

}

La validez del certificado debe poder verificarse cada 50 minutos contra el servicio de OCSP expuesto por la Entidad de Certificación Digital. En la respuesta de este servicio se debe establecer el parámetro NoValidBefore 50 minutos.

El servicio de OCSP debe ser provisto haciendo uso de las librerías criptográficas Bouncy Castle, b6960. La solicitud (request) al servicio de OCSP se realiza haciendo uso del algoritmo 1.3.14.3.2.20 BouncyCastle, el cual equivale al algoritmo SHA1. El response del servicio OCSP se realiza haciendo uso del algoritmo 1.2.840.113549.1.1.5 corresponde al algoritmo SHA1 con RSA de la librería BouncyCastle para la verificación de la firma del servicio OCSP.

6.7. INTERVENCIÓN DE LOS SERVICIOS Y ADAPTADOR DE TRANSFORMACIÓN DE SERVICIOS

El marco de interoperabilidad describe una arquitectura de referencia orientada a la integración de servicios, tanto de exposición o consumo en la plataforma de interoperabilidad. Los servicios que se exponen o consumen a través de X-Road pueden requerir de ajustes (intervención) en sus cabeceras.

Para la intervención de los servicios se debe tener en cuenta si la entidad va a exponer y/o consumir servicios. Nativamente la Plataforma de Interoperabilidad soporta tecnología REST y protocolo SOAP. Los servicios en tecnología REST no requieren la intervención cuando estos son de exposición.

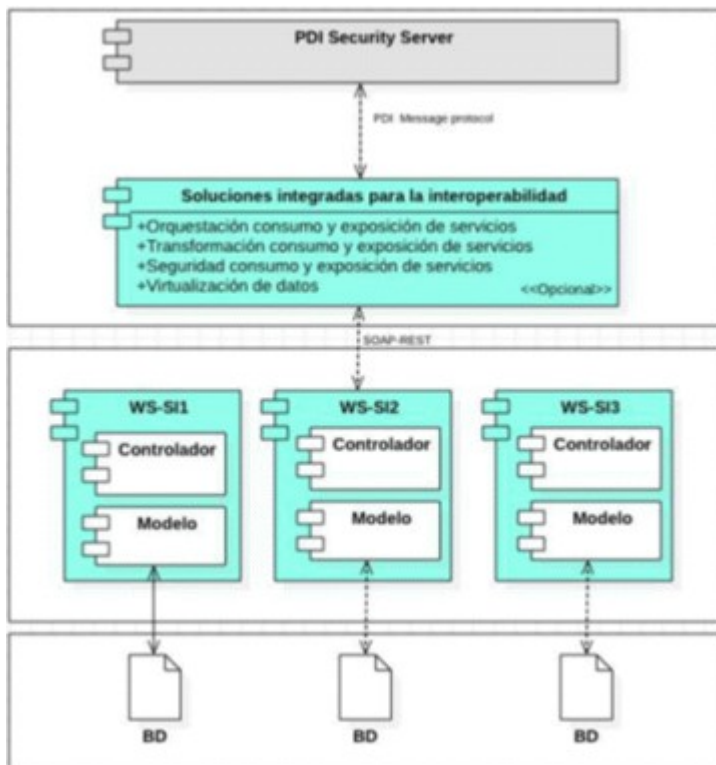


Figura 11 Arquitectura de referencia con Adaptador de Transformación de Servicio

La arquitectura ilustrada muestra el componente de soluciones integradas para interoperabilidad (A) como un componente con la capacidad de:

- Orquestrar los servicios de consumo y exposición.
- Transformar servicios de consumo y exposición.
- Brindar seguridad en el consumo y exposición de servicios.
- Virtualizar datos.

Este componente servirá para agregar los encabezados que se requieren en los servicios Web sin necesidad de intervenir estos directamente en su estructura. Este puede ser implementado por diferentes medios, por ejemplo: un Bus de servicios (ESB Enterprise Service Bus), o un API y es opcional para las entidades dependiendo de la arquitectura interna.

Los encabezados deben tener una estructura y un espacio de nombres correctos, es por esto que los SOAP y REST (consumo) tienen que ser intervenidos para que los siguientes campos obligatorios sean agregados como se describe a continuación:

- Client: campo que identifica al cliente que inició la solicitud, que se describe con los siguientes elementos
 - XRoadInstance.
 - MemberClass.
 - MemberCode
 - SubsystemCode.
- Service: es el campo que especifica el servicio de datos que se utilizará. Además de agregar los elementos descriptivos del campo < client > se adicionan los siguientes elementos
 - (xRoadInstance, memberClass, memberCode y subsystemCode).
 - ServiceCode.
 - ServiceVersion (Opcional).

6.7.1 COMPONENTE ADAPTADOR DE TRANSFORMACIÓN PARA EL CONSUMO Y EXPOSICIÓN DE SERVICIOS WEB EN X-ROAD.

El Adaptador de Transformación de servicios es un componente de software que permite a la entidad consumir servicios web REST y SOAP a través de X-Road. Sirve como componente de soluciones descrito en la sección anterior y cuenta con las siguientes características:

1. Usabilidad. Reducción de tiempo en la configuración de un servicio. Implementa el protocolo X-message protocol al interior del componente. Aunque se puede utilizar un bus de servicios directamente para configurar un bus de servicios para X-ROAD es desgastante, especialmente en SOAP. El Adaptador de Transformación de servicios, tiene la capacidad de hallar y listar automáticamente los subsistemas de los servidores de seguridad. El Adaptador ahorra a una entidad el trabajo de adición de las cabeceras requeridas por los servicios web, lo cual es especialmente útil en el caso de servicios Web que ya han sido creados

particularmente en SOAP, evitando que los servicios existentes en una entidad tengan que ser modificados. Este beneficio no puede ser logrado por ningún bus de servicios por sí solo.

2. Permite desacoplar la transformación de servicios web de los sistemas de información misionales de las entidades.

3. Encolamiento de peticiones.

4. Minimización de errores. Validación de caracteres en la configuración de parámetros.

5. Configurar políticas de acceso al servicio por horarios y número de peticiones.

6. Gestión de servicios y registro de consumos: Ofrece la flexibilidad de gestionar los diferentes servicios de consumo y exposición que se integrarán a X-Road. Permite registrar los consumos en base de datos o en archivo plano.

7. Bajo costo de implementación y mantenibilidad de servicios web sobre X-Road para las entidades.

El siguiente diagrama describe de manera general los componentes del transformador de servicios.

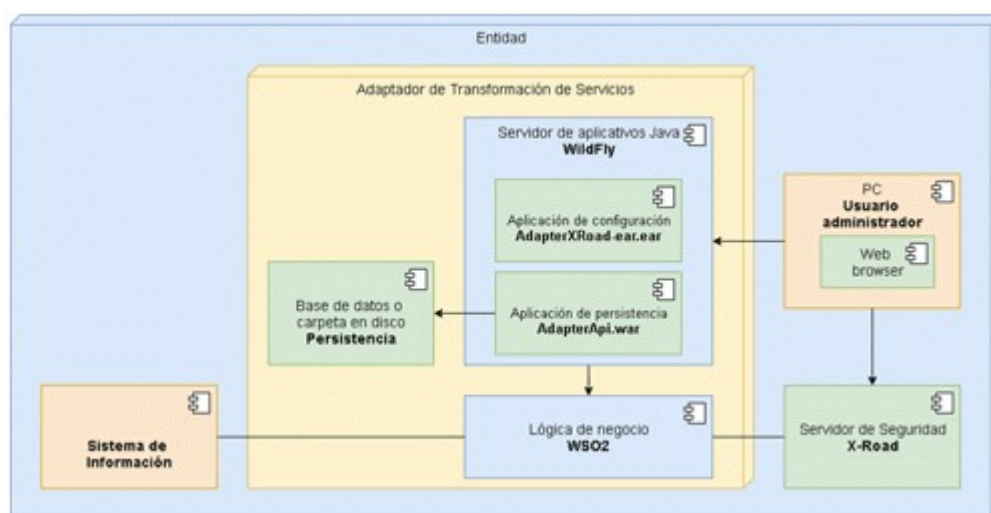


Figura 12 Diagrama de despliegue del Adaptador de integración

Cada uno de los elementos del diagrama se describe en la siguiente tabla:

Tabla 5 Descripción de componentes adaptador de integración

Nombre componente	Descripción
Adaptador de Transformación de Servicios	Conjunto de componentes encargados de intervenir los servicios Web de consumo para habilitar su compatibilidad con X-Road. Comprende un aplicaciónes Java (WildFly), los aplicativos encargados de configurar el bus de el bus de servicios WSO2.
Aplicación de configuración	Componente MVC que implementa la aplicación web para la configuración y administración del componente de transformación de servicios. El usuario administrador únicamente con este componente por medio del navegador. Este componente se compone de los siguientes componentes a través de los siguientes mecanismos: - Base de datos postgresql: JDBC-JPS/Hibernate. - Lógica de negocio: Archivos de mediación XML.
Aplicación de persistencia	Componente desarrollado en Java para registrar en base de datos o archivo consumos realizados a través de X-Road (queries) en los servicios intervenidos.
Lógica de negocio	Componente basado en el bus de servicios WSO2 que implementa el back-end de negocio del componente de transformación de servicios. Dentro de este componente se implementa el protocolo X-Road message protocol para REST y SOAP.
Persistencia	Base de datos postgresql: Base de datos que almacena la configuración (nombre de servicios web) del adaptador. Archivo plano: De manera alternativa la información se puede almacenar en un archivo plano en el disco donde se encuentra instalado el Adaptador.
Sistema de Información	Aplicación perteneciente a la entidad donde se exponen o consumen los servicios.
PC Usuario administrador	Cliente que se conecta al Adaptador o al Servidor de Seguridad para la configuración o administración.
Servidor de Seguridad X-Road	Servidor de Seguridad de la entidad que conectará con la Plataforma de Interoperación.

Se recomienda realizar el despliegue del componente de transformación de servicios en un servidor independiente al servidor utilizado para la instalación del Servidor de Seguridad de X-Road por las siguientes razones:

- Mantener la capacidad y disponibilidad del servidor de seguridad de X-Road.
- Mantener la capacidad y disponibilidad de cada uno de los componentes del adaptador.
- Evitar los recursos compartidos entre ambos componentes a nivel de bases de datos.

La siguiente tabla describe las características mínimas del servidor en donde se recomienda desplegar el componente de transformación.

Tabla 6. Requerimientos del componente Adaptador de transformación.

Ítem	Requisito	Explicación
1	Procesador Dual-core Xeon/Opteron de 4 GHz o superior.	Capacidad de procesamiento mínima. Recomendable 8 núcleos.
2	8 GB de RAM.	Memoria RAM mínima requerida. Recomendable 16 GB.
3	10 GB de espacio libre en disco.	Almacenamiento mínimo requerido. El espacio de almacenamiento debe ser acorde con la estimación de consumo y la decisión de almacenamiento en el archivo o base de datos.
4	Una tarjeta de interfaz de red de 1000 Mbps.	Red mínima requerida.

Puertos requeridos

5	http://IP_ADAPTADOR:8080/AdapterXRoad-web/	Puerto del componente Adap
6	http://IP_ADAPTADOR:8280/SERVICIO /	Servicios creados en el Wso2
7	http://IP_ADAPTER_API:8080/AdapterApi	Puerto del Componente Adap
8	https://IP_WSO2:9443/carbon	Administración de Wso2.

