



Arquitectura Digital de Referencia DPC-BID

Información del documento

Título:		**Versión No:**	1
Preparado por:		**Fecha de producción:**	12/06/2020
Revisado por:		**Fecha de revisión:**	

Lista de distribución

Control de versiones

Versión	Fecha	Descripción	Participantes
0.9	12/06/2020	Versión inicial del documento, arquitectura de sistemas de información, tecnológica y seguridad.	ARMANDO FRADE BELLO, ERNESTO MEDINA, SANDRA GONZALEZ
1.0	27/07/2020	Primer Draft de la arquitectura de referencia.	ARMANDO FRADE BELLO, ERNESTO MEDINA, SANDRA GONZALEZ
1.1	25/08/2020	Fortalecimiento de Arquitectura de Seguridad	ERNESTO MEDINA L.
1.2	16/10/2020	Aclaraciones en Arquitectura Tecnológica.	ERNESTO MEDINA L.
1.3	5/11/2020	Primera versión de la arquitectura de referencia.	ARMANDO FRADE BELLO, ERNESTO MEDINA, SANDRA GONZALEZ

Propósito del documento:

Este documento contiene la definición de los elementos y artefactos que hacen parte de la arquitectura digital de Referencia para la DPC (incluye los dominios de arquitectura (información, sistema de información y tecnología), pero además por su relevancia se incluyen tres dominios adicionales: Interoperabilidad, GIS y Seguridad.

Todo lo anterior se presenta desde la perspectiva de la línea base y las transiciones que se deben seguir para llegar a la arquitectura objetivo.

1 CONTEXTO ESTRATÉGICO 4

2 LINEA BASE DE ARQUITECTURA 8

2.1 NIVEL DE MADUREZ DE ARQUITECTURA 8
2.2 ARQUITECTURA DE INTEROPERABILIDAD 11
2.2.1 NIVEL DE MADUREZ DE INTEROPERABILIDAD 11

3 ARQUITECTURA OBJETIVO 13

3.1 PRINCIPIOS 13
3.2 PILARES DE LA ARQUITECTURA DIGITAL 14
3.3 ARQUITECTURA TECNOLÓGICA. 15
3.3.1 ARQUITECTURA CONCEPTUAL 15
3.3.2 HIPER-AUTOMATIZACIÓN. 16
3.3.3 GESTIÓN DE NUBE. 16
3.4 ARQUITECTURA DE INFORMACIÓN 17
3.4.1 ARQUITECTURA CONCEPTUAL 17
3.4.2 ARQUITECTURA TÉCNICA 20
3.5 ARQUITECTURA DE SISTEMAS DE INFORMACIÓN Y APLICACIONES 23
3.5.1 ARQUITECTURA CONCEPTUAL 23
3.5.2 ARQUITECTURA TÉCNICA 24
3.6 ARQUITECTURA DE SEGURIDAD 26
3.6.1 ADMINISTRACIÓN DE IDENTIDAD 26
3.6.2 SEGURIDAD DE APLICACIONES 27
3.7 ARQUITECTURA DE INTEROPERABILIDAD 28
3.7.1 ARQUITECTURA CONCEPTUAL 28
3.7.2 ARQUITECTURA TÉCNICA. 31
3.7.3 X-ROAD Y LENGUAJE DE INTERCAMBIO MINTIC. 32
3.8 ARQUITECTURA INFORMACIÓN GEOGRÁFICA (SIG) 33
3.8.1 ALMACENAMIENTO DE DATOS 34
3.8.2 SERVIDOR WEB 35
3.8.3 SERVIDOR ARCGIS SERVER 36
3.8.4 ADMINISTRACIÓN Y ESTRUCTURACIÓN DE DATOS 36
3.8.5 SUSCRIPCIÓN ARCGIS ONLINE 37
3.8.6 DESARROLLO DE APLICACIONES WEB GEOGRÁFICAS 37

4 PORTAFOLIO DE PROYECTOS 38

5 GLOSARIO/DEFINICIONES. 40

1 CONTEXTO ESTRATÉGICO

Conforme con los postulados constitucionales la Defensoría del Pueblo forma parte del Ministerio Público (MP), ejerce sus funciones en coordinación con la Procuraduría General de la Nación, y le corresponde esencialmente velar por la promoción, el ejercicio y la divulgación de los derechos humanos. En este sentido, la Defensoría del Pueblo goza de autonomía administrativa y presupuestal y es responsable de impulsar el ejercicio, divulgación, promoción, protección y defensa de los derechos humanos, así como prevenir sus violaciones, fomentar la observancia del Derecho Internacional Humanitario; atender, orientar y asesorar en el ejercicio de sus derechos a los habitantes del territorio nacional y a los colombianos en el exterior; y, proveer el acceso a la administración de justicia.

Por su parte, el Banco Interamericano de Desarrollo (BID), es un organismo multilateral de crédito cuyo propósito principal es financiar proyectos de desarrollo de tipo económico, social e institucional orientados a reducir la pobreza en América Latina y el Caribe, así como a fomentar su crecimiento sostenible. Es una de las principales fuentes de financiamiento del desarrollo en América Latina y el Caribe[1] y actualmente se encuentra financiando, entre otros, programas de fortalecimiento institucional en diferentes entidades del Gobierno nacional y del Ministerio Público, como es el caso de los que se encuentran implementado la Procuraduría General de Nación, la Contraloría General de la República y la Defensoría del Pueblo de Colombia, orientados a modernizar dichas entidades buscando mayor coordinación, eficiencia y eficacia en su gestión.

En el marco de lo expuesto, la Defensoría del Pueblo ha buscado constantemente optimizar su gestión y actuación institucional, de ahí que con el apoyo del BID emprendiera una serie de acciones orientadas al desarrollo de un programa que apuntara a la modernización de los sistemas de control, la promoción de la transparencia y la integridad pública como elementos esenciales para el desarrollo económico y social del país, partiendo de los resultados obtenidos en el año 2017 del análisis realizado por el BID, en el cual se concluyó que “es necesario fortalecer la capacidad institucional mediante la implementación de un modelo de gestión defensorial por resultados (MGDR)(Mendiburu, Morales, & Pereza, 2018)”.

En virtud de lo anterior, el 18 de mayo de 2018 el Consejo de Política Económica y Social emitió mediante Documento CONPES 3925 su “concepto favorable para contratar un empréstito externo con la Banca Multilateral hasta por USD 18 millones, o su equivalente en otras monedas, destinado a financiar el Programa de Fortalecimiento de la Capacidad Institucional de la Defensoría del Pueblo de Colombia”, a partir de lo cual el 8 de octubre de 2018, la República de Colombia y el BID suscribieron el Contrato de Préstamo BID 4550/OC-CO, con el objeto de contribuir a la financiación y ejecución del citado Programa.

Dicho programa es administrado directamente por la Defensoría del Pueblo y se tiene previsto que su ejecución se lleve a cabo en un periodo de estimaci años. Su objetivo es mejorar la efectividad de la gestión institucional de la DPC, lo cual implica (i) incrementar la eficiencia y eficacia en la gestión institucional; (ii) mejorar la calidad y eficiencia en los servicios que presta la DPC; y (iii) fortalecer la rendición de cuentas y la participación ciudadana. Lo anterior representa un esfuerzo por mejorar la capacidad institucional de la DPC de manera transversal, poniendo a su disposición nuevos modelos y herramientas de gestión que apoyen las funciones misionales.

Es preciso señalar que el alcance de este Programa, en principio se articuló con lo dispuesto en el segundo objetivo de la estrategia de buen gobierno del Plan Nacional de Desarrollo 2014 – 2018 "Todos por un nuevo País", expedido mediante Ley 1753 de 2015, que se enfocó en la lucha contra la corrupción, transparencia y rendición de cuentas. Así mismo se encuentra alineado con lo establecido en el "Pacto por la Legalidad: seguridad efectiva y justicia transparente para que todos vivamos con libertad y democracia", incluido en las bases del Plan Nacional de Desarrollo que hacen parte integral de la Ley 1955 de 2019 "Por el cual se expide el Plan Nacional de Desarrollo 2018 -2022 "Pacto por Colombia, pacto la equidad", y el cual insta, entre otras, a la Procuraduría General de la Nación y a la Defensoría del Pueblo a promover la coordinación, eficiencia, eficacia y modernización del Ministerio Público.

El Programa se encuentra estructurado en tres componentes de tipo técnico y un último componente que prevé los recursos para la administración del Programa, tal como se señala a continuación:

Componente 1. Fortalecimiento de la gestión y la planeación estratégica
Componente 2. Atención y servicios al ciudadano
Componente 3. Rendición de cuentas y participación ciudadana.

