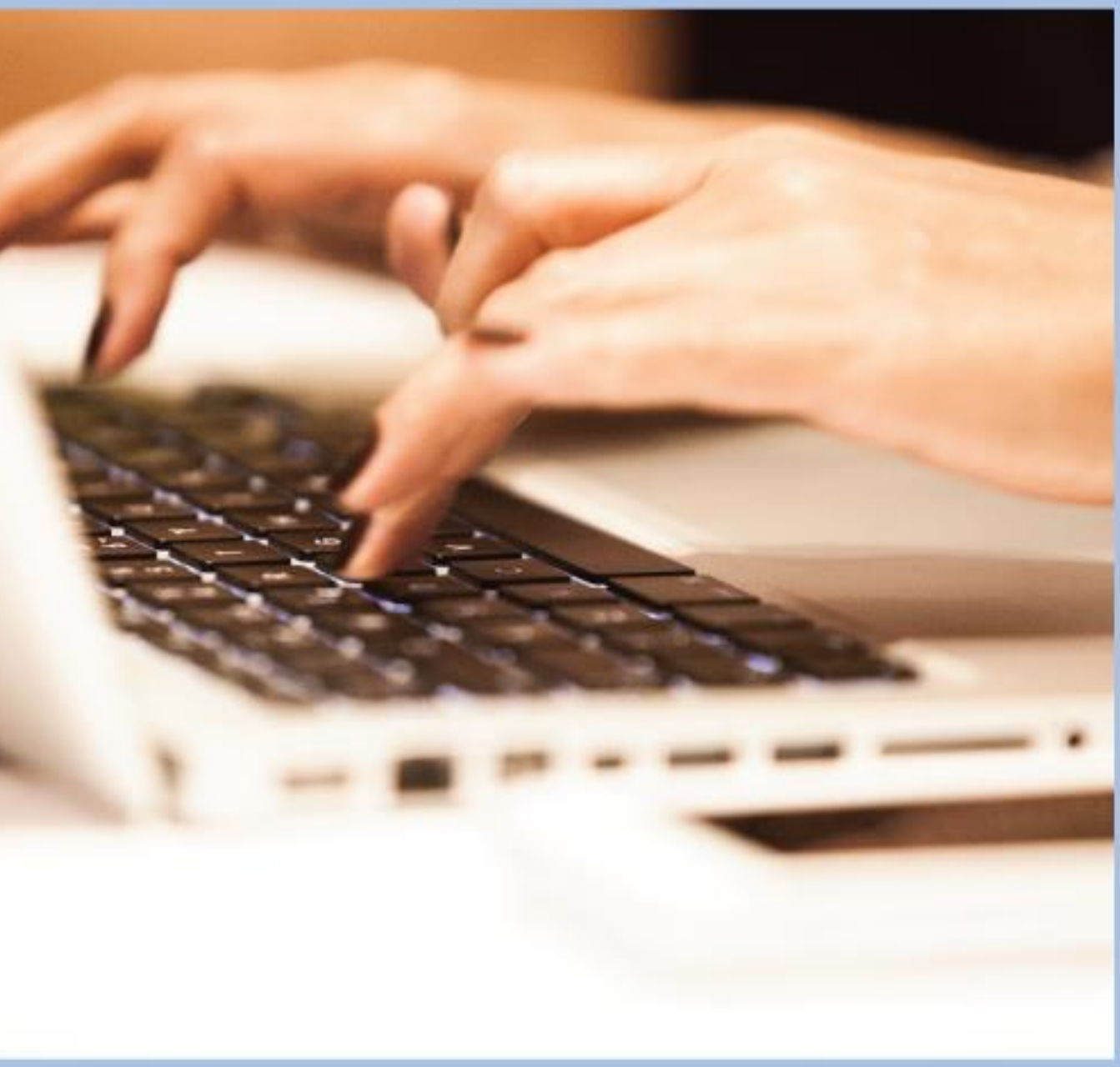


Anexo 2 Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales

Diciembre de 2022

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

Equipo de trabajo
Sandra Milena Urrutia Pérez - Ministra de Tecnologías de la Información y las Comunicaciones
Nohora Mercado Caruso – Viceministra de Transformación Digital
Ingrid Tatiana Montealegre - 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
Dirección 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 Diciembre 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

Tabla de Contenido

Lista de Ilustraciones

1 Introducción

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), de acuerdo con la Ley 1341 de 2009, desarrolla políticas y planes enfocados a las Tecnologías de la Información y las Comunicaciones que constituyen un componente vital para el crecimiento y desarrollo del sector, con el fin de brindar acceso a toda la población, en el marco de la expansión y diversificación de las TIC.

Con base en lo anterior, MinTIC tiene establecido dentro de sus funciones: "*1. Diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones. 2. Definir, adoptar y promover las políticas, planes y programas tendientes a incrementar y facilitar el acceso de todos los habitantes del territorio nacional, a las tecnologías de la información y las comunicaciones y a sus beneficios*". En este sentido, MinTIC ha conceptualizado y diseñado un modelo integral que incorpora los proyectos de Interoperabilidad, Autenticación Digital y Carpeta Ciudadana, bajo el nombre de 'Servicios Ciudadanos Digitales', este modelo tiene por objeto, facilitar a los ciudadanos su interacción con la administración pública y optimizar la labor del Estado.

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

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

c) Carpeta Ciudadana Digital, permitiendo la visualización de los datos que las entidades públicas tienen de cada ciudadano o empresa.

El presente documento tiene como fin, presentar a las entidades públicas la información del modelo de SCD y cómo debe preparar la vinculación para hacer uso de ellos en su proceso de transformación digital, entre otros, se determinan los estándares, modelos, lineamientos y requisitos técnicos específicos de vinculación de los Servicios Ciudadanos Digitales [1].

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

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, aquí se indican cuáles son las condiciones necesarias y los pasos que deben realizar para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán 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 correcta operación y desarrollo de los servicios que las entidades públicas deben ofrecer. 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 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 del Decreto 1078 de 2015 que define los 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. **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.
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 necesarias que el Articulador de los SCD debe cumplir con el fin de garantizar la correcta prestación de los servicios ciudadanos digitales.
5. **Guía para la vinculación y uso de los Servicios Ciudadanos Digitales**: Es el documento expedido y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones destinado a las autoridades referidas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015, que indica cuáles son las condiciones necesarias y los pasos que deben realizar para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán vincular a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad y carpeta ciudadana digital.

6. **Integridad:** es la condición que garantiza que la información consignada en un mensaje de datos permanezca completa e inalterada, salvo la adición autorizada de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.
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 agrupar y presentar por niveles más detallados.
8. **Marco de interoperabilidad:** Es la estructura de trabajo común donde se alinean los conceptos y criterios que guían el intercambio de información. Define el conjunto de principios, recomendaciones y directrices que orientan los esfuerzos políticos, legales, organizacionales, semánticos y técnicos de las entidades, con el fin de facilitar el intercambio seguro y eficiente de información[2].
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 permite que los sistemas de información del Estado conversen entre sí mediante interfaces estándar de comunicación entre procesos y sistemas de información
12. **Prestadores de Servicios Ciudadanos Digitales:** Entidades pertenecientes al sector público o privado, quienes, mediante un esquema coordinado y administrado por el Articulador, pueden proveer los servicios ciudadanos digitales a ciudadanos y empresas, siempre bajo los lineamientos, políticas, guías, que expida el Ministerio de Tecnologías de la Información y las Comunicaciones.
13. **Privacidad por diseño y por defecto:** Desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se deben adoptar medidas preventivas

[2] http://lenguaje.mintic.gov.co/marco-de-interoperabilidad

de diversa naturaleza (tecnológica, organizacional, humana, procedimental) para evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como fallas de seguridad o indebidos tratamientos de datos personales. La privacidad y la seguridad deben hacer parte del diseño, arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan.

14. **Servicios Ciudadanos Digitales:** Es el conjunto de soluciones y procesos transversales que brindan al Estado capacidades y eficiencias para su transformación digital y para lograr una adecuada interacción con el ciudadano, garantizando el derecho a la utilización de medios electrónicos ante la administración pública. Estos servicios se clasifican en servicios base y servicios especiales.
15. **Servicios Ciudadanos Digitales Base:** son los servicios que se consideran fundamentales para brindarle 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, corresponden a innovaciones que realizan los prestadores de servicio a partir de la autorización dada por el titular de los datos y de la integración a los servicios ciudadanos digitales base. bajo un esquema coordinado por el Articulador.
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 que esté utilizando el usuario.
18. **Single Log-Out (SLO):** Permite que un usuario cierre sesión en todos los sitios y aplicaciones abiertas en una 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 "*(...) servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución (...)*".

Que la Ley 527 de 1999, "*Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones*", estableció el reconocimiento jurídico a los mensajes de datos, en las mismas condiciones que se ha otorgado para los soportes que se encuentren en medios físicos. De la misma manera, el Decreto 2364 de 2012 por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica.

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

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

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

entre sus objetivos *"(...) 2. Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación*".