Software

9	Sistema operativo	La solución es multiplataforma. No
10	Componentes de software adicionales	Java 1.8

Para más detalles del Adaptador de integración, por favor consulte los documentos:

- Manual de Instalación del Adaptador de Consumo y Exposición de Servicios de X-Road 6.25. Está con versiones para Ubuntu, Red Hat 7 y Red Hat 8.
- Manual de Configuración del Adaptador de Consumo y Exposición de Servicios de X-Road 6.25.

6.8. ACUERDO DE VINCULACIÓN.

Para la vinculación oficial de entidades al Servicio Ciudadano Digital de Interoperabilidad, se debe entre la entidad y la Agencia Nacional Digital un acuerdo de entendimiento que describe el objeto y compromisos de las partes en la integración y la compartición de la información con las demás entidades públicas dentro de la plataforma de interoperabilidad con el propósito de facilitar el ejercicio de sus constitucionales y legales.

6.9. USO Y APROPIACIÓN.

Una vez finalizado la integración de la entidad a la plataforma de interoperabilidad PDI, la decisión pase a etapa de producción está en manos de la entidad, para ello se recomienda tener en cuenta lo :

El servicio de intercambio de información y los elementos de datos de la entidad debe estar certificados (3) de lenguaje común de intercambio

La entidad comprende el marco de interoperabilidad para gobierno digital el cual se fundamenta en de madurez basado en aspectos legales, técnicos y organizacionales que permite el desarrollo de los servicios de intercambio de información al interior de las entidades, estos dominios son:

Dominio Político – legal: Consiste en garantizar que las entidades públicas realizan el intercambio de información ajustado al marco jurídico vigente, las políticas y estrategias pueden trabajar juntas y no obstaculiza o impide la interoperabilidad.

Dominio Organizacional: se refiere al modo en que las misiones, políticas, procesos y expectativas con aquellos de otras entidades para alcanzar las metas adoptadas de común acuerdo y mutuamente a través del intercambio de información

Dominio Semántico: permite garantizar que, en el momento de intercambiar datos, el significado de la información sea exacto y el mismo para todas las partes interesadas. De igual manera, permite que las entidades del Estado colombiano puedan estandarizar, gestionar y administrar su información

Dominio Técnico: hace referencia a las aplicaciones e infraestructuras que conectan sistemas de información a través de los servicios de intercambio de información. Incluye aspectos como especificaciones de interfaces, protocolos de interconexión, servicios de integración de datos, presentación e intercambio de datos de comunicación seguros.

7. PROCESO DE VINCULACIÓN AL SERVICIO DE AUTENTICACIÓN DIGITAL.

El Servicio de Autenticación Digital tiene como objetivo verificar los atributos digitales de una persona para adelantarse trámites y servicios a través de medios digitales, afirmando que dicha persona es quien solicita el servicio. Este servicio permite generar un ambiente que habilita a los ciudadanos su acceso a los trámites y servicios de las 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 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 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 están asociadas al correo electrónico del usuario, una contraseña de acuerdo con el estándar NIST SP 800-63B de un solo factor o 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 están 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 o OTP, preguntas y respuestas, o 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 de los mecanismos que disponga la Registraduría Nacional del Estado Civil de sus funciones.

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

Tabla 7

Tipo de tramite	Grado de confianza	Requiere previa identificación con Registraduría	Consulta requerida
Riesgo de autenticación errónea nulo o mínimo	Bajo		N/A
Riesgo de autenticación errónea moderado	Medio	X	Consulta ANI y Sistema de Registro Civil – SIRC
Riesgo de autenticación errónea considerable	Alto	X	Consulta bases de datos biométricas
Riesgo de autenticación errónea elevada	Muy Alto	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 identificación 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 requerido.
- 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 los que se cuenta 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 establece 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 desde 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 en el registro.

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

7.1. OBJETIVOS DEL SERVICIO.

El Servicio de Autenticación Digital tiene un valor estratégico que permite ofrecer a las personas un conjunto de mecanismos de autenticación para acceder de un modo seguro y confiable a los servicios y que las entidades puedan confiar que quien accede a un servicio en línea es quien afirma ser, de acuerdo al 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.

La siguiente imagen presenta el diagrama de componentes general del Servicio de Autenticación Digital.

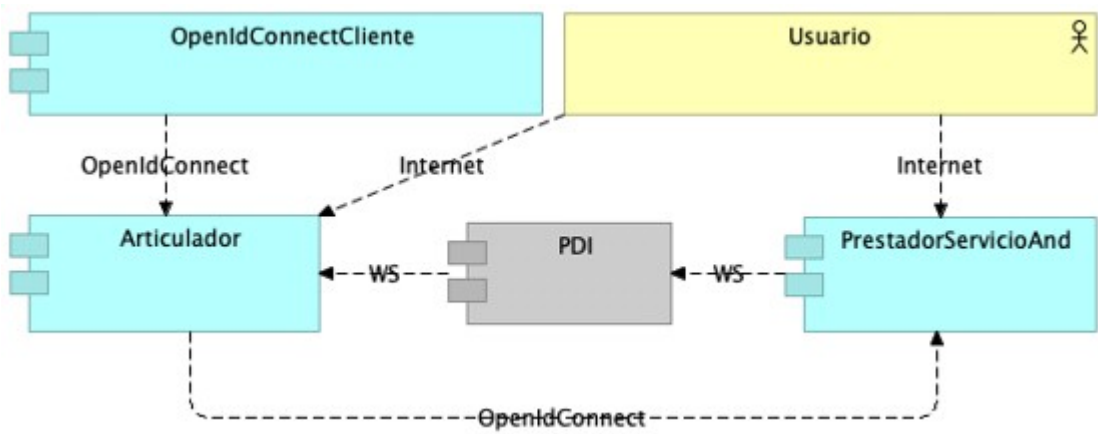


Figura 13 Componente del servicio de Autenticación Digital

Por medio de la siguiente tabla se describen cada uno de los componentes. En el diagrama se pueden observar los protocolos de integración entre los diferentes componentes.

Tabla 8 Descripción de componentes autenticación digital

Nombre elemento	Descripción
OpenId Connnect Cliente	Componente de integración opcional que se desplegaría en las entidades. Este componente implementa el protocolo OpenId Connect.
Articulador	Componente que representa la pasarela de autenticación.
Prestador Servicio And	Componente que tiene por objetivo la implementación de funcionalidades de un prestador de servicio para los grados bajo y medio.

OpenID Connect (OIDC) es el protocolo de uso estándar abierto, ligero e independiente de la plataforma para implementar la administración de identidades

7.2. REQUERIMIENTOS.

- Diagnóstico de los sistemas de información que van a hacer integrados en la plataforma de autenticación y/o autorización de usuarios
- Determinar el grado de confianza (bajo, medio, alto, muy alto), que requiere el trámite y selección de integración del sistema de información de la entidad con la plataforma de autenticación y selección adecuada. A Agencia Nacional Digital ofrece dos formas de integración: (i) librerías OpenId Connect para diferentes tecnologías, (ii) Servidor de integración OpenId Connect.
- La entidad debe disponer de un ambiente de pruebas, preproducción y producción para la integración del sistema de información con la plataforma de autenticación.

La autorización es realizada por el sistema de información de la entidad.

- El flujo implementado por el servicio de Autenticación Digital es OpenIDConnect Authorization

7.3. PREPARACIÓN.

- Diseño técnico para la integración de los sistemas de información de la entidad con la plataforma de autenticación digital. En caso de que las entidades cuenten con implementaciones cuyas funcionalidades similares a la del servicio de autenticación digital, se realizará una evaluación y análisis técnico con el fin de definir la solución de integración más apropiada.
- Construir un plan de trabajo de integración al servicio de autenticación digital.

7.4. ADECUACIÓN.

La Agencia Nacional Digital ofrece dos formas de integración las cuales son: empleando librerías OpenId Connect o empleando el servidor de integración OpenId Connect. Adicionalmente se debe tener en cuenta cualquiera de las formas de integración:

- Diseñar e intercambiar escenarios de casos de uso y diagramas de flujo de mensajes con la Agencia Nacional Digital para evitar cualquier ambigüedad en la comprensión del flujo de comunicación
- Establecer plan de integración que contemple pruebas funcionales y paso a producción.

7.5. INTEGRACIÓN.

Para la integración del componente la entidad cuenta con dos opciones:

7.5.1. EMPLEANDO LIBRERÍAS OPENID CONNECT.

La Agencia Nacional Digital entregará las librerías OpenIdConnect para las siguientes tecnologías:

- Librería de Integración Moodle
- Librería de Integración Drupal 7
- Integración al servicio de Autenticación con Angular y SpringBoot
- Integración al servicio de Autenticación con SpringBoot
- Librería de Integración Java EE
- Librería de Integración Keycloak
- Librería de Integración Node.js
- Librería de Integración JavaScript
- Librería de Integración.Net Core
- Librería de Integración Drupal 8
- Librería de Integración Drupal 9
- Librería Django – Python
- Librería ASP.NET Framework
- Librería de Integración PHP sin framework

Las entidades con estas librerías deberían realizar los siguientes pasos:

1. Importar dentro del proyecto de implementación de cada sistema de la entidad la librería.
2. La entidad podrá implementar una de las dos pantallas para la integración que se describen a continuación:
 - Pantalla Formulario con campos. Por medio de esta integración, desde el cliente se puede optimizar la experiencia de usuario para el flujo de autenticación. Si bien la integración sigue siendo con Pantallas de pasarela no se mostrarían para la autenticación.
 - Pantalla sin formulario con botón únicamente de inicio sesión. Por medio de esta integración no hay ninguna optimización en la experiencia de usuario para ningún flujo ya que no hay datos a validar desde el cliente. Por lo tanto, siempre se mostrarán las pantallas de pasarela.
3. Implementar pantalla Formulario con campos de autenticación en el sistema de información de la entidad para capturar los siguientes datos según corresponda:
 - Tipo de persona (natural o jurídica)
 - Tipo de acceso
 - Id_usuario
 - Nit

- Dígito de verificación
- Botón Entrar
- Botón Registrarse

4. Implementar pantalla con botón de inicio de sesión/registro

5. Implementar pantalla de inicio de sesión para redireccionar al usuario luego de autenticarse en el Autenticación Digital. Esta pantalla deberá tener un controlador que permitirá leer los siguientes parámetros GET enviados desde el Autenticador Digital.

- Id_token
- Code (correspondiente al authorization_code)

Luego de leer estos atributos, el controlador deberá crear el objeto de sesión del ciudadano y esta se creará por el sistema de información de la entidad.

6. Implementar pantalla de cierre de sesión para redireccionar al usuario cuando se ha cerrado sesión en el servicio de Autenticación Digital. Esta pantalla deberá tener un controlador que permita eliminar todos los objetos de sesión (cookies de sesión), en el sistema de información de la entidad.

