El futuro digital es de todos

MinTIC

Anexo Técnico

Guía de integración de prestadores privados de SCD Especiales

MinTIC – Viceministerio de Transformación Digital.
Dirección de Gobierno Digital
Junio 2022

SERVICIOS CIUDADANOS DIGITALES

Anexo I

La “Guía de integración de prestadores privados de Servicios Ciudadanos Digitales Especiales” tiene por objeto establecer los requisitos y las condiciones del trámite que las personas jurídicas de derecho privado deben cumplir para ser habilitados para la prestación de Servicios Ciudadanos Digitales Especiales, así como establecer los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital en su rol de articulador, de conformidad con lo establecido en la Resolución “Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de Servicios Ciudadanos Digitales Especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital”.

Tabla de contenido

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

Equipo de trabajo
Carmen Ligia Valderrama Rojas - Ministra de Tecnologías de la Información y las Comunicaciones
Iván Mauricio Durán Pabón - Vice Ministro de Transformación Digital
Ingrid Tatiana Montealegre Arboleda - Directora de Gobierno Digital

Ivan Dario Marrugo Jimenez – Coordinador Equipo Política Dirección Gobierno Digital
Luis Fernando Bastidas Reyes - Equipo de Política Dirección de Gobierno Digital
Arlington Fonseca Lemus - Equipo de Política Dirección de Gobierno Digital
Gilber Corrales Rubiano - Equipo de Política Dirección de Gobierno Digital
Marco Emilio Sánchez Acevedo - Equipo de Política Dirección de Gobierno Digital
Silvia Helena Pedroza Arias - Equipo de Política Dirección de Gobierno Digital
José Ricardo Aponte Oviedo - Equipo Servicios Ciudadanos Digitales Dirección de Gobierno Digital
Giovanni Alvarado Páez - Equipo Servicios Ciudadanos Digitales Dirección de Gobierno Digital

Versión	Observaciones
Versión 1 Junio 2022	

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co
Documento de Gobierno Digital

Tabla de ilustraciones

1 Introducción

El Ministerio de Tecnologías de la Información y las Comunicaciones (en adelante, MinTIC), de acuerdo con el artículo 17 de la Ley 1341 de 2009, formula políticas y planes enfocados a las Tecnologías de la Información y las Comunicaciones (en adelante, TIC) 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.

Los numerales 1 y 2 del artículo 18 de la Ley 1341 de 2009 establecen las siguientes funciones del MinTIC: “1. Diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones”; y, “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 (…)”.

Por disposición del artículo 2.2.17.2.1.1 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones -(en adelante DUR-TIC), los servicios ciudadanos digitales se clasifican en servicios base y servicios especiales, así:

Son servicios ciudadanos digitales base aquellos que se consideran fundamentales para brindarle al Estado las capacidades en su transformación digital, éstos son:

1. Servicio de interoperabilidad
2. Servicio de autenticación digital
3. Servicio de carpeta ciudadana digital

Por su parte, son servicios ciudadanos digitales especiales aquellos 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 la Agencia Nacional Digital en su rol de Articulador.

El artículo 9 de la Ley 2052 de 2020 dispone que las personas jurídicas privadas podrán prestar servicios ciudadanos digitales especiales previa habilitación, y conforme con los lineamientos que establezca el MinTIC, de conformidad con los principios de integridad, autenticidad y no repudio contenidos en la Ley 527 de 1999.

En consecuencia, la presente guía describe los requisitos técnicos, administrativos, financieros y jurídicos que deben cumplir las personas jurídicas de derecho privado para ser habilitados para la prestación de servicios ciudadanos digitales especiales, además de señalar los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital en su rol de Articulador.

2 Alcance de la Guía

De conformidad con el artículo 2 de la Resolución ”Por la cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Nacional Digital”, serán sujetos obligados de la presente guía las personas jurídicas de derecho privado que soliciten la habilitación para prestar servicios ciudadanos digitales especiales, así como aquellos que obtengan la respectiva habilitación por parte del MinTIC.

3 Definiciones

En aplicación de la presente guía, además de las definiciones contenidas en los artículos 2.2.17.1.4 y 2.2.17.2.1.1. del Decreto 1078 de 2015 (DUR-TIC) y las contenidas en el Anexo 1 y el Anexo 2 de la Resolución 2160 de 2020, se deberán aplicar las siguientes:

1. **Acuerdo de Nivel de Servicio:** Es un acuerdo entre el prestador de servicios ciudadanos digitales especiales y los Usuarios. Un acuerdo de niveles de servicio describe los servicios, documenta los objetivos de nivel de servicio y especifica las responsabilidades del proveedor y el Usuario. Un acuerdo de nivel de servicio también puede establecerse entre prestadores de servicios ciudadanos digitales especiales, o entre un prestador de servicios ciudadanos digitales especiales y sus proveedores de servicios conexos a los servicios ciudadanos digitales. Un acuerdo de nivel de servicio puede incluirse en un contrato u otro tipo de acuerdo documentado.
2. **Agencia Nacional Digital:** Es una entidad descentralizada indirecta, con el carácter de asociación civil, de participación pública y naturaleza privada, sin ánimo de lucro adscrita al MINTIC, que busca contribuir a la construcción de un Estado más eficiente, transparente y participativo, gracias al uso y aplicación de la ciencia y las tecnologías de la información y las comunicaciones, articulando los servicios ciudadanos digitales. Le corresponde desempeñar dos roles: por un lado, es el Articulador de los servicios ciudadanos digitales especiales, y por el otro, es prestador de servicios ciudadanos digitales base.
3. **Autoridad de Certificación:** Prestador de servicios de confianza que valida las identificaciones de las entidades y las vincula a claves criptográficas mediante certificados digitales.
4. **Autoridad de Estampa de Tiempo:** Prestador de servicios de confianza que ofrece sellos de tiempo oficiales.
5. **Base de Datos Maestra:** Redirige las peticiones al Prestador de Servicios Ciudadanos Digitales Especiales, por esta razón solo almacena los datos imprescindibles para esa labor (tipo de documento, número de documento, código del prestador). Es propiedad de la Agencia Nacional Digital.
6. **Base de Datos Primaria:** Almacena únicamente los datos imprescindibles para direccionar las solicitudes realizadas por los Usuarios de los servicios ciudadanos digitales a su respectivo prestador de servicio. Es de propiedad de los prestadores de servicios ciudadanos digitales.

7. **Claim/Claims:** Atributo de los Usuarios finales, por ejemplo, dirección, nombres, teléfono.
8. **Dirección IP:** Conjunto de números que identifica de manera lógica y jerárquica a una interfaz en la red de un dispositivo que utilice el protocolo IP, o que corresponde al nivel de red del modelo TCP/IP.
9. **Proveedor de Identidad IDP:** Servidor de autorización capaz de autenticar Usuarios finales y proveer Claims a los clientes acerca de los eventos de autenticación digital y atributos de los Usuarios finales.
10. **Modelo de Seguridad y Privacidad de la Información:** Imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la política de gobierno digital.
11. **OpenID Connect:** Es un protocolo de autenticación que permite el uso de servidores de autenticación siendo un protocolo abierto e interoperable.
12. **Proxy Inverso:** Se ubica frente a un servidor web y recibe todas las solicitudes antes de que lleguen al servidor de origen.
13. **Prestador:** Es el Prestador de Servicios Ciudadanos Digitales Especiales cuando presta servicios ciudadanos digitales especiales y base, o la Agencia Nacional Digital cuando presta servicios ciudadanos digitales base.
14. **Prestador(es) de Servicios Ciudadanos Digitales Especiales:** Son personas jurídicas de derecho privado, habilitados previamente por el MinTIC, quienes, mediante un esquema coordinado y administrado por la Agencia Nacional Digital en su rol de Articulador, pueden proveer los servicios ciudadanos digitales especiales y base a personas jurídicas y naturales, siempre bajo los lineamientos, políticas y guías que expida el MinTIC.
15. **Puerto Lógico de Red/Puerto/Puertos:** Es una interface de software que permite el ingreso y salida de data por medio de aplicaciones que usan Internet, consiste en el direccionamiento de la capa 4 del modelo OSI que es modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1). Estos puertos pueden referirse a TCP (Transmission Control Protocol) o UDP (User Datagram Protocol) y se identifican por números desde 1 hasta 65.000 pudiendo llegar a más, siendo conocidos los puertos de 1 a 1024.
16. **RP. (Relying Party, Cliente, Entidad del Estado.):** Servicio que requiere de la autenticación digital del usuario final y sus Atributos (Claims) desde el prestador de servicio de autenticación digital. En el modelo del servicio de autenticación digital, la pasarela de la Agencia Nacional Digital es la parte que confía (relying party) de los Prestadores de Servicios Ciudadanos Digitales Especiales, a su vez las entidades del Estado son las partes que confían (relying party) de la pasarela.

17. **Servicio Web:** Medio por el cual se transmiten los resultados de los procesos de autenticación de acuerdo con la especificación técnica informada por la Agencia Nacional Digital en su rol de Articulador.
18. **Servidor:** Conjunto de computadoras capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como «el servidor».
19. **Sistema Operativo:** Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.
20. **Sistema de Nombres de Dominio:** Sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.
21. **Solicitante(s):** Personas jurídicas de derecho privado que pretenden ser habilitados por el MinTIC para la prestación de servicios ciudadanos digitales especiales, mediante un esquema coordinado y administrado por la Agencia Nacional Digital en su rol de Articulador, siempre bajo los lineamientos, políticas y guías que expida el MinTIC.
22. **Trámite:** Conjunto de acciones reguladas por el Estado que deben efectuar los Usuarios para adquirir un derecho o cumplir con una obligación prevista o autorizada por la ley. El trámite se inicia cuando el usuario presenta una petición a la administración y termina cuando esta última se pronuncia, aceptando o denegando la solicitud. Estos pueden ser realizados por medios electrónicos, recibiendo la denominación de trámite en línea.
23. **Usuario(s)**: Son las personas naturales, nacionales o extranjeras, o las personas jurídicas, de naturaleza pública o privada, que hagan uso de los servicios ciudadanos digitales.
24. **X-Road:** 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.

4 Marco Normativo

El artículo 2 de la Constitución Política 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.

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”, reglamentado por el Decreto 2364 de 2012, establece el reconocimiento jurídico a los mensajes de datos en las mismas condiciones que se ha otorgado para los soportes que se encuentren en medios físicos.

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 “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–(…)”, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones en el desarrollo de sus funciones.

En virtud del numeral 2 del artículo 17 de la Ley 1341 de 2009, el MinTIC tiene entre sus objetivos, promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación.

La Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”, reglamentada por el Decreto 1377 de 2013, 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 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 2.2.9.1.1.1. del Decreto 1078 de 2015 (DUR-TIC), la Política de Gobierno Digital, es entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio.

De acuerdo con el artículo 2.2.9.1.2.1. del Decreto 1078 de 2015 (DUR-TIC), la Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo.

De acuerdo con el numeral 3 del artículo 2.2.9.1.2.1. del Decreto 1078 de 2015 (DUR-TIC), los sujetos obligados a la Política de Gobierno Digital desarrollarán las capacidades que les permitan ejecutar las líneas de acción de esta política, mediante la implementación de los siguientes habilitadores: Arquitectura, Seguridad y Privacidad de la Información, Cultura y Apropiación y Servicios Ciudadanos Digitales.

El artículo 2 de la Ley 1955 de 2019 establece que el documento denominado “Bases del Plan Nacional de Desarrollo 2018-2022: Pacto por Colombia, pacto por la equidad”, hace parte integral de esta ley. 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. 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 documento CONPES 3995 de 2020 cuyo fin es desarrollar la confianza digital a través de la mejora de 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 citado artículo 147 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 Decreto 1078 de 2015 (DUR-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 señala 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.

El Articulador señalado en el numeral 3 del artículo 2.2.17.1.5. del Decreto 1078 de 2015 (DUR-TIC), deberá cumplir las condiciones y estándares establecidos en la guía de lineamientos de los servicios ciudadanos digitales, con el fin de garantizar la correcta prestación de los servicios ofertados. Las autoridades señaladas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015 (DUR-TIC) deberán cumplir las condiciones y estándares establecidos en la guía para vinculación y uso de los

servicios ciudadanos digitales, 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, en el numeral 6, se presentan los requisitos para que las personas jurídicas de derecho privado puedan ser habilitados en la prestación de servicios ciudadanos digitales especiales.

4.1 Documentos y guías de referencia

- Decreto 1078 de 2015 (DUR-TIC)
  Disponible en: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30019521

- Resolución MinTIC 2160 de 2020.
  Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-161273_Resolucion_2160_2020.pdf

  Anexo 1 de la Resolución MinTIC 2160 de 2020.
  Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-161274_Anexo1_Resolucion_2160_2020.pdf

  Anexo 2 de la Resolución MinTIC 2160 de 2020.
  Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-161275_Anexo2_Resolucion_2160_2020.pdf

- Resolución MinTIC 2893 de 2020.
  Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-161263_Resolucion_2893_2020.pdf

- Resolución MinTIC 1519 de 2020.
  Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-160770_resolucion_1519_2020.pdf

- Resolución MinTIC 500 de 2021.
  Disponible en: https://normograma.mintic.gov.co/mintic/docs/pdf/resolucion_mintic_2893_2020.pdf

- Modelo de seguridad y privacidad.
  Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MGRSD/

- Marco de referencia de arquitectura empresarial.
  Disponible en: https://www.mintic.gov.co/arquitecturati/630/w3-channel.html

5 Servicios Ciudadanos Digitales

El modelo de servicios ciudadanos digitales es uno de los cuatro (4) habilitadores de la política de gobierno digital de Colombia, como se ilustra a continuación.

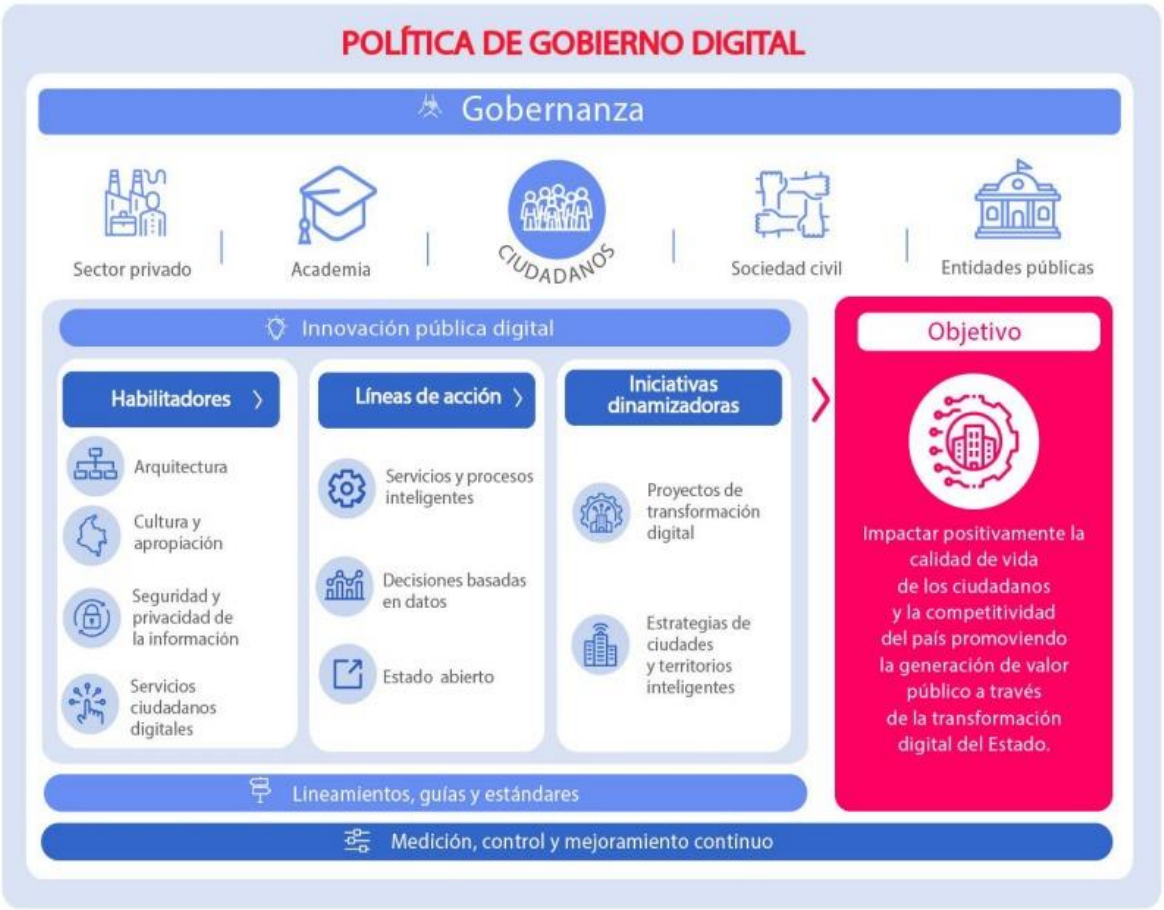


Ilustración 1. Ministerio de Tecnologías de la Información y las Comunicaciones, Dirección de Gobierno Digital

Por disposición del artículo 2.2.9.1.2.1. del Decreto 1078 de 2015 (DUR-TIC), la Política de Gobierno Digital se desarrollará a través de un esquema que articula los

elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo, entendidos así:

1. Gobernanza: Los sujetos obligados implementarán la Política de Gobierno Digital bajo un modelo de gobernanza basado en el relacionamiento entre el orden nacional y territorial, y el nivel central y descentralizado, que involucre a los grupos de interés en la toma de decisiones y defina los focos estratégicos de acción y la distribución eficiente de los recursos disponibles, procurando una gestión pública colaborativa y ágil.

2. Innovación Pública Digital: Los sujetos obligados implementarán la Política de Gobierno Digital con un enfoque transversal basado en el relacionamiento con los Grupos de Interés, que genere valor público a través de la introducción de soluciones novedosas y creativas y que hagan uso de las Tecnologías de la Información y las Comunicaciones y de metodologías de innovación, para resolver problemáticas públicas desde una perspectiva centrada en los ciudadanos yen general, los habitantes del territorio nacional.

Con el fin de fortalecer los procesos de innovación pública digital, los sujetos obligados promoverán la implementación de mecanismos de compra pública que faciliten al Estado la adquisición de bienes o servicios de base tecnológica que den respuesta a desafíos públicos respecto de los cuales no se encuentra una solución en el mercado o, si la hay, requiera ajustes o mejoras. Asimismo, promoverán la adopción de tecnologías basadas en software libre o código abierto, sin perjuicio de la inversión en tecnologías cerradas.

3. Habilitadores: Los sujetos obligados desarrollarán las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital, mediante la implementación de los siguientes habilitadores:

3.1. Arquitectura: Este habilitador busca que los sujetos obligados desarrollen capacidades para el fortalecimiento institucional implementando el enfoque de arquitectura empresarial en la gestión, gobierno y desarrollo de proyectos con componentes de Tecnologías de la Información.

Los sujetos obligados deberán articular su orientación estratégica, su modelo de gestión, su plan de transformación digital, y su estrategia de Tecnologías de Información y las Comunicaciones, con el objetivo de dar cumplimiento a la Política de Gobierno Digital.

3.2. Seguridad y Privacidad de la Información: Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

3.3. Cultura y Apropiación: Este habilitador busca desarrollar las capacidades de los sujetos obligados a la Política de Gobierno Digital y los Grupos de Interés, requeridas para el acceso, uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones. Se promoverá el uso y apropiación .de estas entre las personas en situación de discapacidad y se fomentará la inclusión con enfoque diferencial.

3.4. Servicios Ciudadanos Digitales: Este habilitador busca desarrollar, mediante soluciones tecnológicas, las capacidades de los sujetos obligados a la Política de Gobierno Digital para mejorar la interacción con la ciudadanía y garantizar su derecho a la utilización de medios digitales ante la administración pública.

4. Líneas de Acción: Los sujetos obligados ejecutarán acciones orientadas a desarrollar servicios y procesos inteligentes, tomar decisiones basadas en datos y consolidar un Estado abierto, con el fin de articular las Iniciativas Dinamizadoras de la Política de Gobierno Digital. Estas Líneas de Acción se materializarán en las sedes electrónicas de cada uno de los sujetos obligados, siguiendo los estándares señalados para tal fin. En el proceso de registro de los nombres de dominio requeridos para la implementación de la Política de Gobierno Digital, se deberá realizar la articulación con el Ministerio de Tecnologías de la Información y las Comunicaciones, acorde con la normativa que regula la materia.

4.1. Servicios y Procesos Inteligentes: Esta línea de acción busca que los sujetos obligados desarrollen servicIos y procesos digitales, automatizados, accesibles, adaptativos y basados en criterios de calidad, a partir del entendimiento de las necesidades del usuario y su experiencia, implementando esquemas de atención proactiva y el uso de tecnologías emergentes.

4.2. Decisiones Basadas en Datos: Esta línea de acción busca promover el desarrollo económico y social del país impulsado por datos, entendiéndolos como infraestructura y activos estratégicos, a través de mecanismos de gobernanza para el acceso, intercambio, reutilización y explotación de los datos, que den cumplimiento a las normas de protección y tratamiento de datos personales y

permitan mejorar la toma de decisiones y la prestación de servicios de los sujetos obligados.

4.3. Estado Abierto: Esta línea de acción busca promover la transparencia en la gestión pública con un enfoque de apertura por defecto, y el fortalecimiento de escenarios de diálogo que promuevan la confianza social e institucional, además la colaboración y la participación efectiva de los Grupos de Interés, para fortalecer la democracia y dar soluciones a problemas de interés público a través de prácticas innovadoras, sostenibles y soportadas en Tecnologías de la Información y las Comunicaciones.

5. Iniciativas Dinamizadoras: Comprende los Proyectos de Transformación Digital y las Estrategias de Ciudades y Territorios Inteligentes, a través de lascuales se materializan las Líneas de Acción, que permiten dar cumplimiento al objetivo de la Política de Gobierno Digital con la implementación de mecanismos de compra pública que promuevan la innovación pública digital.

5.1. Proyectos de Transformación Digital: Comprende aquellos proyectos que implementarán los sujetos obligados para aportar a la generación de valor público mediante el aprovechamiento de las capacidades que brindan el uso y la apropiación de las Tecnologías de la Información y las Comunicaciones y así alcanzar los objetivos estratégicos institucionales. Los proyectos de Transformación Digital deberán estar integrados al Plan Estratégico de Tecnología y Sistemas de Información (PETI).

5.2. Estrategias de Ciudades y Territorios Inteligentes: Las entidades territoriales podrán desarrollar estrategias de ciudades y territorios inteligentes, a través del uso de tecnologías de la información y las comunicaciones, como herramientas de transformación social, económica y ambiental de los territorios.

Por disposición del artículo 2.2.17.2.1.1. del Decreto 1078 de 2015 (DUR-TIC), los servicios ciudadanos digitales se clasifican en servicios base y servicios especiales:

1. **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 habilitación dada por el MinTIC y conforme con la autorización dada por el titular de los datos y de la integración a los servicios ciudadanos digitales base, bajo un esquema coordinado por la Agencia Nacional Digital en su rol de Articulador.

2. **Servicios ciudadanos base**: Son servicios que se consideran fundamentales para brindarle al Estado las capacidades en su transformación digital. Estos son, interoperabilidad, autenticación digital y carpeta ciudadana digital.

    2.1 **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.

    2.2 **Servicio de autenticación digital**: Es el procedimiento que, utilizando mecanismos de autenticación digital, permite verificar los atributos digitales de una persona cuando adelante 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 prejuicio de la autenticación notarial.