Componente 1. Fortalecimiento de la Gestión y Planeación Estratégica: Busca mejorar la eficiencia y eficacia de la DPC mediante el fortalecimiento de capacidades de planeación y gestión estratégica. Está integrado por diez (10) Subcomponentes, así:

1. Diseño e implementación de un Modelo de Gestión Defensorial por Resultados (MGDR) que incluirá los sistemas de planeación estratégica, presupuestación, monitoreo y evaluación. Así mismo, incluirá una línea de generación de resultados y un mecanismo de medición de impacto en materia de género, con el propósito de reforzar su atención.
2. Diseño e implementación de una metodología para gestionar alertas y/o recomendaciones incluyendo criterios de priorización, monitoreo y seguimiento poblacional, temático y territorial.
3. Diseño e implementación de una herramienta de monitoreo, análisis y seguimiento de alertas y/o recomendaciones que soporte la metodología diseñada.
4. Diseño e implementación de un Modelo de Arquitectura Empresarial, Arquitectura de Software y Gobierno de TIC y Datos conforme a los lineamientos de MINTIC.
5. Diseño e implementación de un Modelo de Inteligencia de Negocios y Analítica.
6. Diseño e implementación de un Sistema Integrado para la Gestión Defensorial, incluyendo un tablero de control de soporte al MGDR y un instrumento de reportes internos y externos.
7. Diseño e implementación de una plataforma de visualización y georreferenciación de la gestión de la DPC (Mapa Defensorial).
8. Adquisición de servicios, infraestructura y software.
9. Capacitación y gestión del cambio para la asimilación del MGDR y TIC.
10. Diseño e implementación de un piloto para fortalecer la coordinación institucional con la PGN y las Personerías. Los lineamientos y políticas para el diseño e implementación de TIC tendrán en consideración especificaciones orientadas a gestionar información y conocimiento con perspectiva de género y poblaciones vulnerables.

Componente 2. Atención y Servicio al Ciudadano: Busca mejorar la calidad y eficiencia en la atención y prestación de servicios al ciudadano. Está integrado por cinco (5) Subcomponentes, así:

a. Diagnóstico de procesos de gestión de requerimientos ciudadanos identificando brechas que afectan su desempeño. Este diagnóstico comprenderá un análisis de brechas en la gestión de requerimientos en materia de género y poblaciones vulnerables.

b. Diseño e implementación de un modelo de atención de requerimientos ciudadanos con base en el diagnóstico realizado. El modelo incorporará lineamientos y herramientas que permitan gestionar requerimientos ciudadanos en materia de género y poblaciones vulnerables.
c. Diseño, implementación y evaluación de una estrategia para ampliar la cobertura en la prestación de servicios y la atención a poblaciones vulnerables a nivel territorial.
d. Diseño e implementación de un sistema de relacionamiento con los ciudadanos con diversos canales de acceso.
e. Herramienta tecnológica para la gestión de conocimiento en defensoría pública diseñada e implementada.

Componente 3. Rendición de Cuentas y Participación Ciudadana: El objetivo es mejorar la rendición de cuentas y la participación ciudadana. Está integrado por tres (3) Subcomponentes, así:

1. Fortalecimiento de la estrategia de rendición de cuentas, participación ciudadana e incidencia en políticas públicas a nivel nacional. Este Subcomponente incluye: (a) un diagnóstico del estado actual de los mecanismos de rendición de cuentas, participación ciudadana e incidencia en políticas públicas existentes. Esta estrategia concebirá una línea de trabajo específica con enfoque de género y poblaciones vulnerables; (b) el levantamiento de la línea base sobre rendición de cuentas, participación ciudadana e incidencia en políticas públicas de la gestión defensorial; y (c) el diseño e implementación de la estrategia de rendición de cuentas y participación ciudadana.
2. Rediseño e implementación del portal web para el acceso y promoción de la oferta multi-canal habilitando mecanismos interactivos para la administración y consulta de contenidos.
3. Diseño e implementación de un modelo de promoción, divulgación y comunicaciones de la oferta institucional que comprende: (a) un diagnóstico del estado actual de los procesos y mecanismos de promoción, divulgación y comunicaciones existentes; (b) el diseño y aplicación de encuestas de percepción tanto a agentes públicos y privados como a la ciudadanía, con el objetivo de recabar información sobre la evolución de las demandas ciudadanas a la DPC; y (c) el diseño e implementación del modelo de promoción, divulgación y comunicaciones.

A partir de las actividades que se han planificado ejecutar en el marco de cada uno de los componentes y subcomponentes señalados, se espera que con la puesta en marcha del Programa se logre mayor efectividad de la gestión institucional, lo cual se verá reflejado en (i) una mayor eficiencia y eficacia de la gestión institucional medida por un cambio en la eficiencia en la gestión, entre otras cosas, en la emisión de alertas y/o recomendaciones; (ii) un aumento en el cumplimiento de lineamientos de MINTIC; (iii) una mejora en la calidad y eficiencia en la atención y prestación de servicios al ciudadano medida por un cambio en el porcentaje de requerimientos ciudadanos resueltos favorablemente; (iv) un cambio en el porcentaje de requerimientos ciudadanos sobre temas de género resueltos favorablemente; (v) un cambio en el tiempo promedio de respuesta a requerimientos ciudadanos; (vi) un aumento en la cobertura de servicios de la DPC a poblaciones vulnerables; (vii) una mejora en la rendición de cuentas y la participación ciudadana medida por un cambio en la participación ciudadana y (viii) una mejora en la confianza de la ciudadanía en la DPC.

La Defensoría enfrenta una serie de desafíos en materia de gestión pública que pueden inhibir el cumplimiento efectivo de los objetivos del Plan de Desarrollo 2016 – 2020, Estos desafíos son:

(i) Modernizar la capacidad de TIC para apoyar y desarrollar la gestión estratégica. que se evidencia principalmente en la cobertura actual1 que como se señala en el diagnóstico “Actualmente los sistemas misionales de la Defensoría dan cobertura al 44% de los conceptos fundamentales del negocio. Este porcentaje se debe principalmente a que no todos los procesos misionales se encuentran cubiertos por tecnologías de información diferentes a la ofimática, como es el caso

[1] Cobertura de Aplicativos Misionales (Fuente: Diagnostico Situación Tic Consultoría Gtp)

de “Promoción y Divulgación” y las Defensorías delegadas, con excepción de la delegada de víctimas quienes hacen uso de FUD2 y SIIJYP3

(ii) Mejorar la capacidad de gestión de Tecnología4. Esto se explica por:

a. la poca visibilidad del área de tecnología dentro de la estructura organizacional;
b. la escasez de esquemas que promuevan el uso eficiente de los recursos de TIC que por su obsolescencia dificultan el desarrollo de los procesos;
c. El estado de la Arquitectura de la Información: Si bien la entidad cuenta con sistemas de gestión de bases de datos internacionalmente reconocidos, la información se encuentra dispersa en base de datos asiladas que no satisfacen las necesidades de un área/proceso especifico, no se tiene una visión holística de la información institucional que permita generar indicadores de gestión globales para la toma de decisiones en oportunidad y con calidad de información;
d. El estado de la Arquitectura de sistemas de Información: Los sistemas de información existentes, si bien cumplen con lo mínimo requerido, dada su arquitectura y herramientas de desarrollo utilizadas, no cumplen con estándares en cuanto a usabilidad, seguridad e interoperabilidad; en consecuencia, inducen la duplicidad, reproceso y generación de estadísticas poco confiables;
e. El estado de la Arquitectura de Servicios Tecnológicos: Existe un alto nivel de insatisfacción por parte de las áreas usuarias con el servicio recibido por parte del proceso de TIC, no se tienen estadísticas ni acuerdos de niveles de servicio que permita medir la gestión y plantear planes de mejoras, no se tienen políticas de copias de respaldo para la información sensible residentes en estaciones de trabajo de los funcionarios, los backup a nivel de servidores se realiza de manera artesanal, sin políticas de retención dado que no se dispone de recursos tecnológicos para la gestión de aseguramiento de información, no se dispone de un plan de contingencia o recuperación de desastres.

---

2 FUD: El Formulario Único de Declaración (Ley 1448 de 2011)

3 SIIJYP: Sistema de Información. Interinstitucional de Justicia y Paz (Decreto 299 de 2010)

4 COBERTURA DE APLICATIVOS MISIONALES (FUENTE: DIAGNOSTICO SITUACIÓN TIC CONSULTORÍA GTP)

2 LINEA BASE DE ARQUITECTURA

2.1 Nivel de madurez de arquitectura

En el BID no se identificaron ejercicios anteriores de arquitectura empresarial, por lo tanto, se realizó una evaluación de madurez del esquema de arquitectura que permite identificar de acuerdo con un referente la situación de partida y los elementos que se deben desarrollar en términos de arquitectura.

Teniendo en cuenta las recomendaciones del OPEN GROUP[5] y del MINTIC en el Modelo de Arquitectura Empresarial, se utilizó como referente el Modelo de Madurez de Capacidades de Arquitectura del Departamento de Comercio de Estados Unidos con su correspondiente adaptación al contexto de la DPC, este modelo provee un marco de trabajo que incluye los componentes clave de un proceso de arquitectura empresarial productivo. El modelo comprende 5 niveles de madurez de 9 elementos a evaluar[6], cuya definición se resume a continuación

[5] Recomendación tomada de Open Group en: https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap45.html
[6] Definiciones generales del US DoC ACMM Framework en: http://www.aprocessgroup.com/atpl/index.htm