7. Cada librería OpenIdConnect tendrá un archivo readme en donde se describirán las clases/objetos que deberán instanciar por parte de la capa de presentación de la aplicación de la entidad (mencionado en el paso anterior), para hacer uso de las siguientes funcionalidades:

- Authorize (Registro y autenticación). Para este caso, al momento de instanciar/invocar el Authorize, se deberán enviar los siguientes parámetros:

- Client_id
- Response_type: code id_token o únicamente code. Incluir id_token como parte del response_type requerir información adicional del usuario para realizar el proceso de autorización en el sistema de información de la entidad.
- Scope: openid, email (Estos parámetros se pueden cambiar y serán definidos en la fase 1. Definición de integración del Marco de Implementación del servicio de Autenticación Digital del Documento de Vinculación y uso de los servicios ciudadanos digitales)
- Redirect_uri: Parámetro returnUrlLogIn definido en el siguiente paso.
 - Token (Endpoint para obtener el Access_token, Refresh_Token, id_token) del servicio de Autenticación Digital. La librería se encargará de generar la petición post a este servicio web, pero se le debe enviar los siguientes datos:
- authorization_code (recibido anteriormente por el Authorize)
- client_id
- client_secret
- redirect_uri (Parámetro returnUrlLogIn definido en el siguiente paso).

- UserInfo (Obtener información adicional del usuario. La librería implementará el contrato y le usará el usuario userInfo). La librería construirá la petición GET al servicio web enviando el token recibido anteriormente por medio del header.
- Authorization Bearer. El sistema de información de la entidad deberá recibir la petición y gestionar la información del usuario en su sistema de información.
- EndSession. Si bien esta funcionalidad es implementada por la librería, se deberá enviarle a la entidad el id_token para cerrar la sesión en el Autenticador Digital. Una vez la entidad recibe el id_token de cierre de sesión, deberá implementar la eliminación de la sesión del usuario.

8. Configurar los siguientes parámetros en el archivo de configuración descrito en el archivo readme:

- Client_id (parámetro entregado por el administrador del servicio de autenticación digital de la Agencia Nacional Digital).

- Client_secret (parámetro entregado por el administrador del servicio de autenticación digital de la Agencia Nacional Digital).

- redirectUrlLogIn (parámetro definido por la entidad. Es el endpoint que se invoca desde el servicio de autenticación digital para redireccionar al ciudadano al sistema de la entidad luego de iniciar sesión).

- redirectUrlEndSession (parámetro definido por la entidad. Es el endpoint que se invoca desde el servicio de autenticación digital para redireccionar al ciudadano al sistema de la entidad cuando se ha cerrado sesión).

- authorizeEndPoint (parámetro entregado por el administrador del servicio de autenticación digital de la Agencia Nacional Digital).

- endSessionEndPoint (parámetro entregado por el administrador del servicio de autenticación digital de la Agencia Nacional Digital).

- tokenEndPoint (parámetro entregado por el administrador del servicio de autenticación digital de la Agencia Nacional Digital).

- userInfoEndPoint (parámetro entregado por el administrador del servicio de autenticación digital de la Agencia Nacional Digital).

7.5.2. EMPLEANDO EL SERVIDOR DE INTEGRACIÓN OPENID CONNECT.

La Agencia Nacional Digital implementa un componente de integración al servicio de Autenticación Digital que busca:

1. Simplificar la implementación en las aplicaciones de las entidades para integrarse al servicio de Autenticación Digital.

2. Encapsular las funcionalidades del protocolo OpenId Connect con el objetivo de tener una integración transparente al servicio de autenticación digital.

A continuación, se describen los pasos que se deberán llevar a cabo por parte de la entidad:

1. Instalación de servidor con las siguientes características:

- Requiere servidor

- Sistema operativo Windows/Linux cualquier distribución

- Arquitectura del Sistema: 64 bits.
- Tipo Procesador: Intel Xeon Quad Core.
- Cantidad de Procesadores: 2 cores.
- Memoria mínima 8GB
- Disco duro 500 GB
- JDK 13

2. Configurar parámetros en archivo xml indicado en readme del componente:

- Client_id (parámetro entregado por el administrador del servicio de autenticación digital de la Ag Nacional Digital).
- Client_secret (parámetro entregado por el administrador del servicio de autenticación digital de la Nacional Digital).
- returnUrlLogIn (parámetro definido por la entidad).
- returnUrlEndSession (parámetro definido por la entidad).

3. Desplegar EAR componente de integración OpenId Connect siguiendo los pasos descritos en el a readme entregado por la Agencia Nacional Digital.

4. Instalar base de datos mysql 8.0.18 y ejecutar el script.sql entregado por la Agencia Nacional Dig

5. En el sistema de la entidad se deberá:

- Importar 2 archivos JavaScript, el primero, es de configuración el cual se deberá actualizar con lo sistema de información de la entidad. El segundo, corresponde a la lógica del manejo de sesión del transversal en el sistema de información de la entidad. El manejo de sesión será por manejo de cool
- En la pantalla de presentación del sistema de información de la entidad, se deberá agregar un com <DIV> y una función JavaScript al final de este elemento de presentación.
- Implementar cliente consumo de servicio rest en el sistema de información de la entidad. El servicio expuesto por el componente de integración OpenId Connect y se le deberá enviar el id_session recibido anteriormente. El servicio retorna un objeto json con la información del usuario.

7.5.3. IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD.

- Determinar que todas las comunicaciones a través de la red deben estar cifradas. garantizando que comunicaciones se realicen a través del protocolo HTTPS utilizando el cifrado TLS 1.2 en adelante
- Proporcionar claves para los algoritmos criptográficos asimétricos como por ejemplo RSA SHA 5
- Proteger las cookies/objetos de sesión de autenticación para que no estén expuestas a ningún softw en el dispositivo del usuario
- Emplear Secure DNS para evitar ataques de spoofing.
- No almacenar en control de código fuente, credenciales, llaves o contraseñas.

7.6. INTEGRACIÓN DE LA ENTIDAD COMO FUENTE DE ATRIBUTOS.

En esta sección se describe la metodología que se lleva a cabo para ser un sistema de fuentes de atributo sistema de autenticación digital NG2 al flujo de registro y recuperación de contraseña.

La siguiente imagen presenta la metodología.

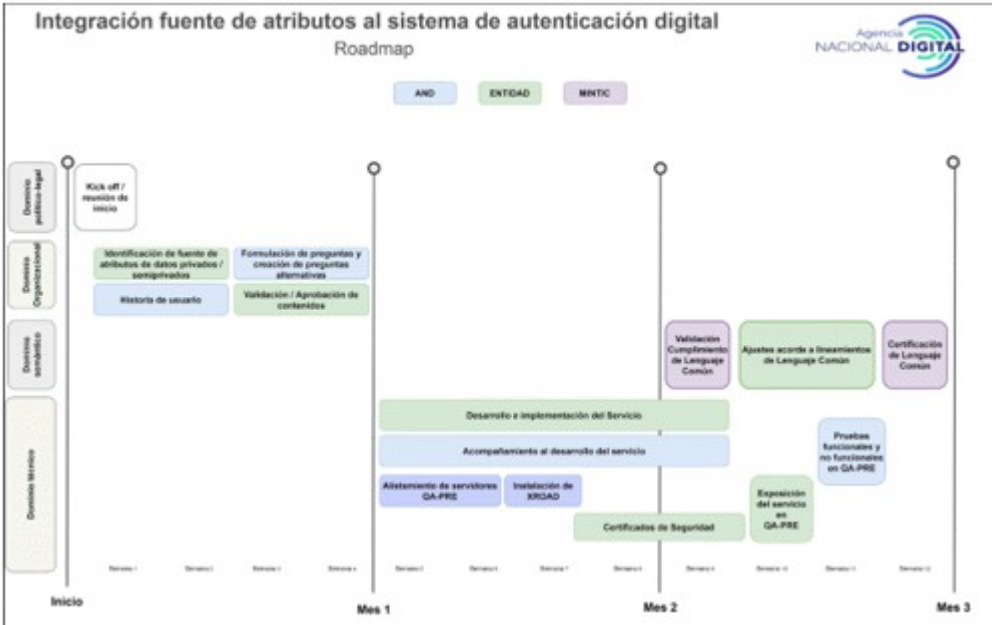


Figura 14 Road Map para la integración como fuente de atributo

Por medio de la siguiente tabla se describen cada una de las actividades/validaciones del diagrama presentado.

Tabla 9

Nombre Actividad	Descripción
1. Kick off/ reunión de inicio	En esta actividad se realiza una contextualización sobre el servicio de a sus niveles de garantía, la arquitectura del servicio de Autenticación característica de los datos o atributos (semi privados, privados, ma información, obligatorios, entre otros), que son candidatos a ser generación de preguntas reto. Una vez la entidad revisa las caracterí atributos, se comparte el diccionario de datos candidatos con su descrip de pruebas para su posterior análisis.
2. Identificación de fuente de atributos de datos privados y semiprivados	La entidad conocedora de los datos existentes en sus bases de datos i datos privados y semiprivados que sirvan para realizar preguntas reto. La Agencia Nacional Digital analiza cada uno de los atributos y se candidatos a ser fuente de atributos a la generación de preguntas reto.
3. Historia de Usuario	La Agencia Nacional Digital elabora una historia de usuario donde s los estados de conexión del servicio a construir.
4. Formulación de preguntas y respuestas alternativas.	Con los datos identificados, la Agencia Nacional Digital formula pr cada uno de los datos. La Agencia Nacional Digital crea las listas de respuestas alternativas.
5. Validación/ aprobación contenido.	La entidad valida las preguntas y respuestas trabajadas por la Agen Digital.

6. Desarrollo e implementación del servicio.	Una vez realizado el diseño técnico, se deberá implementar el servicio de exposición por parte de la entidad fuente de atributos. Este servicio será desde el servicio de Autenticación Digital cuando se va a realizar un cambio de contraseña. Si la integración se realiza de la manera anteriormente, el módulo de preguntas reto del servicio de Autenticación Digital generará las preguntas reto y además la validación de las respuestas. De esta manera se optimiza el acceso y disponibilidad de los sistemas de información de las entidades fuente de atributos.
7. Acompañamiento al desarrollo del servicio	La Agencia Nacional Digital durante la etapa de desarrollo del servicio ayudará y acompañará el desarrollo según lo requiera la entidad.
8. Alistamiento de servidores de seguridad	El consumo del servicio expuesto por la entidad se realizará a través de la plataforma de interoperabilidad de X-Road, de manera paralela al consumo de la entidad deberá trabajar en el alistamiento de los servidores de seguridad en los ambientes de prueba, preproducción y producción.
9. Instalación del X-Road	Una vez se tengan los servidores de seguridad la entidad debe instalar el X-Road. La Agencia Nacional Digital brinda apoyo en esta instalación.
10. Validación de cumplimiento de lenguaje común	Una vez desarrollado el servicio que expone las fuentes de atributo, la entidad deberá solicitar al Ministerio el certificado de lenguaje común.
11. Exposición del servicio	Teniendo el certificado de lenguaje común se expondrá el servicio por lo que se validará comunicación con el servicio de autenticación digital.
12. Pruebas funcionales y no funcionales	Al finalizar la implementación, se deberán llevar a cabo las siguientes pruebas: - Pruebas de conectividad - Pruebas de acceso - Pruebas de consumo al servicio expuesto por la entidad - Pruebas de consumo sobre X-ROAD - Pruebas desde módulo PyR del servicio de Autenticación Digital

7.7. INTEGRACIÓN DE ENTIDADES PÚBLICAS COMO PRESTADORAS DEL SERVICIO.

Los Prestadores de Servicios Ciudadanos Digitales Especiales que ofrezcan el servicio de autenticación interactúan con la pasarela de autenticación digital por medio del protocolo OpenID Connect y sus

- Las aplicaciones de las entidades solo deben conocer e interactuar con la pasarela de servicios, un token (STS) que encapsula la comunicación con otros Prestadores de Servicios Ciudadanos Digitales Especiales. Esto significa que se pueden modificar los Prestadores de Servicios Ciudadanos Digitales sin necesidad de actualizar las aplicaciones de las entidades.