    2.3 **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 señaladas en el artículo 2.2.17.1.2 del Decreto 1078 de 2015 (DUR-TIC). Adicionalmente, este servicio podrá entregar las comunicaciones o alertas que las entidades señaladas tienen para los Usuarios, previa autorización de estos.

El modelo de los servicios ciudadanos digitales considera seis (6) actores: 1) Usuarios de los servicios ciudadanos digitales; 2) Articulador; 3) Prestadores de servicios ciudadanos digitales especiales; 4) Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC; y, 5) 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 servicios ciudadanos digitales especiales.

6 Requisitos

6.1 Requisitos Jurídicos

Los requisitos de capacidad jurídica para ser habilitado como Prestador de Servicios Ciudadanos Digitales Especiales son los siguientes:

1. Encontrarse inscrito en el registro mercantil como persona jurídica.

    1.1. Cuando el Solicitante pretenda prestar el servicio ciudadano digital especial soportado en un servicio digital base prestado por un tercero, deberá aportar el documento contractual que acredita la relación entre estos.
    1.2. El tercero deberá encontrarse inscrito en el registro mercantil como persona jurídica.

De conformidad con el artículo 15 del Decreto Ley 19 de 2012, el MinTIC consultará en el registro público correspondiente los certificados de existencia y representación legal de las personas jurídicas de derecho privado.

2. El representante legal del Solicitante deberá acreditar la capacidad para actuar.

3. Certificar una experiencia mínima de un (1) año relacionada con la prestación de servicios que soportan el modelo de servicios ciudadanos digitales, tales como, autenticación digital, diseño y desarrollo de sistemas de información, construcción de servicios de intercambio de información, e interoperabilidad. En caso de que la experiencia acreditada consista en contratos suscritos en aplicación del régimen general de la contratación pública, el MinTIC verificará la información aportada en la certificación mediante consulta en el registro único de proponentes (RUP) y/o en el sistema electrónico de contratación pública (SECOP). En los casos en que el solicitante se encuentre vinculado al servicio de interoperabilidad, el MinTIC revisará la información de manera oficiosa.

    En otros eventos exceptuados del régimen general de la contratación pública, se aportará documentos que acrediten la experiencia, indicando como mínimo, el tipo de contrato de donde proviene la experiencia, las partes del contrato, fecha de ejecución y finalización, y obligaciones a cargo del contratista.

4. El representante legal del solicitante deberá manifestar bajo gravedad de juramento que no ha sido objeto de sanciones por parte de la Superintendencia de la Industria y Comercio por vulnerar el régimen de protección de datos

personales, dentro de los dos (2) años anteriores a la presentación de la solicitud de habilitación.

6.2 Requisitos Administrativos

Los requisitos de capacidad administrativa para ser habilitado como Prestador de Servicios Ciudadanos Digitales Especiales, son los siguientes:

1. Aportar una certificación bajo la norma NTC-ISO/IEC 27001 y su extensión NTC-ISO/IEC 27701, otorgada al solicitante, con alcance a los procesos asociados al modelo de negocio de los servicios ciudadanos digitales objeto de su solicitud. Si para la fecha de presentación de la solicitud, no se cuenta con esta certificación, deberá manifestarse el compromiso de aportarla a más tardar dentro de los dos (2) años siguientes a la fecha de notificación de la habilitación como Prestador de Servicios Ciudadanos Digitales Especiales, término dentro del cual deberá allegarse al MinTIC la certificación correspondiente, como requisito necesario para operar.
2. Contar con personal adecuado para la prestación de los servicios ciudadanos digitales especiales, en cada uno de los equipos que conforman los cuatro (4) frentes de trabajo, según se describe a continuación:

2.1. **Equipo de centro de procesamiento de datos**: Responsable de la administración de los recursos de procesamiento de información y salvaguardar todos los temas relacionados con la continuidad de la infraestructura tecnológica para prestar los servicios ciudadanos digitales. El número de miembros que conformen el equipo será proporcional al servicio que se pretenda prestar, al menos un miembro del equipo debe contar un (1) año de experiencia certificada como administrador de centros de procesamiento de datos y contar con una certificación CISCO CCNA DATA CENTER o una certificación AUDITOR LÍDER ISO/IEC 22301. En los casos que se usen esquemas en la nube para el centro de procesamiento, se deben entregar la certificación y experiencia equivalente que otorga el proveedor del servicio (Por ejemplo: Certificaciones como AWS Certified DevOps Engineer y AWS Certified Advanced Networking — Specialty entre otras si el proveedor del servicio fuese Amazon Web Service).

2.2. **Equipo de monitoreo de red**: Responsable de administrar, monitorear y corregir los sistemas de redes de comunicaciones. Por lo tanto, debe garantizar la seguridad física, circuitos de cámara, acceso a red y servicios de comunicación mediante la red establecida. El número de miembros que conformen el equipo será proporcional al servicio que se pretenda prestar, al menos un miembro del equipo debe contar con un (1) año de experiencia

certificada en cargos de monitoreo de redes y contar con una certificación de centros de datos (en inglés, DATA CENTER FACILITIES OPERATIONS CERTIFICATION).

2.3. **Equipo de soporte**: Responsable de gestionar de principio a fin el canal de reporte y atención de cualquier incidente, mantenimiento evolutivo, novedad, peticiones, quejas o reclamos frente a los Usuarios. Por lo tanto, debe garantizar los Acuerdos de Nivel de Servicio con los Usuarios, atender los incidentes y gestionar las novedades. El número de miembros que conformen el equipo será proporcional al servicio que se pretenda prestar, al menos un miembro del equipo debe contar con un (1) año de experiencia certificada en cargos de gestión de mesas de ayuda y contar con mínimo una (1) certificación de LÍDER ESTRATÉGICO DE ITIL V4 o AUDITOR LÍDER ISO/IEC 20000-1.

2.4. **Equipo de seguridad**: Responsable del monitoreo, seguimiento, mitigación de riesgo de duplicidad o filtración de la información, propuestas de planes de acción relacionados con la identificación de amenazas de seguridad informática y de la información. Debe contar con:

2.4.1. **Oficial de seguridad de la información**: Un (1) miembro del equipo debe contar con un (1) año de experiencia certificada en ciberseguridad, ciberdefensa, seguridad de la información o seguridad informática. Deberá contar con una de las siguientes certificaciones: (i) certificación AUDITOR LÍDER ISO/IEC 27001; (ii) certificación PROFESIONAL DE CIBERSEGURIDAD (CSX-P); (iii) certificación profesional certificado en seguridad de sistemas de información (CISSP por sus siglas en inglés) del Consorcio Internacional de Certificación de Seguridad de Sistemas de Información también llamado (ISC)²; (iv) certificación auditor de sistemas de información certificado (CISA); y, (v) certificación de Control de Sistemas de Información y Riesgos (CRISC).

2.4.2. **Oficial de protección de datos personales**: Un (1) miembro del equipo deberá contar con experiencia certificada en protección de datos personales y al menos una de las siguientes certificaciones: i) AUDITOR LÍDER ISO/IEC 27001; ii) GERENTE DE SEGURIDAD DE LA INFORMACIÓN (en inglés, Certified Information Security Manager – ISACA); iii) AUDITOR DE SISTEMAS DE INFORMACIÓN (en inglés, Certified Information Systems Auditor – ISACA); o, iv) SOLUCIONES DE PRIVACIDAD DE DATOS (en inglés, Certified Data Privacy Solutions – ISACA).

A efectos de presentar el personal de que trata el presente numeral, es necesario adjuntar: (i) hojas de vida del personal que integrará cada uno de los equipos; (ii) certificaciones de experiencia profesional que deberán contener como mínimo, la labor desarrollada y el tiempo durante el cual se ejecutó la labor; (iii) tabla con la relación de roles que las hojas de vida presentadas desempeñan en la prestación

de servicios ciudadanos digitales especiales o base; (iv) certificación que el equipo se encuentra contratado, o en su defecto, certificar las ofertas vinculantes para contratar el equipo una vez inicie la prestación del servicio.

La experiencia acreditada en labores destinadas a los servicios ciudadanos digitales o afines debe ser mínimo de seis (6) meses que podrá ser acreditada por el Solicitante.

A su vez, debe acreditar el tipo de relación contractual existente entre el solicitante y el personal o equipo de trabajo que estará a cargo de la prestación de servicios ciudadanos digitales.

3. Aportar los certificados pertinentes que den cuenta de la gestión de control de lavado de activos y financiación del terrorismo - SARLAFT, del sistema de administración del riesgo operativo - SARO y del sistema de control interno - SCI. Lo anterior se acreditará aportando una certificación firmada por el representante legal del Prestador de Servicios Ciudadanos Digitales Especiales, que indique su cumplimiento y la descripción del sistema o procedimiento implementado.

3.1. Sistema de Administración de Riesgo Operativo – SARO

El sistema tiene como objetivo mitigar la posibilidad de incurrir en pérdidas debido a fallas de carácter operativo a causa del recurso humano, la tecnología, la infraestructura y su interacción con los procesos o a causa de sucesos externos. Su implementación debe estar acorde con el número proyectado de Usuarios y transacciones para poder medir y controlar los posibles riesgos operativos a los que está expuesto el sistema. Es necesario que se incluya el manual de riesgo operativo que contenga las políticas y procedimientos.

Debe ser implementado acorde al número de Usuarios y transacciones proyectadas para los primeros tres (3) años, deben presentar un manual de riesgo operativo que incluya:

- Políticas.
- Procedimientos.
- Documentación.
- Estructura administrativa.
- Registro de eventos de riesgo operativo.
- Órganos de control sobre el sistema.
- Políticas de divulgación de información.
- Programa de capacitación.
- Plan de continuidad del negocio.

- Cubrimiento del sistema a los terceros en los que se apoye para prestar uno o alguno de los servicios.
- Metodología establecida para identificar: (i) los riesgos y hacer su medición; (ii) las matrices de riesgo inherente y riesgo residual; y (iii) los indicadores de riesgo operacional.

3.2. Sistema de Control Interno

Se refiere al conjunto de políticas, normas y procedimientos que tienen como finalidad reducir los posibles riesgos que afecten al Prestador de Servicios Ciudadanos Digitales Especiales a través de ambientes controlados, evaluación de riesgos y actividades de supervisión. Su implementación debe estar acorde con el número proyectado de Usuarios y transacciones para poder medir y controlar los posibles riesgos operativos a los que está expuesto el sistema.

El Prestador de Servicios Ciudadanos Digitales Especiales deberá contar con un sistema de control interno (SCI) que le permita cumplir con los objetivos operativos, de reporte y de cumplimiento que se describen a continuación:

- Objetivos Operativos: se refiere a la eficacia y eficiencia en los procesos relacionados con la prestación del servicio ciudadano digital especial y el servicio ciudadano digital base.
- Objetivos de información o de reporte: apuntan a que la información generada por el Prestador de Servicios Ciudadanos Digitales Especiales a nivel de sus grupos de interés sea oportuna y transparente.
- Objetivos de cumplimiento: se refiere a la observancia y acatamiento de los lineamientos de esta guía, así como de todas las normas relacionadas con la prestación del servicio ciudadano digital especial para el cual haya sido habilitado.

El Sistema de Control Interno (SCI) debe responder tanto a la estructura del Prestador de Servicios Ciudadanos Digitales Especiales como al monto de los usuarios/transacciones que éste planee tener dentro de los tres (3) primeros años de actividad. Para lo anterior, deberá contar con un manual en el cual se desarrollen todos los aspectos aquí establecidos a saber:

- Principios: son principios generales de un SCI
  i. Autocontrol
  ii. Autorregulación
  iii. Autogestión
  iv. Responsabilidad
- Elementos del SCI
  ii. Ambiente de control

iii. Valoración y gestión de riesgos
iv. Actividades de control
v. Información y Comunicación
vi. Actividades de monitoreo

- Roles y responsabilidades dentro del SCI: deben establecerse roles y responsabilidades al interior del Prestador del Servicio Ciudadano Digital Especial relacionados con el SCI en al menos los siguientes órganos.
  i. Junta directiva u órgano equivalente
  ii. Representante Legal
  iii. Revisor Fiscal (Si le aplica)

4. Estar inscrito en el registro único tributario - RUT y contar con número de identificación tributaria - NIT y anexarlo.

6.3 Requisitos Financieros

Los requisitos de capacidad financiera para ser habilitado como Prestador de Servicios Ciudadanos Digitales Especiales, son los siguientes:

1. Presentar los estados financieros (balance, estado de resultados y flujo de efectivo) del año fiscal inmediatamente anterior al de la solicitud, debidamente suscritos por el revisor fiscal, auditor, contador o por quien corresponda.

   Conforme con el artículo 122 del Decreto 2649 de 1993, se podrán consolidar estados financieros con diferente fecha, en los casos que allí se prevean.

2. Presentar certificación expedida por el revisor fiscal, auditor o contador, conforme a la naturaleza jurídica de la sociedad, donde se acredite que el interesado cuenta con un índice de liquidez igual o superior a 1.5 (uno punto cinco), un nivel de endeudamiento igual o menor a 0.50 (cero punto cincuenta) y una relación de capital de trabajo igual o mayor a 1, conforme a las siguientes fórmulas, respectivamente:

$$índice\ de\ liquidez = \frac{Activos\ corrientes}{Pasivos\ Corrientes}$$

$$Capital\ de\ trabajo = \frac{(Activos\ corrientes - Pasivos\ Corrientes)}{Presupuesto\ de\ la\ propuesta}$$

$$índice\ de\ endeudamiento = \frac{Pasivos\ totales}{Activos\ totales}$$

3. Presentar certificación suscrita por el representante legal del Solicitante mediante la cual asegure que cuenta con los medios necesarios para mantener estos indicadores por el tiempo que dure la habilitación.

6.4 Requisitos técnicos

Esta sección tiene como objetivo definir los requisitos técnicos generales y específicos que las personas jurídicas de derecho privado deben cumplir ante el MinTIC para habilitarse como Prestadores de Servicios Ciudadanos Digitales Especiales.

A continuación, se abordan: 1) Condiciones generales, dentro de los cuales se encuentran el marco de referencia, los niveles de la categorización que tendrá el Prestador de Servicios Ciudadanos Digitales Especiales para los servicios ciudadanos digitales y los requerimientos funcionales y no funcionales. Luego, siguiendo el marco, se abordan, 2) los requisitos técnicos específicos para los servicios ciudadanos digitales de autenticación digital, carpeta ciudadana digital, y los servicios ciudadanos digitales especiales.

6.4.1 Condiciones generales

6.4.1.1 Marco de referencia

En consideración a la normativa sobre gobierno digital, protección de datos personales, seguridad y privacidad de la información, así como los lineamientos establecidos por el Gobierno Nacional a través de MinTIC para la articulación de los servicios ciudadanos digitales y las buenas prácticas internacionales, se establece un marco de referencia de los requerimientos técnicos específicos y la identificación de condiciones técnicas de habilitación.

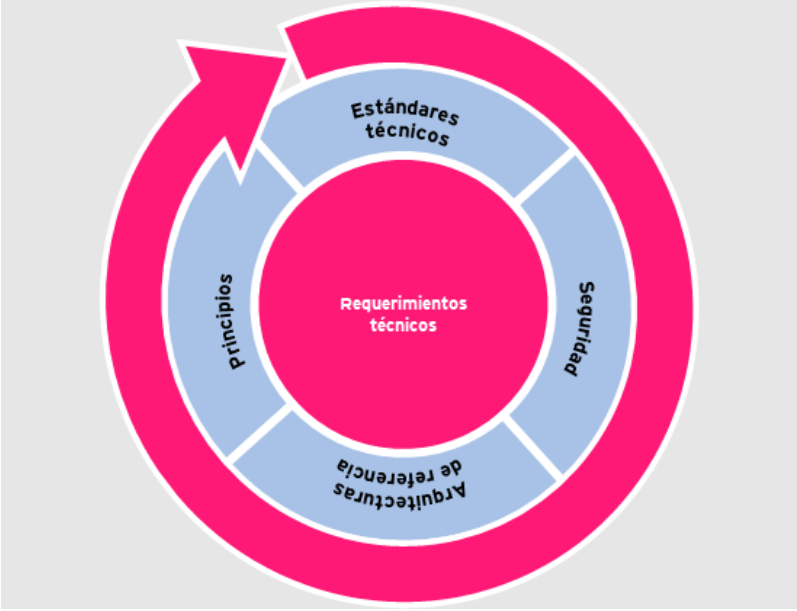
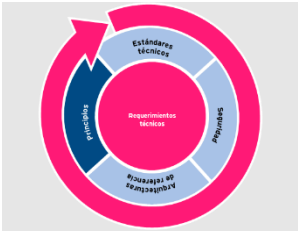
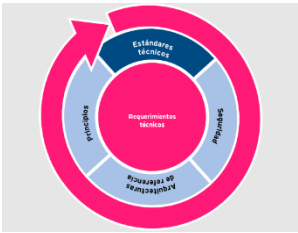


Ilustración 2. Marco de referencia requerimientos técnicos servicios ciudadanos digitales. (Fuente: Insumos técnicos, jurídicos, administrativos y financieros para la reglamentación de la operación de los servicios ciudadanos digitales base y especiales prestados por personas jurídicas de derecho privado, ERNST & YOUNG S A S., junio de 2021, página 6)

A continuación, se describe cada una de las dimensiones con las diferentes capacidades asociadas a este marco de referencia:

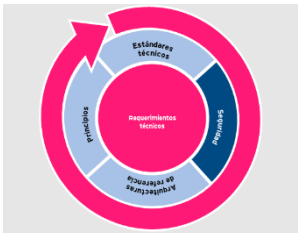


Principios: Definición e identificación de principios rectores de los servicios ciudadanos digitales tomados como base para establecer los requerimientos técnicos habilitantes basados en la información presentada en el Decreto 1078 de 2015 (DUR-TIC), enfocándolo a la prestación de los servicios por parte de personas jurídicas de derecho privado.



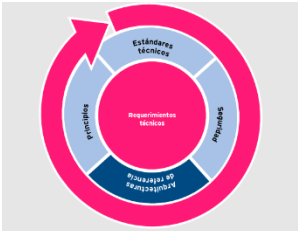
Estándares técnicos: Adecuación y definición de requerimientos técnicos mínimos para la interacción entre entidades gubernamentales y personas jurídicas de derecho privado prestadoras de servicios ciudadanos digitales especiales, enfocado en la articulación con la Agencia Nacional Digital. Definición dada desde los aspectos de:

- Software.
- Hardware.
- Conectividad.
- Protocolos.
- Herramientas.



Seguridad: Establecimiento de lineamientos de seguridad informática y de la información desde los ámbitos de:

- Seguridad informática y de la información.
- Alineación NTC-ISO/IEC 27001 y su extensión NTC-ISO/IEC 27701 vigente, y otros estándares internacionales.
- Alineación con el régimen de protección de datos personales.



Arquitectura de referencia: Definición y articulación de los componentes lógicos de arquitectura de referencia de los servicios ciudadanos digitales.

Teniendo en cuenta el marco de referencia presentado, se identifican los requerimientos no funcionales transversales al funcionamiento global de los

servicios ciudadanos digitales especiales, su habilitación y las particularidades de cada servicio.

6.4.1.2 Niveles de categorización para los servicios ciudadanos digitales especiales

Para efectos de los requisitos técnicos los interesados en habilitarse como Prestadores de Servicios Ciudadanos Digitales Especiales deberán cumplir con criterios de funcionalidad, transaccionalidad y confidencialidad, los cuales se clasifican de la siguiente manera:

6.4.1.2.1 Funcionalidad

Corresponde a la robustez de las funcionalidades presentadas, considerando el impacto dado a los servicios existentes y/o a la continuidad de los servicios ciudadanos digitales especiales prestados, para lo cual se identifica:

- **Nivel alto**: Innovación que impacta los servicios ciudadanos digitales especiales desde su proceso o funcionalidad y/o nuevo servicio de alto impacto funcional según las características identificadas en la justificación del formato de solicitud de habilitación para la prestación de servicios ciudadanos digitales especiales.
- **Nivel Medio**: Nuevo servicio de moderado impacto funcional según las características identificadas en la justificación del formato de solicitud de habilitación para la prestación de servicios ciudadanos digitales especiales.
- **Nivel Bajo**: Nuevo servicio de bajo impacto funcional según las características identificadas en la justificación del formato de solicitud de habilitación para la prestación de servicios ciudadanos digitales especiales.

6.4.1.2.2 Nivel Transaccional

Identificación de los flujos transaccionales y/o volumetrías de procesamiento, relacionadas al uso de los servicios ciudadanos digitales especiales.

- **Nivel alto**: Transaccionalidad superior al millón de registro de conformidad con el atributo de calidad establecido en la tabla 11 del numeral 11.1 Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020.
- **Nivel Medio**: Transaccionalidad superior a cien mil registros e inferior a un millón de registros de conformidad con el atributo de calidad establecido en

la tabla 11 del numeral 11.1 del Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020.

- **Nivel Bajo**: Transaccionalidad inferior o igual a cien mil de conformidad con el atributo de calidad establecido en la tabla 11 del numeral 11.1 Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020.

6.4.1.2.3 Confidencialidad

Nivel de acceso a información sensible o privada de los Usuarios para usos transaccionales o de almacenamiento producto del objeto de los servicios ciudadanos digitales especiales.

- **Nivel alto**: Consumo de datos sensibles y privados para procesamiento analítico de información.
- **Nivel Medio**: Consumo de datos sensibles y privados para transaccionalidad relacionada con los servicios ciudadanos digitales especiales.
- **Nivel Bajo**: No se realiza consumo de datos sensibles o privados para el funcionamiento de los servicios ciudadanos digitales especiales.

Para determinar los requisitos que debe cumplir en los servicios ofertados, se debe tener en cuenta que estos corresponden al nivel más alto alcanzado en las tres (3) categorías antes señaladas.

6.4.1.3Requerimientos funcionales de los servicios ciudadanos digitales

Los requerimientos funcionales son las descripciones de comportamiento que debe tener una solución de software y qué información maneja. Se establecen como declaraciones de intercambio de información del sistema con entradas externas ya sean Usuarios o respuestas automáticas, procesos predefinidos, entre otros. Estos requerimientos están definidos en el Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 del 2020, los cuales deben ser implementados por las personas jurídicas de derecho privado para la prestación de los servicios ciudadanos digitales especiales.

6.4.1.4 Requerimientos no funcionales de los servicios ciudadanos digitales especiales

Los requerimientos no funcionales son aquellos que especifican criterios que pueden ser usados para calificar la calidad en la operación del sistema. A diferencia de los requerimientos funcionales, estos no buscan calificar comportamientos

específicos. Los requerimientos no funcionales que deben cumplir los Prestadores de Servicios Ciudadanos Digitales Especiales se encuentran señalados en el Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 del 2020. Estos requerimientos deben presentarse a la Agencia Nacional Digital en su rol de Articulador, al momento de iniciar la prestación de los servicios.