	No existe*	Iniciado	En Desarrollo	Definido	Gestionado	Medible
Proceso de arquitectura		Procesos adhoc y localizados. Algunos procesos de arquitectura están definidos. No hay procesos de arquitectura en los procesos de gestión de tecnología o en los procesos misionales. El éxito de las iniciativas depende de esfuerzos individuales.	Se ha documentado el proceso de gestión de arquitectura de acuerdo con las recomendaciones del marco de referencia de arquitectura. Se han definido roles y responsabilidades claras.	La arquitectura está definida y se ha comunicado a todo el equipo tanto de IT como de gestión misional, con sus correspondientes responsabilidades. El proceso definido se ejecuta.	La arquitectura empresarial hace parte de la cultura Se miden indicadores de calidad asociados con el proceso de arquitectura.	Hay un esfuerzo consciente por la optimización y mejoramiento continuo del proceso de arquitectura.
Desarrollo de la arquitectura		Los procesos de arquitectura empresarial, su documentación y estándares son particulares a cada caso, se distribuyen en diversos medios adhoc y son informales.	La visión, principios, alineación con la misión, la línea base de arquitectura y la arquitectura objetivo están identificadas. Los estándares de arquitectura existen, pero no necesariamente están relacionados con la arquitectura objetivo. Hay modelos de referencia técnicos y marco de referencia de estándares establecidos.	Existe un análisis de brechas y un plan de transición completado. Los modelos de referencia están desarrollados. Los objetivos de IT y los métodos están identificados.	La documentación de la arquitectura empresarial está actualizada y refleja la situación actual. Las arquitecturas misionales, de datos, de aplicaciones y de tecnología están definidas por estándares apropiados tanto obligatorios por disposiciones del Gobierno como de facto.	Se utilizan los estándares y excepciones definidas para mejorar el proceso de arquitectura.
Alineación con la misión		Alineación mínima con la estrategia y con los objetivos misionales	Alineación explícita con las estrategias misionales y sus drivers	La arquitectura empresarial está integrada con la planeación y se tiene un control de la inversión.	La planeación y la inversión se controlan y se ajustan de acuerdo con la retroalimentación recibida y las lecciones aprendidas de la arquitectura empresarial. Se hace una revisión periódica de los drivers de la misión.	Los indicadores definidos en el proceso de arquitectura son utilizados para optimizar y orientar la alineación con la misión. Las áreas de negocio se involucran continuamente en la mejora de proceso de arquitectura empresarial.
Involucramiento de alto nivel		Conciencia o implicación limitada del equipo directivo en el proceso de arquitectura.	Se tiene conciencia a nivel gerencial y directivo del esfuerzo que conlleva la arquitectura.	El equipo directivo es consciente apoya el proceso de arquitectura de toda la empresa. La administración apoya activamente los estándares de arquitectura.	Equipo directivo directamente involucrado en el proceso de revisión de la arquitectura.	Participación de la alta dirección en la optimización de las mejoras de procesos en el desarrollo y la gobernanza de la arquitectura.

	No existe*	Iniciado	En Desarrollo	Definido	Gestionado	Medible
Participación de las unidades operativas		Aceptación limitada de las unidades operativas en el proceso de arquitectura.	Se asignan responsabilidades y se trabaja en ellas.	La mayoría de las unidades operativas aceptan y trabajan en el proceso de arquitectura empresarial.	Todas las unidades operativas aceptan y trabajan activamente en el proceso de arquitectura empresarial	Las retroalimentaciones del proceso de arquitectura de todas las unidades operativas se usan para las mejoras del proceso de arquitectura.
Comunicación de la arquitectura		La última versión de la documentación de arquitectura empresarial se encuentra en el repositorio especial para este fin. Existe poca comunicación sobre el proceso de arquitectura empresarial y sus posibles mejoras.	El repositorio de arquitectura empresarial se actualiza periódicamente y ya están familiarizados con los entregables de arquitectura.	Los documentos de arquitectura actualizados regularmente en el repositorio de arquitectura.	Los documentos de arquitectura son actualizados regularmente en el repositorio y se incluyen ultimas definiciones de arquitectura y estándares.	Todos los responsables de la toma de decisiones de la organización utilizan los documentos de arquitectura para cada decisión empresarial relacionada con TI.
Seguridad informática		Las consideraciones de seguridad informática son ad hoc y situacionales.	La arquitectura de seguridad informática tiene definidos los roles y responsabilidades claramente	Los estándares de la arquitectura de seguridad se han desarrollado y están integrados a la arquitectura.	Se hacen mediciones de indicadores asociados a la arquitectura de seguridad informática.	Se retroalimentan los indicadores de la arquitectura de seguridad y se usan para mejoramiento del proceso.
Gobernanza de la arquitectura		No hay definición explícita de estándares de gobernanza de la arquitectura.	Se definen algunos estándares para gobernanza y se siguen algunos estándares existentes.	Gobernanza explícita de la mayoría de las inversiones en TI.	Gobernanza explícita de todas las inversiones en TI. Los procesos formales para gestionar las desviaciones se retroalimentan en la arquitectura empresarial.	Gobernanza explícita de todas las inversiones en TI. Se utiliza un proceso de estándares y excepciones para mejorar el proceso de gobernanza.
Proceso de adquisición de TI e inversiones TI		Poca o ninguna participación del personal de planificación estratégica y adquisición en el proceso de arquitectura empresarial. Poca o ninguna adhesión a las normas existentes a estándares existentes.	Poca o ninguna gobernanza formal de la inversión y la estrategia de adquisición de TI. La unidad operativa encargada demuestra cierta adherencia al perfil de normas existente.	La estrategia de adquisición de TI existe e incluye medidas de cumplimiento con la arquitectura empresarial de TI. En la identificación de proyectos se considera el costo beneficio	Todas las adquisiciones y compras de TI planificadas se guían y se rigen por la arquitectura empresarial.	No hay inversión o adquisición de TI no planeada y articulada con la arquitectura.

(*) En el nivel de madurez 0- No existe, no hay ningún programa de arquitectura empresarial que se pueda considerar o valorar.

De acuerdo con este modelo el nivel de desarrollo de arquitectura empresarial del cual se parte en la DPC es el siguiente:

	No existe*	Iniciado	En Desarrollo	Definido	Gestionado	Medible
Proceso de arquitectura						
Desarrollo de la arquitectura						
Alineación con la misión/negocio						
Involucramiento de alto nivel						
Participación de las unidades operativas						
Comunicación de la arquitectura						
Seguridad informática						
Gobernanza de la arquitectura						
Proceso de adquisición de TI e inversiones TI						

Este resultado representa una oportunidad importante para el desarrollo del ejercicio de arquitectura digital que se adelanta y que se establece en el presente documento y que permitirá contar con una estrategia definida que se empiece a gestionar y medir.

2.2 Arquitectura de Interoperabilidad

2.2.1 Nivel de Madurez de interoperabilidad

Con el fin de establecer el nivel de madurez actual de la interoperabilidad, se tomó como referencia el modelo establecido en el Marco de Interoperabilidad de Mintic. De acuerdo con este modelo la DPC tiene un nivel de madurez: INSTITUCIONALIZADO, que se obtiene de dar respuesta a un conjunto de lineamientos y criterios que se resumen a continuación:

LINEAMIENTO	CRITERIO	JUSTIFICACIÓN	NIVEL
LI.IOP.OG.04	Liderazgo del Marco de Interoperabilidad	Existe un grupo responsable de liderar todo lo relacionado con el marco de interoperabilidad de la entidad.	1
LI.IOP.OG.05	Cultura organizacional	Constantemente se mejoran los esquemas y servicios de interoperabilidad.	1
LI.IOP.OG.01 LI.IOP.OG.02 LI.IOP.OG.03	Adecuación de procesos	Los procesos de la entidad están documentados y ajustados para el intercambio de información.	3
LI.IOP.LG.01 LI.IOP.LG.02	Normatividad para el intercambio de información	La entidad cuenta con todos los acuerdos de intercambio y existe normatividad para los servicios de intercambio.	3
LI.IOP.LG.03	Manejo de la información confidencial y personal	La entidad ha socializado las políticas de intercambio y normatividad vigente para la confidencialidad y manejo de datos personales.	3

LINEAMIENTO	CRITERIO	JUSTIFICACIÓN	NIVEL
LI.IOP.SM.01 LI.IOP.SM.04 LI.IOP.SM.06 LI.IOP.SM.03	Lenguaje común de intercambio de información	La entidad tiene registro del lenguaje de intercambio y lo utiliza en los servicios.	1
LI.IOP.SM.02 LI.IOP.SM.05	Documentación de los servicios de intercambio	Los servicios de intercambio están documentados.	1
LI.IOP.TE.01	Uso de servicios ciudadanos digitales	No ha implementado servicios para ciudadanos digitales.	1
LI.IOP.TE.07	Diseño funcional de los servicios web	Se tienen caracterizados las necesidades de intercambio de información.	3
LI.IOP.TE.07	Diseño técnico de los servicios	La entidad tiene documentada todas las necesidades de intercambio de la información.	1
LI.IOP.TE.07	Pruebas de los servicios web	La entidad ha ejecutado y tiene documentado los resultados de las pruebas.	1
LI.IOP.TE.07	Despliegue de los servicios web	La entidad tiene sus servicios desplegados.	3
LI.IOP.TE.02	Infraestructura tecnológica para el intercambio de información	La infraestructura ha sido diseñada teniendo en cuenta las necesidades de intercambio.	1

3 ARQUITECTURA OBJETIVO

3.1 Principios

- **Enfoque al ciudadano:** El enfoque en el diseño y operación de cualquier solución digital debe considerar como primera prioridad la satisfacción de las necesidades y expectativas de los usuarios y en esa medida se calificará su calidad.

- **Efectividad:** Las soluciones digitales que se diseñen y operen deberán resolver de manera efectiva la problemática para la que fueron diseñados.

- **Simplicidad:** Se debe evitar la complejidad innecesaria en todas las soluciones digitales.

- **Adaptabilidad:** Toda solución debe considerar como premisa que se pueda adaptar a nuevas condiciones o necesidades con facilidad y agilidad.

- **Racionalización:** Los recursos que sean involucrados en cualquier servicio digital deberán guardar proporciones razonables con el resultado que entregan y a la capacidad de la entidad.

- **Estandarización:** Se debe propiciar el uso de estándares de reconocimiento de facto y de jure, tanto a nivel nacional e internacional, en lugar de esquemas propietarios.