- Los Prestadores de Servicios Ciudadanos Digitales Especiales por lo general tienen un conjunto de atributos de los Usuarios, el componente de pasarela permite normalizar la información de tal forma que se interactúa con las entidades, reciben siempre la información en un formato único.

- Los Prestadores de Servicios Ciudadanos Digitales Especiales no tienen que configurar cada una de las aplicaciones de las entidades dentro de sus sistemas de autenticación digital.

Diagnóstico del sistema de autenticación actual de la entidad, se identifica el protocolo de autenticación implementado, las bases de datos de usuario, atributos de usuarios almacenados, sistemas integrados, infraestructura utilizada, sistemas de seguridad, identificar los mecanismos de autenticación que actualmente están implementados, entre otros.

Diseño de la solución de integración al servicio de autenticación digital, se deberá revisar y diseñar la migración de usuarios. Tener en cuenta que se toma el ID de usuario como elemento de migración de atributos y credenciales de los usuarios. La migración consiste en pasar el ID del usuario a la base de datos maestra del servicio de autenticación digital que administra el articulador del servicio. Esto para que

momento de que el usuario inicia el flujo de autenticación, el articulador enrute el usuario hacia el servicio que está inscrito para que allí realice el proceso de autenticación.

Implementar la integración de autenticación con el componente del articulador de autenticación. Si la entidad ya implementa el protocolo OpenID Connect 1.0, no será necesario el desarrollo de un adaptador. De lo contrario se deberá llevar a cabo esta implementación para integrarla con el articulador de autenticación.

Implementación y uso de la plataforma de interoperabilidad para la sincronización y monitoreo con el componente del articulador de autenticación. La entidad deberá implementar servicios web para lograr la integración completa al servicio de autenticación digital. El detalle de los servicios se establece en la solución.

Realizar la configuración correspondiente del nuevo prestador en el componente del articulador de autenticación.

Los numerales de diagnóstico y diseño de la solución se realizará en acompañamiento con la Agencia Digital.

7.8. RECOMENDACIONES DE SEGURIDAD.

- Siempre se debe emplear SSL, incluso para los ambientes de desarrollo.
- En caso de emplear secretos compartidos⁽⁴⁾, estos NO PUEDEN estar en control de código fuente de aplicaciones y su manejo debe conformar el estándar de seguridad.
- Emplear mitigaciones para vulnerabilidades XSS, CSRF, en particular soportar HSTS, Content Security Policy.
- Verificar Cross Origin Request Site (CORS) para habilitar el envío de cookies solamente al servicio de autenticación y sitios verificados.

7.9. USO Y APROPIACIÓN.

Para un uso adecuado se realizan las siguientes recomendaciones de seguridad:

- Siempre se debe emplear SSL, incluso para los ambientes de desarrollo. Tener en cuenta TLS 1.2.
- En caso de emplear secretos compartidos, estos NO PUEDEN estar en control de código fuente de aplicaciones y su manejo debe conformar el estándar de seguridad.
- Emplear mitigaciones para vulnerabilidades XSS, CSRF, en particular soportar HSTS, Content Security Policy.
- Verificar Cross Origin Request Site (CORS) para habilitar el envío de cookies solamente al servicio de autenticación y sitios verificados.
- Realizar capacitaciones y/o manuales dirigidos a los usuarios que hagan uso de la plataforma de autenticación.

En caso de eliminación de un trámite o servicio:

- Todos los tokens de acceso de seguridad emitidos para esa parte de confianza deben ser revocados inmediatamente.

- Toda la configuración relacionada con la parte que confía debe ser borrada / deshabilitada / revocados los atributos client_id, client_secret, urls deberán ser deshabilitados. Para conocer todos los atributos de configuración, ver Anexo Técnico en el capítulo de Autenticación Digital.

- La entidad debe eliminar la opción para iniciar / cerrar sesión a través del proveedor de identidad usuarios.

- Se debe solicitar a la parte que confía que borre todos los datos del usuario según el acuerdo adquirido con el proveedor de identidad.

8. PROCESO DE VINCULACIÓN AL SERVICIO DE CARPETA CIUDADANA DIGITAL.

El servicio ciudadano digital de carpeta es aquel que les permite a las personas naturales o jurídicas gestionar digitalmente el conjunto de sus 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 normativa vigente. 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 y el fomento a la conectividad de los ciudadanos.

Como servicio común a las entidades públicas, el servicio de Carpeta Ciudadana trabaja de manera integrada 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 ciudadano desde los custodios responsables en la administración pública.

La siguiente imagen presenta el diagrama de componentes general del Servicio de Carpeta Ciudadana Digital.

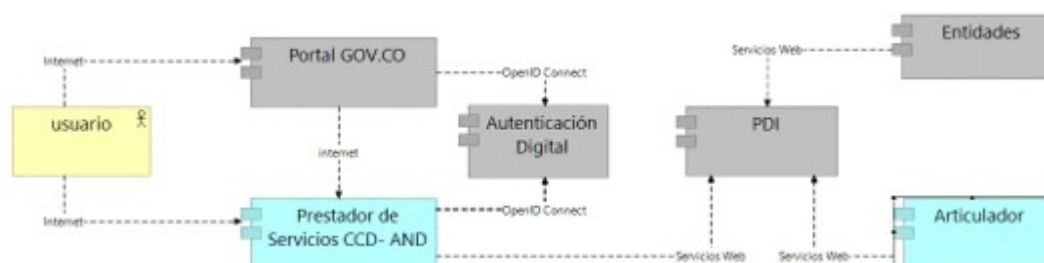


Figura 15 Diagrama de componentes carpeta ciudadana digital

Tabla 10 Descripción de componentes carpeta ciudadana digital

Nombre elemento	Descripción
Prestador de Servicios CCD-AND	Contiene el conjunto de componentes funcionales del servicio para el usuario, visualización de datos, configuración del servicio, historias de trámites y solicitudes, alertas y comunicaciones. Se relaciona con el servicio de autenticación digital para el acceso del usuario a la plataforma de interoperabilidad para el consumo de servicios de las entidades.
Articulador	Representa los componentes funcionales de administración y monitoreo del servicio del articulador. Se relaciona con el prestador de servicios CCD-AND a través de la plataforma de interoperabilidad.

8.1. REQUERIMIENTOS.

Basados en los requerimientos no funcionales y funcionales, establecidos en la guía de lineamiento implementación de los servicios ciudadanos digitales de MinTIC, el servicio de Carpeta Ciudadana criterios de diseño:

1. El usuario podrá acceder al Servicio de Carpeta Ciudadana Digital – CCD, se realizará por medio del Único del Estado GOV.CO.
2. La autenticación del usuario al Servicio de Carpeta Ciudadana se realizará usando el nivel de confianza del servicio de autenticación digital.
3. El consumo y exposición de servicios de Carpeta Ciudadana Digital, se hará a través de la PDI con diferentes Actores: Entidades Públicas y Articulador.
4. El servicio de CCD no almacenará de manera permanente los datos presentados a los usuarios y espacio de almacenamiento de documentos para el ciudadano.
5. Desde el servicio de CCD, el usuario no podrá realizar ningún trámite ante alguna entidad, por lo que el usuario será redireccionado al portal donde podrá iniciar el trámite.

8.2. PREPARACIÓN.

- Identificar las fuentes de datos que almacenan información de los usuarios de Carpeta Ciudadana
- Identificar de acuerdo con las funciones misionales y legales de la entidad, la información de la ciudadanía única.
- Clasificar la información conforme lo estipulado en la Ley [1712](#) del 2014 respecto al índice de información clasificada y reservada.
- Identificar los datos e información candidata a ser consultada y expuesta a los usuarios a través de Carpeta Ciudadana Digital
- Identificar las capacidades tecnológicas actuales para la integración al servicio de Carpeta Ciudadana ya que el servicio requiere la adopción de los lineamientos de servicio de interoperabilidad y el desarrollo de servicios de exposición de datos del ciudadano.

8.3. ADECUACIÓN.

- Construir el diseño técnico de la solución de integración al servicio de Carpeta Ciudadana Digital debe detallar cómo la entidad expondrá los servicios de consulta de información, los servicios de trámites y solicitudes, los servicios de alertas y comunicaciones de los trámites o actuaciones que se realice ante la entidad pública y las solicitudes de actualización y corrección de datos que los usuarios a través del servicio de Carpeta Ciudadana Digital.
- El diseño debe contemplar la utilización de la plataforma de interoperabilidad como servicio de intercambio de datos entre las entidades y los prestadores del servicio de Carpeta Ciudadana Digital.
- El diseño debe contemplar que el desarrollo o modificación de los servicios web de consulta de información que expone la entidad, deben hacerse de acuerdo con los lineamientos de desarrollo de servicios web que menciona el Marco de Interoperabilidad y la guía de uso y vinculación de entidades al servicio de interoperabilidad.
- Establecer los acuerdos de nivel de servicio (ANS) de cada uno de los servicios que exponen las entidades.

cara a la Carpeta Ciudadana Digital.

8.4. INTEGRACIÓN.

El intercambio de datos entre el servicio de Carpeta Ciudadana Digital y las entidades públicas se hace a través de la PDI, para ello la entidad deberá:

- Instalar y configurar un servidor de seguridad.
- Certificar los servicios de exposición y sus elementos de datos en el lenguaje Común de Intercambio de Datos.
- Integrar los servicios de exposición a la plataforma de interoperabilidad, que corresponde a la publicación de los end-point de los servicios web desarrollados para CCD en el servidor de seguridad que disponga la entidad.
- Autorizar en el servidor de seguridad el consumo de los servicios web por parte del servicio de Carpeta Ciudadana Digital.

Las entidades públicas para integrarse al servicio de Carpeta Ciudadana Digital requieren realizar las siguientes acciones:

8.4.1. DESARROLLAR LOS SERVICIOS DE EXPOSICIÓN.

Los servicios que se requieren que las entidades expongan al servicio de CCD son:

1. Servicios de consulta de información: Corresponden a la exposición del servicio de consulta de información. La entidad puede realizar un usuario para conocer la información que tiene la administración pública. Carpeta Ciudadana Digital realiza la petición con el número de identificación del usuario, tipo de documento y la respuesta del servicio deberá ser con los datos que tiene la entidad del usuario.
2. Servicios de alertas y comunicaciones: Corresponde al servicio que la entidad pública expone a la Carpeta Ciudadana Digital para informar acerca del estado de un trámite, de la finalización de un trámite, notificación de interés e información de recordación de un evento asociado a la interacción del usuario con la administración pública. Carpeta Ciudadana Digital realiza la petición con el número de identificación del usuario, tipo de documento y la respuesta del servicio deberá ser con la información de entidad, asunto, mensaje, texto del mensaje, fecha y la url de descargar de documentos si el mensaje lo requiere.
3. Servicios de historial de trámites: Servicio de exposición por parte de la entidad para la visualización del historial de trámites que ha realizado el usuario. Carpeta Ciudadana Digital realiza la petición con el número de identificación del usuario, tipo de documento y la respuesta del servicio deberá ser con la información de nombre del trámite, entidad, la fecha del trámite y el detalle de las consultas que se hicieron a otras entidades para resolverle el trámite al usuario.
4. Servicio de historial de solicitudes: Servicio de exposición por parte de la entidad para la visualización del historial de solicitudes de corrección, actualización o tratamiento de datos personales que ha realizado el usuario. Carpeta Ciudadana Digital realiza la petición con el número de identificación del usuario, tipo de documento y la respuesta del servicio deberá ser con la información del nombre de la solicitud, entidad, estado de la solicitud y la respuesta a la solicitud.