6.4.2 Requerimientos específicos

6.4.2.1Requisitos de Centros

6.4.2.1.1 Centro de Procesamiento de Datos

El centro de procesamiento de datos se encarga de hospedar los recursos de procesamiento de información que soportan los procesos y servicios obtenidos. A continuación, se listan los estándares y características que deben cumplir dichos centros:

			SCD Especial		
Requisito	**Autenticación**	**Carpeta**	**Alto**	**Medio**	**Bajo**
Estar certificado bajo el estándar internacional ANSI/TIA-942	Aplica	Aplica	Aplica	Aplica	Aplica
Estar certificado bajo la clasificación mínima de TIER	TIER III	TIER III	TIER III	TIER II	TIER I
Contar con una disponibilidad mínima	99.982%	99.982%	99.982%	99.741%	95.00 %
Cumplir con estándares de protección de datos personales de la Superintendencia de Industria y Comercio si están en esquemas de nube pública, privada o híbrida.	Aplica	Aplica	Aplica	Aplica	Aplica

Este centro puede operar bajo el esquema de nube (privada, pública, hibrida). Puede ser propiedad del Prestador de Servicios Ciudadanos Digitales Especiales o de terceros. En todo caso, se deberá certificar por el representante legal del Prestador de Servicios Ciudadanos Digitales Especiales que cumple con las características especificadas en este anexo técnico y aportará los contratos suscritos con terceros, de ser el caso. El Prestador de Servicios Ciudadanos

Digitales Especiales deberá garantizar que los terceros que presten el servicio de nube cumpla con las características especificadas en este anexo técnico.

En todo caso, el Prestador de Servicios Ciudadanos Digitales Especiales deberá demostrar que controla y gobierna los procesos operados por terceros.

6.4.2.1.2 Centro de Monitoreo de Red

El centro de monitoreo de red se encarga de administrar, monitorear y corregir los sistemas de redes de telecomunicaciones y es responsable de monitorear los factores que pueden impactar el rendimiento.

Este centro puede ser operado por el Prestador de Servicios Ciudadanos Digitales Especiales o por terceros. En todo caso, se deberá certificar por el representante legal del Prestador de Servicios Ciudadanos Digitales Especiales que cumple con las características especificadas en este anexo técnico y aportará los contratos suscritos con terceros, de ser el caso. El Prestador de Servicios Ciudadanos Digitales Especiales deberá garantizar que los terceros que presten el servicio de centro de monitoreo de red cumplan con las características especificadas en este anexo técnico.

En todo caso, el Prestador de Servicios Ciudadanos Digitales Especiales deberá demostrar que controla y gobierna los procesos operados por terceros.

A continuación, se listan las características físicas y técnicas que debe cumplir el centro de monitoreo de red:

- El Prestador de Servicios Ciudadanos Digitales Especiales debe disponer de la capacidad de administración por el número de días a la semana por el número de horas al día que corresponda al servicio para manejar las operaciones del centro de monitoreo de red que permita garantizar los Acuerdos de Nivel de Servicio y el tiempo de atención estipulado para los servicios.

			SCD Especial		
Requisito	**Autenticación**	**Carpeta**	**Alto**	**Medio**	**Bajo**
Operación del centro en número de días a la semana por número de horas al día, según el nivel del servicio a prestar.	7 días x 24 horas	7 días x 24 horas	7 días x 24 horas	6 días x 16 horas	5 días x 8 horas
Construcción o refuerzo sismorresistente.	Aplica	Aplica	Aplica	Aplica	Aplica

Seguridad de acceso con guardia los siete (7) días a la semana por veinticuatro (24) horas al día.	Aplica	Aplica	Aplica	Aplica	Aplica
Detección inteligente de incendios.	Aplica	Aplica	Aplica	Aplica	Aplica
Seguridad física certificada que indique la existencia de los mecanismos adecuados que llevan a disminuir las probabilidades que ocurran eventos que atenten contra los datos que el Prestador de Servicios Ciudadanos Digitales Especiales utiliza en la prestación de los Servicios Ciudadanos especiales.	Aplica	Aplica	Aplica	Aplica	No aplica
Circuito cerrado de televisión digital.	Aplica	Aplica	Aplica	Aplica	Aplica
Acceso de visitantes con cita previa y control de listas de acceso.	Aplica	Aplica	Aplica	Aplica	Aplica
Operación, centro de atención a clientes y monitoreo en número de días a la semana por número de horas al día según el nivel	7 días x 24 horas	7 días x 24 horas	7 días x 24 horas	6 días x 16 horas	5 días x 8 horas
Sistemas de alimentación ininterrumpida de energía configurados en redundancia.	Aplica	Aplica	Aplica	Aplica	No aplica
Autonomía eléctrica de mínimo de número de horas en caso de interrupción del fluido eléctrico.	24 horas	24 horas	24 horas	12 horas	No aplica
Control ambiental: sistemas de aire acondicionado redundantes.	Aplica	Aplica	Aplica	Aplica	No aplica
Alimentación segura a los sistemas de control ambiental.	Aplica	Aplica	Aplica	Aplica	No aplica
Herramientas de monitoreo para la infraestructura de los diversos fabricantes utilizados.	Aplica	Aplica	Aplica	Aplica	Aplica

6.4.2.1.3 Centro de soporte:

El centro de soporte es el conjunto de canales y mecanismos que se habilitan para que el Usuario reporte cualquier tipo de malfuncionamiento, solicitud, queja o petición además de generar el tiquete y tratar cada incidente en un plazo que varía

según la prioridad del tiquete asignado, manteniendo los registros necesarios desde la creación hasta la culminación del tiquete. A continuación, se presentan las características con las que debe contar dicho centro:

- El Prestador de Servicios Ciudadanos Digitales Especiales tiene que disponer canales de atención (como centro de llamadas, asistentes digitales -callbot, chatbot- o cualquier otro tipo de medio) como punto único de contacto con los diferentes tipos de Usuarios de los servicios ciudadanos digitales que permita, si se presenta alguna interrupción, incidente o alteración en el funcionamiento de los servicios ofrecidos, brindar asesoría y acompañamiento, de igual forma que permita garantizar los Acuerdos de Nivel de Servicio y el tiempo de atención estipulado para los servicios.

		SCD Especial		
Requisito	**Carpeta**	**Alto**	**Medio**	**Bajo**
Operación del centro en número de días a la semana por número de horas al día.	7 días x 24 horas	7 días x 24 horas	6 días x 16 horas	5 días x 8 horas
Estar diseñada bajo prácticas reconocidas como ITIL v4, NTC-ISO/IEC 20000-1 vigente.	Aplica	Aplica	Aplica	Aplica
Deben existir ANS en los cuales se consignan los tiempos que tomara resolver una solicitud de cierto tipo.	Aplica	Aplica	Aplica	Aplica
Debe existir documentación asociada a los Acuerdos de Nivel de Servicio.	Aplica	Aplica	Aplica	Aplica
Recibir y clasificar las peticiones por orden prioritario en tres niveles: alto, medio y bajo dependiendo de la urgencia y el impacto identificado. - Prioridad Alta. Emergencia, tiempo máximo de solución 4 horas: Fallas en la infraestructura atribuibles al Articulador y problemas operacionales de los servicios (Red, virtualización y configuración) entregados por el Articulador y que generen una indisponibilidad critica del negocio de la Entidad. - Prioridad Media. Degradación del servicio, tiempo máximo de solución 24 horas: Fallas en la infraestructura y problemas operacionales de los servicios atribuibles al Articulador (Red, virtualización y configuración) entregados por el Articulador, que afectan el desempeño o confiabilidad de los procesos de negocio de la Entidad.	Aplica	Aplica	Aplica	Aplica

Solicitudes de asesoramiento para la configuración, implementación y administración de servicios. - Prioridad Baja. Solicitudes, tiempo máximo de solución 48 horas: Solicitudes de soporte menores o de información que no tienen impacto en los procesos de negocio de la Entidad, solicitud de información técnica de los servicios, solicitudes de documentación de servicios, solicitudes de información y aclaraciones acerca del uso y operación de los servicios.				
Los incidentes atendidos por el centro de soporte deben quedar documentados de modo que se evidencie su registro, priorización, clasificación, escalamiento, respuesta y finalización.	Aplica	Aplica	Aplica	Aplica
Los incidentes de mayor impacto deben ser tramitados e informados de modo que permitan la mejora del sistema.	Aplica	Aplica	Aplica	Aplica
Los incidentes deberán contar con un estado que permita determinar en qué punto del proceso de soporte está.	Aplica	Aplica	Aplica	Aplica
Debe alimentar una base de conocimiento en la cual se documentan los incidentes previamente identificados con sus soluciones identificadas.	Aplica	Aplica	Aplica	Aplica

6.4.2.1.4 Centro de Operaciones de Seguridad:

El despliegue del centro de operaciones de seguridad se debe implementar en función de los niveles de volumetría, robustez de las organizaciones y nivel de madurez de los servicios ciudadanos digitales especiales que el Prestador de Servicios Ciudadanos Digitales Especiales desea brindar.

Este centro puede ser operado por el Prestador de Servicios Ciudadanos Digitales Especiales o por terceros. En todo caso, se deberá certificar por el representante legal del Prestador de Servicios Ciudadanos Digitales Especiales que cumple con las características especificadas en este anexo técnico y aportará los contratos suscritos con terceros, de ser el caso. El Prestador de Servicios Ciudadanos Digitales Especiales deberá garantizar que los terceros que presten el servicio de centro de operaciones de seguridad cumplan con las características especificadas en este anexo técnico.

En todo caso, el Prestador de Servicios Ciudadanos Digitales Especiales deberá demostrar que controla y gobierna los procesos operados por terceros.

El centro de operaciones de seguridad está compuesto por un grupo de especialistas en ciberseguridad que se encargan del monitoreo del sistema, el seguimiento, la instauración de alertas, la respuesta a ataques informáticos además de la detección de posibles amenazas que puedan afectar el funcionamiento del sistema, entre otros.

El centro de operaciones de seguridad permite mitigar los riesgos de los ataques informáticos y favorece la alta disponibilidad. A continuación, se listan las características que debe cumplir:

			SCD Especial		
Requisito	**Autenticación**	**Carpeta**	**Alto**	**Medio**	**Bajo**
Operación del centro en número de días a la semana por número de horas al día	7 días x 24 horas	7 días x 24 horas	7 días x 24 horas	6 días x 16 horas	No aplica
Incluir análisis del comportamiento del usuario.	Aplica	Aplica	Aplica	Aplica	No aplica
Tratamiento de eventos estratégico basado en las características propias de cada situación.	Aplica	Aplica	Aplica	Aplica	No aplica
Tratar, prevenir, analizar y proteger ante amenazas informáticas.	Aplica	Aplica	Aplica	Aplica	No aplica

6.4.2.2Requerimientos técnicos para el prestador del servicio de autenticación digital

La autenticación digital tiene como objetivo validar los Usuarios de los servicios ciudadanos digitales a partir de los atributos digitales y proveer los procedimientos y mecanismos necesarios para garantizar la identidad de los Usuarios. Este conjunto de mecanismos de autenticación permite a los Usuarios acceder sin temor a que sus datos sean vulnerados por Usuarios no autorizadas y reduce al máximo la posibilidad de suplantación a través de este servicio, fomentando la confianza de los servicios en línea del país y ampliando su interacción, no solo con el Estado sino con organizaciones privadas con garantías de confianza y seguridad. A raíz de esto,

los Usuarios cuentan con una plataforma que, basada en la interoperabilidad, permite brindar admisibilidad y fuerza probatoria a los mensajes de datos ampliando la cantidad de servicios que se pueden realizar a través de los servicios ciudadanos digitales.

6.4.2.2.1 Principios rectores

El marco de desarrollo y construcción de enlaces entre sector público y privado debe estar desarrollado bajo determinados principios que garanticen, entre otros, la interoperabilidad y accesibilidad. Además de los siguientes, deberá aplicarse aquellos señalados en el artículo 2.2.17.1.6 del Decreto 1078 de 2015 (DUR-TIC), así como los principios para el tratamiento de datos personales consagrados en el artículo 4 de la Ley 1581 de 2012:

- Validar la identidad digital de los Usuarios.
- Prevenir riesgos de suplantación de identidad.
- Garantizar la seguridad para los trámites digitales.
- Asegurar la autenticidad de las comunicaciones digitales.
- Prevenir alteraciones de la información.
- Garantizar la identidad del remitente de los mensajes de datos.
- Asegurar que no exista un filtrado de datos que exponga a los Usuarios.
- Cuantificar el riesgo de cada Trámite y asociarlo a un grado de confianza.
- Seleccionar y proporcionar una integración adecuada a la plataforma de autenticación.
- Permitir la realización de pruebas previas a la integración a la plataforma.
- Garantizar la alta disponibilidad de la prestación de servicios.
- Establecer los roles de las entidades y Usuarios para la autorización de trámites.
- Establecer independencia con las entidades y establecer las responsabilidades para la realización de trámites.
- Alinearse con los esquemas de interoperabilidad de la plataforma X-Road ofrecidos por el Estado articulados por la Agencia Nacional Digital.

6.4.2.2.2 Estándares técnicos

6.4.2.2.2.1 Componentes

El servicio de autenticación digital atenderá dos componentes principales: el registro de Usuarios y el uso de factores de autenticación. De igual manera, se toma en consideración el detalle de los requisitos de hardware, software, conectividad y seguridad:

6.4.2.2.2.1.1 Registro de Usuarios

De conformidad a lo consagrado en el artículo 54 de la Ley 1437 de 2011, toda persona tiene el derecho de actuar ante las autoridades utilizando medios electrónicos, caso en el cual deberá realizar sin ningún costo un registro previo como usuario ante la autoridad competente, motivo por el cual surge la necesidad de prestar los servicios de autentificación digital.

Con el objetivo de contar con unas condiciones de operación del servicio y en concordancia con lo estipulado en el Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020, se presentan a continuación las condiciones correspondientes a los Prestadores de Servicios Ciudadanos Digitales Especiales:

- La autenticación digital debe soportar el protocolo de identificación OpenID Connect en la versión que designa la Agencia Nacional Digital en su rol de Articulador, con el propósito de facilitar la integración de los sistemas de información propios de cada Prestador de Servicios Ciudadanos Digitales Especiales.
- Administrar los accesos de autenticación a la plataforma del Prestador de Servicios Ciudadanos Digitales Especiales. En caso de que se detecten accesos no autorizados, el Prestador de Servicios Ciudadanos Digitales Especiales deberá reportar la incidencia de seguridad al Grupo Interno de Trabajo de Servicios Ciudadanos Digitales en un plazo máximo de diez (10) días una vez ocurrido el incidente.
- Definir la criticidad de los niveles de riesgo a los que se exponen los Usuarios, de acuerdo con el trámite que realice cada uno y articularlos con la Agencia Nacional Digital con el fin de evitar los accesos no permitidos y en caso de ser necesario suspender la operación hasta que los riesgos sean mitigados.
- El Prestador de Servicios Ciudadanos Digitales Especiales debe contar con el personal adecuado para el desempeño de sus funciones y este debe estar capacitado en seguridad, privacidad y protección de datos personales. Para cumplir con este objetivo se deben abordar cuatro (4) frentes de trabajo a partir de los cuales se busca controlar el ecosistema del Prestador de los Servicios Ciudadanos Digitales Especiales como se detalla en los requisitos administrativos.

El Prestador de Servicios Ciudadanos Digitales Especiales debe contar con una estrategia de seguridad digital documentada, en la cual se incorporen los elementos

de valoración que se requieran para contar con garantías que cubran los costos asociados a ataques cibernéticos.

Por otra parte, el Prestador de Servicios Ciudadanos Digitales Especiales debe advertir al usuario de las políticas de tratamiento de datos respecto a las implicaciones, alcances, límites, deberes y responsabilidades del servicio según lo estipulado en el capítulo 25 del Decreto 1074 de 2015 y cualquier otra normativa vigente. Todo esto en concordancia de los términos y condiciones estipulados en el Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020, en donde se hace énfasis en la importancia de las medidas técnicas, humanas y administrativas para garantizar la seguridad de los datos, las condiciones de uso, los derechos y obligaciones de los Usuarios, además de todo lo relacionado con las condiciones y políticas de seguridad de la información y datos personales de acuerdo con la normativa vigente en el país.

Alineado con la normativa anterior, el Usuario tiene el derecho de desvincular en cualquier momento sus datos de la plataforma y decidir entre migrar a otro Prestador de Servicios Ciudadanos Digitales Especiales de autenticación digital (portabilidad del usuario), o por el contrario prescindir del uso del servicio. En caso de querer desvincularse por completo, los datos serán eliminados además de la revocación de las credenciales y autorizaciones otorgadas, esto trae consigo que no se tendrá acceso a dichos datos.

Portabilidad de usuario: El Prestador de Servicios Ciudadanos Digitales Especiales deberá facilitar la portabilidad de sus Usuarios a otro Prestador de Servicios Ciudadanos Digitales Especiales de libre escogencia, establecida en el numeral 4 del artículo 2.2.17.1.6. del Decreto 1078 de 2015.

En los casos de suspensión temporal o definitiva de la prestación del servicio ciudadano digital especial habilitado, el Prestador de Servicios Ciudadanos Digitales Especiales deberá contar con un proceso de migración de datos estandarizado hacia otros Prestadores de Servicios Ciudadanos Digitales Especiales o a la Agencia Nacional Digital con el objetivo de que los Usuarios puedan continuar usando los servicios ciudadanos digitales. Este proceso deberá contar, como mínimo, con los siguientes elementos:

- La disponibilidad de las interfaces necesarias para cumplir con la migración de información de Usuarios, contar con la conexión de OpenID Connect en la versión que designa la Agencia Nacional Digital en su rol de Articulador para realizar la integración entre Prestadores de Servicios Ciudadanos Digitales Especiales.

- Contar con interfaces de programación de aplicaciones y protocolos para comunicación entre plataformas. Enunciar los derechos y obligaciones de los Usuarios.
- Enunciar los derechos y obligaciones del Prestador de Servicios Ciudadanos Digitales Especiales migrados y migrantes.
- Los costos asociados a la migración de datos corresponden a los Prestadores de Servicios Ciudadanos Digitales Especiales.

Lo anterior, también aplica en caso de que el Prestador de Servicios Ciudadanos Digitales Especiales de autenticación digital decida terminar la prestación del servicio. Además, deberá proporcionar formas de acceder a los datos de auditoría y registros durante el siguiente año fiscal dado que esta información puede servir de medio de prueba en procesos administrativos y judiciales. Se reitera que todas las acciones o costos relacionados en la migración de datos corresponden a las entidades implicadas en dicha actividad y este proceso se realiza en caso tal que un Prestador de Servicios Ciudadanos Digitales Especiales quiera dejar de prestar el servicio de autenticación digital. Así, los Prestadores de Servicios Ciudadanos Digitales Especiales tienen la capacidad de realizar traslados de Usuarios y validación de credenciales de autenticación.

Cabe resaltar que los datos recolectados, producidos, almacenados y relacionados al servicio de autenticación digital únicamente podrán ser usados para los fines que fueron recolectados y la prestación de los servicios de autenticación digital será gratuita para los Usuarios.

Para que un Usuario pueda acceder a los servicios de autenticación digital es necesario que haga un proceso de registro previo ante el Prestador en donde se hace la verificación de la identidad del Usuario el cual puede ser presencial o digital. Respecto a dicha verificación, el Prestador debe corroborar los datos con la Registraduría Nacional del Estado Civil, además los resultados de este proceso deben ser almacenados con estampa cronológica. El Prestador tiene la capacidad de consultar en las bases de datos de entes públicos con el objetivo de obtener datos con previa autorización del dueño de la información, sin embargo, no puede almacenar dichos datos debido a lo dispuesto en la Resolución 2160 de 2020. Por lo tanto, los datos consultados deben ser eliminados apenas termine el proceso de consulta. Todo bajo la articulación de la Agencia Nacional Digital que actúa con el objetivo de velar por el cumplimiento de los derechos de los Usuarios.

Los trámites y servicios que requieran la autenticación del usuario se debe realizar a través del servicios ciudadano base de Autenticación Digital y atendiendo lo dispuesto en la resolución 2160 de 2020 y su Guía de lineamientos de los servicios

ciudadanos digitales capítulo 9 Modelo del Servicio de Autenticación Digital, donde la Agencia Nacional Digital en su rol de Articulador se encargará de redireccionar la solicitud al Prestador del servicio correspondiente al Usuario de modo que las credenciales obtenidas sean válidas para identificarse en los sistemas de información de cualquier entidad pública, para ello se usaran los mecanismos de Servicio Web y OpenID Connect.

La recolección de los datos se debe realizar únicamente con la autorización previa del usuario y sometiéndose a lo estipulado en el régimen de protección de datos personales. Los Prestadores de autenticación digital solo deben recolectar la información mínima necesaria para su funcionamiento. Dependiendo del nivel de confianza del Usuario se podrán almacenar una mayor cantidad de datos de ser necesario y acorde con el principio de privacidad por diseño. Esta constancia debe ser expresa, además los Usuarios tendrán acceso a sus datos personales y podrán actualizarlos y eliminarlos según lo previsto en el régimen de protección de datos personales.

En caso de tratarse de un menor de edad, la verificación se debe hacer con autorización de sus padres o tutor legal quienes deben acompañar al menor en el proceso. Al cumplir la mayoría de edad el menor debe actualizar los datos.

En caso de ser un extranjero, los datos de identificación se verificarán con las bases de datos de la entidad pertinente a Migración Colombia.

En caso de ser una persona jurídica, su representante legal debe haber realizado el proceso de registro como persona natural en el servicio de autenticación digital con anterioridad, la persona jurídica tendrá las siguientes opciones:

- Tras haber verificado que la persona natural está habilitada para ejercer el rol de representante legal, se establece como representante legal de la persona jurídica.
- Se verifican los datos de existencia y representación legal de la persona jurídica, posteriormente se procede a recolectar la información básica pertinente para finalmente generar las credenciales de acreditación de la persona jurídica.

El representante legal de la persona jurídica deberá tener la capacidad de asignar, cambiar y revocar los roles y capacidades de personas naturales respecto la organización en el servicio de autenticación. Como medida preventiva, los sistemas de información del Prestador deben contar con mecanismos que le permitan al representante legal de la persona jurídica o su apoderado, asignar o revocar roles y autorizaciones a cualquiera de sus colaboradores en el servicio de autenticación.

6.4.2.2.2.1.2 Factores de autenticación

Tomando como base el acápite 9.5.8 contenido en el Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” y el Anexo 2 “Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020, se establecen los requerimientos relacionados a la emisión de credenciales, los requisitos para Prestadores de Servicios Ciudadanos Digitales Especiales en torno a los factores de autenticación. A continuación, se describen los posibles factores de autenticación con los que cuenta el usuario:

- **Secreto memorizado:** Conjunto de números, letras y caracteres especiales establecidos por el Usuario para poder ingresar a la plataforma. Inicialmente el Prestador de Servicios Ciudadanos Digitales Especiales genera una contraseña de un solo uso para que el Usuario acceda y pueda establecer su contraseña propia.
- **Dispositivo de contraseña de un solo uso o de un solo factor:** Es un generador que contiene una contraseña (generalmente numérica) incrustada y que debe ser introducida manualmente por el Usuario como método de autenticación demostrando que el Usuario tiene en su poder el dispositivo.
- **Dispositivo multi factor:** Es la suma de dos o más factores de autenticación que puede por ejemplo estar instalado en dispositivos móviles para reforzar la seguridad, demostrando un factor de conocimiento o inherencia además del factor de posesión. Donde el primer factor es la generación de una contraseña en el dispositivo y el segundo factor hace referencia a un lector biométrico integral (como una huella digital).
- **Software criptográfico de un solo factor:** Se refiere a una clave criptográfica almacenada en un medio blando (como un disco) y su autenticación se basa en la demostración de posesión y control del dispositivo.
- **Dispositivo criptográfico de un solo factor:** Hardware que realiza operaciones criptográficas que utiliza claves protegidas y genera su autenticación a través de una conexión directa al punto final del usuario.
- **Software criptográfico multi factor:** Se refiere a una clave criptográfica almacenada en un medio blando (como un disco) y requiere de un segundo factor de autenticación (generalmente es un tipo de mensaje firmado).
- **Dispositivo criptográfico multi factor:** Hardware que realiza operaciones criptográficas que utiliza claves protegidas) y requiere de un segundo factor de autenticación (generalmente es un tipo de mensaje firmado).
- **Certificado digital:** Corresponde a un documento digital, en el que se identifica la información de una persona, junto con una llave privada y otra pública. Ese

documento, está almacenado en un dispositivo criptográfico certificado, al cual, solo el titular puede acceder. Se expide con el objeto de demostrar que una firma digital cuenta con los atributos jurídicos necesarios para tener el mismo valor probatorio y fuerza obligatoria de una firma manuscrita, esto es, la integridad de la información, autenticidad de la identidad del firmante y el no repudio de la transacción. Debe estar avalado por una entidad, o quien haga sus veces, de las que trata el cápitulo 48 del Decreto 1074 de 2015, o la norma que lo adicione, modifique o sustituya.