Que la Ley 1581 de 2012, "*Por la cual se dictan disposiciones generales para la protección de datos personales*", desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información personal que se haya recogido en las bases de datos o archivos, con pleno respeto a los principios establecidos en el artículo 4, determinando en los artículos 10, 11, 12 y 13, entre otros asuntos, las condiciones bajo las cuales las entidades públicas pueden hacer tratamiento de datos personales y pueden suministrar información en ejercicio de sus funciones legales.

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

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", la Política de Gobierno Digital se desarrolla 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 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. Que las "*Bases del 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 e integración de los servicios ciudadanos digitales, (carpeta ciudadana, autenticación electrónica e interoperabilidad de los sistemas del Estado), de forma paralela a la definición y adopción de estándares tecnológicos, al marco de arquitectura TI, a la articulación del uso de la tecnología, y todo lo anterior en el marco de la seguridad digital.

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

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

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

Ciudadanos Digitales base y se implementarán por parte de las autoridades de conformidad con los estándares que establezca el MinTIC.

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

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

Para materializar lo anterior, MinTIC dispone los lineamientos que se deben cumplir para la prestación de los Servicios Ciudadanos Digitales y para facilitar a los usuarios el acceso a la administración pública a través de medios digitales, desde la aplicación de los principios de accesibilidad inclusiva, escalabilidad, gratuidad, libre elección y portabilidad, privacidad por diseño y por defecto, seguridad, privacidad y circulación restringida de la información y usabilidad. Por lo cual, el articulador señalado en el numeral 3 del artículo 2.2.17.1.5. del Decreto 1078 de 2015, deberá cumplir las condiciones y estándares establecidos en la Guía de lineamientos de los servicios ciudadanos digitales que se encuentran señaladas, con el fin de garantizar la correcta prestación de los servicios ofertados, y, las autoridades señaladas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015, deberán cumplir las condiciones y estándares establecidos en la Guía para vinculación y uso de los servicios ciudadanos digitales que se encuentran señaladas para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán integrar a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad, carpeta ciudadana digital y vincularlos al Portal Único del Estado colombiano.

De acuerdo con lo mencionado, se ha determinado la necesidad de presentar los estándares de implementación de los Servicios Ciudadanos Digitales contenidos en la guía de lineamientos de los servicios ciudadanos digitales. Esto incluye en el articulado las mejoras funcionales del modelo de los Servicios Ciudadanos Digitales que permitan al Articulador tener el rol de prestador de servicios para las entidades públicas, así mismo, se incluyeron mejoras a las definiciones y características de los servicios, se fortalecen los mecanismos de vinculación que estarán a disposición de las entidades para el uso y aprovechamiento de los SCD en su transformación digital.

5 Servicios Ciudadanos Digitales

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

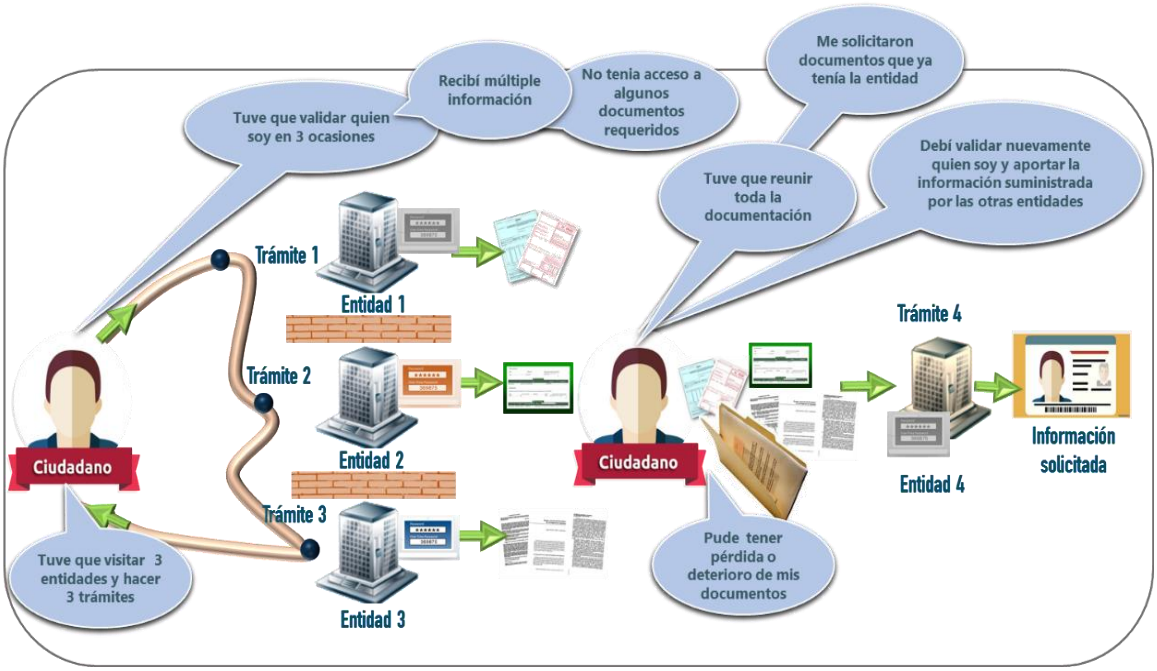


Figura 1 Problemática a resolver

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 física o virtualmente a varias entidades, cada una de ellas le solicita tener un usuario y contraseña para autenticarse, recibe múltiple información de manera dispersa o no tienen acceso a todos los documentos que necesita, le solicitan siempre los mismos documentos y lo termina siendo un mensajero para recolectar toda la información, sin contar que el usuario al tener estos documentos en formatos físicos los puede perder o deteriorar o simplemente 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 solicitud de

documentos que el ciudadano ya ha presentado previamente y la complejidad para identificar a las personas 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 lograr una adecuada interacción con el ciudadano, garantizando el derecho a la utilización de medios electrónicos ante 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 adecuado flujo de información e interacción entre los sistemas de información de las entidades, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad.
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 mensaje de datos, o la persona a la que se atribuya el mismo en los términos de la Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen, y sin perjuicio de la autenticación notaria
3. Servicio de Carpeta Ciudadana Digital: Es el servicio que le permite a los usuarios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las entidades. 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, atendiendo 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 públicas y que puede ser intercambiada e integrada a los trámites por parte de estas sin convertir al ciudadano en mensajero del Estado.
5. Crear las condiciones de confianza en el uso de los medios digitales con medidas para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos y las comunicaciones.
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 hayan recogido sobre ellas en las entidades públicas.

El modelo de los Servicios Ciudadanos Digitales considera los siguientes actores cuyos roles se describen a 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, nacionales 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 los usuarios y que colaboraran armónicamente con otras entidades para intercambiar información en el ámbito de sus funciones.

3. **Articulador:** Es la entidad 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. Este actor podrá prestar los servicios de Carpeta Ciudadana Digital y Autenticación Digital, al igual que los prestadores de servicios, y será el único actor que podrá ofrecer el servicio de Interoperabilidad. Todo esto siguiendo las definiciones y 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, mediante un esquema coordinado y administrado por el Articulador, pueden proveer los servicios ciudadanos digitales bajo 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 serán 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 uso 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 y legales ejercerán vigilancia y control sobre las actividades que involucran 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 comunes para 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 intercambiar y utilizar información, dentro Gobierno Digital su interpretación se extiende más allá del concepto 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, empresas 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 eficiente que les 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 entre éstas y el ciudadano deben estar a la par del sector público, garantizando el aprovechamiento de las TIC. Una sociedad digital debe contar con un Gobierno Digital.

El Marco de Interoperabilidad es genérico y aplicable a todas las entidades públicas y privadas en Colombia, el marco establece las condiciones básicas que se deben considerar para alcanzar la interoperabilidad tanto a nivel local, interinstitucional, sectorial, nacional o internacional y orientado a todos los involucrados en definir, diseñar, 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 del uso 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 todos aquellos que quieran intercambiar información, mediante un conjunto de lineamientos sobre cómo mejorar 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 vigente 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 alinean los conceptos y criterios que guían el intercambio de información. Este marco cuenta con nueve (9) principios, cuatro (4) dominios con veinte (20) lineamientos distribuidos a lo largo de cada uno de los dominios así: tres (3) 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 interoperabilidad

El marco define el conjunto de principios, recomendaciones y lineamientos que orientan los esfuerzos políticos y legales, organizacionales, semánticos y técnicos de las entidades con el fin de facilitar el intercambio seguro y eficiente de información. Además ofrece un modelo de madurez, un conjunto de actividades que pueden ser usadas 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 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 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 realizan el intercambio de información ajustado al marco jurídico vigente, las políticas y estrategias pueden trabajar juntas 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 expectativas interactúan con aquellos de otras entidades para alcanzar las metas adoptadas de común acuerdo y mutuamente beneficiosas, a través del intercambio de información. Para lograrlo es necesario la integración, adaptación o incluso la eliminación o definición de nuevos procesos, trámites, servicios y otros

procedimientos administrativos, así como realizar la identificar 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 conectan sistemas de información, las aplicaciones con los servicios de intercambio de información. Incluye aspectos como especificaciones de interfaz, protocolos de interconexión, servicios de integración de datos, presentación e 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 que mediante el uso de un conjunto de protocolos y estándares permite el intercambio de información. Este 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 permite que los sistemas de información del Estado interactúen entre sí mediante interfaces estándar de comunicación entre procesos y sistemas de información.