- **Interoperabilidad:** Utilizar los estándares que fortalezcan la plena interoperabilidad entre las soluciones digitales y que faciliten el intercambio de información entre las entidades nacionales, internacionales y los sectores.

- **Cero confianza:** Todos los controles de seguridad que se desarrollen deberán garantizar el cumplimiento de este principio, mediante el cual no se puede omitir ningún control de acceso aun cuando ya se hayan otorgado autorizaciones por otros componentes o procesos.

- **Privacidad por defecto:** Toda solución digital deberá garantizar que la información privada esté disponible solo para el titular de esta información, y se debe evitar el uso de esta información para propósitos diferentes de los autorizados por éste mismo, lo anterior de acuerdo con lo previsto en la Ley de Protección de Datos Personales y en los derechos constitucionales a la privacidad.

- **Orientación a datos:** Toda solución digital deberá considerar como eje principal los datos de recibe, gestiona o transforma y no los mecanismos que permiten procesarlos.

- **Sostenibilidad:** El diseño e implementación de cada solución digital debe considerar esquemas de garanticen la sostenibilidad técnica y económica de las mismas por lo menos por 5 años.

- **Neutralidad tecnológica:** Toda solución digital deberá considerar los requerimientos de acuerdo con la problemática real de los diferentes usuarios y no a la oferta de soluciones tecnológicas vigente.

- **Vigilancia tecnológica:** Toda solución digital que se diseñe deberá tomar en consideración las mejores prácticas y tendencias disponibles e integrarlas de ser necesario a la arquitectura digital.

- **Innovación:** La arquitectura y las soluciones digitales que de esta se derivan, deben diseñarse siguiendo metodologías

- **Agile:** En la medida que se considere pertinente se deben privilegiar las metodologías ágiles frente a las metodologías tradicionales para la implementación de cualquier solución digital.

- **Reutilización:** Cada componente o solución digital debe crearse con el propósito de ser la única proveedora de esos servicios, pero podrá ser utilizada para integrarse a otros componentes y soluciones. Esto quiere decir que sólo debería existir un componente o solución para el mismo propósito.

- **Costo/Beneficio:** Toda solución digital deberá diseñarse e implementarse cumpliendo con criterios de costo eficiencia y además de manera alineada con la arquitectura definida, garantizando un retorno de la inversión en el tiempo. Este retorno se debe definir desde la formulación de cualquier proyecto.

- **Trazabilidad:** Toda funcionalidad, componente o servicio digital deberá generar trazas digitales que permitan realizar auditoría por organismos y personas autorizadas para tal fin, de acuerdo con los controles establecidos en el Sistema de Gestión de Seguridad de la Información.

- **Gobierno:** Todo cambio, adaptación o mejora a las soluciones digitales deberá consultar la arquitectura digital aquí definida de acuerdo con el esquema definido para tal fin.

3.2 Pilares de la Arquitectura Digital

Se establecen cuatro bases fundamentales que rigen el diseño y reflejan los aspectos críticos definidos en la estrategia de transformación digital como se presenta en la siguiente ilustración:



Ilustración 1. Pilares de la ADR

3.3 Arquitectura Tecnológica.

3.3.1 Arquitectura conceptual

Se define la implementación de una arquitectura basada en el uso de nube pública diseñada para reflejar de manera nativa lo esencial de la experiencia en la nube: agilidad, innovación continua y entrega rápida.

El modelo PaaS (Plataforma como Servicio) es el esquema de arquitectura elegido para ser utilizado en las soluciones y servicios, ya que ofrece una serie de beneficios basados en TI:

- Ofrece más agilidad empresarial a una empresa que un enfoque tradicional de desarrollo de software.
- El desarrollo de una aplicación "Nativa PaaS" ofrece un mejor factor TTM (Time to Market) porque tales aplicaciones se pueden desarrollar e implementar más rápido. Las aplicaciones nativas PaaS reducen el tiempo de puesta en producción y cuestan menos dinero.
- También ofrece una entrega escalable altamente estandarizada y una plataforma de autogestión.
- Este es un beneficio masivo para el despliegue y desarrollo de aplicaciones empresariales.

A partir lo anterior es necesario que las aplicaciones a implementar usen servicios del catálogo de proveedor de nube como:

- Bases de datos relacionales y no relacionales.
- Almacenamiento de objetos
- Gestión de API
- Caches distribuidos.
- Servicios analíticos y cognitivos.
- Modelos de aplicación en arquitectura Cloud Nativa.
- Eventos de negocio y Colas.

Se busca que la plataforma tecnológica cumpla con un conjunto de características, que permitan:

- **Desacoplar las soluciones**. Una arquitectura de orientación a servicios y microservicios que permita ofrecer soluciones tecnológicas que convivan en el ecosistema, pero sean flexibles para actualizarse sin grandes inversiones de integración o re-arquitectura de estas.
- **Homogenizar**. Aunque existe una gran variedad de escenarios en la entidad, las políticas tecnológicas que deben cumplir las soluciones (construcción y/o adquisición) minimizan el riesgo que puede causar la gran variedad de tecnologías disponibles en una arquitectura Cloud.
- **Estandarizar**. El uso de estándares de mercado para evitar la cautividad tecnológica con proveedores en aspectos críticos de la organización son otra herramienta para garantizar un ecosistema saludable y evolutivo en el tiempo.
- **Interoperar**. Dada la arquitectura orientada a servicios y microservicios, la interoperabilidad es un atributo nativo dentro del modelo propuesto que, mediante el uso de estándares, servicios transversales y mejores prácticas ofrece una base unificada y sólida para permitir la interoperabilidad de todos los servicios
- **Auditar y trazar**. La gran magnitud de servicios debe ofrecer un esquema de auditoría y trazabilidad transversal que permita a todas las soluciones la entrega de información con propósitos de seguimiento y verificación, así como su explotación para determinar comportamientos, situaciones y riesgos operativos, funcionales o de negocio.

- **Asegurar**. Un modelo de identidad unificado es la columna vertebral de todas las soluciones de la entidad, para ofrecer una experiencia unificada de las actividades de cualquier ciudadano que consuma servicios disponibles sean estos internos o concesionados.
- **Gobernar y automatizar**. Facilitar todas las actividades operativas y funcionales de la organización mediante la automatización de actividades (despliegues, auditorías, chequeos, detección de riesgos, análisis de telemetría, etc.) son una herramienta fundamental para gobernar eficientemente el ecosistema.

3.3.2 Hiper-automatización.

La digitalización de procesos (DPA – Automatización Digital de Procesos) busca ir más allá de la simple definición de BPMN y BPMS como los estándares para lograr la implementación de procesos. Se pretende la inclusión nativa y uso de tecnologías como la inteligencia artificial (IA), machine learning (ML) y automatización mediante robots (RPA) para definir y optimizar los procesos actuales de forma que se puedan completar tareas que usualmente son realizadas por humanos, permitiendo liberar a los usuarios de tareas repetitivas y de bajo valor para que se orienten a tareas más importantes.

Entre los beneficios se encuentran:

- Flexibilidad. Dada la variedad de tecnologías, las organizaciones pueden utilizar las que mejor se adapten a las necesidades.
- Productividad. Al automatizar tareas repetitivas, los usuarios podrán realizar más trámites con menos recursos.
- Integración. Soportar los estándares del mercado e integrarlos a lo largo de la entidad.
- ROI mejorado. Al tener indicadores e información analítica, se pueden optimizar los recursos y reducir los costos.

3.3.3 Gestión de nube.

Como medio para la materialización de los objetivos de estrategia tecnológicos de la DPC, se busca lograr una adopción acelerada de las capacidades del cómputo en la nube, razón por la cual se considera que estos servicios sean entregados de forma integral, disminuyendo las complicaciones y obstáculos producto de la adopción de plataformas nube pública, en especial del universo tan amplio de alternativas, así como la atomicidad de los servicios.

Para tal fin, se busca que exista un único proveedor que cargue el rol de “Operador de Nube”, que en el contexto será quien integre sus capacidades en los modelos de cómputo en la nube y su experiencia para facilitar la adopción y gestión de plataformas de misión crítica, permitiendo a la DPC la disminución de costos y riesgos de integración y compatibilidad, el agrupamiento de los niveles de servicio, la agilidad en los aspectos de gestión, de forma muy relevante reducir la complejidad administrativa y contractual en torno a las funciones de plataforma.

Para la implementación de la plataforma se seguirá un modelo Cloud Preferida, donde las soluciones misionales de la entidad se implantan usando la nube preferida y servicios no disponibles en la nube elegida podrán usar una nube secundaria.

Cabe aclarar que el uso de servicios en nubes secundarias deberá ser evaluado hacia el interior para evitar incrementar la complejidad y gobierno de los servicios, así como también restringir el uso de tecnologías homologas a servicios existentes en la nube preferida.

3.4 Arquitectura de información

3.4.1 Arquitectura conceptual

La arquitectura de información comprende la categorización adecuada de los datos y las capacidades de gestión para su aprovechamiento desde fuentes transaccionales y analíticas.

Se ha previsto contar con un repositorio de datos que permita alimentar las diferentes funciones de negocio, en lugar de varias instancias y bases de datos para cada propósito en las cuáles se replica información innecesaria, lo cual dificulta su aprovechamiento.

El repositorio deberá contar con mecanismos de seguridad que garanticen el acceso a la información solamente para los propósitos específicos y autorizados a cada rol, permitirá también el relacionamiento de información de diferentes procesos de negocio para los procesos de analítica avanzada, todo el marco de la normatividad de protección de datos personales y acuerdos de confidencialidad vigentes.