Los factores antes mencionados pueden ser complementados con nuevos mecanismos propuestos por los Prestadores siempre y cuando estos cumplan con los niveles descritos en la norma NIST SP 800-63B vigente emitida por el Instituto Nacional de Normas y Tecnología (en inglés, National Institute of Standards and Technology, NIST).

De acuerdo con el Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020 se identificaron cuatro (4) niveles de autenticación con el objetivo de brindar los lineamientos necesarios para establecer las garantías de seguridad que se deben tener de acuerdo con el nivel del riesgo que exista. A mayor riesgo es necesario contar con mayores factores de autenticación que garanticen que la información del usuario está protegida y solo tendrá acceso quien esté autorizado a tratar los datos.

Los (4) cuatro niveles de autenticación establecidos son bajo, medio, alto y muy alto. A continuación, se profundiza en cada uno de los niveles:

Nivel de autenticación bajo: El nivel bajo aplica cuando los riesgos asociados a la autenticación incorrecta son mínimos. Se requiere que el Usuario tenga como mínimo un factor de autenticación de los presentados a continuación:

- Secreto memorizado.
- Dispositivo de un solo factor de autenticación.

Nivel de autenticación medio: El nivel medio se usa cuando los riesgos asociados a la autenticación incorrecta son moderados. Se necesita que el Usuario tenga como mínimo un factor de autenticación de los presentados a continuación:

- Secreto memorizado.
- Dispositivo de un solo factor.
- Dispositivo multi factor.
- Software criptográfico de un solo factor.
- Dispositivo criptográfico de un solo factor.
- Software criptográfico multi factor.

- Dispositivo criptográfico multi factor.
- Certificado digital.

Nivel de autenticación alto: El nivel alto se usa cuando los riesgos asociados a la autenticación incorrecta son considerables. Se necesita que el Usuario tenga como mínimo dos factores de autenticación de los presentados a continuación:

- Dispositivo criptográfico multi factor.
- Dispositivo criptográfico de un solo factor + Secreto memorizado.
- Dispositivo multi factor + Dispositivo criptográfico de un solo factor.
- Dispositivo multi factor + Software criptográfico de un solo factor.
- Dispositivo de un solo factor + Software criptográfico multi factor.
- Dispositivo de un solo factor + Software criptográfico de un solo factor + Secreto memorizado.
- Certificado digital + Secreto memorizado.

Nivel de autenticación muy alto: El nivel muy alto se usa cuando los riesgos asociados a la autenticación incorrecta son muy elevados. Se necesita revisar la cédula de ciudadanía digital ante la Registraduría Nacional del Estado Civil y la biometría del Usuario además de ser complementado con algunos de los factores de autenticación de los presentados a continuación:

- Dispositivo criptográfico multi factor.
- Dispositivo criptográfico de un solo factor + Secreto memorizado.
- Dispositivo multi factor + Dispositivo criptográfico de un solo factor.
- Dispositivo multi factor + Software criptográfico de un solo factor.
- Dispositivo de un solo factor + Software criptográfico multi factor.
- Dispositivo de un solo factor + Software criptográfico de un solo factor + Secreto memorizado.
- Certificado digital + Secreto memorizado.

Los factores de autenticación antes mencionados como secretos memorizados, de un solo factor y de múltiple factor deben cumplir la norma técnica NIST SP 800-63B. El proveedor es quien inicialmente le asigna una clave temporal para acceder a los servicios ciudadanos digitales especiales y el Usuario la modifica cambiándola por un secreto memorizado.

Se puede complementar el proceso de autenticación con base en códigos de validación de un solo uso para confirmar que quien está ingresando a la sesión es quien debería y así se refuerzan los criterios de garantía y los controles para mitigar las amenazas externas.

Así mismo, los factores basados en certificados digitales deben cumplir con los requisitos definidos por la entidad encargada en Colombia según el cápitulo 48 del Decreto 1074 de 2015, el RFC 3647, la ITU X.1254 y en la ISO/IEC 29115 vigentes. Respecto a la firma digital, es necesario que se cumpla con el artículo 28 de la Ley 527 de 1999 y el Decreto 2364 de 2012. Se garantiza a través de la verificación para que sea intransferible y única la sesión por cada uno de los Usuarios, además de velar por la protección de los datos que existen dentro de los servicios ciudadanos digitales. Adicionalmente, existe como el XADES, PADES o CADES que cumplen con las normas anteriormente mencionadas y que estan acreditado por la entidad encargada en Colombia según el cápitulo 48 del Decreto 1074 de 2015.

Los trámites y servicios que requieran la Autenticación de la identidad del Usuario deben hacerlo a través del servicio de identificación digital en donde la Agencia Nacional Digital en su rol de Articulador se encargará de redireccionar la solicitud al Prestador del servicio del Usuario de modo que las credenciales obtenidas sean válidas para identificarse en los sistemas de información de cualquier entidad pública, para ello se usaran los mecanismos de Servicio Web y OpenID Connect.

Por otro lado, para las personas jurídicas el proceso de autenticación está a cargo del representante legal quien debe autenticarse previamente y validar la información para formar parte del ecosistema de servicios ciudadanos digitales especiales.

En cuanto a las bases de datos de Usuarios los Prestadores cuentan con bases de datos primarias las cuales almacenan los datos de identificación de sus Usuarios (tipo y número de identificación); estas últimas deben alimentar la Base de Datos Maestra que resguarda la Agencia Nacional Digital y que contiene los datos de identificación de los Usuarios y el código de identificación del Prestador del servicio (tipo, número de identificación y código del Prestador del servicio). Al acceder a los servicios de autenticación digital será necesario solicitarlo al Articulador el cual haciendo uso de la Base de Datos Maestra redirigirá la solicitud al Prestador que corresponda.

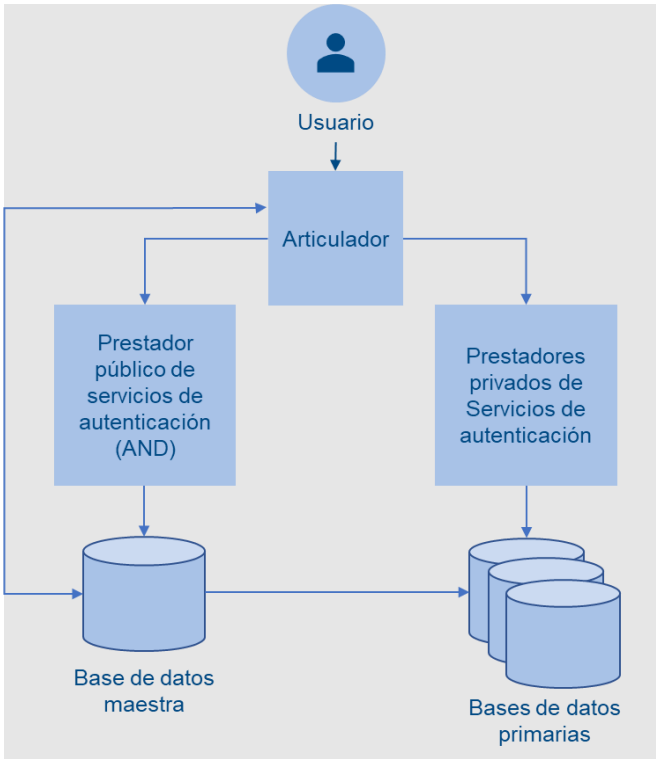


Ilustración 3. Modelo General de Articulación con la Agencia Nacional Digital.
(Fuente: Insumos técnicos, jurídicos, administrativos y financieros para la reglamentación de la operación de los servicios ciudadanos digitales base y especiales prestados por personas jurídicas de derecho privado, ERNST & YOUNG S A S., junio de 2021, página 34)

Alineado con la Ley de Protección de Datos Personales 1581 del 2012 y la Ley 1266 del 2008, el usuario tiene el derecho en cualquier momento a desvincular sus datos de la plataforma, por consiguiente, se revocan las credenciales y autorizaciones otorgadas y los Prestadores de Servicios Ciudadanos Digitales ya no tendrían acceso a dichos datos, en este caso el Usuario decidirá si quiere migrar a otro Prestador del servicio de autenticación o desistir del uso del servicio.

En caso de migración, la interacción entre Prestadores se debe realizar teniendo como base la información a la que tiene acceso una persona jurídica y que, por medio de la autorización del dueño de los datos, va a ser compartida con otra entidad.

En caso de migración, la Agencia Nacional Digital en su rol de Articulador deberá actualizar los registros de la Base de Datos Maestra por el código del nuevo Prestador al cual migró el Usuario. En caso de que el Usuario retire la autorización y no opte por migrar a otro Prestador las credenciales deberán ser eliminadas de la Base de Datos Maestra.

6.4.2.2.2.2 Hardware

6.4.2.2.2.2.1 Centro de Procesamiento de Datos

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.1.

6.4.2.2.2.3 Conectividad

6.4.2.2.2.3.1 Centro de Monitoreo de Red

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.2.

6.4.2.2.2.3.2 Centro de soporte:

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.3.

6.4.2.2.2.3.3 Canal de conexión:

El canal de conexión es el medio por el cual se conecta o accede a un servicio, establece una ruta de comunicación que puede ser usada para acceder a un servicio. La característica principal con la que debe contar el canal de conexión es disponer de canal de conexión doble.

6.4.2.2.2.3.4 Plataforma de interoperabilidad:

El servicio de autenticación digital se apoya en gran medida en el servicio de interoperabilidad, sobre el cual las entidades, la Agencia Nacional Digital en su rol de Articulador y el Usuario interactúan para garantizar que se realice el proceso correcto de autenticación y la emisión de certificados digitales. Para el despliegue del servicio de interoperabilidad se debe seguir lo estipulado en los requerimientos técnicos de integración de esta guía.

6.4.2.2.3 Seguridad

La seguridad de la autenticación digital debe estar centrada en:

- Evitar la suplantación y duplicidad de información (teniendo en cuenta que una persona solo puede autenticarse con un Prestador a la vez) con el fin de garantizar un ecosistema seguro para los Usuarios, donde el manejo de los datos privados y semi privados sea adecuado y quienes dispongan de dichos datos tengan una autorización previa del Usuario en cuestión. Todo esto alineado con la normativa NTC-ISO/IEC 27001 vigente, que propone un sistema

de gestión para preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos.

- El registro a la plataforma debe estar alineado con los estándares de seguridad mínimos para evitar que se filtre información de los Usuarios o que se acceda a información sin permiso alguno como lo dispone el artículo 5 de la Ley 1266 de 2008 relacionado con la circulación de la información almacenada en bases de datos.
- La privacidad está relacionada directamente con la transparencia del servicio y a su vez esto genera la base para empezar a crear servicios adicionales que fomenten los servicios en línea y beneficien tanto a los Usuarios, al Estado y a las organizaciones privadas que van a hacer parte del modelo.
- La evaluación de impacto en la privacidad es un análisis de riesgos con el cual se pretende presentar y establecer los derechos de los Usuarios que tienen datos en la plataforma además de mitigar los riesgos asociados a compartir información para acceder a los servicios ciudadanos digitales especiales. Esta evaluación identifica los riesgos específicos, la probabilidad de que sucedan y el posible daño si se llega a filtrar información. La norma NTC-ISO/IEC 27701 establece en el numeral 7.2.5 el siguiente control: "La organización debería evaluar la necesidad de realizar, e implementar cuando proceda, una evaluación del impacto sobre la privacidad cada vez que se planifique un nuevo procesamiento de la IIP o cambios en el procesamiento existente de la IIP." (Información de Identificación Personal - IIP).
- Es importante tener en cuenta el régimen hibrido de protección de datos personales y de habeas data, así como que la privacidad desde el diseño y por defecto es un componente basado en el Decreto 1078 de 2015 (DUR-TIC) que de conformidad con el artículo 2.1.1.2 rige tanto para las entidades públicas como privadas, para que estas tomen las medidas preventivas para anticipar la pérdida de la privacidad de la información y aplicar las medidas apropiadas.
- Los Prestadores de Servicios Ciudadanos Digitales Especiales deben implementar los requerimientos para desplegar un sistema de gestión de la seguridad de la información y la privacidad alineado a los parámetros establecidos en el estándar internacional NTC-ISO/IEC 27001 vigente y su extensión NTC-ISO/IEC 27701. El uso de este estándar permitirá garantizar un uso confidencial y seguro de la información de los Usuarios, a través de un sistema de gestión de riesgos.
- La metodología también debe contar con una aplicación de procesos de valoración de riesgos que permita identificar cuales riesgos pueden causar la perdida de confidencialidad o faltar con los principios de seguridad de la información (integridad, confidencialidad y disponibilidad). Esto se logra a partir de la definición de criterios medibles que expresen la pérdida potencial en el

caso que un tercero acceda a los datos sin autorización previa, se debe a su vez determinar los niveles de riesgo a los que los datos están expuestos.

- Con el objetivo de garantizar la seguridad de los procedimientos de autenticación es necesario contar con una comunicación segura utilizando el protocolo seguro de transferencia de hipertexto HTTPS y el protocolo descifrado de seguridad de la capa de transporte TLS 1.2, o superior, que usen algoritmos asimétricos seguros de tipo RSA SHA 512 o equivalentes.
- Con el objetivo primordial de evitar la suplantación se debe usar un sistema de nombres de dominio seguro para proteger los Usuarios y evitar que se presenten alteraciones en los datos privados o que se compartan a entidades que no ha sido aprobadas.
- Adicional, para completar la protección y asegurar que no existan modificaciones a los datos, no se debe permitir que se almacenen claves o credenciales en el código fuente del sistema y se debe priorizar el aseguramiento de los niveles de seguridad adecuados siguiendo las políticas y las buenas prácticas de seguridad.
- Otro de los protocolos necesarios está destinado a la protección de cookies y objetos de sesión de autenticación para que no estén expuestas y sean hackeadas por terceros.

6.4.2.2.3.1 Estándares de seguridad

Para obtener unos niveles de seguridad aceptables se toman como referencia los estándares aceptados por la Agencia Nacional Digital y la Resolución MinTIC 500 de 2021 en los cuales se basan los requisitos que deben cumplir los Prestadores de Servicios Ciudadanos Digitales Especiales. A continuación, se indican los estándares de referencia que se deben cumplir o estándares equivalentes:

- NTC-ISO/IEC 27001 y su extensión NTC-ISO/IEC 27701 vigente en seguridad de la información.
- ISO 22301 vigente en seguridad, resiliencia y continuidad del negocio.
- ITIL V4, NTC-ISO/IEC 20000-1 vigente.
- ISO/IEC 24762 en lineamientos sobre servicios de tecnología de la información y comunicación para recuperación de desastres.
- NIST 800-53 Revisión 5 en controles de seguridad y privacidad.
- El documento que contiene los diez (10) riesgos de seguridad más importantes en aplicaciones web según la organización OWASP.
- Modelo de Seguridad y Privacidad de la Información definido por MinTIC.

6.4.2.2.3.2 Centro de Operaciones de Seguridad:

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.4.

6.4.2.2.3.3 Sistemas de Gestión de Seguridad de la Información:

Desde el estándar NTC-ISO/IEC 27001 se plantea el concepto de un sistema de gestión de seguridad de la información. Es un compendio de políticas y prácticas que permiten garantizar la seguridad de la información. A continuación, se listan las características que debe poseer el sistema de gestión de seguridad de la información.

Adicionalmente este sistema de gestión de seguridad de la información debe estar alineado con las políticas definidas por el Modelo de Seguridad y Privacidad de la Información liderado por el MinTIC. Este sistema se acredita con el requisito administrativo establecido en la presente guía.

- Otros requerimientos de seguridad:

Tomando como base los estándares aprobados por la Agencia Nacional Digital, a continuación, se señalan los requisitos generales en términos de seguridad de la red:

  - Contar con una lista de control de acceso.
  - Usar cifrado simétrico y/o asimétrico de longitud no menor a 2048 bits.
  - Proteger las claves de acceso con algoritmos especializados para ello.
  - Contar con un cortafuegos de aplicaciones web.
  - Contar con un antivirus de nueva generación.
  - Utilizar sistemas de detección de intrusos en un host.
  - Utilizar virtualización del host.
  - Segmentar las redes.
  - Utilizar protocolos de acceso a un directorio tipo LDAP.
  - Contar con el conjunto de protocolos para asegurar las comunicaciones sobre el protocolo de internet.
  - Usar los protocolos criptográficos de seguridad de la capa de transporte y su antecesor de capa de puertos seguros, que proporcionan comunicaciones seguras en internet.
  - Contar con una red privada virtual.

- Los siguientes requisitos hacen referencia a la seguridad física del lugar en el cual se alojan los servidores y equipos:

    - Seguridad en los accesos físicos al edificio.
    - Seguridad interna de salas.
    - Seguridad en el bastidor de comunicaciones.
    - Control y filtrado de accesos.
    - Control medioambiental.
    - Control de energía.

- Los requisitos de seguridad perimetral son:

    - Contar con sistemas anti denegación del servicio.
    - Contar con un sistema de detección de intrusos.
    - Contar con un sistema de prevención de intrusos.
    - Contar con un cortafuegos de nueva generación.
    - Contar con un balanceador de carga.
    - Contar con una zona desmilitarizada.

6.4.2.2.3.4 *Política de Copia de Seguridad y Recuperación*

Dentro de la política de copia de seguridad y recuperación se debe establecer un conjunto de acciones con el objetivo de salvaguardar los activos de información, evitar pérdidas de datos en caso de algún desastre y permitir la restauración oportuna de la información. Estas acciones se presentan a continuación:

- Identificación de información crítica: El Prestador de Servicios Ciudadanos Digitales Especiales debe identificar y clasificar los activos de información estableciendo la criticidad de los datos y definiendo los niveles de seguridad que debe tener cada grupo de datos.
- Frecuencia de respaldo: Todos los grupos de datos deben tener una frecuencia de respaldo con el objetivo de evitar que exista una fuga de información. También se deben definir los medios de almacenamiento que se van a usar para realizar el respaldo de los datos y las frecuencias para los datos que maneja el Prestador de Servicios Ciudadanos Digitales Especiales:

    - Realizar la copia de información de los servidores cada vez que se realice un cambio significativo del sistema.
    - Realizar un respaldo diferencial cada semana de los servidores de bases de datos y los servidores web.

- Realizar un respaldo completo de manera mensual de los servidores de bases de datos y los servidores web.
- Realizar un respaldo completo de manera anual de los servidores de bases de datos y los servidores web.

Se debe tener en cuenta que el proceso de respaldo se debe hacer en un horario de baja carga transaccional (para los servicios de siete (7) días a la semana por veinticuatro (24) horas al día) y en un horario no hábil (para los que no funcionan siete (7) días a la semana).

- Protección de los medios de respaldo: Se debe garantizar la custodia de los medios de respaldo en un lugar seguro con el objetivo de ser puestos en funcionamiento de ser requeridos. Adicional, como medida de seguridad se debe contar con una copia en un lugar secundario para mitigar los riesgos.
- Protección de la información en los medios de respaldo: Se deben documentar los registros de las copias de respaldo y contar con un lugar protegido para almacenar la información de manera segura.
- Periodo de existencia de las copias: Los Prestadores de Servicios Ciudadanos Digitales Especiales deben almacenar la información durante un año fiscal. Sin embargo, cabe aclarar que el Prestador de Servicios Ciudadanos Digitales Especiales debe hacer una disposición segura de la información de los Usuarios de servicios ciudadanos digitales especiales con el fin de no incumplir con las leyes emitidas de protección de datos personales por el Estado colombiano.

Para cumplir con las estrategias de respaldo y continuidad de negocio se pueden incluir esquemas en la nube.

Además de seguir los estándares antes mencionados, a continuación se muestran requisitos adicionales que se deben tomar en cuenta en la prestación de los servicios ciudadanos digitales especiales:

6.4.2.2.3.5 Sistema de Administración de Riesgo Operativo

Se debe cumplir de acuerdo con los términos indicados en ítem 3.1 del numeral 6.2 Requisitos Administrativos.

6.4.2.2.3.6 Sistema de Control Interno

Se debe cumplir de acuerdo con los términos indicados en ítem 3.2 del numeral 6.2 Requisitos Administrativos.

6.4.2.2.3.7 Otros requerimientos de seguridad

Para ser habilitado como Prestador de Servicios Ciudadanos Digitales Especiales, el Solicitante deberá cumplir las siguientes condiciones:

Acreditar el plan de contingencia que asegure la continuidad de operación relacionada con la alta disponibilidad del servicio de conformidad con los requisitos de la norma ISO/IEC 20000-1. Para ello, deberá indicar los requisitos mínimos, procesos, procedimientos, controles, periodicidad mínima de realización de controles que garanticen la continuidad de la operación, así como, acciones para restablecer el servicio y recuperación de la operación en caso de inconvenientes tecnológicos. Esta información deberá estar contenida en un documento que será actualizado anualmente, suscrito por el representante legal del Prestador de Servicios Ciudadanos Digitales Especiales, junto con los soportes.

6.4.2.2.4 Arquitectura de referencia

La arquitectura de referencia establece los elementos que interactúan en el servicio de autenticación digital, sus componentes generales y como se relacionan entre ellos, facilitando el entendimiento del funcionamiento general del servicio.