La PDI cuenta con varios componentes como se muestra en la Figura 3 Componentes de la PDI, el componente base de la plataforma es X-ROAD que es el encargado de habilitar

las capacidades para realizar el intercambio seguro de datos 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 y el servidor X-ROAD instalado.

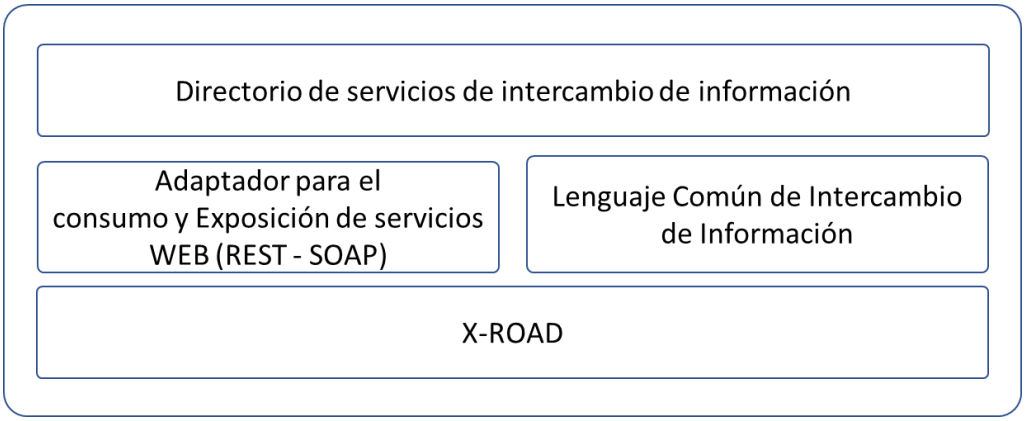


Figura 3 Componentes de la PDI

El Directorio de Servicios de Intercambio de Información es una herramienta que permite la publicación de la información general, semántica y técnica de servicios de intercambio de información dispuestos por las autoridades y disponibles en la PDI que cumplen con los lineamientos del Marco de Interoperabilidad para 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 de datos 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 sean más sostenibles (social, económica y medioambientalmente), más eficientes y efectivos en la contribución de 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 contratos de 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 y 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 estandarizada, consistente, unificada e integral.
e) Reducir el gasto público y mejorar la coordinación entre diferentes servicios y administraciones públicas.
f) Apoyar y mejorar la toma de decisiones por parte 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 a través de los tramites de las entidades.
h) Medir los resultados de la gestión de la interoperabilidad y su impacto en la administración pública, el relacionamiento con las empresas y la calidad de vida del ciudadano.
i) Evolucionar hacia un modelo auto gestionado y sostenible tanto en consumo de recursos como en eficiencia en 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 tecnológica 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 y lecciones 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 1.2 y 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 utiliza para estampar todas las solicitudes salientes, solitudes entrantes, respuestas salientes y respuestas entrantes entre los servidores de seguridad.
7. Los mensajes intercambiados en la PDI tienen valor jurídico y pueden ser usados como evidencia digital de 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.

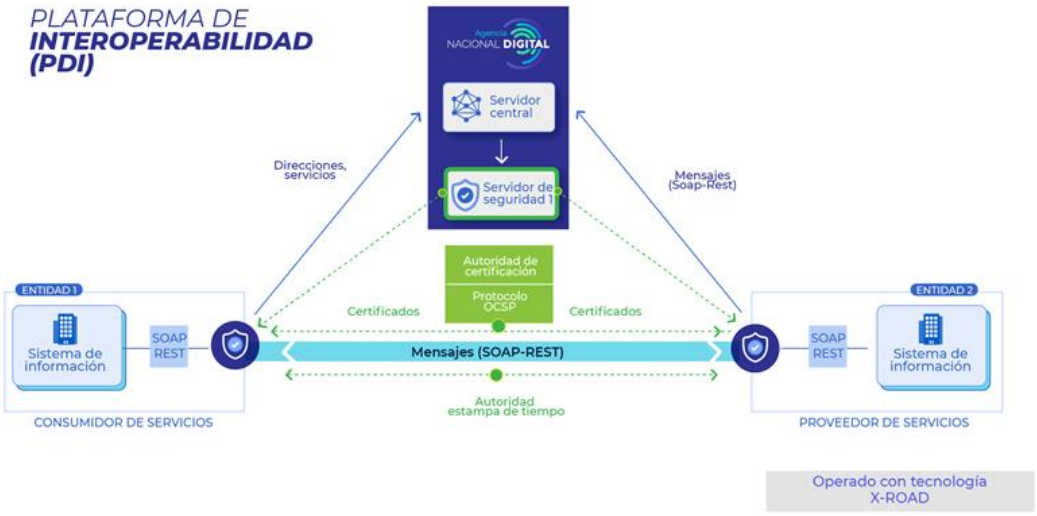


Figura 4 Modelo Conceptual de la PDI operada con X-ROAD

El Articulador de los SCD administrará los componentes centrales de la plataforma de interoperabilidad, prestará a través de las Entidades de Certificación Digital acreditadas ante la ONAC, los servicios de confianza (Certificados Digitales, Estampa Cronológica de tiempo y validación del estado de un certificado), razón por la cual en el momento en que se selecciona la o las entidades que prestan dichos servicios, estas deben cumplir con 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 componentes 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 mecanismos de cifrado. Los componentes de X-ROAD dentro del ecosistema se comunican a través de servicios de gestión para la sincronización de la configuración y auditoría.

Cada uno de los miembros, servidores de seguridad y servicios dentro del ecosistema de X-ROAD serán identificado 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. Existirán 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 GOB 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 legal de cada entidad.
- **Código de Miembro**: Es el identificador único de cada miembro dentro de su Clase Membro, este código permanece sin modificarse durante todo el tiempo de permanencia dentro del ecosistema. Este código será 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 del 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 en el ecosistema X-ROAD. El código es el nombre que haya establecido la entidad al servicio en estilo CamelCase.

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 plataforma de interoperabilidad de acuerdo con la arquitectura de componentes de la Figura 5.

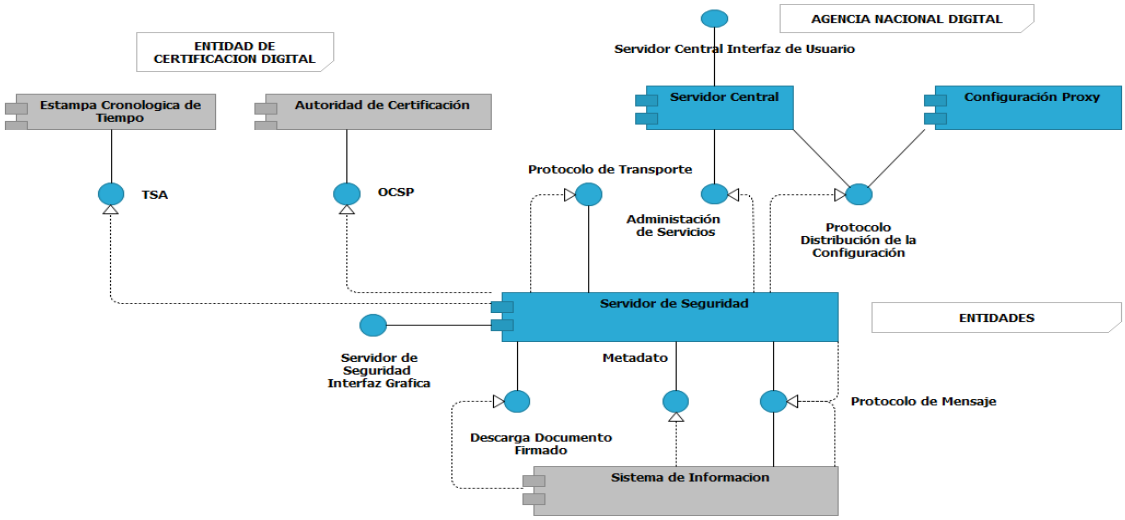


Figura 5 Arquitectura de componentes de la PDI

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. Además, el servidor central contiene la política de seguridad de la instalación de X-ROAD. La política de seguridad consta de 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 de gestión y distribución de la configuración compartida hacia otros servidores de seguridad. La configuración que se comparte entre los servidores de seguridad incluye los parámetros de configuración de red necesarios para la comunicación entre servidores de seguridad, la 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 horas 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 tareas de 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 en el 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 el protocolo de sellado de tiempo.

Los servidores de seguridad utilizan el sellado de tiempo por lotes. Esto reduce la carga del servicio de estampa 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)[3] 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.

[3] Por sus siglas en inglés (Certification Authority).