Aunque dentro de la carpeta ciudadana la entidad puede publicar servicios independientes, se recomienda como una buena práctica, tener un servicio de consulta de información bajo el cual se publicarán los otros servicios como historiales y alertas.

Para el desarrollo de los servicios web de exposición de las entidades se define realizarse bajo la tecnología de la Carpeta Ciudadana Digital.

REST, Content-type: Application/json, con el objetivo de estandarizar y optimizar la integración al Carpeta Ciudadana Digital.

Las siguientes tablas corresponden a la descripción de los servicios web de exposición hacia el serv Carpeta Ciudadana Digital

Servicio web de alertas y comunicaciones

Propiedad	Descripción
Technology	REST
Content-Type	application/json
Componente que lo expone	Componente de Integración con Otros sistemas
Request	/alertasycomunicaciones/{tipoid}/{idUserario}
Parámetros del request	
/ {tipoId}	Tipo de identificación del usuario.
/ {idUserario}	Número de identificación de la persona de la cual se buscan comunicaciones a enviar en la petición
Response	{ "mensajeColeccion": [{ "idMensaje": "", "asunto": "", "textoMensaje": "", "urlDescargueAdjuntos": "", "fechaMensaje": "" }, ...] }
idMensaje	Identificador único del mensaje (Alerta o Comunicación) ante
- asunto	Asunto de la Alerta o Comunicación
- textoMensaje	Texto con el contenido del mensaje que se quiere enviar a la p
- urlDescargueAdjuntos	URL donde puede descargar el adjunto al mensaje
- fechaMensaje	Fecha del mensaje AAAA-MM-DD

Servicio Web de Consultar Información del usuario

Propiedad	Descripción
Technology	REST
Content-Type	application/json
Method	GET
Request	/servicio/{tipoid}/{idUserario}
Parámetros del request	
/ {tipoId}	Tipo de identificación del usuario.
/ {idUserario}	Número de identificación de la persona de la cual se información a enviar en la petición.

Response

La respuesta es un arreglo JSON de objetos llamado datoConsultado que tiene dos campos (c valorDato). Adicionalmente, un campo llamado urlDescarga. A continuación, se presenta una la respuesta JSON

Cuando campoDato NO tienen el texto archivoBase64 o archivoURL para descarga de archivo	Cuando campoDato tiene el texto archivoBase64 o archivoURL para descarga del archivo.
<pre>{ "datoConsultado": [{ "campoDato ":"", "valorDato ":"" },...], "urlDescarga ":"" }</pre>	<pre>{ "datoConsultado": [{ "campoDato ":" ", "valorDato ":" ", "tipoArchivo ":" ", "nombreArchivo ":" ", "descripcionArchivo ":" ", },...], "urlDescarga ":" " }</pre>
campoDato	Cuando es un archivo en base64 para ser descargado, el campoDato debe tener el texto "archivoBase64". Cuando es una ruta de archivo, el campoDato debe tener el texto "archivoURL"
valorDato	Cuando campoDato contenga la palabra "archivoBase64" deberá contener la cadena base64 del archivo. Cabe mencionar que el archivo no debe superar los 10 MB de tamaño o si se trata de varios archivos, en total no deben superar los 10MB. Cuando campoDato contenga la palabra "archivoURL": valorDato debe ser la ruta http publica para la descarga del documento. Esto cuando el archivo(s) en total supere(n) los 10 MB de tamaño o la intención es establecer una URL para descargar el archivo. Cuando campoDato contenga la palabra "archivoBase64Todos", se entiende que viene un archivo.zip en base64 con todos los archivos por descargar y su tamaño no debe superar las 10MB.
tipoArchivo	Corresponde al tipo de archivo del documento a descargar. Solo se maneja "PDF".
nombreArchivo	Corresponde al nombre con el cual se guardará el nombre del archivo al descargarse.
descripcionArchivo	Corresponde a la descripción del archivo que se va a descargar.
urlDescarga	URL para descargar archivo de resultado del servicio.

Servicio Web de historial de solicitudes

Propiedad	Descripción
Technology	REST
Content-Type	application/json
Method	GET
Request	/solicitudesusuarios/{tipoid}/{idUserio}
Parámetros del request	
/ {tipoId}	Tipo de identificación del usuario.
/ {idUserio}	Número de identificación de la persona de la cual se buscan comunicaciones a enviar en la petición
Response	{ "solicitudesPqr": [{ "idSolicitud": "", "nomSolicitud": "", "fechaSolicitud": "", "estadoSolicitudPqrUsuario": "", "textoRespuesta": "" }, ...] }
idSolicitud	Identificador único de la solicitud dado por la Entidad
nomSolicitud	Texto descriptivo de la solicitud que realiza el usuario
- fechaSolicitud	Fecha en la cual la Entidad registra la solicitud del usuario , DD HH24:MM:SS.FF
- estadoSolicitudPqrUsuario	Estado en el cual se encuentra la solicitud realizada por el usuario
- textoRespuesta	Cuerpo de la respuesta de la entidad al usuario
- Technology	REST

Servicio Web de historial de trámites

Propiedad	Descripción
Technology	REST
Content-Type	application/json
Método	GET
Componente que lo expone	Componente de Integración con Otros sistemas
Request	/tramitesinicializadosusuarios/{tipoid}/{idUserio}
Parámetros del request	
/ {tipoId}	Tipo de identificación del usuario.
/ {idUserio}	Número de identificación de la persona de la cual se buscan comunicaciones a enviar en la petición
Response	{ "tramiteUsuarioEntidad": [{ "idTramiteEntidad": "", "nomTramiteGenerado": "", "fechaRealizaTramiteUsuario": "", "servicioConsulta": "", "estadoTramiteUsuario": "", "entidadConsultada": [{ "nomEntidad": "", "fechaConsulta": "" }] } }

	}...] }...] }
- idTramiteEntidad	Identificador único del trámite dado por la Entidad
- nomTramiteGenerado	Nombre del Trámite realizado por el usuario
- fechaRealizaTramiteUsuario	Fecha en la cual el usuario realizó el Trámite AA. HH24:MM:SS.FF
- servicioConsulta	Nombre del servicio de consulta de información del usu Entidad desde donde se inicializa el Trámite debe ser el m registra en servicio CCD
estadoTramiteUsuario	Estado del Trámite en la entidad
- Elemento: entidadconsultada	
- nomEntidad	Nombre de la Entidad consultada por la Entidad donde el usu trámite para dar resolución al mismo
- fechaConsulta	Fecha de la consulta

1 Integrar los servicios web a la plataforma de interoperabilidad

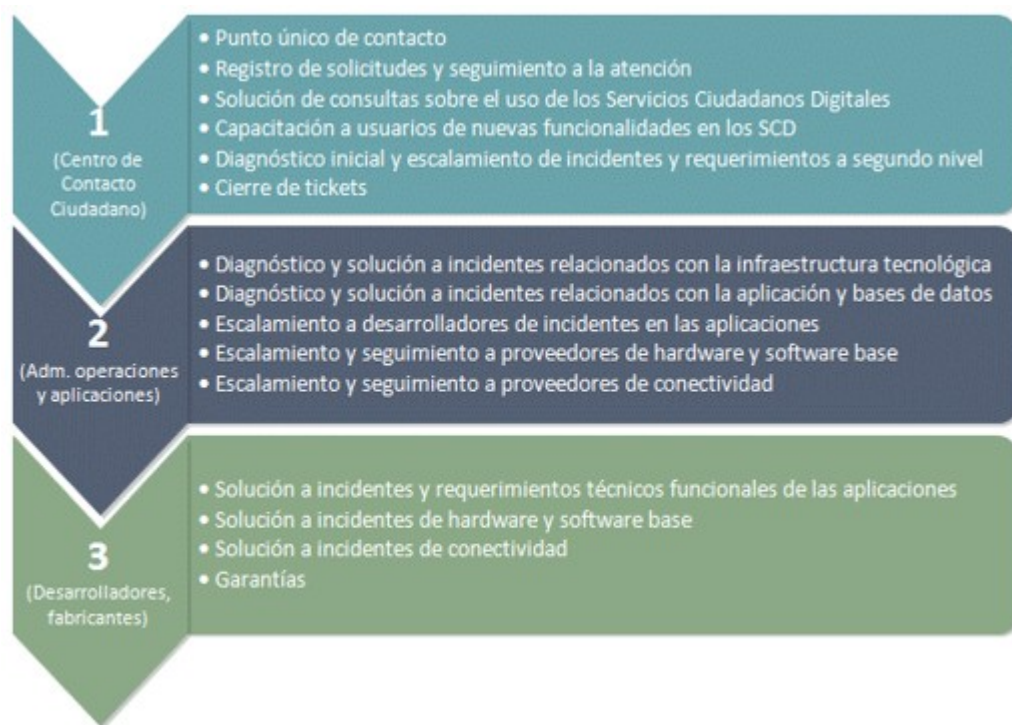
El intercambio de datos entre el servicio de Carpeta Ciudadana Digital y las entidades públicas se h
de la PDI, para ello la entidad deberá:

- Instalar y configurar un servidor de seguridad.
- Integrar los servicios de exposición a la plataforma de interoperabilidad, que corresponde a la pub
end-point del servicio web de consulta de información, de alertar y comunicaciones y de temas de i
- Autorizar en el servidor de seguridad el consumo de los servicios web por parte del servicio de C
Ciudadana Digital.

El detalle de la integración a la PDI se encuentra en la sección de integración al servicio de interop
este documento.

9. MESA DE SERVICIO DE LOS SERVICIOS CIUDADANOS DIGITALES.

El modelo para la atención de solicitudes acerca de los Servicios Ciudadanos Digitales comprende
niveles de atención: el primer nivel de servicio será prestado por el Centro de Contacto al Ciudadar
Ministerio TIC, el segundo y tercer nivel será prestado por la Agencia Nacional Digital.



<NOTAS DE PIE DE PÁGINA>

1. <http://lenguaje.mintic.gov.co/marco-de-interoperabilidad>
2. Por sus siglas en inglés (Certification Authority).
3. <https://csrc.nist.gov/glossary/term/Online-Certificate-Status-Protocol>
4. 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.

INFORME TÉCNICO.

VINCULACIÓN A SERVICIOS CIUDADANOS BASE /X-ROAD DE EMPRESAS PRIVADAS

Contexto

Conforme al principio de “masificación del Gobierno en Línea”, consagrado en el numeral 8 del artículo 10 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 ejercicio de sus funciones.