La presente arquitectura de datos pretende apoyar los procesos descritos en la Guía Técnica de información de MinTIC: Eficiencia operativa, conocimiento del dato y uso de la información. Así mismo se presenta como un soporte a la estrategia de Gobierno del Dato de la institución que la llevará a través del marco de madurez propuesta por la misma guía.

3.4.1.1 Categorías de datos

Las categorías que permitirán clasificar los datos son las siguientes:



CATEGORÍA	CONTENIDO
Metadatos	Consiste en las estructuras que describen las entidades de datos a través de atributos como su nombre, definición o dimensión. Por ejemplo, las tablas del dominio de gestión documental.
Datos transaccionales	Aquellos datos que resultan de las transacciones en los sistemas de información misionales o de apoyo, los cuales son capturados durante la operación y procesos diarios.
Datos maestros	Se refiere la representación de los datos que son de valor estratégico para DPC. Estas entidades no son de naturaleza volátil ni transaccional, dado que una vez creadas permanecen con pocas modificaciones en el tiempo y son usadas como valores de referencia por múltiples sistemas.
Datos de referencia	Son estructuras conformadas por información de origen interno o externo a la DPC usada para soportar actividades, un ejemplo son los informes o reportes de otras entidades del Estado como el DANE, el Ministerio de Hacienda, entre otras.
Datos no estructurados	Son aquellos activos de información que soportan las actividades de los funcionarios de la Entidad como lo pueden Archivos en Excel, presentaciones en PowerPoint, reportes en Word e imágenes (activos de información), y que pueden estar o no bajo una plataforma de gestión documental.
Datos analíticos	Consiste en un grupo de datos que pueden ser parte de los datos maestros y transaccionales, los cuales suelen ser utilizados para generar reportes estadísticos o análisis financieros, y que soportan la toma de decisiones de la Entidad.
Grandes volúmenes de datos (Big Data)	Se refiere al conjunto de datos que representan un gran reto para su almacenamiento, búsqueda, distribución, visualización y análisis.
Datos abiertos	Conjunto de datos la DPC publica, promoviendo así la transparencia y el acceso a la información con el fin de incentivar la competitividad, el desarrollo y la generación de impacto social que busca la estrategia de gobierno en línea.

3.4.1.2 Capacidades de Gestión de la Información:

Modelo de Datos Empresarial: Las necesidades de datos de la DPC direccionan el modelo de datos. A partir del análisis de la cadena de valor de los procesos misionales, se identifican los límites de los dominios de datos. Los modelos de datos conceptual y lógico son la base para el desarrollo del modelo de datos institucional para la Entidad. Permite conectar y correlacionar la información entre diferentes áreas.



Ilustración 2 Capacidades de gestión de la información

CAPACIDADES	DESCRIPCIÓN
Captura, Adquisición y Entrega de Datos	Esta capacidad establece cómo la información es entregada y capturada a través de herramientas y procedimientos adecuados de tal forma que se garantice la integridad de la información en la DPC.
Analítica	Se refiere a la capacidad de proporcionar a los usuarios y a involucrados clave, conocimiento sobre el comportamiento misional de la DPC. Los sistemas diseñados para soportar esta capacidad ofrecen a los usuarios finales la opción de crear reportes de información y cuadros de mando para soportar la toma de decisiones estratégicas. Las herramientas que apoyan esta capacidad incluyen bases de BI, bodegas de datos tradicionales, modelos de inteligencia artificial y analítica de datos.
Interoperabilidad	Hoy en día las organizaciones son cada vez más dependientes de la interoperabilidad de los activos de información para apoyar las decisiones de negocio, por lo cual la DPC debe definir esquemas de Arquitectura de Datos alineados a los esquemas de orquestación e integración de la Arquitectura de Solución que se encuentra definida por una Arquitectura Orientada a Servicios (SOA por sus siglas en inglés).
Gestión de los Datos Maestros	Se refiere a la capacidad de gestionar los datos a través de la definición de los activos de información fundamentales dentro de la Entidad. Además, realiza la definición de las funciones que aseguran la integridad de los datos por medio de reglas y estructuras específicas.
Gestión del Contenido	Existe una gran porción de los activos de información de la Entidad que no es estructurada, por lo tanto, la gestión de contenidos es necesaria para el manejo de los registros documentales, multimedia o la captura de videos y audios de audiencias las cuales tienen una estructura específica y metadatos que deben ser usados para encontrar de manera eficiente la información. Además, se requieren mecanismos de búsqueda y flujo de trabajo adecuados para permitir una rápida recuperación de la información pertinente para la toma de decisiones dentro de la Rama Judicial.

CAPACIDADES	DESCRIPCIÓN
Gestión del ciclo de vida de los datos	Se refiere a la capacidad desarrollada mediante procedimientos y herramientas que aseguran que en el ciclo de vida de los datos solo se retiene la información necesaria para la operación del negocio y el cumplimiento a regulaciones tanto internas como externas, determinando la vida útil de la información y su pertinencia legal.
Seguridad de los Datos	Deben existir controles de seguridad sobre los datos, que permitan proteger la integridad, confidencialidad y disponibilidad de la información. Los datos deben estar protegidos en todos los estados de su ciclo de vida: en tránsito, en almacenamiento y en uso.
Calidad y Depuración de Datos:	Se refiere a la capacidad de gestionar mediante políticas y procedimientos la calidad, disponibilidad, integridad y depuración de los datos.

3.4.2 Arquitectura técnica

A nivel técnico se han contemplado cinco grandes capas (ver Ilustración 3) sobre las cuales se construye la arquitectura de datos de la entidad, soportando así una estrategia orientada al dato y a la toma de decisiones basadas en datos

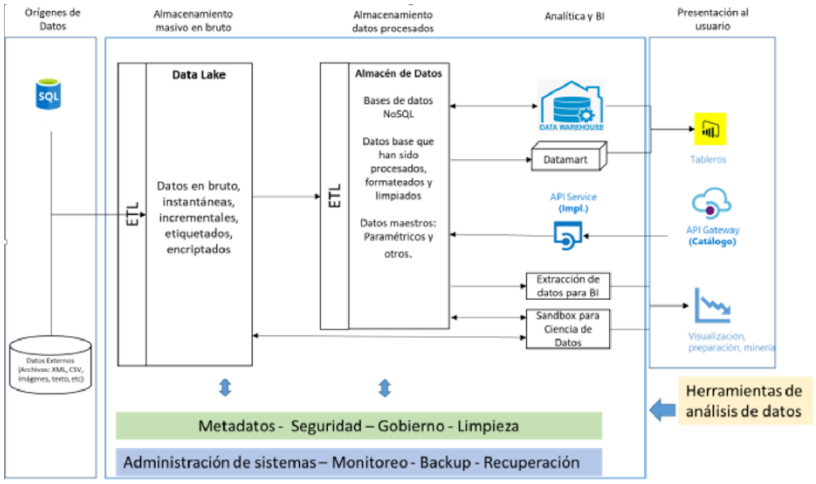


Ilustración 3 Arquitectura técnica

CAPA	DESCRIPCIÓN
Orígenes de datos	Constituyen todos los almacenes de datos en bruto que posee la entidad: datos estructurados (como los que subyacen al sistema Visión Web), semiestructurados (datos en archivos planos, archivos tipo xml[7] o json[8]) y no estructurados(documentos, videos). Adicional a esto también se tienen las fuentes de datos externas que corresponden a convenios de la entidad con otras organizaciones.

[7] Extensible Markup Language
[8] JavaScript Object Notation

CAPA	DESCRIPCIÓN
Almacenamiento masivo en bruto	Corresponde al repositorio de datos de alta capacidad donde se ponen disponibles todos los datos para posterior procesamiento analítico.
Almacenamiento de datos procesados	Los datos maestros o que han sido procesados, se almacenan en otros repositorios que dependiendo del tipo de estudio que se vaya a hacer sobre éstos, pueden ser almacenamientos documentales, geográficos, orientados a grafos, etc., un ejemplo de datos que pueden ir en este tipo de almacenamiento puede ser la compilación de información exógena para declaraciones sugeridas o información para posteriormente ser procesada por programas de analítica.
Analítica y BI	En esta capa se tienen herramientas especializadas para transformar, enriquecer y analizar los datos por parte de expertos de negocio, estadísticos y científicos de datos de distintas áreas y niveles de la DPC, bajo políticas de seguridad y acceso a los datos definidas por el Grupo de Sistemas o quien haga sus veces.
Presentación al usuario	La capa de presentación comprende herramientas informáticas necesarias para presentar los resultados de la capa anterior: estas herramientas permiten la visualización y análisis de datos a través de gráficos, mapas y tableros de control. Con ello se brinda soporte para la toma de decisiones a nivel operativo o estratégico dentro de la DPC, desde los grupos de trabajo hasta la Dirección General.