La CA debe distribuir la información de validez del certificado vía el protocolo OCSP, los servidores de seguridad guardan en caché las respuestas OCSP[4] 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, media las llamadas de servicio y las respuestas de servicio entre los sistemas de información de las entidades. El servidor de Seguridad encapsula los aspectos de seguridad involucrados Enel intercambio de datos: gestión de claves para la firma y autenticación, envío de mensajes a través de un canal seguro, creación del valor de prueba para 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 protocolo es el mismo 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 criptográficamente seguros con los otros servidores de seguridad. Las claves de firma se asignan a los clientes del servidor 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 incluso cuando las fuentes de información no están disponibles.

[4] https://csrc.nist.gov/glossary/term/Online-Certificate-Status-Protocol

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 una entidad 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 punto de entrada a todos los servicios de X-ROAD. El consumidor puede descubrir miembros registrados de X-ROAD y 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 servicios REST 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 central. 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 y la descargar 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 en caché 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 de servicio 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 varias partes 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 del servicio 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 descripciones de servicio.

El protocolo de metadatos de servicio se utiliza para la configuración del sistema de información de las entidades, por lo tanto, la disponibilidad, el rendimiento y la latencia

de sus componentes de implementación no son críticos para el funcionamiento de X-ROAD.

6.5.2.11. 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 sincrónico 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 los datos 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 servicio de administración es un protocolo sincrónico 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 un Certificado En línea) que permite consultar la información de validez sobre los certificados de firma y autenticación.

El protocolo OCSP es un protocolo sincrónico que será ofrecido por una Entidad de Certificación Digital 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 como parte del Protocolo de transporte de mensajes. Esto garantiza que los servidores de seguridad no necesiten detectar el 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 servicio 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 OCSP 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 integridad y autenticidad a largo plazo de los mensajes intercambiados. Los servidores de seguridad registran los logs todos los mensajes y sus firmas. Estos registros se marcan para crear evidencias a largo plazo. Es un protocolo sincrónico 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 tiempo por 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 en 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 todos aquellos que quieran intercambiar información, mediante un conjunto de lineamientos sobre cómo mejorar 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 vigente y con garantía 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 integración de la Plataforma de Interoperabilidad.

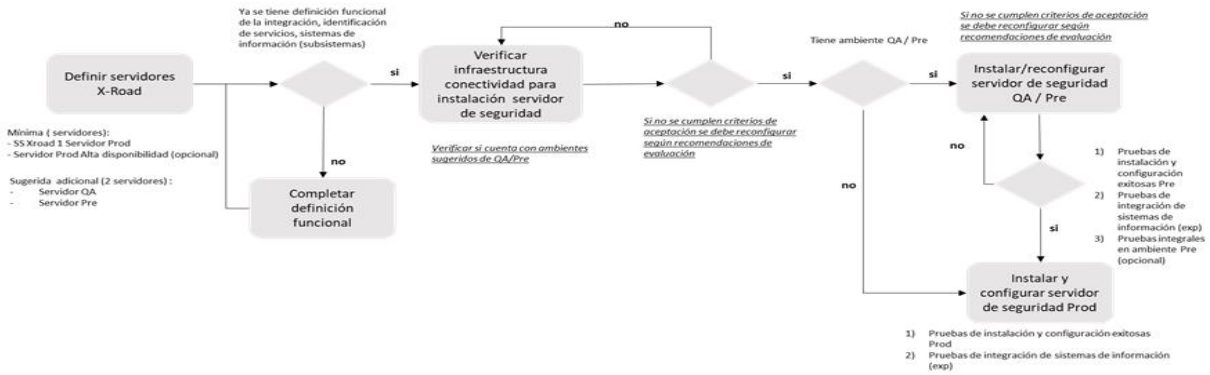


Figura 6 Metodología para la instalación y configuración de los ambientes requeridos para el servidos de seguridad

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, se deberá definir la disponibilidad y aprovisionamiento por parte de la entidad de: 4 servidores (Ambiente QA, ambiente preproducción, producción, producción en alta disponibilidad). Como caso excepcional y luego de haber validado la carga transaccional de los servicios de consumo y exposición, la entidad podría definir 3 servidores (Ambiente QA, ambiente preproducción y producción sin alta disponibilidad).

Ítem	Requisito	Explicación
		Las características del sistema operativo base para cada uno de los servidores se describen más adelante.
2	Validación funcional previo a despliegue en servidor QA	Previo a la instalación, despliegue y configuración del Servidor de Seguridad X-Road en el ambiente de producción, QA o preproducción según corresponda, se valida: - Formato de pruebas de conectividad y configuración diligenciado. - Diseño funcional y técnico con la información de los subsistemas que harán parte del intercambio de información. Si cumple con los criterios de aceptación antes mencionados, se realiza la ejecución del ítem 4. De lo contrario, se deberá complementar por medio de la ejecución del ítem 3.
3	Completar definición funcional	Completar la información funcional, técnica contemplando la siguiente información: Contrato de servicios Definición de las variables: código miembro y subsistema del ecosistema X-ROAD. Si no se ha diligenciado el formato de conectividad por parte de la entidad, deberá completarlo 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 presente documento. 2. Anclaje del servidor de seguridad al nodo central.

Ítem	Requisito	Explicación
		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 en el punto 3 únicamente. Luego de realizar los pasos antes mencionados, se deberán generar las siguientes evidencias: ✓ Formato de pruebas de instalación y configuración X-ROAD en ambiente QA. ✓ Formato de pruebas de integración de sistemas de información (aplica cuando el 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 QA ✓ Formato de pruebas de integración de sistemas de información (aplica cuando el servicio es de exposición) ✓ Formato de pruebas integrales en ambiente de QA Adicionalmente, las pruebas integrales hayan sido ejecutadas de manera exitosa. Si la validación es satisfactoria, se realiza la instalación en ambiente pre-productivo (item 6). De lo contrario, se deberá volver a la tarea anterior (item 4) y 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 presente documento.

Ítem	Requisito	Explicación
		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 en el punto 3 únicamente. Luego de realizar los pasos antes mencionados, se deberán generar las siguientes evidencias: ✓ Formato de pruebas de instalación y configuración X-ROAD en ambiente Preproducción. ✓ Formato de pruebas de integración de sistemas de información (aplica cuando el 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 ambiente Pre, si aplica ✓ Formato de pruebas de integración de sistemas de información (aplica cuando el servicio es de exposición) ✓ Formato de pruebas integrales en ambiente de Preproducción, si aplica. Si la validación es satisfactoria, se realiza la instalación/configuración en ambiente productivo (ítem 8). De lo contrario, se deberá volver a la tarea anterior (ítem 6) y completar los criterios que hagan falta.
8	Instalar/reconfigurar servidor de seguridad Producción	Una vez validados los criterios de aceptación descritos en el ítem 7, se deberá realizar la instalación/configuración de la versión Colombia del

Ítem	Requisito	Explicación
		Servidor de Seguridad de X-Road. En este ítem se deben realizar las siguientes tareas: 1. Instalación del servidor según la descripción en el titulo 6.6.4 del presente documento. 2. Anclaje del Servidor de Seguridad al nodo central 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 en el punto 3 únicamente. Luego de realizar los pasos antes mencionados, se deberán generar las siguientes evidencias: ✓ Formato de pruebas de instalación y configuración X-Road en ambiente Preproducción. Formato de pruebas de integración de sistemas de información (aplica cuando el servicio es de exposición).

6.6.2. Requerimientos

A continuación, se describen las características mínimas que deben tener los servidores de seguridad descritos 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.	X-Road soporta únicamente estas versiones en sistemas operativos.

Ítem	Requisito	Explicación
	Nota: Los servidores de seguridad puede ser físicos o virtuales.	
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 (placa base, CPU, tarjetas de interfaz de red, sistema de almacenamiento) debe ser compatible con RHEL7 o Ubuntu en general.
3	4 GB de RAM.	Memoria RAM mínima requerida. de acuerdo con la transaccionalidad de la entidad pude 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 mínimo 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 repositorios 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	Segmentación de Red y Seguridad.

Ítem	Requisito	Explicación
	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.	

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 (placa base, CPU, tarjetas de interfaz de red, sistema de almacenamiento) debe ser compatible con RHEL7 o Ubuntu en general.
3	6 GB de RAM	Memoria RAM mínima requerida. de acuerdo con la transaccionalidad de la entidad pude 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 mínimo 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 repositorios 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 Seguridad.

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 únicamente estas versiones en sistemas operativos.
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 (placa base, CPU, tarjetas de interfaz de red, sistema de almacenamiento) debe ser compatible con RHEL7 o Ubuntu en general.
3	16 GB de RAM	Memoria RAM mínima requerida. de acuerdo con la transaccionalidad de la entidad pude aumentar la memoria RAM.
4	20 GB de espacio libre en disco (partición del sistema operativo)	Almacenamiento mínimo requerido.

	20-40 GB de espacio libre en disco (/var/partición);	
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 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 Seguridad.
8	Alta disponibilidad	Hacer uso de un balanceador y método Round-robin como recomendado.