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones (DUR-TIC), “[l]a Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de alcanzar el objetivo (...)”.

Igualmente, indica el artículo [2.2.9.1.1.1](#) del mismo decreto que la Política de Gobierno Digital es “el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio, mejorando la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitiendo el ejercicio de los derechos de los usuarios del ciberespacio”.

El artículo [90](#) del Decreto 2106 de 2019, “por el cual se dictan normas para simplificar, suprimir y reorganizar trámites, procesos y procedimientos innecesarios existentes en la administración pública”, señala que las autoridades deberán integrarse y hacer uso del modelo de Servicios Ciudadanos Digitales y se implantará por parte de las autoridades de conformidad con los estándares que establezca el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Los numerales 6 y 7 del artículo [2.2.17.1.4](#). del Decreto 1078 de 2015 definen la “Guía de lineamientos para la prestación de servicios ciudadanos digitales” como “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 servicios ciudadanos digitales debe cumplir con el fin de garantizar la correcta prestación de los servicios ciudadanos digitales”; y, asimismo, la “Guía de vinculación y uso de los servicios ciudadanos digitales” se define como el documento expedido y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones destinado a las autoridades receptoras de los servicios ciudadanos digitales, el cual indica las condiciones necesarias y los pasos que éstas deben seguir para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, 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.

El numeral 13 del artículo [2.2.17.1.4](#). del DUR-TIC define los Servicios Ciudadanos Digitales como “un conjunto de soluciones y procesos transversales que brindan al Estado capacidades y eficiencias para la transformación digital y para lograr una adecuada interacción con el ciudadano, garantizando el derecho de acceso y utilización de medios electrónicos ante la administración pública. Estos servicios se clasifican en servicios básicos y servicios especiales”.

El artículo [2.2.17.4.1](#). del DUR-TIC señala como obligaciones del MinTIC, en concordancia con el numeral 2 del artículo [18](#) de la Ley 1341 de 2009, entre otras, expedir y publicar la Guía de lineamientos para la prestación de servicios ciudadanos digitales y la Guía para vinculación y uso de los servicios ciudadanos digitales; las cuales fueron debidamente publicadas para participación ciudadana entre los días 5 de junio y el 6 de julio de 2019.

Mediante la Resolución [2160](#) de 2020, el Ministerio de las Tecnologías de la Información y las Comunicaciones expidió la “Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de los servicios ciudadanos digitales”.

En Colombia existen entidades privadas que están habilitadas para ejercer funciones públicas de acuerdo con los casos taxativamente señalados en la Constitución Política (artículos [48](#), [49](#), [68](#), [123](#), [210](#) y [365](#)) y las entidades pueden investirse de la autoridad del Estado. Dentro de las actividades que pueden ser delegadas a los privados, se encuentran, entre otras:

1. La seguridad social
2. La atención en salud
3. El saneamiento ambiental

4. La educación

5. La que desarrollan los notarios y los registradores

Teniendo en cuenta lo anterior y en el proceso de vinculación a los Servicios Ciudadanos Digitales (Decreto [620](#) ⁽²⁾ y Resolución [2160](#) ⁽³⁾, ambos de 2020) por parte de las entidades públicas de orden territorial, y en especial en el desarrollo de algunos proyectos propios de algunas de las entidades que prestan o realizan actividades públicas, se ha evidenciado la necesidad de contar con información que primaria son entidades privadas o se evidencia la necesidad de la participación de estas últimas respecto Hábeas Data y la reserva de la misma.

Por ejemplo, en el proyecto de Interoperabilidad de la Historia Clínica Electrónica (IHCE) (Ley 2011 de 2011) se requiere el intercambio de información de la historia clínica de Instituciones Prestadoras de Servicios de Salud (IPS) Públicas y Privadas; en el proyecto de diseño de automatización del trámite de cargue y de contratos en el Sistema Electrónico para la Contratación Pública (SECOP), la Agencia Nacional de Contratación Pública -Colombia Compra Eficiente- y la Superintendencia Financiera de Colombia, la necesidad de que sean las empresas aseguradoras quienes proporcionen la información sobre las pólizas de seguro de los contratos.

Por necesidades como las enunciadas anteriormente es necesario vincular al SCD Base de Interoperabilidad a estas entidades privadas, por lo que se deben precisar las condiciones legales, administrativas, funcionales y técnicas que correspondan.

Justificación

En particular, en el avance del proceso de vinculación a los Servicios Ciudadanos Digitales, se está adelantando desde MinTIC en coordinación con Ministerio de Salud y Protección Social (MinSalud), en el proyecto de Interoperabilidad de datos de la Historia Clínica Electrónica, proceso que requiere obligatoriamente la participación de las IPS públicas y privadas con el Ministerio de Salud y Protección Social, por las siguientes expuestas a continuación:

Uno de los derechos fundamentales de las personas, es el derecho a la salud (artículos [44](#) y [49](#) de la Constitución) mediante condiciones de accesibilidad, oportunidad y continuidad adecuadas respecto a los servicios prestados. Actualmente los prestadores de servicios de salud requieren datos de la Historia Clínica de las personas para apoyar el proceso de atención de salud, pero esta se encuentra de forma fragmentada y no estandarizada por cada uno de los prestadores de servicios de salud con los cuales un individuo se relaciona, lo que genera inconvenientes en la calidad, oportunidad y continuidad de la atención del mismo.

Para tal efecto, actualmente se desarrollan procesos de transformación digital⁽⁵⁾ en el sector de la salud, donde se han establecido los principios, las definiciones normativas y técnicas, los elementos de datos, los estándares internacionales a utilizar, protocolos de seguridad y en general los lineamientos que permitan avanzar en esta vía, pero garantizando la reserva y confidencialidad de la información que se genera. Estos lineamientos y reglamentaciones se deben establecer por parte del Ministerio de Salud y Protección Social y el Ministerio de Tecnologías de la Información y las Comunicaciones.

Las TIC aplicadas en el campo de la salud tienen el potencial de optimizar el gasto, mejorar la calidad de la asistencia, contribuir a la seguridad y la equidad en la atención de los pacientes. Por otro lado, el sector de la salud en Colombia demanda un alto grado de intercambio de información entre las IPS, tanto públicas como privadas, para mejorar la continuidad en la asistencia médica, contar a tiempo con la información de las personas, fortalecer la toma de decisiones por parte de los profesionales de la salud, agilizar el acceso y ejercicio de los derechos a la salud, combatir la corrupción y fomentar la competitividad del sector y del país.

En Colombia, la información clínica de los pacientes se encuentra actualmente fragmentada y dispuesta en múltiples bases de datos, múltiples sistemas de información y tecnologías no integradas.

Dado lo anterior, en coordinación entre el Ministerio de Tecnologías de la Información y las Comunicaciones y el Ministerio de Salud y Protección Social, en Colombia se ha desarrollado el Modelo tecnológico de Interoperabilidad de la Historia Clínica Electrónica (IHCE), un modelo que permite que los prestadores de servicios de salud realicen el intercambio de un conjunto de datos clínicos y administrativos de un paciente, utilizando además estándares semánticos y técnicos internacionales, con lo cual se buscan obtener los beneficios ya mencionados.

Este mecanismo beneficia a toda persona en Colombia que requiera de la prestación de un servicio de salud, independientemente de su posición geográfica, si pertenece o no a uno de los regímenes del sistema de seguridad social en Colombia o si es nacional o extranjero. Al menos 50 millones de colombianos se verán beneficiados.

La IHCE se desarrolló en el marco de la Política de Gobierno Digital a través de la utilización de los Ciudadanos Digitales, los cuales tienen tres componentes: 1) Autenticación Digital, 2) Interoperabilidad de la información a través de la herramienta X-Road, y 3) Carpeta Ciudadana Digital. Además, se aplican las políticas de seguridad de la información, datos abiertos, inteligencia artificial, “machine learning” y “block chain” para la transformación de la política pública en el país y de esta manera poder encaminar al Estado colombiano hacia la cuarta revolución industrial.

En Colombia, se avanza en la implementación del modelo en las regiones a través de los prestadores de servicios de salud públicos, sin embargo, el servicio de salud en el país es prestado también por entidades privadas lo que permite la universalidad y el cubrimiento del servicio de salud pública en más del 95% de la población del país. Al implementar el modelo de interoperabilidad de datos de la historia clínica en Colombia utilizando la plataforma de interoperabilidad del Estado Colombiano, es decir la herramienta X-Road, es necesario incluir al sector privado de salud en el uso de dicha herramienta, asegurando como ya se establece en la Ley 100 de 1993, las condiciones de confidencialidad, integridad, accesibilidad, oportunidad y continuidad adecuadas.

La Ley 100 de 1993 en su artículo 4 establece que: “La Seguridad Social es un servicio público obligatorio que la dirección, coordinación y control están a cargo del Estado y que será prestado por las entidades públicas o privadas en los términos y condiciones establecidos (...)”.

Adicional a lo anterior, la Ley 215 de 2020, por medio de la cual se crea la historia clínica interoperable, establece en el artículo 3, correspondiente al ámbito de aplicación, lo siguiente:

“Los prestadores de servicios de salud están obligados a diligenciar y disponer los datos, documentos y expedientes de la historia clínica en la plataforma de interoperabilidad que disponga el Gobierno Nacional”.

Además, el artículo 4 de la citada Ley señala:

- “Los Ministerios de Salud y Protección Social y el de Tecnologías de la Información y las Comunicaciones, o aquellos que hagan sus veces, reglamentarán el modelo de Interoperabilidad de la Historia Clínica Electrónica (IHCE) y el Ministerio de Tecnologías de la Información y las Comunicaciones será el responsable de la administración de la herramienta tecnológica de la plataforma de interoperabilidad.”

Parágrafo. El modelo de Interoperabilidad de la Historia Clínica Electrónica deberá ser reglamentado en un término máximo de doce (12) meses, contados a partir de la entrada en vigencia de la presente ley” (fuera de texto)

En el artículo 12 de la ley antes citada se establece la prohibición de divulgar datos de cualquier persona consignados en la Historia Clínica Electrónica, mientras que en el artículo 13 se establecen disposiciones generales en cuanto a la Seguridad de la información y seguridad digital.

Por su parte, la Resolución 866 de 2021 del Ministerio de Salud y Protección Social y del Ministerio de Tecnologías de la Información y las Comunicaciones que reglamenta inicialmente la Ley 2015 de 2013 establece:

“Artículo 2. **Ámbito de aplicación.** Las disposiciones contenidas en el presente acto administrativo aplicables a los actores que a continuación se relacionan, quienes deberán cumplir los lineamientos establecidos en el marco de interoperabilidad para Gobierno Digital y el modelo de seguridad y privacidad política de gobierno digital:

2.1 La persona titular de la historia clínica.

2.2 Los prestadores de servicios de salud públicos y privados.

2.3 Las Entidades Promotoras de Salud -EPS.

2.4 Las Entidades Adaptadas al Sistema General de Seguridad Social en Salud - SGSSS.

2.5 Las Entidades que administren planes voluntarios de salud.

2.6 Las Administradoras de Riesgos Laborales y los fondos de pensiones en sus actividades de salud.

2.7 Las entidades pertenecientes a los Regímenes de Excepción o Especial de salud, Las secretarías, unidades administrativas departamentales, distritales y municipales de salud, siempre que accedan a la información de forma innominada.