A continuación, se observa el diagrama de arquitectura del servicio de autenticación digital:

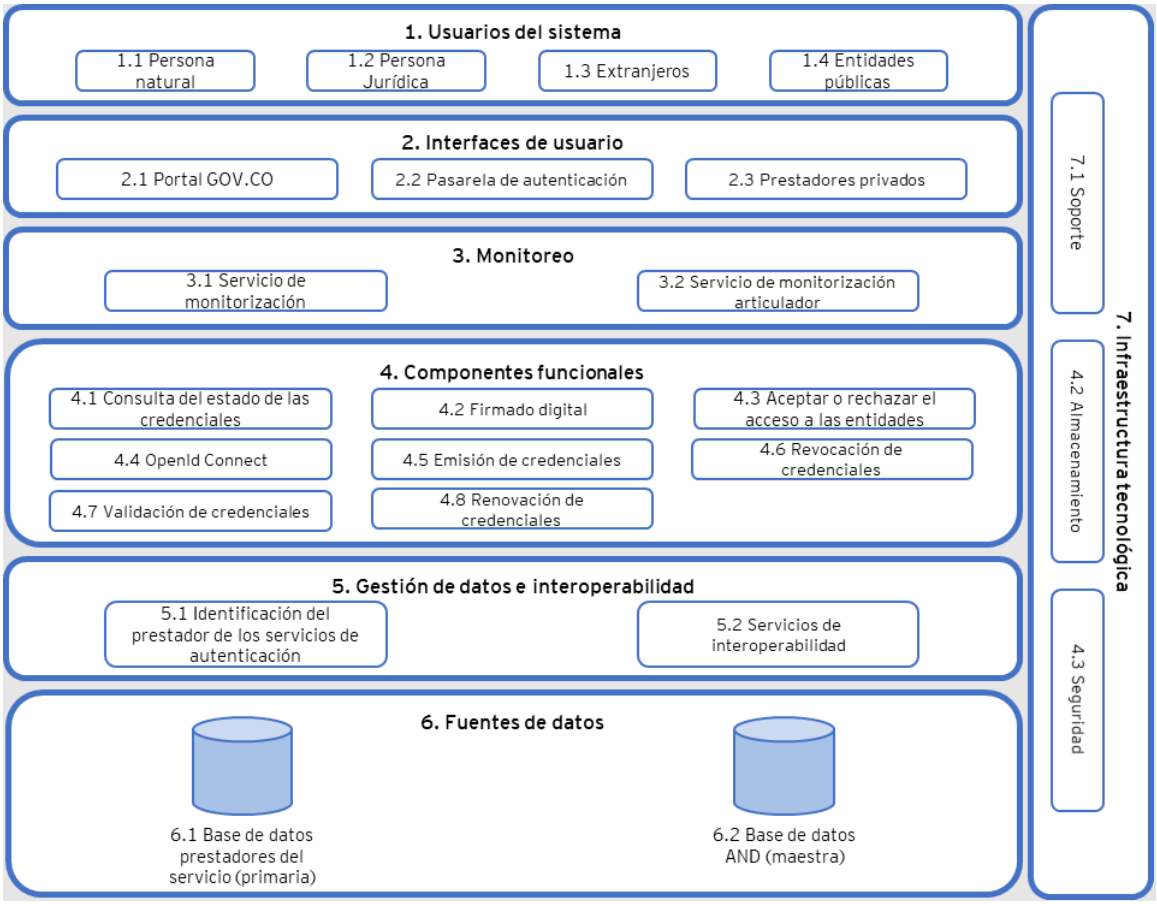


Ilustración 4. Diagrama de arquitectura del servicio de autenticación digital.
(Fuente: Insumos técnicos, jurídicos, administrativos y financieros para la reglamentación de la operación de los servicios ciudadanos digitales base y especiales prestados por personas jurídicas de derecho privado, ERNST & YOUNG S A S., junio de 2021, página 43)

6.4.2.3Requerimientos técnicos del Prestador de Servicios Ciudadanos Digitales Especiales de carpeta ciudadana digital

El servicio de carpeta ciudadana digital busca fortalecer la relación entre el Estado, los ciudadanos y los entes privados, aportando un servicio adecuado para optimizar dichas relaciones y proporcionar los insumos necesarios para la generación de unos servicios ciudadanos digitales fáciles de usar.
El servicio de carpeta ciudadana digital permite a los Usuarios el acceso a los datos que tiene el Estado.

A través de la carpeta ciudadana digital el Usuario tiene la oportunidad de interactuar de manera más directa con entidades de carácter público y privado además de gestionar de manera personalizada la información que comparte con terceros. Esto en el cumplimiento del régimen de protección de datos personales

con el objetivo de optimizar la transferencia de información entre diferentes actores del ecosistema.

De acuerdo con el marco de referencia, a continuación, se establecen los principios rectores, los requerimientos técnicos, los requerimientos de seguridad y la arquitectura de referencia para la carpeta ciudadana digital. Estas secciones permitirán establecer los requerimientos a los cuales un Prestador de Servicios Ciudadanos Digitales Especiales se vería enfrentado para habilitarse en la prestación de servicios ciudadanos digitales especiales.

6.4.2.3.1 Principios rectores

El marco de desarrollo y construcción de enlaces entre sector público y privado debe estar desarrollado bajo determinados principios que garanticen, entre otros, la interoperabilidad, accesibilidad, seguridad y privacidad de la información. A continuación, se detallan los principios rectores necesarios:

- Simplificar, facilitar y centralizar el acceso a los servicios del Estado.
- Garantizar la seguridad de los datos de los Usuarios y evitar la suplantación.
- Facilitar al Usuario el acceso a la información que el Estado tiene sobre él, además de la entidad y la veracidad de los datos.
- Garantizar la interacción de los Prestador de Servicios Ciudadanos Digitales Especiales y la Agencia Nacional Digital en su rol de Articulador para prestar el servicio de carpeta ciudadana digital por medio de la interoperabilidad.
- Optimizar y agilizar los trámites del Estado.
- Presentar las responsabilidades de la carpeta ciudadana digital y establecer la independencia frente a las entidades adscritas al servicio.
- Permitir que las personas jurídicas y naturales controlen el acceso a sus datos y puedan editar ciertos campos.
- Gestionar los procesos administrativos desde la carpeta ciudadana digital en los que se ven involucrados personas jurídicas y naturales.

6.4.2.3.2 Estándares técnicos

Se refieren a aquellos requisitos tecnológicos tanto de hardware como de software necesarios para prestar de manera efectiva los servicios de carpeta ciudadana digital además de los requisitos que garantizan el cumplimiento de los niveles mínimos de seguridad del servicio. Estos requerimientos están basados en el Anexo 1 “Guía de Lineamientos de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 del 2020, que instaura los requisitos técnicos de la Agencia Nacional

Digital alineándolos con los Prestadores de Servicios Ciudadanos Especiales, los requerimientos son:

6.4.2.3.2.1 Hardware

6.4.2.3.2.1.1 Centro de Procesamiento de Datos

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.1.

6.4.2.3.2.2 Conexión

6.4.2.3.2.2.1 Centro de Monitoreo de Red

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.2.

6.4.2.3.2.2.2 Centro de soporte

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.3.

6.4.2.3.2.2.3 Canal de conexión

El canal de conexión es el medio por el cual se conecta o accede a un servicio, establece una ruta de comunicación que puede ser usada para acceder a un servicio. La característica principal con la que debe contar el canal de conexión es disponer de canal de conexión doble.

6.4.2.3.2.2.4 Plataforma de interoperabilidad

El servicio de carpeta ciudadana digital se apoya en el servicio de interoperabilidad, sobre el cual las entidades púbicas, la Agencia Nacional Digital en su rol de Articulador y el Usuario interactúan para desarrollar los diferentes trámites que pueden estar asociados a la carpeta ciudadana digital. Para el despliegue del servicio de interoperabilidad se deben seguir los lineamientos y estándares para la integración de este servicio base y la coordinación de los Prestadores de Servicios Ciudadanos Digitales Especiales con la Agencia Nacional Digital en su rol de Articulador, definidos en la presente guía.

El Prestador de Servicios Ciudadanos Digitales Especiales es responsable del tratamiento de datos personales que los Usuarios le proporcionen y de igual manera de los datos que otras entidades le envíen por la prestación de un servicio.

El Prestador de Servicios Ciudadanos Digitales Especiales durante la prestación del servicio de la carpeta ciudadana digital interactúa con las entidades públicas a través de la plataforma de interoperabilidad con el objetivo de consultar información de la que estas disponen. Cuando termine la interacción, el Prestador de Servicios Ciudadanos Digitales Especiales deberá eliminar de manera inmediata todos aquellos documentos a los que haya tenido acceso.

Es necesario que el Prestador de Servicios Ciudadanos Digitales Especiales cumpla con las directrices establecidas por el MinTIC en el marco de interoperabilidad y del lenguaje común de intercambio de información con la finalidad de facilitar la interacción con la Agencia Nacional Digital en su rol de Articulador.

Además de esto, se espera que la integración del servicio de carpeta ciudadana digital con la plataforma de interoperabilidad contemple la instalación y configuración del servidor de seguridad, la certificación de los servicios de exposición por medio de la publicación del punto final de los servicios web y la autorización en el servidor de seguridad. Para el despliegue del servicio de carpeta ciudadana digital se requiere la estructuración de los ambientes de pre-producción, producción y calidad, los cuales estarán asociados a unos servidores que permitirán prestar el servicio.

Para todas las entidades se deben desarrollar los servicios de exposición en la carpeta ciudadana digital, dentro de los cuales se encuentran el servicio de consulta de información, el servicio de alerta y comunicaciones, el servicio de historial de trámites y el servicio de historial de solicitudes. Estos servicios de exposición se desarrollan a través de la tecnología REST, CONTENT TYPE: APLLICATION/JSON.

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben seguir los lineamientos de los requisitos para la integración del servicio de interoperabilidad.

6.4.2.3.3 Seguridad

El modelo de seguridad tiene que velar por preservar la confidencialidad de los datos y la disponibilidad de la información con el fin de cumplir con los objetivos estratégicos de la entidad implicada, ya sea pública o privada. El buen uso de los datos y la privacidad de estos tienen como resultado un ecosistema más transparente y colaborativo que invita a la participación ciudadana y de la mano del sector público es posible construir un entorno abierto a la ciudadanía y a las organizaciones privadas que cumpla con todos los requisitos necesarios para garantizar las buenas prácticas de gestión de la información.

El documento debe contar con una metodología que permita definir los protocolos para gestionar los riesgos de seguridad, además de la valoración de conflictos que permita identificar cuales pueden causar la perdida de confidencialidad. Adicionalmente, el documento debe respetar los principios de seguridad de la información (integridad, confidencialidad y disponibilidad), así como incluir una metodología que indique las estrategias para reducir el riesgo (transferir o mitigar).

Para garantizar la seguridad de los servicios de carpeta ciudadana digital es necesario asegurar la comunicación usando el protocolo seguro de transferencia de hipertexto HTTPS y el protocolo de cifrado TLS 1.2 o versiones superiores que usen algoritmos asimétricos seguros aprobados del tipo RSA SHA 512 o equivalentes alineados con normas XADES o similares. Para protegerse frente a la suplantación de sistema de nombres de dominio (spoofing) únicamente se debe usar sistema seguro de nombres de dominio que brinda seguridad de la identidad del servidor. Además, la plataforma debe asegurar la confidencialidad de la transferencia de la información por medio de un cifrado punto a punto de los mensajes y garantizar la identificación de los receptores y los emisores para que las comunicaciones tengan un nivel de transparencia aceptable.

Los Prestadores de Servicios Ciudadanos Digitales Especiales no deberán almacenar claves, secretos o credenciales de ningún tipo en el código fuente de sus sistemas, además, deben garantizar la seguridad de dichos sistemas.

Se deben establecer mecanismos adecuados para reducir los riesgos de un ataque de falsificación de petición en sitios cruzados XSRF o XSS, con conexiones de seguridad de transporte estricta HSTS y política de contenido seguro, además, se deben utilizar mecanismos de intercambio de recursos de origen cruzado CORS que permitan el envío de cookies únicamente a servidores con plena autorización.

Para garantizar la validación de Usuarios es necesario contar con un protocolo de accesos y asegurar la alta transaccionalidad de los Usuarios. Para lograrlo hay que contar con un tiempo de sesión de 900 segundos.

6.4.2.3.3.1 Estándares de seguridad

Para obtener unos niveles de seguridad aceptables se toman como referencia los estándares aceptados por la Agencia Nacional Digital en los cuales se basan los requisitos que deben cumplir los Prestador de Servicios Ciudadanos Digitales Especiales de carpeta ciudadana digital. A continuación, se indican los estándares de referencia que se deben cumplir:

- NTC-ISO/IEC 27001 vigente en seguridad de la información.
- ISO/IEC 22301 vigente en seguridad, resiliencia y continuidad del negocio.
- ITIL V4, NTC-ISO/IEC 20000-1.
- ISO/IEC 24762 en lineamientos sobre servicios de tecnología de la información y comunicación para recuperación de desastres.
- NIST 800-53 Revisión 5, en controles de seguridad y privacidad.
- El documento que contiene los diez (10) riesgos de seguridad más importantes en aplicaciones web según la organización OWASP.
- Modelo de seguridad y privacidad de la información definido por MinTIC.

6.4.2.3.3.2 Centro de Operaciones de Seguridad

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.4.

6.4.2.3.3.3 Sistemas de Gestión de Seguridad de la Información

Desde el estándar NTC-ISO/IEC 27001 se plantea el concepto de sistemas de gestión de seguridad de la información. Es un compendio del conjunto de políticas y prácticas que permiten garantizar la seguridad de la información. Se acredita con el requisito administrativo establecido en la presente guía.

6.4.2.3.3.4 Sistema de Administración de Riesgo Operativo

Se debe cumplir de acuerdo con los términos indicados en ítem 3.1 del numeral 6.2 Requisitos Administrativos.

6.4.2.3.3.5 *Sistema de Control Interno*

Se debe cumplir de acuerdo con los términos indicados en ítem 3.2 del numeral 6.2 Requisitos Administrativos.

6.4.2.3.3.6 Otros requerimientos de seguridad

Tomando como base los estándares aprobados por la Agencia Nacional Digital antes mencionados, a continuación, se listan los requisitos generales en términos de seguridad de la red:

- Contar con una lista de control de acceso.
- Usar cifrado simétrico y/o asimétrico de longitud no menor a 2048 bits.
- Proteger las claves de acceso con algoritmos especializados para ello.

- Contar con un cortafuego de aplicaciones web.
- Contar con un antivirus de nueva generación.
- Utilizar sistemas de detección de intrusos en un host.
- Utilizar virtualización del host.
- Segmentar las redes.
- Utilizar protocolos de acceso a un directorio tipo LDAP.
- Contar con el conjunto de protocolos para asegurar las comunicaciones sobre el protocolo de internet.
- Usar los protocolos criptográficos de seguridad de la capa de transporte y su antecesor de capa de puertos seguros, que proporcionan comunicaciones seguras en internet.
- Contar con una red privada virtual.

Los siguientes requisitos hacen referencia a la seguridad física del lugar en el cual se alojan los servidores y equipos:

- Seguridad en los accesos físicos al edificio.
- Seguridad interna de salas.
- Seguridad en los racks de comunicaciones.
- Control y filtrado de accesos.
- Control medioambiental.
- Control de energía.

Los requisitos de seguridad perimetral son:

- Contar con sistemas contra ataques de denegación del servicio.
- Contar con un sistema de detección de intrusos.
- Contar con un sistema de prevención de intrusos.
- Contar con un firewall de nueva generación.
- Contar con un balanceador de carga.
- Contar con una zona desmilitarizada.

6.4.2.3.4 Arquitecturas de referencia

La arquitectura de referencia establece los elementos que interactúan en el servicio de carpeta ciudadana digital, sus componentes generales y como se relacionan entre ellos facilitando el entendimiento del funcionamiento general del servicio.

A continuación, se observa el diagrama de arquitectura de la carpeta ciudadana digital:

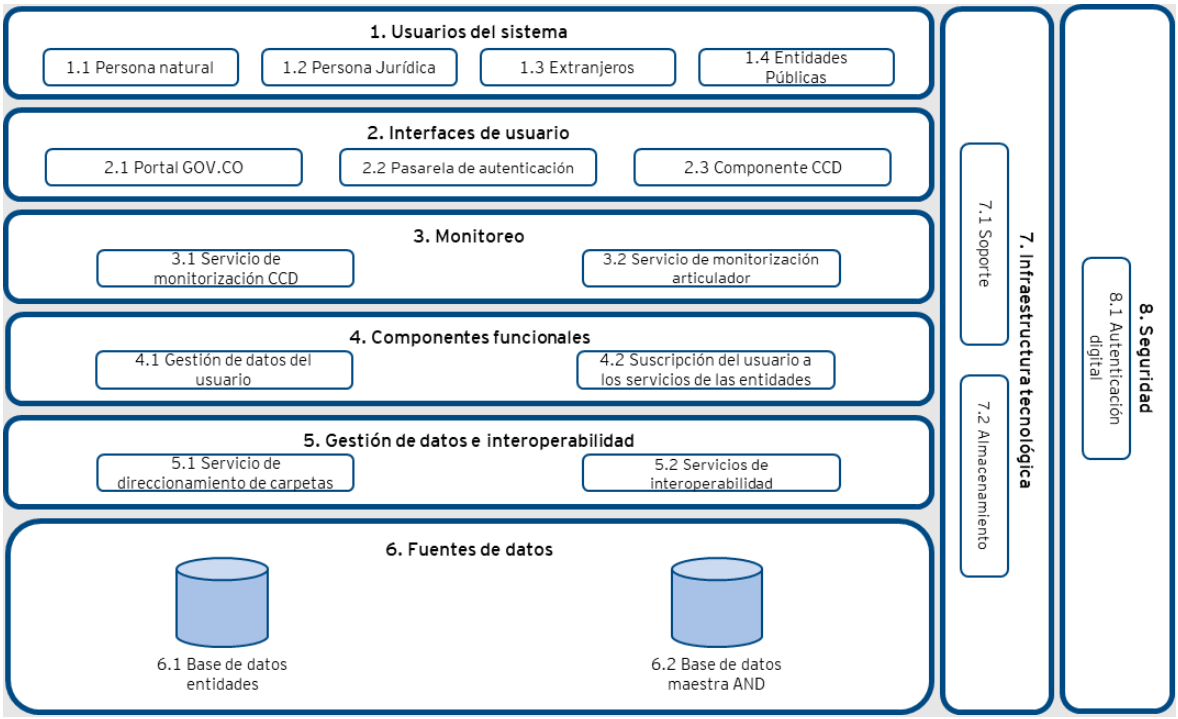


Ilustración 5. Diagrama de arquitectura del servicio de carpeta ciudadana digital
(Fuente: Insumos técnicos, jurídicos, administrativos y financieros para la reglamentación de la operación de los servicios ciudadanos digitales base y especiales prestados por personas jurídicas de derecho privado, ERNST & YOUNG S A S., junio de 2021, página 54)

6.4.2.4Requerimientos técnicos para la prestación de los servicios ciudadanos digitales especiales

Entendiendo la necesidad de acatar los marcos regulatorios de protección de datos y de privacidad, la apertura de información y servicios del sector público a terceros va a traer como beneficio el crecimiento de los servicios ciudadanos digitales, la competitividad y la creación de proyectos públicos, privados o mixtos para continuar con la adaptación de enfoques innovadores para diseñar y ofrecer mejores servicios basados en las necesidades de los Usuarios.

Bajo la definición de servicios ciudadanos digitales especiales dada en la Resolución MinTIC 2160 de 2020, las personas jurídicas de derecho privado que pretendan habilitarse para la prestación de servicios ciudadanos digitales especiales, deben diseñar servicios de alto nivel de innovación, con el objetivo de ofrecer valor a la prestación de los servicios ciudadanos base.

A continuación, se presenta el diagrama del modelo de servicios ciudadanos digitales especiales:

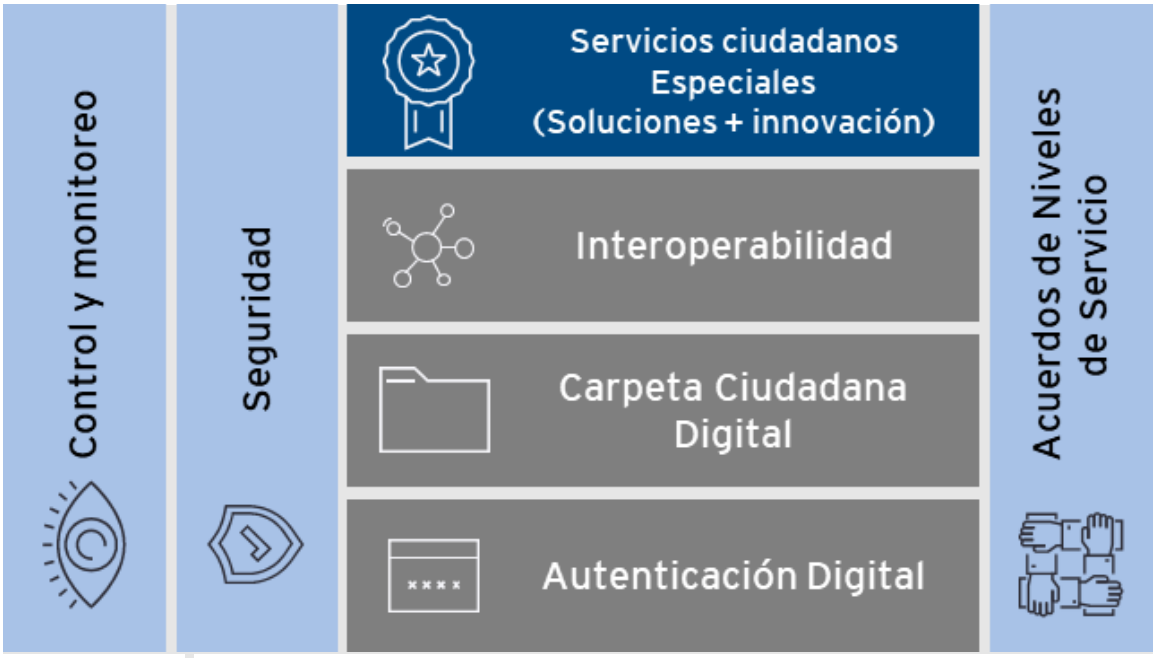


Ilustración 6. Diagrama del modelo de servicios ciudadanos digitales especiales
(Fuente: Insumos técnicos, jurídicos, administrativos y financieros para la reglamentación de la operación de los servicios ciudadanos digitales base y especiales prestados por personas jurídicas de derecho privado, ERNST & YOUNG S A S., junio de 2021, página 56)

El diagrama del modelo de los servicios ciudadanos digitales lo constituyen los siguientes componentes:

- **Control y monitoreo:** Definición de requisitos para el seguimiento y control de los servicios ciudadanos digitales especiales, en línea con los lineamentos establecidos en los servicios ciudadanos digitales base.
- **Seguridad:** Identificación de lineamientos para cubrir con las características de seguridad informática y de la información para salvaguardar la integridad de los datos de los ciudadanos.
- **Autenticación digital:** Procedimiento que utilizando mecanismos de autenticación digital, permite verificar los atributos digitales de una persona cuando adelanten trámites y servicios a través de medios digitales.
- **Carpeta ciudadana digital:** Servicio que le permite a los Usuarios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las entidades señaladas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015 (DUR-TIC). Adicionalmente, este servicio podrá entregar las comunicaciones o alertas que las entidades señaladas tienen para los Usuarios, previa autorización de estos.

- **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.
- **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 la Agencia Nacional Digital en su rol de Articulador.
- **Acuerdos Niveles de Servicio (ANS):** Como se explica en el capítulo de definiciones de la Guía.

Considerando los esquemas de interoperabilidad entre los servicios ciudadanos digitales base y los servicios ciudadanos digitales especiales, se definen los siguientes principios rectores:

6.4.2.4.1 Principios rectores

- Alineación con estándares internacionales para garantizar la identificación de prácticas líderes.
- Garantizar el establecimiento de un precio justo para el ciudadano.
- Generar soluciones innovadoras para la prestación de servicios al ciudadano.
- Optimizar y agilizar los trámites del Estado.
- Vincular las interacciones entre el ciudadano y el Estado a través del portal único del Estado colombiano.