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 (concurrencia).
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, Pre y 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 OCSP, servicio 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 calidad, inconsistencia en los datos, logs de evidencias innecesarias, errores en el intercambio, uso de datos productivos 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, sin garantizar la validación de las diferentes variables de los ecosistemas QA, Pre de X-ROAD, se convertiría a dicho Servidor de Seguridad en un único punto de acceso a todos los ambientes. Este escenario generaría 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 se afectaría la operación. No se podría utilizar este ambiente para reinstalaciones de QA o Pre producción y próximas integraciones.
- Cuando una entidad no tiene servicios operando, enfrentarse a la reinstalación del Servidor de Seguridad sería la única opción para garantizar ambientes. De cara a migrar de QA a PRE debería reinstalarse el servidor de QA o Pre pero esto generaría un desgaste operativo no recomendado, inconsistencias en el Nodo Central de X-Road, entregas sin calidad, reprocesos operativos, costos altos de mantenibilidad, no escalabilidad para realizar futuras integraciones.

- En el Nodo Central, en el ambiente productivo de la AND, se tendrían miembros, subsistemas que son de ambiente QA y/o Pre, y no los productivos. Se tendría un ambiente productivo en Nodo Central para una misma entidad con diferentes miembros, subsistemas. Según las buenas prácticas establecidas para el ecosistema de X-ROAD, esto generará inconsistencias en la validez jurídica, errores en el monitoreo, datos sin calidad en los 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 no requieren ajustes para ser implementados. Por el contrario, los servicios SOAP requieren de ajustes en sus 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 Tiempo).

Actualmente, los servidores de seguridad se instalan en el Sistema Operativo Linux Ubuntu 18.04 y Red Hat, y la comunicación entre ellos se lleva a cabo a través de los Puertos 80, 443 y 5500. Varios servidores de X-Road se pueden instalar en una misma máquina a través de contenedores o máquinas virtuales, por ejemplo, para 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 Ubuntu18.04.

Nombre del archivo: Instalación X-Road 6.25 servidor de seguridad entidades Ubuntu18.04. 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 CAs 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 hayan autorizadas en el entorno nacional. El servidor central supervisa cuáles son las autoridades de confianza de certificados. 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, es decir una Entidad de Certificación subordinada, por lo cual es necesario configurar el servicio OSCP 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 ecosistema de producción de X-Road, la Agencia Nacional Digital a través de la Entidad de Certificación Digital entregará un certificado de autenticación y un certificado de firma para que estos sean importados en el servidor de seguridad al momento de la configuración.

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

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

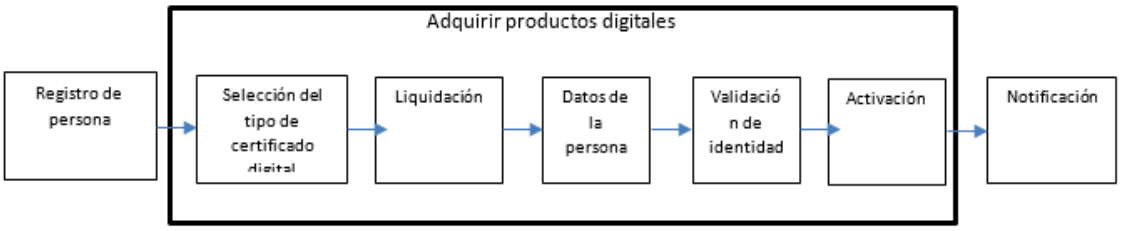


Figura 7 Proceso de solicitud de certificados

Registro de persona: el CIO, director o jefe del área de tecnologías de la información de la entidad pública 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 este paso la 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 un 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 los 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 al correo electrónico registrado con el estado de la solicitud.

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

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

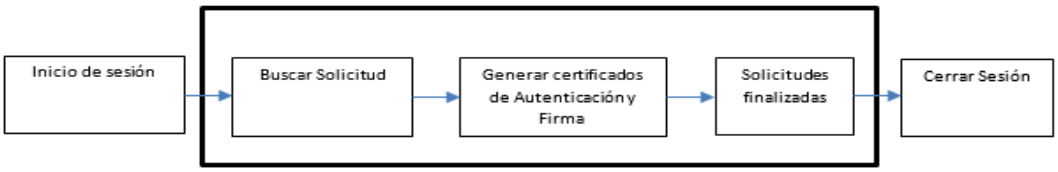


Figura 8 Proceso de firma de certificados

Inicio de sesión: el CIO, director o jefe del área de tecnologías de la información deberá ingresar las 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 firma de los certificados y cargarlos en el portal. 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 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 ecosistema 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 al momento de la configuración.

La Entidad de Certificación Digital dispondrá de un mecanismo para que 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, este puede diferir dependiendo de las Entidades de Certificación Digital:

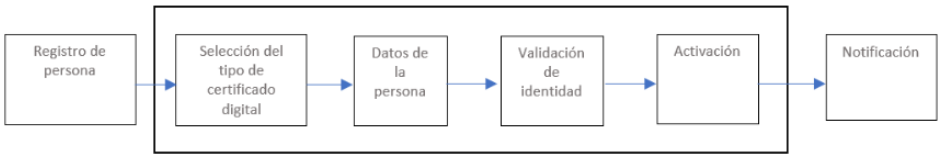


Figura 9 Proceso de solicitud de certificados
(Fuente: Suministrada por la Agencia Nacional Digital)

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

Validación de identidad: El representante legal de la entidad privada o quien haga sus veces deberá cargar los 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 al 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
(Fuente: Suministrada por la Agencia Nacional Digital)

Inicio de sesión: El representante legal de la entidad privada o quien haga sus veces deberá ingresar las 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 firma de los 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 firmados por 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 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 Digital a través de la Entidad de Certificación Digital, en el caso de las entidades privadas no sucede lo mismo y deberán entregar a la Agencia Nacional Digital la siguiente configuración: Certificados de autenticación digital 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 para 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 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 Servidores de seguridad.

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

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 de Colombia – ONAC, dando cumplimiento al 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 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 el sistema X-Road versión 6.25 Colombia para el intercambio de información.

2. Prestar el Servicio de Estampado Cronológico (Timestamping) como mecanismo on-line que permite 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 Public Key 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 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 criptográficas Bouncy Castle (OpenSource), bajo el RFC 3161. La solicitud (request) al servicio de Autoridad de Estampa de Tiempo se realiza haciendo uso del algoritmo de cifrado 2.16.840.1.101.3.4.2.3 de la librería BouncyCastle correspondiente al algoritmo SHA512. El 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 Public 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 "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 NextUpdate en 50 minutos.

El servicio de OCSP debe ser provisto haciendo uso de las librerías criptográficas Bouncy Castle, bajo el RFC 6960. La solicitud (request) al servicio de OCSP se realiza haciendo uso del algoritmo 1.3.14.3.2.26 de 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 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 Web en tecnología REST no requieren la intervención cuando estos son de exposición.

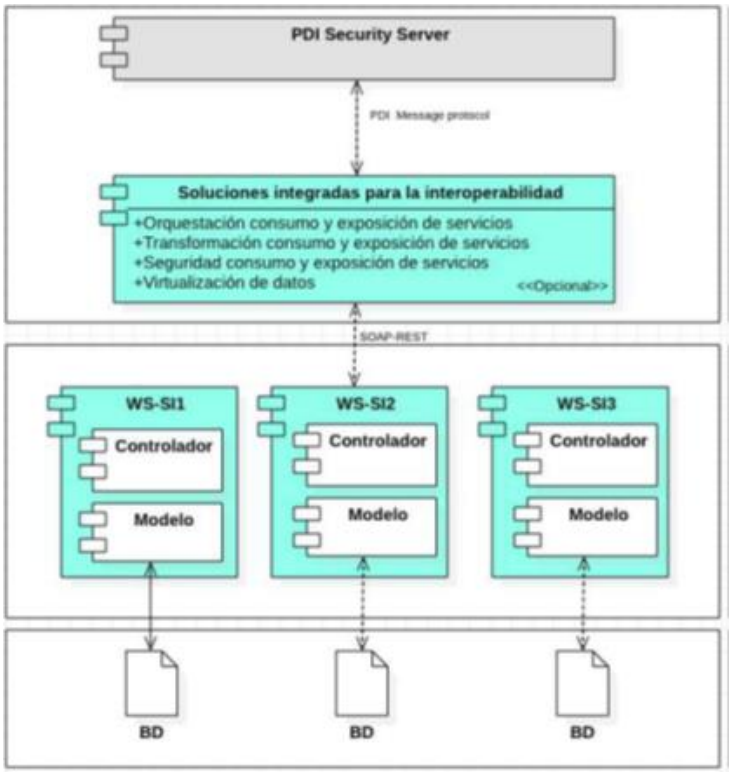


Figura 11 Arquitectura de referencia con Adaptador de Transformación de Servicio

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

- Orquestar 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 como, 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 servicios SOAP y REST (consumo) tienen que ser intervenidos para que los siguientes campos obligatorios de X-Road 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 exponer y consumir servicios web REST y SOAP a través de X-Road. Sirve como componente de soluciones integradas 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-Road message protocol al interior del componente. Aunque se puede utilizar un bus de servicios directamente, configurar un bus de servicios para X-ROAD es desgastante, especialmente en SOAP. El Adaptador es fácil de parametrizar, 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 X-Road en 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 web 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.