2.9 Las compañías de seguros que emiten pólizas de seguros de accidentes de tránsito, siempre que cuenten con la autorización del titular de la información o de quien este legitime para autorizar el conocimiento de la información.

(...)

Artículo 23. **Servicios ciudadanos digitales.** Los sujetos referidos en el artículo 2o de la presente resolución deberán cumplir las condiciones y estándares establecidos en la guía para vinculación y uso de los servicios ciudadanos digitales que se encuentran señaladas en el Anexo Técnico 2 de la Resolución 2160 de 2013 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales se integran a sus sistemas de información los mecanismos de interoperabilidad”.

Por consiguiente, los sujetos obligados a la política de gobierno digital y los actores privados, para el cumplimiento y prestación de servicios, deben interoperar con las autoridades públicas.

Desarrollo técnico

Para realizar la conexión de los servidores de seguridad de entidades privadas que están habilitadas para funciones públicas y sus servicios al ecosistema de producción de X-Road o la consulta de información de entidades públicas, cuya fuente primaria son entidades particulares, la Entidad Privada deberá adquirir un certificado de autenticación digital y un certificado de firma a una de las Entidades de Certificación acreditadas vigentes en el Organismo Nacional de Acreditación Nacional – ONAC, en los términos del Decreto 527 de 1999, para que estos sean importados en el servidor de seguridad al momento de la configuración.

La Entidad de Certificación Digital dispondrá de un mecanismo para que la entidad privada pueda solicitar la solicitud de los certificados y la solicitud de firma de los Certificados.

Si bien las entidades públicas reciben los certificados de manera gratuita por parte de la Agencia Nacional de Seguridad Digital a través de la Entidad de Certificación Digital, en el caso de las entidades privadas no sucederá lo mismo, deberán entregar a la Agencia Nacional Digital la siguiente configuración: Certificados de autenticación de firma, URL, Autoridad de Estampa de Tiempo y el Protocolo de comprobación del estado del certificado en línea (OCSP por sus siglas en inglés: Online Certificate Status Protocol), con el propósito de realizar las respectivas configuraciones a nivel central. Los certificados de la Entidad de Certificación (CA por sus siglas en inglés Certification Authority), deberán cumplir con las siguientes especificaciones técnicas:

1. Los certificados emitidos deben permitir la compatibilidad e integración con el sistema X-Road y el intercambio de información con la versión 6.25 Colombia.

2. Estructura del certificado de la CA-Subordinada:

a. La estructura del certificado subordinado se genera a partir de certificado Raíz de la Entidad de Certificación Digital.

b. Algoritmo de firma: SHA256.

c. Uso de Claves: contener el uso de firma de certificados y firma de lista de revocación de certificados.

d. Usos Mejorados: contener el uso de firma de OCSP.

3. Estructura de los certificados de firma y autenticación digital.

Los certificados de firma y autenticación digital emitidos son firmados por la Subordinada de la Entidad de Certificación Digital, las solicitudes de estos certificados se generan desde los servidores de seguridad X-Road bajo la extensión (.PEM) y bajo el formato X.509 para dos (2) usos: Firma y Autenticación digital de seguridad.

Al recibir la petición, la Entidad de Certificación Digital, construye un certificado X.509 con base en la clave privada y la llave pública que está en la petición del certificado y datos propios del mismo con extensión (.PEM).

Los certificados de firma digital de persona jurídica deben tener las siguientes características:

Emitido por: Certificado subordinado de la Entidad de Certificación Digital.

1. Algoritmo de firma: SHA256.

2. Uso de Claves: Sin repudio.

3. Acceso a información de autoridad:

a. Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)

b. Nombre alternativo: URL=https:// Url del servicio para OCSP

c. Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)

d. Nombre alternativo: URL=https:// Url nombre alternativo

La Entidad de Certificación Digital debe estar acreditada por el Organismo Nacional de Acreditación.

Colombia – ONAC, dando cumplimiento al artículo [30](#) de la Ley 527 de 1999, modificado por el artículo 1 del Decreto-Ley 019 de 2012, por lo menos en las siguientes actividades:

- a. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.
- b. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles.
- c. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

El servicio de Estampa Cronológica de Tiempo debe cumplir las siguientes características:

1. El servicio de Estampa cronológica de tiempo debe permitir la compatibilidad e integración con X-Road versión 6.25 Colombia para el intercambio de información.
2. Prestar el Servicio de Estampado Cronológico (Timestamping) como mecanismo on-line que permita demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. La implementación debe cumplir con el protocolo definido en la norma RFC 3161 “Internet X.509 Infrastructure Time-Stamp Protocol (TSP)” o posteriores.
3. El servicio no deberá leer el contenido de los mensajes de datos para estampar la Transacción.
4. La Entidad de Certificación mantendrá un registro de las estampas emitidas para su futura verificación.
5. El servicio de estampa cronológica deberá soportar un rendimiento de mínimo 1000 transacciones criptográficas por segundo de las operaciones de firma.
6. Una solicitud a la Autoridad de Estampa de Tiempo que utiliza el método POST se construye de la siguiente manera: El encabezado Content-Type tiene el valor “application/timestamp-query”, mientras que el cuerpo del mensaje es el valor binario Time-Stamp Request Message.
7. Una respuesta de la Autoridad de Estampa de Tiempo basada en HTTP se compone del valor binario de codificación del Time-Stamp Response Message. El encabezado

Content-Type tiene el valor “application/timestamp-reply”.

URL: url del servicio de Autoridad de Estampa de Tiempo

Método: Post

Parámetro: Header = Content – Type (application/timestamp-query)

Body = TimeStampRequest

Returns: Header = Content – Type (application/timestamp-reply)

Body = TimeStampResponse.

8. El servicio de Autoridad de Estampa de Tiempo debe ser provisto haciendo uso de las librerías de Bouncy Castle (OpenSource), bajo el RFC 3161. La solicitud (request) al servicio de Autoridad de Tiempo se realiza haciendo uso del algoritmo de cifrado 2.16.840.1.101.3.4.2.3 de la librería Bouncy Castle correspondiente al algoritmo SHA512. La respuesta (response) del servicio se realiza haciendo uso del algoritmo de cifrado 1.3.14.3.2.26, el cual corresponde al algoritmo SHA1.

9. La entidad privada deberá en conjunto con la entidad certificadora que presta el servicio de Auto Estampa de Tiempo, llevar el control / filtro de consumo de las estampas, utilizando los mecanismos considere adecuados.

El protocolo de comprobación del estado de un certificado en línea (OCSP) debe cumplir las siguientes características:

1. El protocolo de comprobación del estado de un certificado en línea debe permitir la compatibilidad e integración con el sistema X-Road para el intercambio de información.
2. Integrar a la plataforma de X-Road el servicio de OCSP que permita por medio de una URL verificar el estado de los certificados vigentes o revocados dando pleno cumplimiento al RFC 6960 – X.509 Internet Key Infrastructure Online Certificate Status Protocol – OCSP.
3. Una solicitud OCSP que utiliza el método POST y se debe construir de la siguiente manera: El encabezado Content-Type tiene el valor “application/ocsp-request”, mientras que el cuerpo del mensaje es el valor de la OCSPRequest.
4. Una respuesta OCSP basada en HTTP se debe componer del valor binario de la codificación del OCSPResponse. El encabezado Content-Type tiene el valor “aplicación/ocsp-response” este encabezado especifica la longitud de la respuesta.

URL: Url del servicio de OCSP

Método: Post

Parametro: Header = Content-Type (application/ocsp-request)

```
Body = {  
  TBSRequest  
}
```

Respuesta: Header = Content-Type (application/ocsp-response)

```
Body = {  
  OCSPResponseStatus,  
  OCSPCertificado  
}
```

La validez del certificado debe poder verificarse cada 50 minutos contra el servicio de OCSP expuesto por la Entidad de Certificación Digital. En la respuesta de este servicio se debe establecer el parámetro No Validar por 50 minutos.

El servicio de OCSP debe ser provisto haciendo uso de las librerías criptográficas Bouncy Castle, versión 1.6.0. La solicitud (request) al servicio de OCSP se realiza haciendo uso del algoritmo 1.3.14.3.2.20 BouncyCastle, el cual equivale al algoritmo SHA1. El response del servicio OCSP se realiza haciendo uso del algoritmo 1.2.840.113549.1.1.5, que corresponde al algoritmo SHA1 con RSA de la librería BouncyCastle para la verificación de la firma del servicio OCSP.

Conclusiones y recomendaciones

Teniendo en cuenta todas las consideraciones anteriores y dado que en Colombia el servicio de salud es prestado tanto por empresas públicas como privadas, lo que permite el cubrimiento del servicio público en más del 95% de la población del país, al obedecer el mandato de la Ley 2160 de 2020 y 866 del 2021⁽⁶⁾ de implementar el modelo de interoperabilidad de datos de la historia clínica en Colombia utilizando la plataforma de interoperabilidad del estado colombiano, es decir la herramienta X-Road, la inclusión del sector privado de salud en Colombia asegurando, como ya se mencionó, condiciones de accesibilidad, oportunidad y continuidad adecuadas del servicio de salud en el país.

Así mismo, es necesario contar con la especificación de condiciones técnicas, jurídicas y administrativas necesarias para la eventual vinculación de entidades privadas al intercambio de información a través de la X-Road, cuyos datos sean indispensables para la transformación digital de trámites y servicios de las entidades del Estado.

Ante lo anterior, se propone realizar el siguiente ajuste al anexo 2 de la Resolución 2160 de 2020.

Detalle de los ajustes:

Se incluyen las secciones 6.6.7 y 6.6.8 de la siguiente forma:

6.6.7. Proceso de solicitud de certificados digitales para Entidades Privadas

Para realizar la conexión de los servidores de seguridad de entidades privadas y sus servicios al ecosistema de X-Road, la Entidad Privada deberá adquirir un certificado de autenticación digital y un certificado de firma a una de las Entidades de Certificación Digital con acreditación vigente en el Centro Nacional de Acreditación Nacional - ONAC, para que estos sean importados en el servidor de seguridad en el momento de la configuración. La Entidad de Certificación Digital dispondrá de un mecanismo para el cual la entidad privada pueda realizar la solicitud de los certificados y la solicitud de firma de los certificados.

El proceso general de la solicitud de certificados que se describe a continuación es un ejemplo del proceso que puede diferir dependiendo de las Entidades de Certificación Digital:

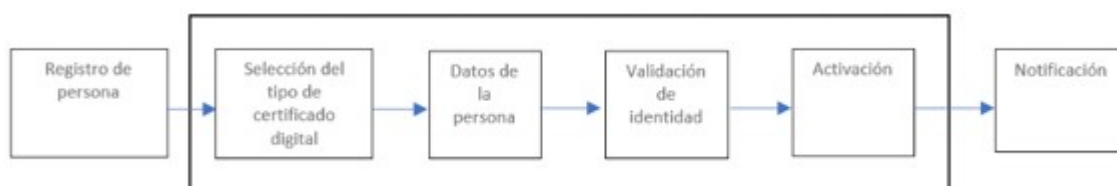


Figura 9. Proceso de solicitud de certificados

(Fuente: Suministrada por la Agencia Nacional Digital)

Registro de persona: El representante legal de la entidad privada o quien haga sus veces deberá hacer el registro y la solicitud de los certificados digitales en el portal de la Entidad de Certificación Digital.