Con la finalidad de robustecer el esquema de funcionamiento de los servicios ciudadanos digitales base se realiza la identificación de proyectos que generen valor adicional bajo conceptos de innovación y soluciones que cumplan las necesidades de los Usuarios, se identifican los principios rectores de los servicios ciudadanos digitales especiales alineados con la necesidad de acatar los marcos regulatorios de protección de datos y de privacidad, la apertura de información y servicios del sector público a terceros, va a traer como beneficio el crecimiento de los servicios ciudadanos digitales, la competitividad y la creación de proyectos públicos, privados o mixtos para continuar con la adaptación de enfoques innovadores para diseñar y ofrecer mejores servicios basados en las necesidades de los Usuarios.

Esta identificación de proyectos parte de la categorización de innovaciones tecnológicas, que toman el espectro de dos grandes categorías:

- **Innovación de producto:** El Solicitante presentará proyectos que aporten servicios nuevos o significativamente mejorados, en cuanto a uso y/o funcionalidad, enfocados a generar valor a los servicios ciudadanos digitales base prestados a los Usuarios. Se toma como premisa de este tipo de proyecto la mejora tecnológica, de componentes, optimización de tiempos o integralidad entre los niveles de arquitectura.
- **Innovación de proceso:** El Solicitante presentará proyectos que aporten mejoras significativas en los procedimientos, metodologías, o marcos de trabajo relacionados con los servicios prestados a los Usuarios, tomando como objeto la optimización de cuellos de botella, aumento de niveles de calidad y/o la introducción de nuevas tecnologías que busquen mejorar la eficiencia de los servicios actuales.

Considerando estas características se establecen niveles de categorización para los servicios ciudadanos digitales especiales, como se determina en el numeral 6.4.1.2 de este mismo anexo.

6.4.2.4.2 Estándares técnicos

6.4.2.4.2.1 Requerimientos Nivel Alto

Los modelos de negocio clasificados como nivel alto según la evaluación de criterios deben garantizar que el sistema soporte una volumetría alta de manera constante y que garantice la seguridad de los datos sensibles además de tener la capacidad de realizar analítica de los datos a los que tiene alcance.

Para el despliegue de un sistema de nivel alto se tendrán en cuenta la implementación de los servidores para la interoperabilidad descritos en la Tabla - Requisitos de los servidores de seguridad del numeral 6.6.2 del Anexo 2 “Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020. Siendo un sistema de nivel alto se deberá cumplir con la implementación de todos los servidores descritos y con la replicabilidad del servidor de producción, adicionalmente se establece que el almacenamiento en estos servidores sea mayor para poder almacenar mayores niveles de información y que su velocidad de transferencia sea amplia para poder cumplir con los niveles de transaccionalidad adecuados para los servicios que se desean prestar.

A continuación, se presentan los requerimientos que debe cumplir el Prestador de Servicios Ciudadanos Digitales Especiales donde se detallan las secciones de hardware, software, conectividad y seguridad:

6.4.2.4.2.1.1 Hardware

6.4.2.4.2.1.1.1 Centro de procesamiento de datos

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.1.

6.4.2.4.2.1.2 Canal de conexión

El canal de conexión es el medio por el cual se conecta o accede a un servicio, establece una ruta de comunicación que puede ser usada para acceder a un servicio. La característica principal con la que debe contar el canal de conexión es disponer de canal de conexión doble.

6.4.2.4.2.1.2.1 Centro de Monitoreo de Red

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.2.

6.4.2.4.2.1.2.2 Centro de soporte

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.3.

6.4.2.4.2.1.3 Seguridad

6.4.2.4.2.1.3.1 Centro de Operaciones de Seguridad

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.4.

6.4.2.4.2.2 Requerimientos nivel medio

Los modelos de negocio clasificados como nivel medio según la evaluación de criterios deben garantizar que el sistema soporte picos de alta transaccionalidad y tenga la capacidad de garantizar la seguridad de datos sensibles.

Para el despliegue de un sistema de nivel medio se tendrán en cuenta la implementación de los servidores para la interoperabilidad descritos en la Tabla 1 -

Requisitos de los servidores de seguridad del numeral 6.6.2 del Anexo 2 “Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020. Siendo un sistema de nivel medio se deberá cumplir con la implementación de todos los servidores descritos, sin tener en cuenta la replicabilidad del servidor de producción, adicionalmente se establece que el almacenamiento en estos servidores sea mayor para poder almacenar mayores niveles de información y que su velocidad de transferencia sea amplia para poder cumplir con los niveles de transaccionalidad adecuados para los servicios que se desean prestar.

A razón de esto a continuación se presentan los requerimientos que debe cumplir el Prestador de Servicios Ciudadanos Digitales:

6.4.2.4.2.2.1 Hardware

6.4.2.4.2.2.1.1 Centro de Procesamiento de Datos

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.1.

6.4.2.4.2.2.2 Canal de conexión

El canal de conexión es el medio por el cual se conecta o accede a un servicio, establece una ruta de comunicación que puede ser usada para acceder a un servicio. La característica principal con la que debe contar el canal de conexión es disponer de canal de conexión doble.

6.4.2.4.2.2.3 Centro de Monitoreo de Red

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.2.

6.4.2.4.2.2.3.1 Centro de soporte

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.3.

6.4.2.4.2.2.4 Seguridad

6.4.2.4.2.2.4.1 Centro de Operaciones de Seguridad

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.4.

6.4.2.4.2.3 Requerimientos nivel bajo

Los modelos de negocio clasificados como nivel bajo según la evaluación de criterios tienen un componente técnico inferior al requerido por los otros niveles, sin embargo, es necesario garantizar la funcionalidad desde el carácter técnico.

Para el despliegue de un sistema de nivel bajo se tendrán en cuenta la implementación de los servidores para la interoperabilidad descritos en la Tabla 1 - Requisitos de los servidores de seguridad del numeral 6.6.2 del Anexo 2 “Guía para la Vinculación y Uso de los Servicios Ciudadanos Digitales” de la Resolución MinTIC 2160 de 2020. Siendo un sistema de nivel bajo se deberá cumplir con la implementación de todos los servidores descritos, sin tener en cuenta la replicabilidad del servidor de producción, cumpliendo con los requerimientos mínimos de cada servidor.

A continuación, se presentan los requerimientos que debe cumplir el Prestador de Servicios Ciudadanos Digitales Especiales:

6.4.2.4.2.3.1 Hardware

6.4.2.4.2.3.1.1 Centro de Procesamiento de Datos

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.1.

6.4.2.4.2.4 Canal de conexión

El canal de conexión es el medio por el cual se conecta o accede a un servicio, establece una ruta de comunicación que puede ser usada para acceder a un servicio. La característica principal con la que debe contar el canal de conexión es disponer de canal de conexión doble.

6.4.2.4.2.4.1 Centro de Monitoreo de Red

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.2.

6.4.2.4.2.4.2 Centro de soporte

Se debe cumplir de acuerdo con los términos indicados en el numeral 6.4.2.1.3.

6.4.2.4.2.5 Seguridad

El modelo de seguridad tiene que velar por preservar la confidencialidad de los datos y la disponibilidad de la información con el fin de cumplir con los objetivos estratégicos de la entidad implicada ya sea pública o privada. El buen uso de los datos y la privacidad de estos, tienen como resultado un ecosistema más transparente y colaborativo que invita a la participación ciudadana y de la mano del sector público es posible construir un entorno abierto a la ciudadanía y a las organizaciones privadas que cumpla con todos los requisitos necesarios para garantizar las buenas prácticas de gestión de la información.

Para garantizar la seguridad de los servicios ciudadanos digitales especiales, es necesario asegurar la comunicación usando el protocolo de transferencia de hipertexto HTTPS y el protocolo de seguridad de la capa de transporte TLS 1.2 o versiones superiores, que usen algoritmos asimétricos seguros aprobados del tipo RSA SHA 512 o equivalentes, alineados con normas XADES o similares. Para protegerse frente a la suplantación de sistema de nombres de dominio (técnica conocida en inglés como spoofing) únicamente se debe usar sistema de nombres de dominio seguro, que brinda seguridad de la identidad del servidor. Además, la plataforma a través del despliegue de X-Road asegurará la confidencialidad de la transferencia de la información por medio de un cifrado punto a punto de los mensajes y garantizará la identificación de los receptores y los emisores para que las comunicaciones tengan un nivel de transparencia aceptable. Como medida adicional de seguridad y alineado con los servicios base, es importante contar con un mecanismo de inicio de sesión único con el objetivo de realizar de manera más rápida el ingreso a la plataforma. Todo bajo el control del Usuario, quien es el que puede autorizar el acceso a los datos y hacer uso de los servicios ciudadanos digitales especiales brindados por el Prestador de Servicios Ciudadanos Digitales Especiales, favoreciendo el intercambio electrónico de manera segura de documentos e información.

Siguiendo las buenas prácticas y las políticas de seguridad no se debe permitir que se almacenen claves, secretos, o credenciales de ningún tipo en el código fuente del sistema, además, se debe asegurar niveles de seguridad adecuados inclusive en los entornos de desarrollo.

Se deben establecer mecanismos adecuados para reducir los riesgos de un ataque de falsificación de petición en sitios cruzados XSRF o XSS como conexiones de seguridad de transporte estricta HSTS y política de contenido seguro, además, se deben usar mecanismos de intercambio de recursos de origen cruzado CORS que permitan el envío de cookies únicamente a servidores con plena autorización.

Para garantizar la validación de Usuarios es necesario contar con un protocolo de accesos y asegurar la alta transaccionalidad de los Usuarios. Para lograrlo hay que contar con tiempos de 900 segundos.

6.4.2.4.2.5.1 Estándares de seguridad

Para obtener unos niveles de seguridad aceptables se toman como referencia los estándares aceptados por la Agencia Nacional Digital y la Resolución MinTIC 500 de 2021 en los cuales se basan los requisitos que deben cumplir los Prestadores de Servicios Ciudadanos Digitales Especiales. A continuación, se listan los estándares de referencia que se deben cumplir o estándares equivalentes:

- NTC-ISO/IEC 27001 vigente en seguridad de la información.
- ISO/IEC 22301 vigente en seguridad, resiliencia y continuidad del negocio.
- ITIL V4, NTC-ISO/IEC 20000-1.
- ISO/IEC 24762 en lineamientos sobre servicios de tecnología de la información y comunicación para recuperación de desastres.
- NIST 800-53 revisión 5 en controles de seguridad y privacidad.
- Contar con el conjunto de protocolos para asegurar las comunicaciones sobre el protocolo de Internet.
- Modelo de Seguridad y Privacidad de la Información definido por MinTIC.

6.4.2.4.2.5.2 Sistemas de Gestión de Seguridad de la Información

Desde el estándar NTC-ISO/IEC 27001 se plantea el concepto de un Sistema de Gestión de Seguridad de la Información como un compendio del conjunto de políticas y prácticas que permiten garantizar la seguridad de la información.

6.4.2.4.2.5.3 Otros Requerimientos de Seguridad

Tomando como base los estándares aprobados por la Agencia Nacional Digital antes mencionados, a continuación, se lista los requisitos generales en términos de seguridad de la red:

- Contar con una lista de control de acceso.
- Usar cifrado simétrico y/o asimétrico de longitud no menor a 2048 bits.
- Proteger las claves de acceso con algoritmos especializados para ello.
- Contar con un cortafuegos de aplicaciones web.

- Contar con un antivirus de nueva generación.
- Utilizar sistemas de detección de intrusos en un host.
- Utilizar virtualización del host.
- Segmentar las redes.
- Utilizar protocolos de acceso a un directorio tipo LDAP.
- Contar con el conjunto de protocolos para asegurar las comunicaciones sobre el protocolo de internet.
- Usar los protocolos criptográficos de seguridad de la capa de transporte y su antecesor de capa de puertos seguros, que proporcionan comunicaciones seguras en internet.
- Contar con una red privada virtual.

- Los siguientes requisitos hacen referencia a la seguridad física del lugar en el cual se alojan los servidores y equipos:

  - Seguridad en los accesos físicos al edificio.
  - Seguridad interna de salas.
  - Seguridad en los racks de comunicaciones.
  - Control y filtrado de accesos.
  - Control medioambiental.
  - Control de energía.

- Los requisitos de seguridad perimetral son:

  - Contar con sistemas anti denegación de servicio.
  - Contar con un sistema de detección de intrusos.
  - Contar con un sistema de prevención de intrusos.
  - Contar con un firewall de nueva generación.
  - Contar con un balanceador de carga.
  - Contar con una zona desmilitarizada.

Además de seguir los estándares antes mencionados, se deben tomar en cuenta en la prestación de los servicios ciudadanos digitales especiales los siguientes:

6.4.2.4.2.5.4 Sistema de Administración de Riesgo Operativo

Se debe cumplir de acuerdo con los términos indicados en ítem 3.1 del numeral 6.2 Requisitos Administrativos.

6.4.2.4.2.5.5 Sistema de Control Interno

Se debe cumplir de acuerdo con los términos indicados en ítem 3.2 del numeral 6.2 Requisitos Administrativos.

6.4.3 Requisitos para la integración con la Agencia Nacional Digital en su rol de Articulador

Una vez los Prestador de Servicios Ciudadanos Digitales Especiales se han habilitado para prestar servicios ciudadanos digitales especiales deben cumplir con los requisitos que les permitan la interconexión con la Agencia Nacional Digital en su rol de Articulador del sistema de acuerdo con lo estipulado en esta guía en los términos que se ilustran a continuación.

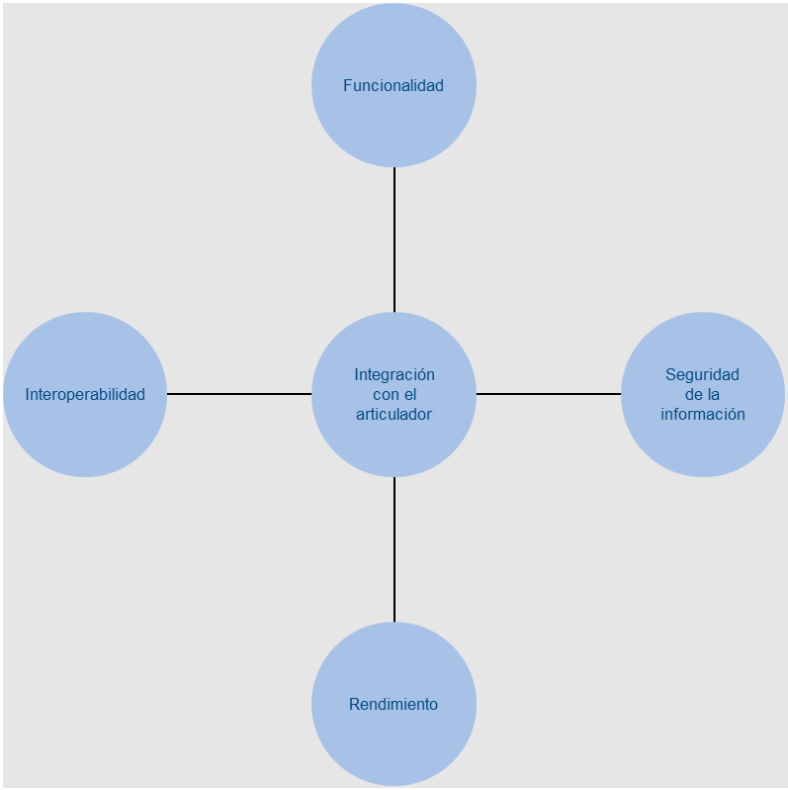


Ilustración 7. Requisitos para la integración con la Agencia Nacional Digital en su rol de Articulador. (Fuente: Insumos técnicos, jurídicos, administrativos y financieros para la reglamentación de la operación de los servicios ciudadanos digitales base y especiales prestados por personas jurídicas de derecho privado, ERNST & YOUNG S A S., junio de 2021, página 72)

7 Integración con el Articulador

Esta sección presenta los lineamientos y estándares para la integración de los Servicios Ciudadanos Digitales Especiales y la coordinación de los Prestador de Servicios Ciudadanos Digitales Especiales con la Agencia Nacional Digital en su rol de Articulador del modelo de servicios ciudadanos digitales.

7.1 Requisitos de integración del servicio de autenticación digital

El presente numeral tiene el objetivo de describir los requisitos técnicos que deben cumplir los Prestadores de Servicios Ciudadanos Digitales Especiales para la integración del servicio de autenticación digital con la Agencia Nacional digital en su rol de Articulador.

7.1.1 Esquema de integración

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 relacionados en esta guía.

En el siguiente diagrama se muestra la relación entre los Prestadores de Servicios Ciudadanos Digitales Especiales y la pasarela de servicios.

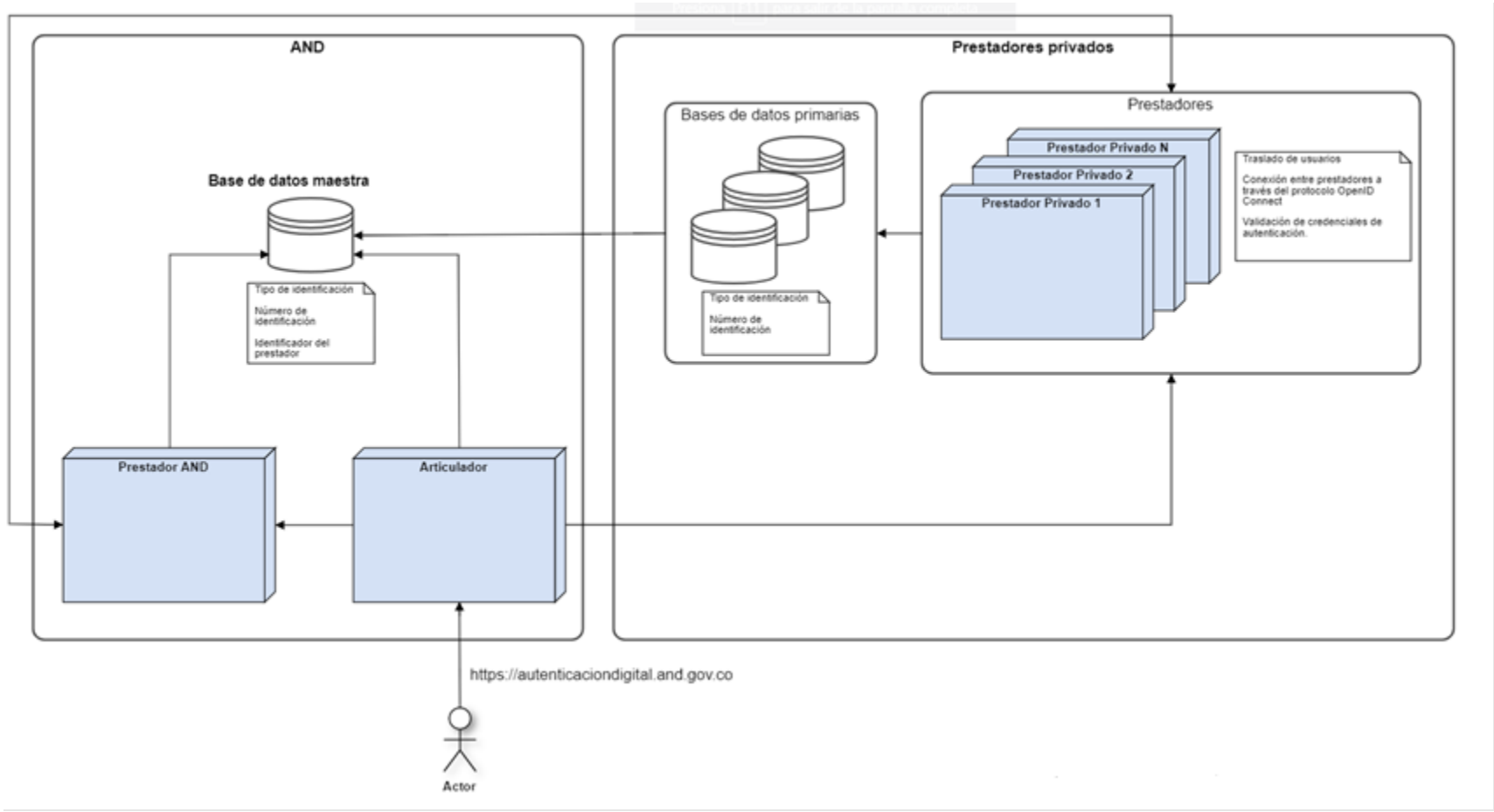


Ilustración 8**.** Prestador de Servicios Ciudadanos Digitales Especiales y la pasarela de servicios.
(Fuente: Suministrada por la Agencia Nacional Digital)

Este esquema presenta las siguientes ventajas para las entidades del estado y los Prestadores de Servicios Ciudadanos Digitales Especiales.

- 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.

7.1.2 Requisitos técnicos de Prestadores de Servicios Ciudadanos Digitales Especiales para el servicio de autenticación digital

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben soportar los siguientes protocolos de autenticación digital:

7.1.2.1 Guía de identidad digital (NIST 800-63-3)

El servicio ciudadano de autenticación digital sigue las guías de identidad digital NIST 800-63-3 del Instituto Nacional de Estándares y Tecnología de los Estados Unidos que cubren la validación y autenticación de Usuarios y su interacción con sistemas informáticos de gobiernos. Contiene requerimientos técnicos en las áreas de verificación de Usuarios, registro, autenticadores, manejo de procesos, protocolos de autenticación, federación y manejo de Claims.

Esta guía contiene lineamientos para determinar el nivel de confianza bajo el cual se autenticarán los Usuarios.

El Prestador de Servicios Ciudadanos Digitales Especiales deberá verificar la identidad de acuerdo con los niveles de confianza especificados en el estándar.

7.1.2.2 OpenID Connect

- OpenID Connect Core 1.0 (N. Sakimura N. J., 2014) [1]

Define las bases de la funcionalidad del protocolo OpenID Connect, autenticación construida sobre OAUTH 2.0 y el uso de Claims para comunicar información acerca de los Usuarios finales, también describe las consideraciones de privacidad y seguridad para el uso del protocolo.

- OpenID Connect Discovery 1.0 (N. Sakimura N. J., 2014)[2]

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben ofrecer la metadata que describe su configuración de acuerdo con la sección 3 del estándar.

Debe existir el endpoint .well-known/openid-configuration donde se expone como documento JSON la ubicación de los endpoints, los Claims que se soportan sobre los Usuarios finales, y los algoritmos de firmado de tokens soportados.

- OpenID Connect RP-Initiated Logout 1.0 - draft 01 (M. Jones M. B., n.d.)[3]

Esta especificación complementa el estándar OpenID Connect Core, con la descripción del funcionamiento del cierre de sesión. En el contexto de Prestador de Servicios Ciudadanos Digitales Especiales, la pasarela opera como RP y el Prestador de Servicios Ciudadanos Digitales Especiales como IDP, por lo que este estándar describe cómo se realiza el cierre de sesión iniciando desde la pasarela.

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben proveer el endpoint de cierre de sesión y debe soportar los parámetros post_logout_url y state marcados en el rfc como opcionales.

Para el manejo de cierre de sesión, existen tres estándares relacionados que permiten realizar el cierre de sesión iniciado desde el Prestador de Servicios Ciudadanos Digitales Especiales, quien debe soportar alguno de los siguientes estándares de cierre de sesión.