Dentro de las cinco capas referidas, se incluyen también los siguientes elementos:

Elemento	Descripción
Data Lake	Repositorio de almacenamiento preparado para manejar una vasta cantidad de datos en crudo (en su formato nativo, sin procesar) para que posteriormente sean procesados y llevados a al almacén de datos
Almacén de datos	Donde se concentra la ingente cantidad de datos que administra la DPC. Almacena datos estructurados y semiestructurados provenientes de del Data Lake y de las distintas bases de datos de la DPC asociadas a sus servicios electrónicos en funcionamiento.
Data Warehouse	Base de datos donde se integra y depura la información proveniente de diversas fuentes para ser procesada y analizada desde múltiples dimensiones o perspectivas. Esta base de datos es optimizada para consultas a gran velocidad.
Datamart	Los *datamart* son versiones especializadas de un *Datawarehouse*. Son subconjuntos de datos que tienen el objetivo de ayudar a áreas específicas de la DPC a tomar mejores decisiones.
API *Service*	Conjunto de servicios implementados para el intercambio de información. Éstos exponen datos al público (interno o externo a la organización)
Extracción de datos para inteligencia de negocios (BI por sus siglas en inglés)	Servicios de extracción de datos para alimentar procedimientos de minería de datos, visualización en tableros, etc.
Sandbox para Ciencia de Datos	Almacenes de datos temporales donde se extrae información para analizarla y generar conocimiento útil para la DPC
Tableros	Gráficos y cifras importantes para la ayuda en la toma decisiones de nivel estratégico, táctico y operativo.

Elemento	Descripción
API Gateway (Catálogo)	Permite gobernar (crear, publicar, mantener, monitorear y asegurar) la gran cantidad de servicios que puede llegar a tener la Entidad para el intercambio de datos.
Visualización, preparación, minería	Distintas herramientas de ciencia de datos para procesar y visualizar resultados de los distintos algoritmos que se pueden aplicar en los proyectos de Ciencia de Datos.
Metadatos, Seguridad, Gobierno, Limpieza	Corresponde a las distintas políticas aplicables a los datos y que se deben implementar
Administración de sistemas, Monitoreo, Backup, Recuperación	Distintos servicios de plataforma que ofrece el área de TI para proteger la infraestructura y los datos.

3.5 Arquitectura de sistemas de información y aplicaciones

3.5.1 Arquitectura conceptual

Se ha considerado la implementación de una arquitectura de Nube lo cual posibilita un esquema amplio de posibilidades tecnológicas para la implementación de soluciones de negocio con modelos de arquitecturas muy variadas.

La arquitectura de las soluciones en el ecosistema de la organización se rige según el diagrama que se presenta a continuación:

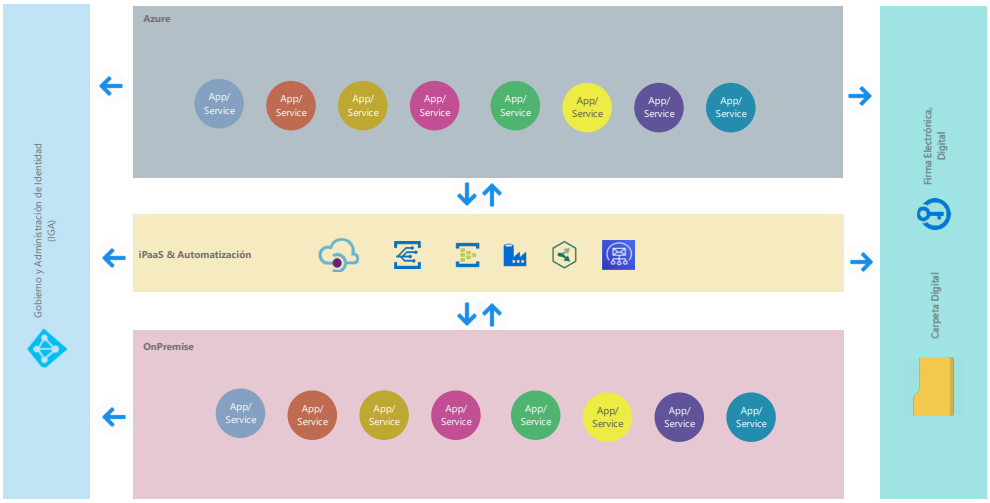


Ilustración 4. Diagrama de la arquitectura conceptual de soluciones.

Aunque puede verse como una fortaleza del esquema escogido, también prevalecen los riesgos ante el gobierno de un ecosistema tan variado en sus posibilidades de modelamiento arquitectónico.

Por ende, se definen un conjunto de lineamientos soportados en tecnología para:

- **Desacoplar las soluciones**. Una arquitectura de orientación a servicios y microservicios que permita ofrecer soluciones tecnológicas que convivan en el ecosistema, pero sean flexibles para moverse y actualizarse sin grandes inversiones de integración o re-arquitectura de las mismas.
- **Homogenizar**. Aunque existe una gran variedad de escenarios en la entidad, las políticas tecnológicas que deben cumplir las soluciones (construcción y/o adquisición) minimizan el riesgo que puede causar la gran variedad de tecnologías disponibles en una arquitectura Multi Cloud Híbrida.
- **Estandarizar**. El uso de estándares de mercado para evitar la cautividad tecnológica con proveedores en aspectos críticos de la organización son otra herramienta para garantizar un ecosistema saludable y evolutivo en el tiempo.
- **Interoperar**. Dada la arquitectura orientada a servicios y microservicios, la interoperabilidad es un atributo nativo dentro del modelo propuesto que, mediante el uso de estándares, servicios transversales y mejores prácticas ofrece una base unificada y sólida para permitir la interoperabilidad de todos los servicios

- **Auditar y trazar**. La gran magnitud de servicios que comprenderá la entidad, debe ofrecer un esquema de auditoría y trazabilidad transversal que permita a todas las soluciones la entrega de información con propósitos de seguimiento y verificación, así como su explotación para determinar comportamientos, situaciones y riesgos operativos, funcionales o de negocio.
- **Asegurar**. Un modelo de identidad transversal es la columna vertebral de todas las soluciones de la organización, garantizando y facilitando una visión unificada de las actividades de cualquier usuario participante en el consumo de servicios de la organización.
- **Gobernar y automatizar**. Facilitar todas las actividades operativas y funcionales de la organización mediante la automatización de actividades (despliegues, auditorias, chequeos, detección de riesgos, análisis de telemetría, etc.) son una herramienta fundamental para gobernar eficientemente el ecosistema.

Sin embargo, uno de los propósitos de utilizar diferentes nubes es acceder a capacidades y servicios tecnológicos que permitan a la entidad ser ágil en el uso de tecnologías emergentes presentes y futuras. La estandarización, por ende, establece flexibilidades en el uso de las tecnologías.

3.5.2 Arquitectura técnica

La arquitectura tecnológica de una solución para la DPC estará compuesta por un conjunto de microservicios, que se unen para ofrecer la funcionalidad total.

Por ende, responderá un conjunto de componentes contenerizados (portables) que consumen los servicios transversales para manejar aspectos como:

- Exposición de servicios.
- Autenticación y autorización.
- Auditoria y Trazabilidad.
- Digitalización de procesos.
- Uso de la plataforma de integración para interoperar con otros microservicios, soluciones o sistemas externos.
- Toma de decisiones y reglas de negocio.
- Interacción con usuarios a través de canales.
- Uso de Firma Electrónica y Digital.

Entre otros.

A continuación, se presenta un diagrama que muestra la anatomía de una solución en la arquitectura de la DPC:

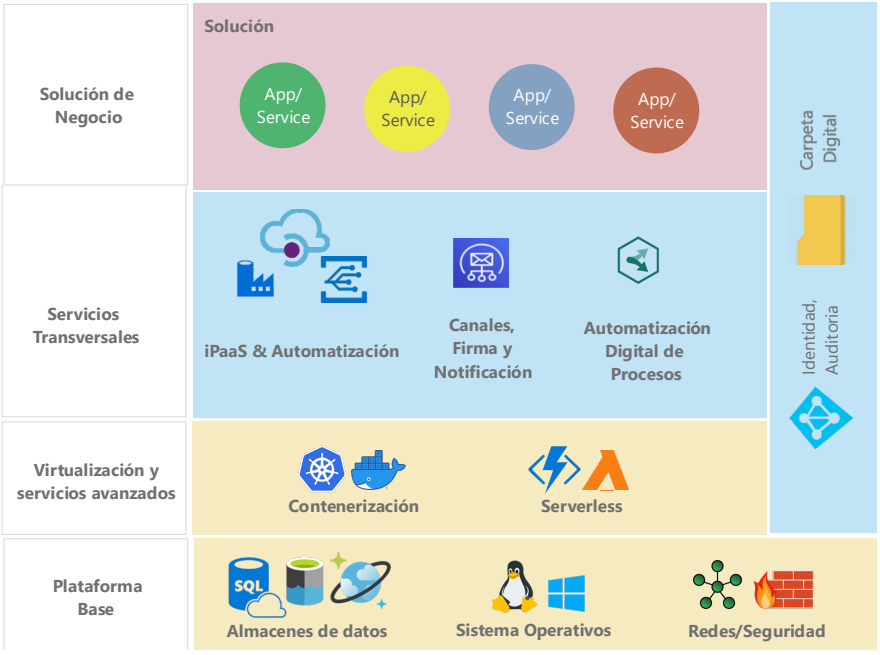


Ilustración 5. Arquitectura general de una solución.

Esta arquitectura aplica tanto para soluciones on-premise como Cloud y se presenta en forma de capas para entender como las dependencias se dan.

3.6 Arquitectura de seguridad

Las aplicaciones basadas en la nube requieren un rigor de diseño similar a una aplicación que se conecta a Internet; la aplicación debe proporcionar la seguridad sin que se hagan suposiciones sobre el entorno externo. Sin embargo, las amenazas a las que las aplicaciones estarán expuestas en un entorno en la nube serán mayores que las experimentadas en un centro de datos tradicional. Esto crea la necesidad de prácticas rigurosas que deben seguirse al desarrollar aplicaciones para la nube. Se parte del principio “Zero Trust" (cero confianza) para maximizar la seguridad, donde se asume que los actores que no son de confianza ya existen dentro y fuera de la red. Por lo tanto, la confianza implícita (ejemplo: por estar dentro de una red que se considera segura) o explícita (ejemplo: confiar en que el paso por el punto de autenticación una única vez es suficiente) debe ser completamente eliminada. Zero Trust requiere poderosos servicios de identidad para asegurar el acceso de cada usuario a las aplicaciones e infraestructura.