Selección de tipo de certificado digital: El producto que se debe seleccionar es el tipo de certificado digital perteneciente a persona jurídica.

Datos de la persona: El representante legal de la entidad privada o quien haga sus veces deberá diligenciar el formulario con datos del Prestador Privado y personales.

Validación de identidad: El representante legal de la entidad privada o quien haga sus veces deberá

documentos que acrediten la relación laboral con el Prestador Privado.

Activación: La Entidad de Certificación Digital revisará y aprobará la solicitud.

Notificación: El CIO (Chief Information Officer) líder de la gestión estratégica de Tecnologías de Información o jefe del área de tecnologías de la información recibirá una notificación al correo electrónico con el estado de la solicitud.

El proceso general para la solicitud de la firma de los certificados digitales que se generan desde el sistema de seguridad es el siguiente.



Figura 10. Proceso de firma de certificados

(Fuente: Suministrada por la Agencia Nacional Digital)

Inicio de sesión: El representante legal de la entidad privada o quien haga sus veces deberá ingresar credenciales creadas en el proceso anterior.

Buscar solicitud: Ingresar y buscar el ID de la solicitud enviado al correo electrónico registrado.

Generar certificados: Generar desde el Servidor de Seguridad en formato (.PEM) las solicitudes de certificados y proceder a firmarlos a través de la entidad certificadora correspondiente. En la siguiente sección se detallará el proceso de generación de los certificados.

Solicitudes finalizadas: Buscar en la opción de solicitudes finalizadas y descargar los certificados desde la Entidad de Certificación Digital. La entidad deberá almacenar estos certificados de manera segura de acuerdo con su política de seguridad y privacidad de la información.

Cerrar Sesión: Salir del portal de firma de certificados de la Entidad de Certificación Digital.

6.6.8. Condiciones técnicas de los certificados que deben proporcionar las Entidades Privadas

Si bien las entidades públicas reciben los certificados de manera gratuita por parte de la Agencia Nacional Digital a través de la Entidad de Certificación Digital, en el caso de las entidades privadas no sucederá lo mismo. Estas deberán entregar a la Agencia Nacional Digital la siguiente configuración: Certificados de autenticación, firma, URL, Autoridad de Estampa de Tiempo y OCSP, con el propósito de realizar las respectivas configuraciones a nivel central.

Los certificados CA, deberán cumplir con las siguientes especificaciones técnicas:

1. Los certificados emitidos deben permitir la compatibilidad e integración con el sistema X-Road y el intercambio de información con la versión 6.25 Colombia.
2. Estructura del certificado de la CA-Subordinada:
 - a. La estructura del certificado subordinado se genera a partir de certificado Raíz de la Entidad de Certificación Digital.
 - b. Algoritmo de firma: SHA256.

- c. Uso de Claves: contener el uso de firma de certificados y firma de lista de revocación de certificados.
- d. Usos Mejorados: contener el uso de firma de OCSP.

3. Estructura de los certificados de firma y autenticación digital.

Los certificados de firma y autenticación digital emitidos son firmados por la Subordinada de la Entidad de Certificación Digital, las solicitudes de estos certificados se generan desde los servidores de seguridad Road bajo la extensión (.PEM) y bajo el formato X509 para dos (2) usos: Firma y Autenticación de seguridad.

Al recibir la petición, la Entidad de Certificación Digital, construye un certificado X.509 con base en la clave privada y la llave pública que está en la petición del certificado y datos propios del mismo con extensión (.PEM).

Los certificados de firma digital de persona jurídica deben tener las siguientes características:

Emitido por: Certificado subordinado de la Entidad de Certificación Digital.

1. Algoritmo de firma: SHA256.
2. Uso de Claves: Sin repudio
3. Acceso a información de autoridad:
 - a. Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1)
 - b. Nombre alternativo: URL=https:// Url del servicio para OCSP
 - c. Método de acceso=Emisor de la entidad de certificación (1.3.6.1.5.5.7.48.2)
 - d. Nombre alternativo: URL=https:// Url nombre alternativo

La Entidad de Certificación Digital debe estar acreditada por el Organismo Nacional de Acreditación Colombia – ONAC, dando cumplimiento al artículo [30](#) de la Ley 527 de 1999, modificado mediante el [Decreto 161](#) del Decreto Ley 019 de 2012, en las siguientes actividades:

- a. Emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas.
- b. Emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje y de documentos electrónicos transferibles.
- c. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

El servicio de Estampa Cronológica de Tiempo debe cumplir las siguientes características:

1. El servicio de Estampa cronológica de tiempo debe permitir la compatibilidad e integración con X-Road versión 6.25 Colombia para el intercambio de información.
2. Prestar el Servicio de Estampado Cronológico (Timestamping) como mecanismo on-line que permita demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. La implementación debe cumplir con el protocolo definido en la norma RFC 3161 “Internet X.509 Infrastructure Time-Stamp Protocol (TSP)” o posteriores.

3. El servicio no deberá leer el contenido de los mensajes de datos para estampar la transacción.
4. La Entidad de Certificación mantendrá un registro de las estampas emitidas para su futura verificación.
5. El servicio de estampa cronológica deberá soportar un rendimiento de mínimo 1000 transacciones criptográficas por segundo de las operaciones de firma.
6. Una solicitud Autoridad de Estampa de Tiempo que utiliza el método POST se construye de la siguiente manera: El encabezado Content-Type tiene el valor “application/timestamp-query”, mientras que el cuerpo del mensaje es el valor binario Time-Stamp Request Message.
7. Una respuesta Autoridad de Estampa de Tiempo basada en HTTP se compone del valor binario de la codificación del Time-Stamp Response Message. El encabezado Content-Type tiene el valor “application/timestamp-reply”.

URL: url del servicio de Autoridad de Estampa de Tiempo

Método: Post

Parámetro: Header = Content – Type (application/timestamp-query)

Body = TimeStampRequest

Returns: Header = Content – Type (application/timestamp-reply)

Body = TimeStampResponse.

8. El servicio de Autoridad de Estampa de Tiempo debe ser provisto haciendo uso de las librerías de Bouncy Castle (OpenSource), bajo el RFC 3161. La solicitud (request) al servicio de Autoridad de Tiempo se realiza haciendo uso del algoritmo de cifrado 2.16.840.1.101.3.4.2.3 de la librería Bouncy Castle correspondiente al algoritmo SHA512. La respuesta (response) del servicio se realiza haciendo uso del algoritmo de cifrado 1.3.14.3.2.26, el cual corresponde al algoritmo SHA1.
9. La entidad privada deberá en conjunto con la entidad certificadora que presta el servicio de Autoridad de Estampa de Tiempo, llevar el control / filtro de consumo de las estampas, utilizando los mecanismos que considere adecuados.

El protocolo de comprobación del estado de un certificado en línea debe cumplir las siguientes características:

1. El protocolo de comprobación del estado de un certificado en línea debe permitir la compatibilidad e integración con el sistema X-Road para el intercambio de información.
2. Integrar a la plataforma de X-Road el servicio de OCSP que permita por medio de una URL verificar el estado de los certificados vigentes o revocados dando pleno cumplimiento al RFC 6960 - X.509 Internet Key Infrastructure Online Certificate Status Protocol – OCSP.
3. Una solicitud OCSP que utiliza el método POST y se debe construir de la siguiente manera: El encabezado Content-Type tiene el valor “application/ocsp-request”, mientras que el cuerpo del mensaje es el valor binario de la OCSPRequest.
4. Una respuesta OCSP basada en HTTP se debe componer del valor binario de la codificación del OCSPResponse. El encabezado Content-Type tiene el valor “application/ocsp-response” este encabezado especifica la longitud de la respuesta.

URL: Url del servicio de OCSP

Método: Post

Parametro: Header = Content-Type (application/ocsp-request)

Body = {

TBSRequest

}

Respuesta: Header = Content-Type (application/ocsp-response)

Body = {

OCSPResponseStatus,

OCSPCertificado

La validez del certificado debe poder verificarse cada 50 minutos contra el servicio de OCSP expuesto por la Entidad de Certificación Digital. En la respuesta de este servicio se debe establecer el parámetro NoCache para 50 minutos.

El servicio de OCSP debe ser provisto haciendo uso de las librerías criptográficas Bouncy Castle, b6c2066960. La solicitud (request) al servicio de OCSP se realiza haciendo uso del algoritmo 1.3.14.3.2.201. BouncyCastle, el cual equivale al algoritmo SHA1. El response del servicio OCSP se realiza haciendo uso del algoritmo 1.2.840.113549.1.1.5, que corresponde al algoritmo SHA1 con RSA de la librería BouncyCastle para la verificación de la firma del servicio OCSP.

Adicionalmente se ajusta la sección 8.4.1 en concordancia a lo anterior incluyendo el siguiente texto:

“(…) Aunque dentro de la carpeta ciudadana la entidad puede publicar servicios independientes, se recomienda como una buena práctica, tener un servicio de consulta de información bajo el cual se publicarán los servicios de historiales y alertas”.

BIBLIOGRAFÍA

- Ley 2015 de 2020, por medio del cual se crea la historia clínica electrónica interoperable y se dictan disposiciones.
- Resolución 866 de 2021 del Ministerio de Salud y Protección Social y el Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se reglamenta el conjunto de elementos de datos clínicos relevantes para la interoperabilidad de la historia clínica.
- Resolución [2160](#) de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos.
- Decreto número [1078](#) de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones (DUR- TIC), título IX Y XVII.

<NOTAS DE PIE DE PÁGINA>

1. Artículo [6](#) de la Ley 1341 de 2009, modificado por el artículo [5](#) de la Ley 1978 de 2019.
2. **“Por el cual se subroga el título [17](#) de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, [54](#), [60](#), [61](#) y [64](#) de la Ley 1437 de 2011, los literales a) del párrafo 2 del artículo [45](#) de la Ley 1753 de 2015, el numeral 3 del artículo [147](#) de 1955 de 2019, y el artículo [9](#) del Decreto 2106 de 2019, estableciendo los lineamientos generales de operación de los servicios ciudadanos digitales”.**
3. **“Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía de vinculación y uso de estos”.**
4. **“Por medio del cual se crea la Historia Clínica Electrónica interoperable y se dictan otras disposiciones”.**
5. De acuerdo con el Decreto [1078](#) de 2015, adicionado mediante el Decreto 1263 de 2022, la Transformación Digital **“Corresponde al proceso de explotación de tecnologías digitales que tiene la capacidad de crear nuevas formas de hacer las cosas en todos los sectores de la administración pública, generando nuevos modelos de desarrollo, procesos y la creación de productos y servicios, que producen valor, principalmente a través de la digitalización que representa la conversión de procesos análogos hacia formatos que pueden ser entendidos y procesados por máquinas”.**
6. Expedida por el Ministerio de Salud y Protección Social y el Ministerio de Tecnologías de la Información y las Comunicaciones.



Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.

Compilación Jurídica MINTIC

n.d.

Última actualización: 31 de mayo de 2024 - (Diario Oficial No. 52.755 - 13 de mayo de 2024)