  - OpenID Connect Back-Channel Logout 1.0 - draft 06 (M. Jones M. , 2020)[4]

---

[1] OpenID Connect Core 1.0 incorporating errata set 1. Fuente: https://openid.net/specs/openid-connect-core-1_0.html

[2] OpenID Connect Discovery 1.0 incorporating errata set. Fuente: https://openid.net/specs/openid-connect-discovery-1_0.html

[3] OpenID Connect RP-Initiated Logout 1.0 - draft 01 Fuente: https://openid.net/specs/openid-connect-rpinitiated-1_0.html

[4] OpenID Connect Back-Channel Logout 1.0 - draft 06. Fuente: https://openid.net/specs/openid-connect-backchannel-1_0.html

- OpenID Connect Session Management 1.0 - draft 30 (B. de Medeiros G. N., 2020)[5]
- OpenID Connect Front-Channel Logout 1.0 - draft 04 (M. Jones M. J., 2020)[6]

7.1.2.3 OAuth 2.0

7.1.2.3.1 OAuth 2.0 ((IETF), 2012)

Este protocolo permite obtener a aplicaciones acceso limitado de un recurso HTTP, orquestando la interacción entre el dueño del recurso y el servicio del Prestador de Servicios Ciudadanos Digitales Especiales, es la base sobre la que se construye el protocolo OpenID Connect.

Para los flujos de autenticación digital, el Prestador de Servicios Ciudadanos Digitales Especiales debe soportar el flujo de authorization code, y para la conectividad backend a los servicios de autenticación digital se requiere soportar client credentials.

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben completamente soportar los siguientes RFC:

7.1.2.3.2 OAuth 2.0 Bearer Token Usage (RFC 6750)

Requerido para acceder a interfases de aplicaciones aseguradas con OAUTH2.

7.1.2.3.3 OAuth 2.0 Multiple Response Types (B. de Medeiros E. M., 2014)

Provee una guía sobre la codificación de las solicitudes a los endpoints, cuando estas incluyen espacios.

7.1.2.3.4 OAuth 2.0 Form Post Response Mode (M. Jones M. B., 2015)

Complementa el protocolo OAUTH2 para usar solicitudes tipo POST.

---

[5] OpenID Connect Session Management 1.0 - draft 30. Fuente: https://openid.net/specs/openid-connect-session-1_0.html

[6] OpenID Connect Front-Channel Logout 1.0 - draft 04. Fuente: https://openid.net/specs/openid-connect-frontchannel-1_0.html

7.1.2.3.5 OAuth 2.0 Security Best Current Practice (T. Lodderstedt, 2021)

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben implementar las últimas recomendaciones de seguridad de OAUTH 2.0 plasmadas en el documento de mejores prácticas versión 12 de abril de 2021.

Estas actualizan las recomendaciones incluidas en el RFC6749 al uso actual que tienen las aplicaciones web, se incluyen entre otros, emplear el flujo PKCE (RFC 7636) cuando se emplee authorization code, la deprecación del flujo implícito, validaciones de audiencia cuando se emiten los tokens.

El flujo recomendado para la interacción de autenticación es Authentication code con Proof Key for Code Exchange (RFC 7636) que no emplea secretos compartidos para autenticar la pasarela.

Se puede emplear JWT para la autenticación digital del Usuario de acuerdo con el JSON Web Tokens for Client Authentication (RFC 7523), de tal forma que en caso de emplear secretos compartidos estos sean de la forma JWT y no se envían secretos en texto plano.

Se recomienda emplear OAuth 2.0 Mutual TLS Client Authentication and Certificate-Bound Access Tokens (RFC 8705) como mecanismo de autenticación digital mutua entre el Prestador de Servicios Ciudadanos Digitales Especiales y la pasarela.

- OAuth 2.0 Token Revocation (RFC 7009): Permite la revocación de tokens antes de su expiración.
- OAuth 2.0 Token Introspection (RFC 7662): Define un endpoint protegido para consultar el estado de un token OAuth2 y determinar meta información sobre el token.

7.1.2.4 Interfaz de usuario requerida por los Prestador de Servicios Ciudadanos Digitales Especiales.

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben contar con las siguientes páginas web en su interfaz de usuario:

- Inicio de sesión:

Dentro del flujo de autenticación digital definido en OpenID Connect, la pasarela redirige el Usuario por medio de una respuesta 302[7], éste se autentica por medio de cualquiera de los mecanismos de autenticación digital definidos por el Prestador de Servicios Ciudadanos Digitales Especiales, que pueden ser usuario y contraseña, token de autenticación, revisión biométrica o sistema passwordless.

La autenticación digital es responsabilidad del Prestador de Servicios Ciudadanos Digitales Especiales y éste debe retornar al Usuario autenticado con sus tokens de acceso a la pasarela de servicios.

- Personalización.

El Prestador de Servicios Ciudadanos Digitales Especiales debe contar con una página web que permita al Usuario actualizar su información de contacto, modificar su mecanismo de autenticación digital, cambiar su contraseña en los casos en que esta se use como mecanismo de autenticación, eliminar la cuenta y su asociación con autenticación digital.

- Términos y condiciones:

El Prestador de Servicios Ciudadanos Digitales Especiales debe contar con términos y condiciones y política de privacidad de datos.

- Consentimiento de acuerdo al RFC OpenID Connect Core 1.0

El Prestador de Servicios Ciudadanos Digitales Especiales debe informar al Usuario de forma clara cuales datos personales serán compartidos con la pasarela de servicios ciudadanos.

7.1.2.5 Servicios a consumir y a exponer

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben consumir y exponer servicios para soportar las siguientes operaciones funcionales de coordinación con la Agencia Nacional Digital.

- Consumir el servicio para la creación de un usuario en la pasarela: Los Prestador de Servicios Ciudadanos Digitales Especiales notifican el registro de un nuevo Usuario en el servicio ciudadano de autenticación digital.

---

7 Respuesta de redirección 302 Found o HTTP 302 Found:
Este código de respuesta significa que el recurso del identificador de recursos uniforme (En inglés, Uniform Resource Identifier - URI) solicitada ha sido cambiado temporalmente. Nuevos cambios en la URI serán agregados en el futuro. Por lo tanto, la misma URI debe ser usada por el cliente en futuras solicitudes.

- Consumir el servicio para la eliminación de un Usuario en la pasarela: Eliminar Usuario de la pasarela, esta acción debe responder sólo a una acción iniciada por el Usuario.
- Consumir el servicio para la actualización de un Usuario en la pasarela: Actualizar datos personales del Usuario, esta acción debe responder sólo a una acción iniciada por el Usuario.

Los servicios se deben consumir por la plataforma de X-Road y autenticados con el RFC 6750.

7.1.2.6 Nota de privacidad de información.

La información de los Usuarios debe cumplir con el régimen de protección de datos personales y habeas data.

7.1.2.7 Requerimientos misceláneos.

- El Prestador de Servicios Ciudadanos Digitales Especiales debe sincronizarse con la hora legal colombiana[8] con una tolerancia máxima de 5 segundos.

- El Prestador de Servicios Ciudadanos Digitales Especiales debe realizar encriptación de datos de Usuarios tanto en tránsito como en reposo.

- El Prestador de Servicios Ciudadanos Digitales Especiales debe mantener y actualizar sus sistemas informáticos para mantener compatibilidad con la evolución de los sistemas de información de la Agencia Nacional Digital y revisiones a los estándares referenciados en esta guía.

- El Prestador de Servicios Ciudadanos Digitales Especiales debe ajustarse a las indicaciones que la Agencia Nacional Digital en su rol de Articulador establezca en relación con el mantenimiento de su sistema y dispositivos con las últimas versiones, paquetes de servicios y parches, por medio de una actualización frecuente de su hardware, software y dispositivos de comunicación.

- El Prestador de Servicios Ciudadanos Digitales Especiales debe entregar periódicamente reportes de la operación del sistema, con el formato e

---

8 La hora legal para el territorio de la República de Colombia es la del Tiempo Universal Coordinado (En inglés, Universal Time Coordinated - UTC) disminuido en 5 horas. De acuerdo al numeral 14 del artículo 6 del Decreto 4175 de 2011, es gestionada por el Instituto Nacional de Metrología – INM y puede ser consultada en el sitio web http://horalegal.inm.gov.co

información que define la Agencia Nacional Digital (Ver “Documento técnico lineamientos de indicadores SCDE”).

- El Prestador de Servicios Ciudadanos Digitales Especiales debe revisar periódicamente si el “Documento técnico lineamientos de indicadores SCDE” ha sido actualizado, ya que el plazo máximo para aplicar las actualizaciones a los requerimientos será de 45 días calendario.

7.1.2.8 Requerimientos operacionales

- Los Prestadores de Servicios Ciudadanos Digitales Especiales deben asegurar una infraestructura en alta disponibilidad que permita mantener los niveles de servicio.
- El Prestador de Servicios Ciudadanos Digitales Especiales no debe permitir consulta masiva de Usuarios.

- El Prestador de Servicios Ciudadanos Digitales Especiales debe soportar la conexión con la Agencia Nacional Digital a través de un sistema de nombres de dominio seguro y una IP fija.

- La comunicación entre los Prestadores de Servicios Ciudadanos Digitales Especiales y la pasarela de servicios deberá realizarse por X-Road.

- Los Prestadores de Servicios Ciudadanos Digitales Especiales deberán disponer de los ambientes de pruebas, preproducción y producción, que permitan realizar por parte de la Agencia Nacional Digital las verificaciones de cumplimiento de requisitos técnicos para su integración al servicio base.

- Los Usuarios deben optar por emplear el servicio de Autenticación Digital voluntariamente, es decir, los Prestadores de Servicios Ciudadanos Digitales Especiales no pueden inscribir Usuarios al servicio sin su aprobación.

- La definición de los contratos de los servicios se encuentra disponibles en el documento de la Agencia Nacional Digital “Documento técnico integración Autenticación”.

NOTA: La Agencia Nacional Digital podrá modificar estos servicios, por lo tanto, el Prestador de Servicios Ciudadanos Digitales se compromete a mantener actualizada su funcionalidad.

- El Prestador de Servicios Ciudadanos Digitales deberá estar en capacidad de generar logs de eventos y suministrarlos a la Agencia Nacional Digital. La estructura de los logs y su detalle se encuentran en el “Documento técnico lineamientos de indicadores SCDE”.

- El Prestador de Servicios Ciudadanos Digitales Especiales debe revisar periódicamente si el “Documento técnico lineamientos de indicadores SCDE” ha sido actualizado, ya que el plazo máximo para aplicar las actualizaciones a los requerimientos será de 45 días calendario.

7.2 Requisitos para la integración del servicio de carpeta ciudadana digital y la coordinación de los prestadores con la Agencia Nacional Digital

A continuación, se describen los requisitos que deben cumplir los Prestadores de Servicios Ciudadanos Digitales Especiales en la prestación del servicio de carpeta ciudadana digital y su coordinación con la Agencia Nacional Digital.

7.2.1 Requisitos de los Prestador de Servicios Ciudadanos Digitales Especiales

Los prestadores de Servicios Ciudadanos Digitales Especiales deberán integrarse al servicio de autenticación digital para el manejo de las autorizaciones y autenticaciones de usuarios; de igual manera, necesitará contar con la integración al servicio de Interoperabilidad como medio seguro de comunicación entre su carpeta y las demás entidades vinculadas en la plataforma encontrándose entre ellas el articulador del servicio de Carpeta Ciudadana Digital.

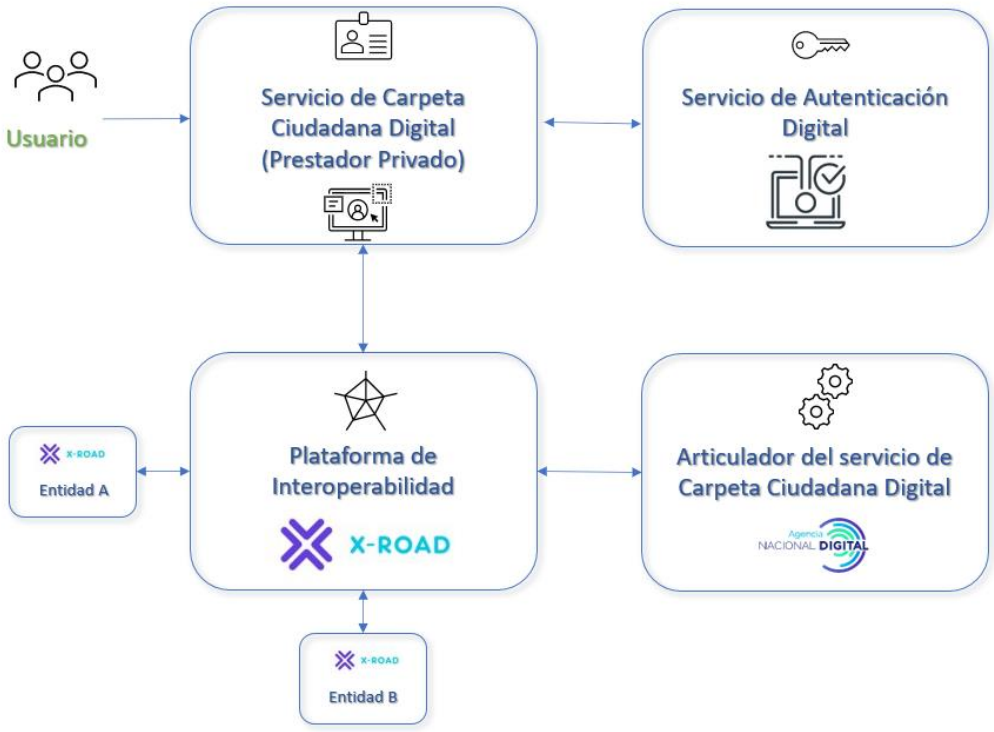


Ilustración 9. Diagrama general del servicio ciudadano de carpeta ciudadana digital
(Fuente: Suministrada por la Agencia Nacional Digital)

7.2.2 Seguridad de la información

7.2.2.1 Autorización e Identificación

Los Prestadores de Servicios Ciudadanos Digitales Especiales de carpeta ciudadana digital tienen que integrar su servicio de carpeta al servicio ciudadano de autenticación digital, esto quiere decir que solo pueden acceder a su información personas autenticadas e identificadas por este servicio, iniciando desde el nivel medio de autenticación digital.

Se debe garantizar que el consumo de la información esté acorde con el nivel de seguridad del servicio ciudadano de autenticación digital, esto significa que la información solo puede ser consumida si el nivel de seguridad del token de autenticación digital es igual al autorizado para el servicio.

7.2.2.2 Comunicación

Los servicios de comunicación que ofrece el Prestador de Servicios Ciudadanos Digitales Especiales a los Usuarios deben realizarse a través del protocolo HTTPS.

El Prestador de Servicios Ciudadanos Digitales Especiales de carpeta ciudadana digital debe realizar el intercambio de información con las demás entidades públicas o privadas a través de la plataforma de interoperabilidad X-Road.

7.2.2.3 Seguridad y protección de la información

El Prestador de Servicios Ciudadanos Digitales Especiales debe mantener los lineamientos y requisitos solicitados en temas de privacidad y seguridad de la información.

7.2.2.4 Observaciones adicionales

El Prestador de Servicios Ciudadanos Digitales Especiales debe implementar una política de tratamiento de datos personales, habeas data y términos y condiciones del uso del servicio.

El servicio de carpeta ciudadana digital no almacenará de manera permanente los datos presentados a los Usuarios y no será un espacio de almacenamiento de documentos para el Usuario.

Desde el servicio de carpeta ciudadana digital, el Usuario no podrá realizar ningún trámite ante alguna entidad, por lo cual el Usuario será redireccionado al portal único del Estado www.gov.co donde podrá iniciar el trámite.

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben ajustarse a las indicaciones que la Agencia Nacional Digital en su rol de Articulador establezca en relación al mantenimiento de su sistema y dispositivos con las últimas versiones, paquetes de servicios y parches, por medio de una actualización frecuente de su hardware, software y dispositivos de comunicación.

Los Prestadores de Servicios Ciudadanos Digitales Especiales deben estar pendientes de la hoja de ruta y evolución de los sistemas de la Agencia Nacional Digital.

Cuando el Prestador de Servicios Ciudadanos Digitales Especiales realice tratamiento de datos personales, deberá adoptar medidas de responsabilidad demostrada para garantizar el debido tratamiento de dicha información. Esas medidas deben ser apropiadas, efectivas, útiles, eficientes y demostrables, para garantizar la seguridad, la confidencialidad, la veracidad y calidad y el uso y la circulación restringida de esa información.

7.2.3 Interoperabilidad

Toda la comunicación con las entidades y con la Agencia Nacional Digital en su rol de Articulador del servicio de carpeta ciudadana digital debe realizarse usando el protocolo X-Road y la plataforma de interoperabilidad de la Agencia Nacional Digital.

7.2.4 Funcionalidad

El servicio de carpeta ciudadana digital que ofrezca el Prestador de Servicios Ciudadanos Digitales Especiales debe implementar como mínimo los servicios de consulta de información, historial de solicitudes, historial de trámites y consulta de alertas y comunicaciones. Estos servicios son provistos por las entidades usando los contratos definidos.

Adicionalmente, debe disponer los servicios de registro en prestador de carpeta ciudadana digital y de cambio de Prestador de Servicios Ciudadanos Digitales Especiales en cualquier momento, de acuerdo con los lineamientos del Articulador que se describen en este mismo documento en la sección de integración con la Agencia Nacional Digital en su rol de Articulador.

También, debe permitir al Usuario ver la lista de los diferentes Prestador de Servicios Ciudadanos Digitales Especiales de carpeta ciudadana digital con todos los beneficios que ofrece cada uno. Esta información de los distintos Prestadores de Servicios Ciudadanos Digitales Especiales la proporciona la Agencia Nacional Digital en su rol de Articulador mediante la exposición de un servicio Web.

Además, en cada inicio de sesión de un Usuario, el Prestador de Servicios Ciudadanos Digitales Especiales debe verificar que no esté registrado en otra carpeta ciudadana digital, si el Usuario está registrado en otra carpeta ciudadana digital no se debe permitir el ingreso. Esto se haría mediante la invocación de los servicios expuestos por la Agencia Nacional Digital en su rol de Articulador de carpeta ciudadana digital.

Asimismo, debe proporcionar un punto de entrada para admitir el cambio de Prestador de Servicios Ciudadanos Digitales Especiales de un Usuario hacia su servicio.

Igualmente, debe mantener los registros de auditoría de los servicios consumidos por los Usuarios de manera que se puedan extraer los datos, y así la Agencia Nacional Digital en su rol de Articulador genere estadísticas de número de Usuarios registrados en su carpeta, con cantidad de servicios consumidos diariamente por los Usuarios en donde se pueda discriminar por servicio.

El Prestador de Servicios Ciudadanos Digitales deberá estar en capacidad de generar logs de eventos y suministrarlos a la Agencia Nacional Digital. La estructura de los logs y su detalle se encuentran en el “Documento técnico lineamientos de indicadores SCDE”.

El Prestador de Servicios Ciudadanos Digitales Especiales debe revisar periódicamente si el “Documento técnico lineamientos de indicadores SCDE” ha sido actualizado, ya que el plazo máximo para aplicar las actualizaciones a los requerimientos será de 45 días calendario.

Así mismo, debe funcionar correctamente en los siguientes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge, Opera y Safari en sus versiones actualizadas.

7.2.5 Servicios web expuestos por la Agencia Nacional Digital en su rol de Articulador

Los servicios web que la Agencia Nacional Digital en su rol de Articulador pondrá a disposición para la integración de los Prestadores de Servicios Ciudadanos Digitales Especiales a través de X-Road se encuentran publicados en el documento “Documento Contratos Carpeta Ciudadana Digital” y deberán ser consumidos en su totalidad por el Prestador de Servicios Ciudadanos Digitales Especiales del servicio de Carpeta Ciudadana Digital.

NOTA: El Prestador de Servicios Ciudadanos Digitales Especiales deberá estar atento a las actualizaciones o los cambios realizados a la “Documento Contratos Carpeta Ciudadana Digital” para así cumplir con los requerimientos que la Agencia Nacional Digital solicita, el plazo máximo para aplicar las actualizaciones a los requerimientos será de 45 días calendario.

7.3 Requisitos para la integración del servicio de Interoperabilidad

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.

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.

El presente capitulo describe el proceso de vinculación de entidades privadas al Servicio Ciudadano Digital de Interoperabilidad. En la primera parte se presentan definiciones y requisitos técnicos.

Seguidamente se plantea la metodología de vinculación de entidades privadas y enlaces a los manuales de instalación y configuración de los servidores de seguridad de X-Road utilizados para exponer y consumir servicios de manera segura. Finalmente se describen las condiciones técnicas que deben satisfacer los certificados de confianza.

7.3.1 Esquema de Interoperabilidad

A continuación, se presenta el esquema de Interoperabilidad de la asociación de servicios y sus relaciones.

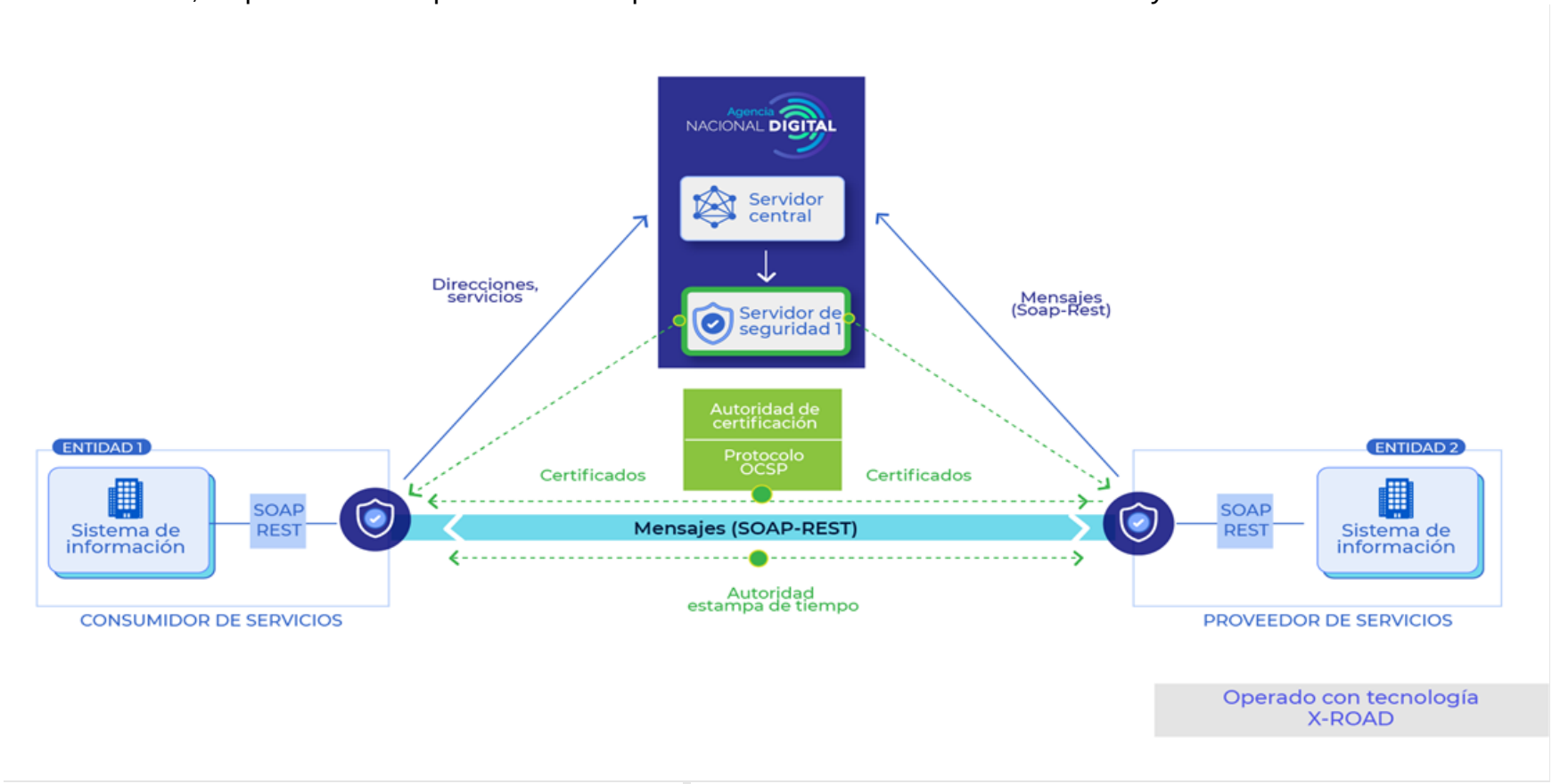


Ilustración 10. Esquema Interoperabilidad
(Fuente: Suministrada por la Agencia Nacional Digital)

La Agencia Nacional Digital en su rol de Articulador de los Servicios Ciudadanos Digitales administrará los componentes centrales de la plataforma de interoperabilidad, prestará a través de una Entidad de Certificación Digital acreditada ante el Organismo Nacional de Acreditación de Colombia, o la entidad que haga sus veces, los servicios de confianza (Certificados Digitales, estampa cronológica de tiempo y validación del estado de un certificado). 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 identificados 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 tres (3) instancias correspondientes a los ambientes de QA, Pre-producción 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 Miembro, este código permanece sin modificarse durante todo el tiempo de permanencia dentro del ecosistema.
- **Código del servidor de seguridad**: Código que identifica un servidor de seguridad de los demás servidores dentro del ecosistema.
- **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 (UpperCamelCase ó lowerCamelCase).