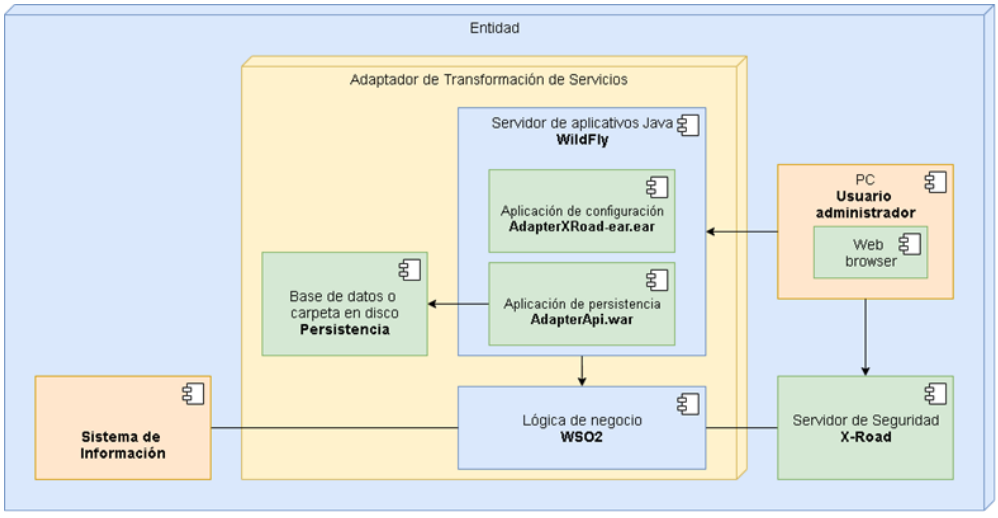


Figura 12 Diagrama de despliegue del Adaptador de integración

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 exposición o consumo para habilitar su compatibilidad con X-Road. Comprende un servidor de aplicaciones Java (WildFly), los aplicativos encargados de configurar el bus de servicios, y 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 interactúa únicamente con este componente por medio del navegador. Este componente se integra con 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 plano de los 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 la lógica 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, url, tipo 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 Web.
PC Usuario administrador	Cliente que se conecta al Adaptador o al Servidor de Seguridad para procesos de configuración o administración.
Servidor de Seguridad X-Road	Servidor de Seguridad de la entidad que conectará con la Plataforma de Interoperabilidad.

Se recomienda realizar el despliegue del componente de transformación de servicios en un servidor diferente 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 4 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 se deberá escalar de acuerdo con la estimación de consumo de la entidad 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 Adaptador.
6	http://**IP_ADAPTADOR**:8280/SERVICIO /	Servicios creados en el Wso2.
7	**Error! Hyperlink reference not valid. IP_ADAPTER_API**:8080/AdapterApi	Puerto del Componente AdapterApi.
8	https://**IP_WSO2**:9443/carbon	Administración de Wso2.
Software		
9	Sistema operativo	La solución es multiplataforma. No aplica
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. Esta guía cuenta con versiones para Ubuntu, Red Hat 7 y RedHat 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 suscribir entre la entidad y la Agencia Nacional Digital un acuerdo de entendimiento que describe el objeto y los 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 funciones constitucionales y legales.

6.9. Uso y apropiación

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

El servicio de intercambio de información y los elementos de datos de la entidad debe estar certificada en nivel tres (3) de lenguaje común de intercambio

La entidad comprende el marco de interoperabilidad para gobierno digital el cual se fundamenta en un modelo de madurez basado en aspectos legales, técnicos y organizacionales que permite el desarrollo progresivo 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 se obstaculiza o impide la interoperabilidad.

Dominio Organizacional: se refiere al modo en que las misiones, políticas, procesos y expectativas interactúan con aquellos de otras entidades para alcanzar las metas adoptadas de común acuerdo y mutuamente beneficiosas, 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 interfaz, protocolos de interconexión, servicios de integración de datos, presentación e intercambio de datos y protocolos 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 cuando se adelanten trámites y servicios a través de medios digitales, afirmando que dicha persona es quien dice ser. El servicio permite generar un ambiente que habilita a los ciudadanos su acceso a los trámites y servicios de entidades públicas y privadas por medios electrónicos, con plenas garantías de confianza y seguridad.

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

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

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

- **Bajo:** Ofrece un nivel de confianza mínimo en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es mínimo. Para este nivel las credenciales de usuario estarán asociadas al correo electrónico del usuario, una contraseña de acuerdo con el estándar NIST SP 800-63B de un solo factor OTP.

- **Medio:** Ofrece cierto nivel de confianza en el proceso de Autenticación Digital. Se emplea cuando el riesgo que conlleva una autentificación errónea es moderado.

Para este nivel las credenciales de usuario estarán asociadas al ID del usuario, datos obtenidos en la identificación, correo electrónico, teléfono, dirección, una contraseña de acuerdo con el estándar NIST SP 800-63B de un solo factor OTP, preguntas y respuestas reto, mecanismos de factor múltiple de autenticación de acuerdo con el estándar NIST SP 800-63B Multi-Factor Cryptographic Software y NIST SP 800-63B Multi-Factor.

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

En caso de los ciudadanos colombianos, la siguiente tabla nuestra la relación de trámite, el grado de confianza 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 Información de Registró 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 identidad de la persona a registrar y verificar que estos le correspondan según el grado de confianza.

Se deben tener las siguientes consideraciones:

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

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

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

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

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

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

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

7.1 Objetivos del servicio

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

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

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

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

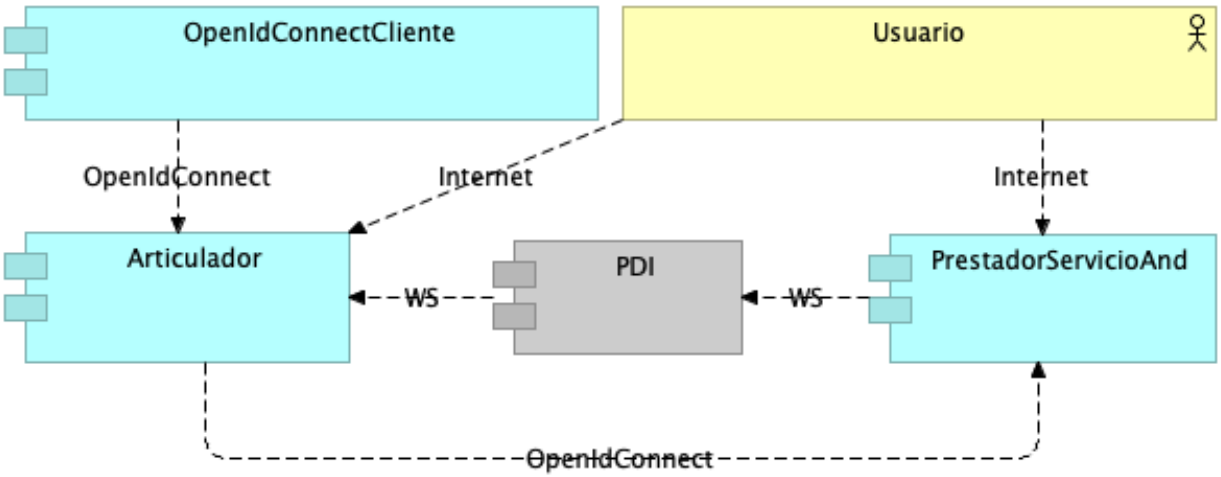


Figura 13 Componente del servicio de Autenticación Digital

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 los sistemas de las entidades. Este componente implementa el protocolo openIdConnect cliente.

Articulador	Componente que representa la pasarela de autenticación.
Prestador Servicio And	Componente que tiene por objetivo la implementación de las funcionalidades de un prestador de servicio para los grados de confianza 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, si la entidad tiene mecanismos de autenticación y/o autorización de usuarios

- Determinar el grado de confianza (bajo, medio, alto, muy alto), que requiere el trámite y seleccionar la forma de integración del sistema de información de la entidad con la plataforma de autenticación y seleccionar la más adecuada. a Agencia Nacional Digital ofrece dos formas de integración: (i) librerías OpenId Connect cliente 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 Code.

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 sean 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 en cualquier 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 Pasarela, las 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 adicionales 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 servicio de 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 será gestionada 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 se deberán instanciar por parte de la capa de presentación de la aplicación de la entidad (mencionado en el punto anterior), para hacer uso de las siguientes funcionalidades:
    - Authorize (Registro y autenticación). Para este caso, al momento de instanciar/invocar el endpoint 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 depende de 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. Definir parámetros de integración del Marco de Implementación del servicio de Autenticación Digital del Documento Guía para la vinculación y uso de los servicios ciudadanos digitales)
        - Redirect_uri: Parámetro redirectUrlLogIn 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 deberán enviar los siguientes datos:
        - authorization_code (recibido anteriormente por el Authorize)
        - client_id
        - client_secret

        - redirect_uri (Parámetro redirectUrlLogIn definido en el siguiente paso).
    - UserInfo (Obtener información adicional del usuario. La librería implementará el contrato y lógica para usar el usuario userInfo). La librería construirá la petición GET al servicio web enviando el token.
    - Access_Token recibido anteriormente por medio del header.
    - Authorization Bearer. El sistema de información de la entidad deberá recibir la petición y gestionar esta información del usuario en su sistema de información.
    - EndSession. Si bien esta funcionalidad es implementada por la librería, se deberá enviarle a la función respectiva el id_token para cerrar la sesión en el Autenticador Digital. Una vez la entidad recibe el redirect 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 el cual 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 más 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 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).
    - redirectUrlEndSession (parámetro definido por la entidad).