3.6.1 Administración de Identidad

La administración de identidad es un componente de seguridad fundamental para ayudar a garantizar que los usuarios tengan el acceso que necesitan, y que los sistemas, datos y aplicaciones sean inaccesibles para usuarios no autorizados. A partir de políticas organizacionales de administración de identidad y acceso (IAM, Identity Access Management) se determina:

- Los sistemas, la información y otras áreas protegidas por IAM.
- Los niveles correctos de protección y acceso para datos confidenciales, sistemas, información y ubicaciones.
- Cómo se identifican los usuarios y los roles que se les asignan.
- Gestión de usuarios en el sistema IAM.
- Administración de roles en el sistema IAM.

Existen tecnologías para simplificar la administración de contraseñas y otros aspectos de IAM que se deben implementar como elementos base:

Single Sign On (SSO): un sistema de acceso e inicio de sesión que permite a los usuarios autenticarse una vez y luego le otorga acceso a todo el software, los sistemas y los datos que necesitan sin tener que iniciar sesión en cada una de esas áreas individualmente. Esto se hace teniendo en cuenta los lineamientos dados por la Agencia Nacional Digital respecto a la autenticación digital que permitirá al ciudadano acceder de manera eficiente a los servicios y trámites del Estado a través de medios electrónicos.

Autenticación multifactor: este sistema utiliza una combinación de algo que el usuario sabe (por ejemplo, una contraseña), algo que el usuario tiene (por ejemplo, un token de seguridad) y algo que el usuario es (por ejemplo, una huella digital) para autenticar a las personas y otorgarles acceso.

Gestión de identidades privilegiadas: es la definición de políticas de gestión de roles y usuarios a través de la cual se gestiona el uso de las credenciales con privilegios. Para esto se parte desde el entendimiento de las distintas verticales de negocio de la DPC (tributario, aduanero, cambiario), se identifican los recursos críticos, se almacenan de forma segura las credenciales y se definen los perfiles de los usuarios acorde a sus roles, funciones y niveles de acceso.

Capacidades de B2B. La creación de un ecosistema sobre la plataforma conlleva a la existencia de diversos participantes en la cadena de trámites y procesos de la entidad lo que implica el soporta de múltiples tipos de identidad, delegación de usuarios a diferentes niveles, fuerte autenticación, auto-gestión y automatización.

Enrolamiento y verificación de contacto. Los servicios de auto-gestión que permitan realizar el registro y la habilitación de usuarios sin ocupar recurso humano para dicha tarea es clave para el crecimiento que se espera, así como garantizar que la información de contacto del ciudadano sea validado al momento de su registro (correo, celular, etc).

3.6.2 Seguridad de aplicaciones

Deben seguirse los siguientes principios para desarrollar un diseño seguro para las aplicaciones. Cuando una arquitectura en la nube no pueda cumplir estos principios, deberían remediarse mediante controles técnicos y / o compensatorios adecuados.

Privilegios mínimos. Este principio sostiene que un individuo, proceso u otro tipo de entidad debe recibir los privilegios y recursos mínimos durante el período mínimo de tiempo requerido para completar una tarea. En muchos casos, el privilegio mínimo solo se puede implementar de manera efectiva utilizando una gestión de autorización de aplicaciones contextual y detallada con mecanismos de automatización de políticas de seguridad.

Segregación de funciones. Esta es una política de control según la cual ninguna persona debe tener la responsabilidad o el acceso a más de una función relacionada.

Defensa en profundidad. Esta es la aplicación de múltiples capas de protección en las que una capa posterior proporcionará protección si se rompe una capa anterior.

A prueba de fallas. Si un sistema en la nube falla, debería fallar a un estado en el que la seguridad del sistema y sus datos no se vean comprometidos. Por ejemplo, para garantizar que el sistema se predetermina a un estado en el que un usuario o proceso no tiene acceso al sistema.

Economía de mecanismo. Esto promueve el diseño y la implementación simples y comprensibles de los mecanismos de protección, de modo que las rutas de acceso no deseadas no existen o pueden identificarse y eliminarse fácilmente.

Mediación completa. Aquí es donde cada solicitud de una entidad para acceder a un objeto en un sistema informático debe ser autorizada.

Diseño abierto. Este es un diseño de sistema de nube de acceso abierto que ha sido evaluado y revisado por una comunidad de expertos, lo que resulta en un diseño más seguro.

Mecanismo menos común. Esto indica que un número mínimo de mecanismos (especialmente mecanismos de protección) debería ser común en múltiples aplicaciones, minimizando la capacidad de una aplicación para corromper o subvertir otra aplicación.

Enlace más débil. Es importante identificar los mecanismos más débiles en la cadena de seguridad y las capas de defensa y mejorarlos, de modo que los riesgos para el sistema se mitiguen a un nivel aceptable.

3.7 Arquitectura de interoperabilidad

El diseño de la interoperabilidad para la entidad se orienta hacia un modelo nativo de colaboración, con capacidades para la automatización, democratización y consumo de servicios (propios y terceros), definición y estandarización semántica, suscripción a eventos de negocio (propios y terceros), auditoría, trazabilidad y seguridad digital, servicios conversacionales multicanal e ingesta/entrega masiva de información.

El gobierno y aplicación de políticas de seguridad de la información y ciberseguridad son transversales a todos los servicios de interoperabilidad, ya que estos son regidos por la arquitectura de seguridad que lo soporta.

Sin embargo, aunque este documento se enfoca al dominio técnico de la interoperabilidad se deben tener en cuenta los otros dominios:

- **Dominio legal**: Corresponde al conjunto de instrumentos legales que facilitan la interoperabilidad en la entidad.
- **Dominio organizacional**: Habilita los medios para la colaboración entre entidades a nivel de procesos, trámites, identificación de la información susceptible a intercambiar.
- **Dominio semántico**: Garantiza a través de políticas, estándares y guías que el significado de la información sea exacto, comprensible, sin ambigüedades y el mismo para las partes involucradas en el intercambio de información.
- **Dominio técnico**: Incluye aspectos como protocolos de comunicaciones, arquitectura y plataformas, estándares y normas técnicas, seguridad informática y privacidad, los cuales permiten conectar los sistemas de información y las aplicaciones con los servicios de intercambio de información.

3.7.1 Arquitectura conceptual

La visión de colaboración se materializa mediante los servicios de la plataforma de interoperabilidad (iPaaS) para la entidad con base en los servicios PaaS ofrecidos por Azure. Comprende el conjunto de capacidades encaminadas a lograr ser “interoperable por diseño”, cuyos servicios son transversales a las soluciones/aplicaciones que sobre esta se ofrezcan.

Los escenarios de colaboración contemplados dentro del marco de la “Estrategia de Transformación Digital” están cubiertos por los servicios ofrecidos en la arquitectura, donde el intercambio de datos, información y conocimiento se podrá dar en forma directa o indirecta. El uso de los estándares para el intercambio y la aplicación de mejores prácticas es integral a la arquitectura y permite ofrecer libertad en el diseño de los mecanismos de integración de soluciones propias y de terceros para cumplir efectivamente con las necesidades particulares de cada uno.

A continuación, se presenta el diagrama general de los servicios y capacidades del modelo de interoperabilidad que para la Plataforma de Integración de la entidad:

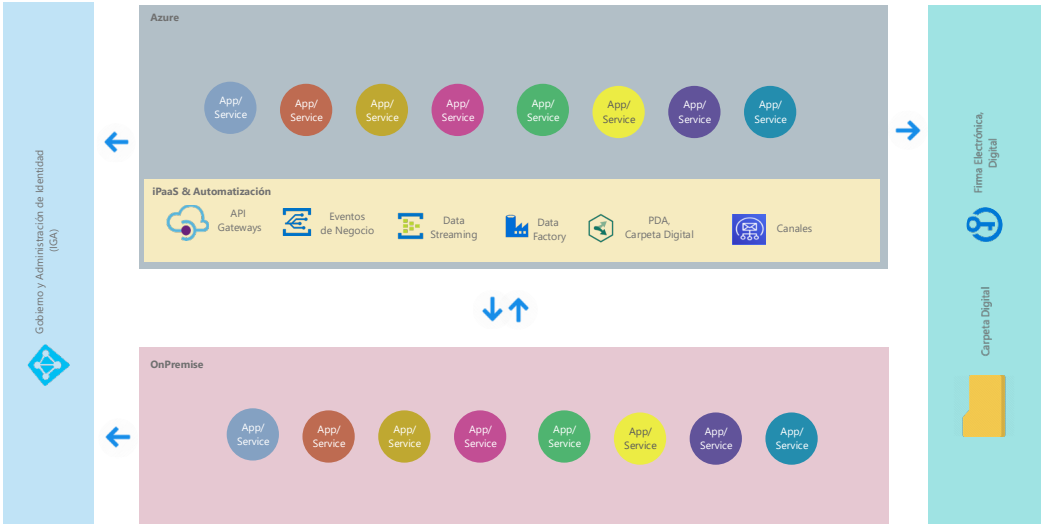


Ilustración 6. Diagrama general de servicios y capacidades de interoperabilidad.