Los componentes del sistema se describen en la siguiente sección

7.3.2 Diagrama de componentes

Se presentan los principales componentes e interfaces del sistema X-Road. La Agencia Nacional Digital (AND) desempeña el papel de Articulador del servicio ciudadano de Interoperabilidad, suministrando y gestionando los componentes de la plataforma X-Road.

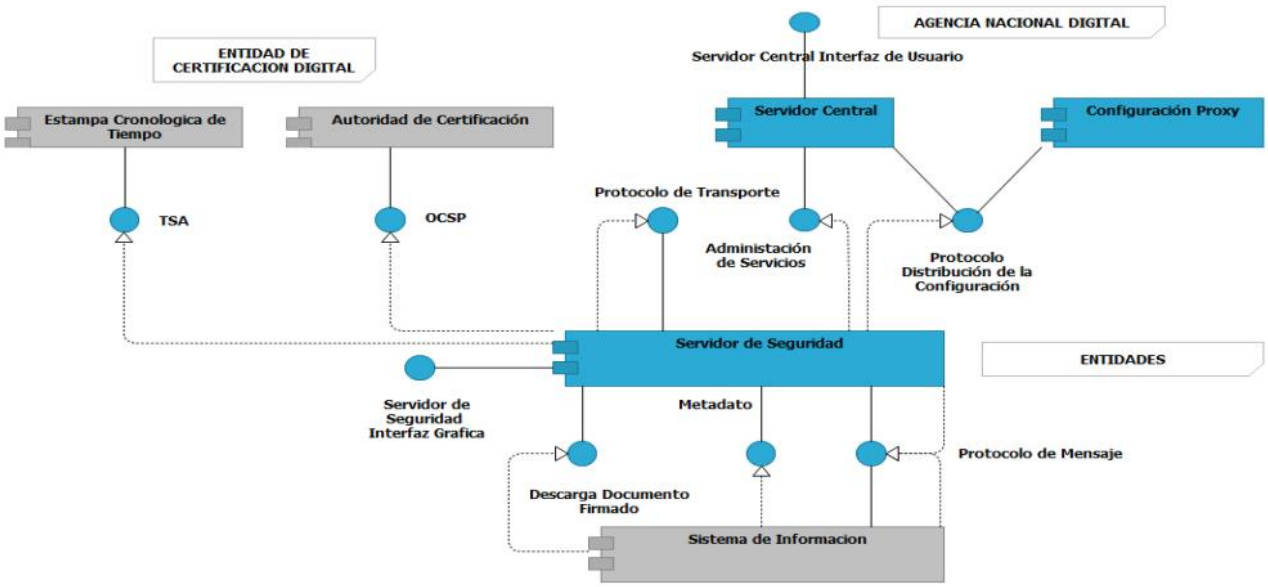


Ilustración 11. Arquitectura de Componentes
(Fuente: Suministrada por la Agencia Nacional Digital)

La Agencia Nacional Digital instala y presta mantenimiento al servidor central y al servidor de seguridad de administración de los servicios central, y valida los certificados de confianza. El proxy de configuración es un componente opcional que normalmente se usa para distribuir la configuración a instancias federadas de X-Road.

La conexión entre entidades se realiza pasando por servidores de seguridad hospedados en cada una de las entidades. Los servidores de seguridad tienen conexión entre sí y son aprobados y supervisados por el servidor central. Adicionalmente, los módulos de monitoreo están conectados al servidor central, al servidor de seguridad de administración o a los servidores de seguridad que hacen parte del ecosistema.

Si bien cada servidor de seguridad puede exponer y consumir servicios, para fines ilustrativos, uno de ellos se focalizará en la exposición de un servicio, y el otro

servidor tendrá la función de consumir el servicio que presta su contraparte. Los mensajes intercambiados reciben una firma de tiempo generada desde la Autoridad de Estampa de Tiempo.

7.3.3 Servidor de Seguridad de Administración

Luego de la configuración inicial del servidor de seguridad perteneciente a una determinada entidad, el servidor central se comunica con los servidores de seguridad de las entidades a través de los servicios de administración, los cuales convencionalmente son llevados a cabo dentro de un servidor de seguridad ubicado en el área de servicios centrales, estableciendo comunicación por los Puertos 5500 y 5577.

A este servidor de seguridad se le denomina servidor de administración, servidor de seguridad administrativa o servidor de seguridad central.

7.3.4 Servidor Central

El servidor central es administrado por la Agencia Nacional Digital, y se encarga de listar los servidores de seguridad y subsistemas válidos. A continuación, se describen las principales partes y operaciones presentes en el servidor central.

Ingreso de un Servidor de Seguridad: El proceso por el cual un servidor de seguridad se registra en el servidor central se denomina anclaje. La comunicación durante la configuración inicial entre el servidor de seguridad de una entidad y el servidor central, se lleva a cabo por los Puertos 80 y 4001.

Servicios de Confianza: La Agencia Nacional Digital genera dentro del servidor central la lista de Autoridades de Certificación Digital (CA) aprobadas y de autoridades de estampado cronológico de tiempo. Los servicios de confianza cargados en el servidor central permiten demostrar que una entidad interactuó con un servicio, permitiendo el no repudio. La comunicación entre los servidores de seguridad y los servicios de confianza es realizada por los Puertos 80 y 443.

Servicios de administración: Los servicios de administración son servicios proporcionados por la Autoridad de Gobierno de X-Road para administrar los servidores de seguridad.
Los servicios de administración son invocados por los servidores de seguridad, al momento de registrar en el servidor central los cambios de configuración realizados por el administrador del servidor de seguridad. Los servicios de administración son los siguientes:

- clientReg: registrar un subsistema X-Road como cliente del servidor de seguridad.
- clientDeletion: eliminar un cliente del servidor de seguridad.

- authCertReg: agregar un certificado de autenticación digital al servidor de seguridad.
- authCertDeletion: eliminar un certificado de autenticación digital del servidor de seguridad.
- ownerChange: cambiar el miembro propietario del servidor de seguridad.

Para más información sobre los servicios de administración, puede referirse al protocolo para servicios de administración de X-Road (NIIS Management Services, 2020).

7.3.5 Servidor de seguridad de Exposición

Es el servidor de seguridad configurado en la entidad que expone un servicio. Este mismo servidor se puede configurar para consumir servicios de otras entidades. Si los servicios a exponer son REST, no es necesario realizar ajustes a los servicios.

7.3.6 Servidor de Seguridad de consumo

Es el servidor de seguridad configurado como intermediario entre el sistema de información de la entidad que consume, y el servidor de seguridad de la entidad que expone el servicio. Este mismo servidor se puede configurar para exponer servicios.

7.3.7 Vinculación al servicio de Interoperabilidad

El Marco de Interoperabilidad proporciona la orientación necesaria a las entidades públicas / privadas 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.

7.3.8 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 Prestador de Servicios Ciudadanos Digitales Especiales en su integración a la Plataforma de Interoperabilidad.

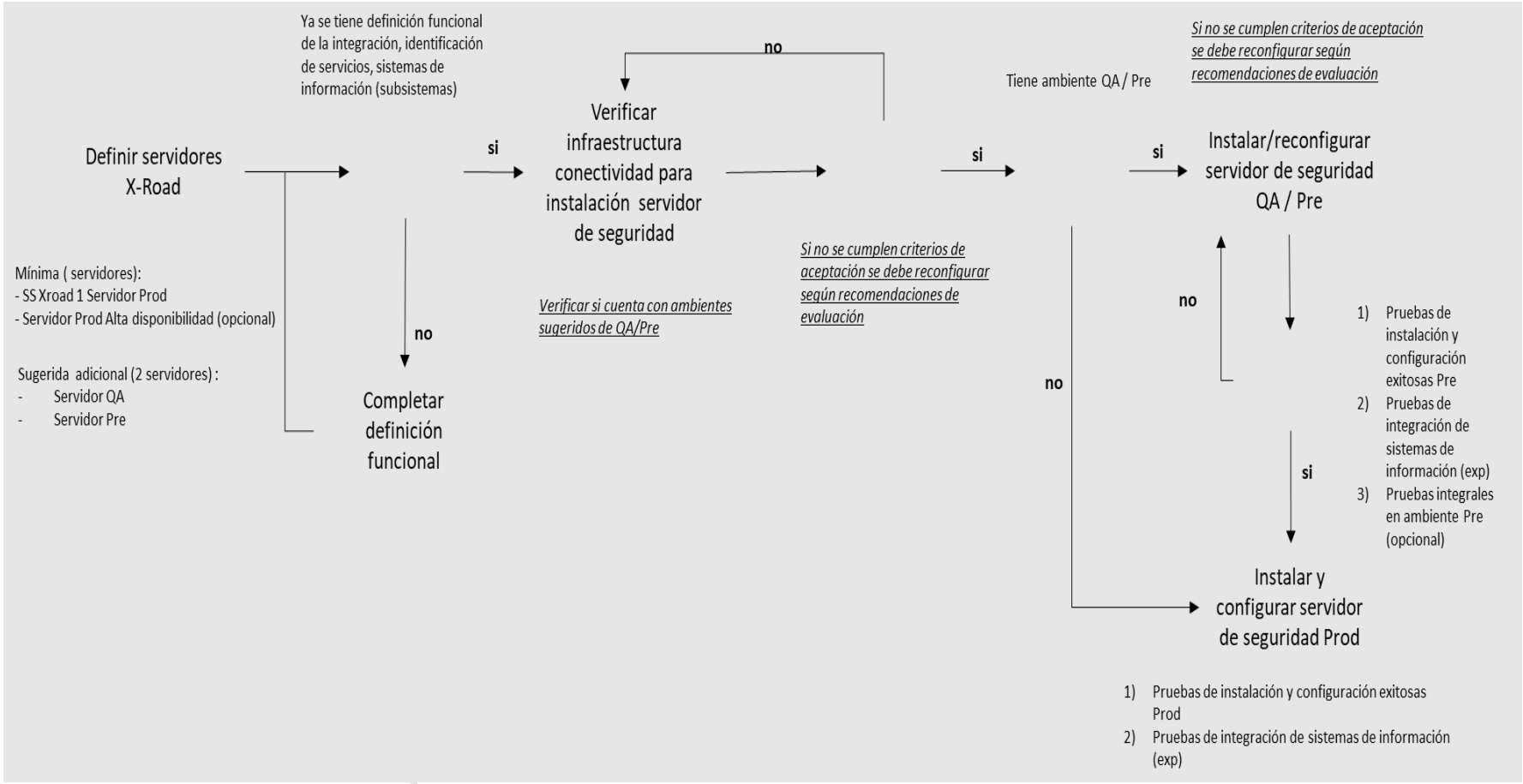


Ilustración 12. Instalación y configuración ambientes para el servidor de seguridad
(Fuente: Suministrada por la Agencia Nacional Digital)

Por medio de la siguiente tabla se describen los pasos y validaciones de la metodología.

Tabla 1 Metodología para la instalación y configuración del servidor de seguridad.

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 del Prestador de Servicios Ciudadanos Digitales Especiales de: Cuatro (4) servidores (Ambiente QA, ambiente pre-producción, producción, producción en alta disponibilidad). Como caso excepcional y luego de haber validado la carga transaccional de los servicios de consumo y exposición, del Prestador de Servicios Ciudadanos Digitales Especiales podría definir tres (3) servidores (Ambiente QA, ambiente pre-producción y producción sin alta disponibilidad). 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 pre-producción 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 del Prestador de Servicios Ciudadanos Digitales Especiales,

		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 de esta guía 2) Anclaje del servidor de seguridad al nodo central 3) Configuración de los subsistemas definidos para el miembro del ecosistema Si los pasos 1) y 2) ya se han realizado, se deberá entonces trabajar 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, verificar que las pruebas integrales hayan sido ejecutadas de manera exitosa. Si la validación es satisfactoria, se realiza la instalación en ambiente pre-productivo (ítem 6). De lo contrario, se deberá volver a la tarea anterior (ítem 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 del presente documento 2) Anclaje del servidor de seguridad al nodo central pre-productivo 3) Configuración de los subsistemas definidos para el miembro del ecosistema. Si los pasos 1) y 2) ya se han realizado, se deberá entonces trabajar 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 pre-producción. ✓ 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, sí aplica ✓ 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, sí 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 Servidor de Seguridad de X-Road. En este ítem se deben realizar las siguientes tareas: 1) Instalación del servidor de acuerdo al manual respectivo. 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 pre-producción. ✓ Formato de pruebas de integración de sistemas de información (aplica cuando el servicio es de exposición).

7.3.9 Requerimientos técnicos

7.3.9.1 Requerimientos para servidor de seguridad

A continuación, se describen las características mínimas que debe tener el servidor físico o virtual donde se instalará el componente del servidor de seguridad de X-Road.

Tabla 2. Requerimientos para servidor de seguridad

ÍTEM	REQUISITO	EXPLICACIÓN
1.0	Sistema Operativo Ubuntu 18.04 Long-Term Support (LTS), 64 bits. Nota: Los servidores de seguridad pueden ser físicos o virtuales.	X-Road soporta únicamente estas versiones en sistemas operativos
1.1	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 RHEL-7 o Ubuntu en general.
1.2	6 GB de RAM	Memoria RAM mínima requerida. de acuerdo con la transaccionalidad de la entidad pude aumentar el requerimiento de memoria RAM
1.3	20 GB de espacio libre en disco (partición del Sistema Operativo) 20-40 GB de espacio libre en disco (/var/partición).	Almacenamiento mínimo requerido.
1.4	Para la instalación del servidor de seguridad, se requiere que el servidor instalado tenga conectividad a internet para acceder a los repositorios de instalación que se detallan en el anexo técnico.	Acceso a repositorios de instalación
1.5	Una tarjeta de interfaz de red de 1000 Mbps.	Red mínima requerida
1.6	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	Segmentación de Red y Seguridad.

	administración del Sistema Operativo (como Sistema de Nombres de Dominio, NTP y SSH) se encuentran fuera del alcance de esta guía. Si el servidor de seguridad tiene una Dirección IP privada, se debe crear un registro NAT en el firewall.	

7.3.9.2 Preparación para servidor de seguridad

Para la instalación del servidor de seguridad el Prestador de Servicios Ciudadanos Digitales Especiales deberá hacer las siguientes configuraciones:

Tabla 3. Preparación para servidor de seguridad

ÍTEM	REQUISITO	EXPLICACIÓN
1.0	https://[URL_REPOSITORIO COLOMBIA]	Repositorio de paquetes X-Road
1.1	[CLAVE REPOSITORIO COLOMBIA]	La clave del repositorio
1.2	Conexiones entrantes	Puerto para conexiones entrantes (desde la red externa al servidor de seguridad)
	TCP 5500	Intercambio de mensajes entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (en la lista blanca solo de AND IP y Nodos).
	TCP 5577	Consulta de respuestas OCSP entre servidores de seguridad. Se recomienda utilizar el filtrado de IP (en la lista blanca solo de AND IP y Nodos)
	TCP 9011	Puerto de escucha JMX del demonio de monitoreo de datos operativos
	TCP 9999	Puerto de escucha JMX del demonio de monitoreo ambiental
1.5	Conexiones salientes	Puertos para conexiones salientes (desde el servidor de seguridad a la red externa)
	TCP 5500	Intercambio de mensajes entre servidores de seguridad.
	TCP 5577	Consulta de respuestas OCSP entre servidores de seguridad.

	TCP 4001	Comunicación con el servidor central. Luego de anclarse, se deberá deshabilitar.
	TCP 80	Descarga de la configuración global desde el servidor central. Luego de anclarse, se deberá deshabilitar (externo).
1.6	TCP 4000	Interfaz de usuario (red local). ¡No debe ser accesible desde internet!
1.7	TCP 80, 443	Puntos de acceso al sistema de información (en la red local). ¡No debe ser accesible desde internet!
	TCP 9011	Puerto de escucha JMX del demonio de monitoreo de datos operacionales
1.8	Direcciones IP	Direcciones IP públicas y locales (únicamente del servidor del Prestador de Servicio Ciudadanos Digitales Especiales) de servidores de seguridad y nombre (s) de host con las entidades y los Prestadores de Servicio Ciudadanos Digitales Especiales con los que se intercambia información.
1.13	IP PÚBLICA	Monitoreo de seguridad del servidor IP en instancia de Gobierno

Una vez se dispone el Sistema Operativo base, se ingresan las configuraciones de usuario, se establece la configuración regional del sistema para que posteriormente se instalen los paquetes de plataforma X-Road Colombia.

Si durante la instalación se generan errores, algunos de los más comunes se encuentran documentados en los manuales de instalación y configuración. En caso de requerir soporte puede contactar a la Agencia Nacional Digital.

Frente a la preparación del Sistema Operativo, es necesario que cuente con las siguientes características, las cuales garantizan que se cumplan con todos los lineamientos necesarios para interoperar.

Consideraciones para tener en cuenta para servidor de administración de seguridad en el momento de alistamiento:

- Se debe tener acceso a los repositorios y actualizaciones en el sistema donde se va a realizar la instalación.
- Verificar en el firewall no tener restricciones de navegación tales como puertos cerrados, acceso a páginas donde están alojados los repositorios de X-Road.
- Tener permisos sobre las IPs o dominios que van a interoperar con el servidor.
- El servidor debe estar en el mismo segmento o poder acceder a los servicios web de la entidad.

7.3.10 Proceso de configuración de X-Road

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).

7.3.11 Características de los certificados

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. Sólo se reconocerán certificaciones emitidas por las entidades acreditadas, o quien haga sus veces, según el cápitulo 48 del Decreto 1074 de 2015, o la norma que lo adicione, modifique o sustituya.

La Agencia Nacional Digital registra en el servidor central tantas autoridades 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. Todas las Autoridades de Certificación Digital de Colombia, o quien haga sus veces, tienen una subordinación, una Autoridad de Certificación subordinada. 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.

7.3.11.1 Proceso de solicitud de certificados digitales

Para realizar la conexión de los servidores de seguridad de los Prestadores de Servicios Ciudadanos Digitales Especiales entidades y sus servicios al ecosistema de producción de X-Road, el Prestador de Servicios Ciudadanos Digitales Especiales deberá adquirir un certificado de autenticación digital y un certificado de firma a una de las autoridades de certificación digital con acreditación vigente según lo definido por la entidad de la que trata el Cápitulo 48 del Decreto 1074 de 2015, o quien haga sus veces, o la norma que lo adicione, modifique o sustituya, para que estos sean importados en el servidor de seguridad al momento de la configuración.

La Autoridad de Certificación Digital, o quien haga sus veces, dispondrá de un mecanismo para que el Prestador de Servicios Ciudadanos Digitales Especiales pueda realizar la solicitud de los certificados y realizar 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:

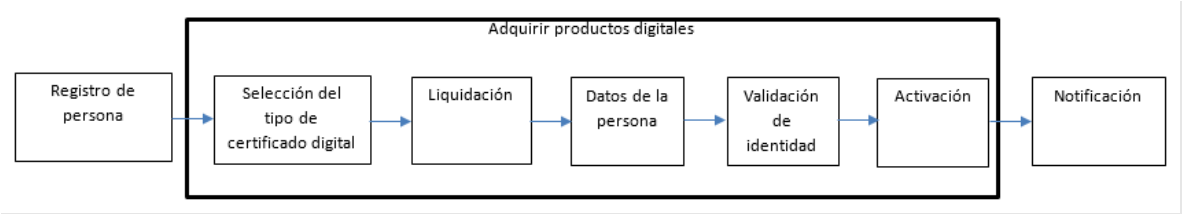


Ilustración 13. Proceso de solicitud de certificados
(Fuente: Suministrada por la Agencia Nacional Digital)

Elaborado por: Agencia Nacional Digital.

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

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

Liquidación: Los certificados digitales son entregados a la entidad. En este paso el Prestador de Servicios Ciudadanos Digitales Especiales deberá seleccionar el paquete “Convenio Agencia Nacional Digital – 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 del Prestador de Servicios Ciudadanos Digitales Especiales 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 el Prestador de Servicios Ciudadanos Digitales Especiales.

Activación: La Autoridad de Certificación Digital, o quien haga sus veces, 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.

Ilustración 14. Proceso de firma de certificados
(Fuente: Suministrada por la Agencia Nacional Digital)

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, o quien haga sus veces. 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, o quien haga sus veces.

7.3.11.2 Condiciones técnicas de los certificados

Los Prestadores de Servicios Ciudadanos Digitales Especiales 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 por la Autoridad de Certificación Digital, o quien haga sus veces, son firmados por la Subordinada de la Autoridad 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 Autoridad de Certificación Digital – CA, o quien haga sus veces, 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:

1. Emitido por: Certificado subordinado de la Autoridad de Certificación Digital.
2. Algoritmo de firma: SHA256.
3. Uso de Claves: Sin repudio
4. 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 Autoridad de Certificación Digital, o quien haga sus veces, debe estar acreditada por la entidad de la que trata el cápitulo 48 del Decreto 1074 de 2015, o la norma que lo adicione, modifique o sustituya, dando cumplimento 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.

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, o quien haga sus veces, 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. La Autoridad de Certificación, o quien haga sus veces, debe estar acreditada por la entidad de la que trata el Capitulo 48 del Decreto 1074 de 2015, o la norma que lo adicione, modifique o sustituya, dando cumplimento al artículo 161 del Decreto Ley 019 de 2012 en la siguiente actividad:

   a. Ofrecer o facilitar los servicios de registro y estampado cronológico en la generación, transmisión y recepción de mensajes de datos.

7. 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.

8. 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: https:// 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.

9. Las consultas al servicio de Autoridad de Estampa de Tiempo deben realizarse sin usuario y contraseña, ya que dentro de la configuración de la Autoridad de Estampa de Tiempo en la plataforma de X-Road no es posible parametrizar un usuario y contraseña para su autenticación digital, como medida de seguridad, se deben restringir las IP's de acceso a este método.

10. 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.

11. El Prestador de Servicios Ciudadanos Digitales Especiales 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, o quien haga sus veces. 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.