3. Desplegar EAR componente de integración OpenId Connect siguiente los pasos descritos en el archivo 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 Digital.

5. En el sistema de la entidad se deberá:
    - Importar 2 archivos JavaScript, el primero, es de configuración el cual se deberá actualizar con los datos del sistema de información de la entidad. El segundo, corresponde a la lógica del manejo de sesión del componente transversal en el sistema de información de la entidad. El manejo de sesión será por manejo de cookies.
    - En la pantalla de presentación del sistema de información de la entidad, se deberá agregar un componente <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 es 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 todas las 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 512
- Proteger las cookies/objetos de sesión de autenticación para que no estén expuestas a ningún software cliente 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 atributos del sistema de autenticación digital NG2 al flujo de registro y recuperación de contraseña.

La siguiente imagen presenta la metodología.

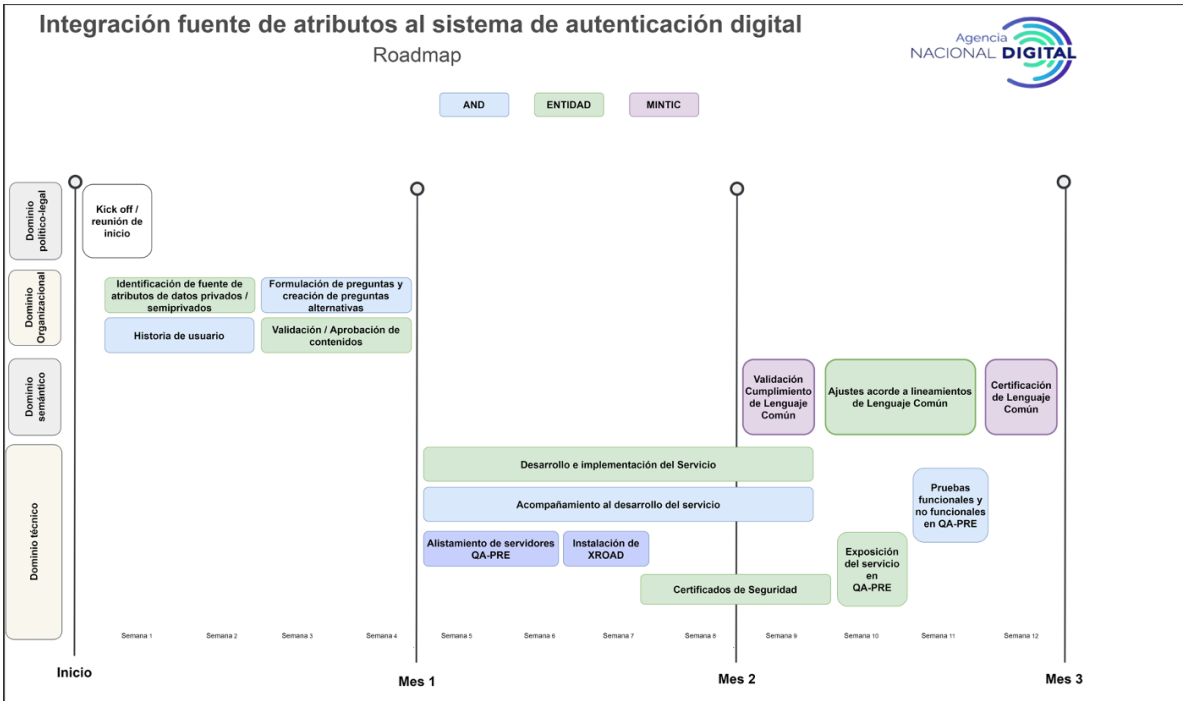


Figura 14 Road Map para la integración como fuente de atributo

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

Tabla 9

Nombre Actividad	Descripción
1. Kick off/ reunión de inicio	En esta actividad se realiza una contextualización sobre el servicio de autenticación, sus niveles de garantía, la arquitectura del servicio de Autenticación Digital y la característica de los datos o atributos (semi privados, privados, maestros de la información, obligatorios, entre otros), que son candidatos a ser parte de la generación de preguntas reto. Una vez la entidad revisa las características de los atributos, se comparte el diccionario de datos candidatos con su descripción y un set 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 identifica los datos privados y semiprivados que sirvan para realizar preguntas reto. La Agencia Nacional Digital analiza cada uno de los atributos y selecciona los 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 se identifican los estados de conexión del servicio a construir.
4. **Formulación de preguntas y respuestas alternativas.**	Con los datos identificados, la Agencia Nacional Digital formula preguntas para 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 Agencia Nacional Digital.
6. **Desarrollo e implementación del servicio.**	Una vez realizado el diseño técnico, se deberá implementar el servicio web de exposición por parte de la entidad fuente de atributos. Este servicio será consumido desde el servicio de Autenticación Digital cuando se va a realizar un registro o un cambio de contraseña. Si la integración se realiza de la manera descrita 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 estará presta a ayudar y acompañar 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 desarrollo, la entidad deberá trabajar en el alistamiento de los servidores de seguridad para los ambientes de prueba, preproducción y producción.
9. **Instalación del X-Road**	Una vez se tengan los servidores de seguridad la entidad debe instalar 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 debe solicitar al Ministerio el certificado de lenguaje común.
11. **Exposición del servicio**	Teniendo el certificado de lenguaje común se expondrá el servicio por X-Road y se validara 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 digital, interactúan con la pasarela de autenticación digital por medio del protocolo OpenID Connect y sus estándares

- Las aplicaciones de las entidades solo deben conocer e interactuar con la pasarela de servicios, un servidor de tokens (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 Especiales sin necesidad de actualizar las aplicaciones de las entidades.
- Los Prestadores de Servicios Ciudadanos Digitales Especiales por lo general tienen un conjunto de Claims, o atributos de los Usuarios, el componente de pasarela permite normalizar la información de tal forma que cuando 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 el proceso de migración de usuarios. Tener en cuenta que se toma el ID de usuario como elemento de migración y no los 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 al momento de que el usuario inicia el flujo de autenticación, el articulador enrute el usuario hacia el prestador del 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 el sistema de autenticación de 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 del servicio.

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 el diseño de 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 Nacional Digital.

7.8 Recomendaciones de seguridad

- Siempre se debe emplear SSL, incluso para los ambientes de desarrollo.

- En caso de emplear secretos compartidos[5], estos NO PUEDEN estar en control de código fuente de las 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 servidor 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 adelante.
- En caso de emplear secretos compartidos, estos NO PUEDEN estar en control de código fuente de las 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 él envió de cookies solamente al servidor 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

[5] 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.

- 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 / revocada. Los atributos client_id, client_secret, urls deberán ser deshabilitadas. 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 de todos sus usuarios.
- Se debe solicitar a la parte que confía que borre todos los datos del usuario según el acuerdo adquirido del 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, acceder y 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 normatividad 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 conjunta con los otros servicios digitales base. La autorización de acceso es canalizada por el servicio de Autenticación Digital, mientras que el servicio de Interoperabilidad permite realizar las consultas de los datos del usuario desde los custodios responsables en la administración pública

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

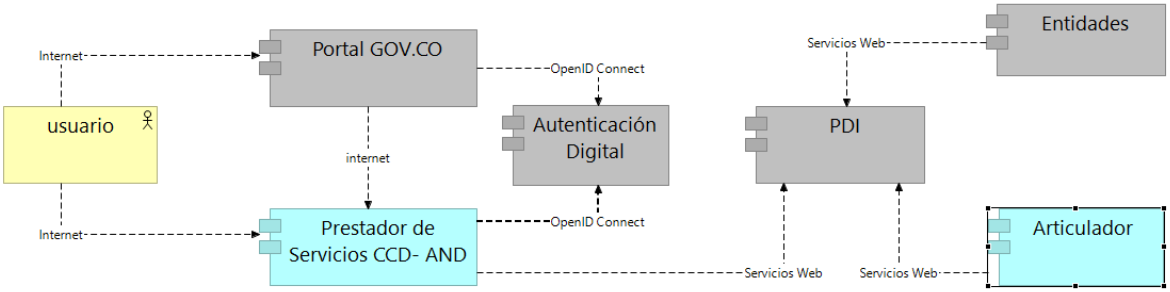


Figura 15 Diagrama de componentes carpeta ciudadana digital

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 y con la plataforma de interoperabilidad para el consumo de servicios de las entidades.
Articulador	Representa los componentes funcionales de administración y monitoreo del servicio por parte 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 lineamientos de implementación de los servicios ciudadanos digitales de MinTIC, el servicio de Carpeta Ciudadana Digital criterios de diseño:

1. El usuario podrá acceder al Servicio de Carpeta Ciudadana Digital – CCD, se realizará por medio el Portal Único del Estado GOV.CO.
2. La autenticación del usuario al Servicio de Carpeta Ciudadana se realizará usando el nivel de confianza medio del servicio de autenticación digital.
3. El consumo y exposición de servicios de Carpeta Ciudadana Digital, se hará a través de la PDI con los diferentes Actores: Entidades Públicas y Articulador.
4. El servicio de CCD no almacenará de manera permanente los datos presentados a los usuarios y no será un 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 cual 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 Digital
- Identificar de acuerdo con las funciones misionales y legales de la entidad, la información de la cual son fuente 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 del servicio de Carpeta Ciudadana Digital
- Identificar las capacidades tecnológicas actuales para la integración al servicio de Carpeta Ciudadana Digital, 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, el diseño debe detallar cómo la entidad expondrá los servicios de consulta de información, los servicios de historial de trámites y solicitudes, los servicios de alertas y comunicaciones de los trámites o actuaciones que el usuario realice ante la entidad pública y las solicitudes de actualización y corrección de datos que los usuarios realicen 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 de 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 hará 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.
- Integrar los servicios de exposición a la plataforma de interoperabilidad, que corresponde a la publicación del 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 datos que 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, noticias, información 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 del 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 de los 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 del 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 de las 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 respuesta a la solicitud.

Aunque dentro del 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 de historiales y alertas.

Para el desarrollo de los servicios web de exposición de las entidades se define realizarse bajo la tecnología REST, Content-type: Application/json, con el objetivo de estandarizar y optimizar la integración al servicio de Carpeta Ciudadana Digital.

Las siguientes tablas corresponden a la descripción de los servicios web de exposición hacia el servicio de 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}/{idUsuario}
Parámetros del request	
/{tipoId}	Tipo de identificación del usuario.
/{idUsuario}	Número de identificación de la persona de la cual se buscan las alertas o comunicaciones a enviar en la petición

Response	{
	"mensajeColeccion":
	[{
	"idMensaje":"",
	"asunto":"",
	"textoMensaje":"",
	"urlDescargueAdjuntos":"",
	"fechaMensaje":""
	},...]
	}

idMensaje	Identificador único del mensaje (Alerta o Comunicación) ante la Entidad
• **asunto**	Asunto de la Alerta o Comunicación
• **textoMensaje**	Texto con el contenido del mensaje que se quiere enviar a la persona
• **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}/{idUsuario}
Parámetros del request	
/{tipoId}	Tipo de identificación del usuario.
/{idUsuario}	Número de identificación de la persona de la cual se consulta la información a enviar en la petición.
Response	

<table>
<tr><td colspan="2">La respuesta es un arreglo JSON de objetos llamado datoConsultado que tiene dos campos (campoDato y valorDato). Adicionalmente, un campo llamado urlDescarga. A continuación, se presenta una muestra de la respuesta JSON</td></tr>
<tr><td>Cuando campoDato NO tienen el texto archivoBase64 o archivoURL para descarga de archivo</td><td>Cuando campoDato tiene el texto archivoBase64 o archivoURL para descarga del archivo.</td></tr>
<tr><td>{
"datoConsultado":
[{
"campoDato ":"",
"valorDato ":""
},...
],
"urlDescarga ":""
}</td><td>{
"datoConsultado":
[{
"campoDato":" ",
"valorDato":" ",
"tipoArchivo":" ",
"nombreArchivo":" ",
"descripcionArchivo":" ",
},...
],
"urlDescarga":" "
}</td></tr>
<tr><td>campoDato</td><td>Cuando es un archivo en base64 para ser descargado, el campoDato debe tener el texto “archivoBase64”.

Cuando es una ruta de descarga el campoDato debe tener el texto “archivoURL”</td></tr>
<tr><td>valorDato</td><td>Cuando campoDato contenga la palabra “archivoBase64”: valorDato 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 una lista de archivos, en total no deben superar los 10MB de tamaño.

Cuando campoDato contenga la palabra “archivoURL”: valorDato deberá contener la ruta http publica para la descarga del documento. Esto cuando el(los) archivo(s) en total supere(n) los 10 MB de tamaño o la entidad decida establecer una URL para descargar el archivo.</td></tr>
</table>

	Al final de esta guía se encuentra una ampliación explicada de este contrato. Cuando campoDato contenga la palabra "archivoBase64Todos", se entiende que en valodDato 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. Actualmente 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}/{idUsuario}
Parámetros del request	
/{tipoId}	Tipo de identificación del usuario.
/{idUsuario}	Número de identificación de la persona de la cual se buscan las alertas o 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 AAAA-MM-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}/{idUsuario}
Parámetros del request	
/{tipoId}	Tipo de identificación del usuario.
/{idUsuario}	Número de identificación de la persona de la cual se buscan las alertas o 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 AAAA-MM-DD HH24:MM:SS.FF
• **servicioConsulta**	Nombre del servicio de consulta de información del usuario ante la Entidad desde donde se inicializa el Trámite debe ser el mismo que se registra en servicio CCD
estadoTramiteUsuario	Estado del Trámite en la entidad
• **Elemento: entidadconsultada**	
• **nomEntidad**	Nombre de la Entidad consultada por la Entidad donde el usuario realiza el trámite para dar resolución al mismo

1 Integrar los servicios web a la plataforma de interoperabilidad

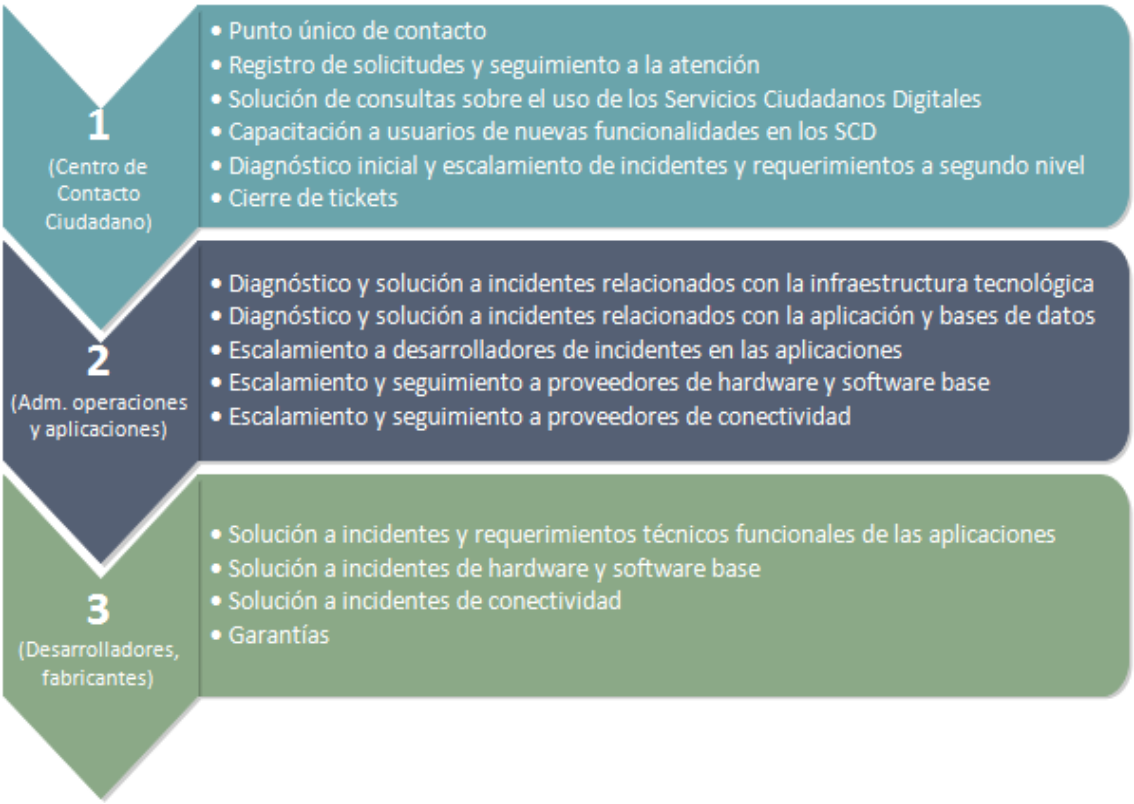
El intercambio de datos entre el servicio de Carpeta Ciudadana Digital y las entidades públicas se hará a través de la PDI, para ello la entidad deberá:

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

El detalle de la integración a la PDI se encuentra en la sección de integración al servicio de interoperabilidad de 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 de tres niveles de atención: el primer nivel de servicio será prestado por el Centro de Contacto al Ciudadano del Ministerio TIC, el segundo y tercer nivel será prestado por la Agencia Nacional Digital.



MINISTERIO DE TECNOLOGÍAS
DE LA INFORMACIÓN Y LAS
COMUNICACIONES