Las capacidades de la plataforma de interoperabilidad se alcanzan mediante un conjunto de servicios transversales que se describen a continuación como son:

3.7.1.1 Automatización Digital de Procesos (DPA, por sus siglas en ingles)

Aunque estas capacidades y herramientas generalmente están consideradas como un elemento para apoyar la Arquitectura de Negocio, en el marco de interoperabilidad cumplen una función base para responder a los principios de la arquitectura de interoperabilidad.

El enfoque de uso está orientado a la implementación de procesos mediante la reutilización de servicios y la orquestación de estos. Ofrecerá la capacidad de consumir en forma nativa cualquier servicio del catálogo de la entidad mediante el uso de estándares de mercado y permitir responder ágilmente a la dinámica de la DPC.

Al hacer parte de la oferta de capacidades de la interoperabilidad, se convierte en una herramienta transversal para que pueda ser utilizada tanto internamente como por los terceros que quieran intercambiar información o construir trámites y procesos complejos con la organización.

La incorporación de la automatización de procesos WIDE (Power Automatey y Power Apps), permitirá la democratización del uso de los servicios y la creación de flujos de trabajo simples a usuarios de negocio, sin experiencia en la codificación y conocimiento en desarrollo de software. Por el contrario, el soporte para automatización de procesos DEEP, permitirá implementar los procesos misionales.

3.7.1.2 Eventos de negocio.

Representa la gestión de un evento de interés ante cualquier cambio de estado en un dato (Ej. Pago de un impuesto, actualización del correo electrónico de un usuario, etc.) o en un proceso (Ej. Inicio de un proceso de exportación, rechazo de una inspección, entre otras). Esto facilitará implementar arquitectura dirigida por eventos, eliminando el acoplamiento entre soluciones y servicios.

- El uso de patrones “Pulling” de datos, que consumen recursos innecesariamente y son generadores de carga tecnológica.
- La acoplación de sistemas externos con los servicios de la DPC.

Igualmente, este servicio también permite el diseño de arquitecturas Orientadas a Eventos (Event-Driven Architecture -EDA- por su sigla en inglés). Sin embargo, en el marco de la interoperabilidad tiene un alcance específico para garantizar su simplicidad y adopción.

3.7.1.3 Data Factory.

El método de intercambio de información “preferido” para todas las soluciones es el consumo de APIs, pero existen escenarios con restricciones técnicas que exigen otro tipo de enfoque para la integración como consecuencia de volumen y velocidad con que los datos se generan o cambian.

Este servicio está orientado principalmente para soluciones al interior de la entidad, donde se requiere mover información entre diferentes dominios y sistemas de almacenamiento (Bases SQL, Bases NoSQL, Data Lakes, Blob Storage, Archivos, entre otros.).

3.7.1.4 Data Streaming.

Otra capacidad de interoperabilidad crítica requerida en diferentes escenarios para la entidad es la ingesta de datos constantes a alta velocidad (eventos de riesgo, logs, etc.) y su procesamiento.

Aunque la analítica no haga parte de la interoperabilidad en forma directa, este tipo de ingesta de datos debe ser procesada secuencial e incrementalmente y utilizada para una variedad de análisis que incluyen la correlación, agregación, filtrado y muestreo. Con base en este procesamiento en tiempo real, se pueden tomar decisiones oportunas o responder rápidamente ante la detección de condiciones específicas.

3.7.1.5 Comunicaciones (Correo electrónico, SMS, Voz, Notificación Electrónica).

La interoperabilidad también considera los escenarios de colaboración con usuarios finales permitiendo el envío de información o la interacción de mensajes a través de canales estándares del mercado como son el correo electrónico, mensajes de texto, llamadas telefónicas y mensajes (WhatsApp).

Esta es una funcionalidad transversal y constante en las diferentes soluciones tecnológicas misionales de la entidad y hace parte de la estrategia de transformación en aspectos como el acercamiento y conocimiento de los usuarios de la entidad.

3.7.1.6 Notificación electrónica.

Es un habilitante en la eliminación de papel y aceleración de los trámites, mediante la interacción con usuarios finales en forma rápida y eficiente.

3.7.1.7 Asistentes y bots.

Otras capacidades ofrecidas por la plataforma se relacionan con los chatbots y asistentes, herramientas que permiten automatizar procesos repetitivos mediante el uso de tecnologías emergentes como Inteligencia Artificial y Machine Learning.

3.7.1.8 Carpeta Digital y servicios ciudadanos digitales.

La existencia de una versión electrónica de las carpetas de los flujos de negocio es central a la estandarización, trazabilidad y seguimiento de los diferentes procesos. Igualmente es complementaria a las necesidades de integración con los servicios ciudadanos digitales que plantea MinTic en sus esquemas de interoperabilidad y centralización de trámites.

3.7.2 Arquitectura técnica.

El conjunto de capacidades que componen los habilitadores de interoperabilidad están conformados por soluciones, herramientas y servicios que funcionen en forma integrada y transversal para todo el conjunto de aplicaciones de negocio de la entidad.

La homogeneidad y transversalidad de los servicios de interoperabilidad y el uso de estándares (APIs, JSON, etc.) en toda la arquitectura garantizan el desacoplamiento al momento de utilizarlos, pero al mismo tiempo ofrecen niveles de integración que facilitan y aceleran la implementación de intercambio de información tanto en escenarios simples como complejos.

A continuación, se presenta el diagrama técnico de alto nivel de los servicios ofrecidos por la plataforma de interoperabilidad que constituye la arquitectura propuesta.:

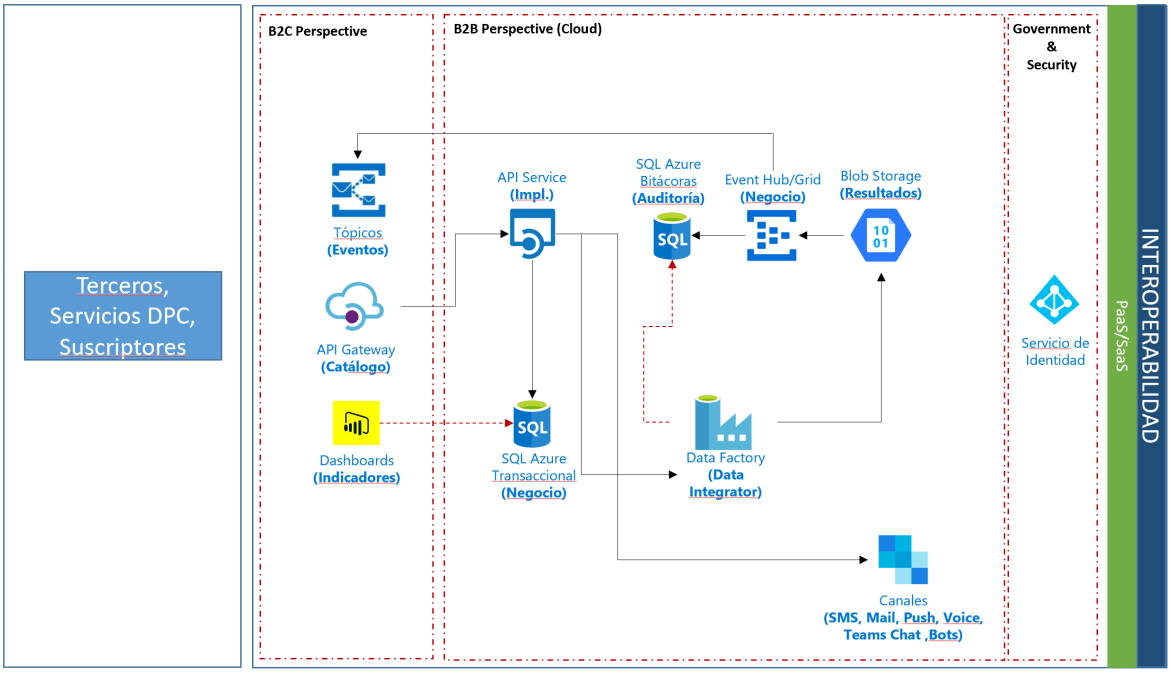


Ilustración 7. Arquitectura Técnica de la Interoperabilidad

3.7.3 X-Road y Lenguaje de Intercambio MinTic.

La plataforma definida por MinTic en su estrategia de interoperabilidad también está incluida dentro del marco definido como un canal adicional para el intercambio de datos, sin convertirse o restringirse al único disponible.

El lenguaje común de intercambio también hace parte de la taxonomía de los servicios en general, la cual se estandarizará y publicará conforme a los lineamientos de MinTic.

Sin embargo, el consumo de dichos servicios deberá estar desacoplado de las soluciones internas de la DPC mediante la utilización de una fachada de servicios (sobre estándares DPC) que eliminen el acoplamiento de los servicios con tecnologías y lineamientos externos.

3.8 Arquitectura Información Geográfica (SIG)

Los componentes básicos de una arquitectura de SIG son: almacenamiento de datos, gestión de datos, publicación de datos y desarrollo de aplicaciones mediante el consumo de esos datos; éstos se pueden estructurar en diferentes niveles según las necesidades del negocio y recursos disponibles. Se requiere de una infraestructura que soporte las herramientas que permiten administrar esos elementos; en la Defensoría la infraestructura solía estar hasta hace un tiempo conformada por servidores *On-Premise*, hoy en día existe la posibilidad de implementar estos aspectos a través de recursos en la nube, las herramientas para su administración corresponden al software con las capacidades necesarias para hacer las tareas asociadas.

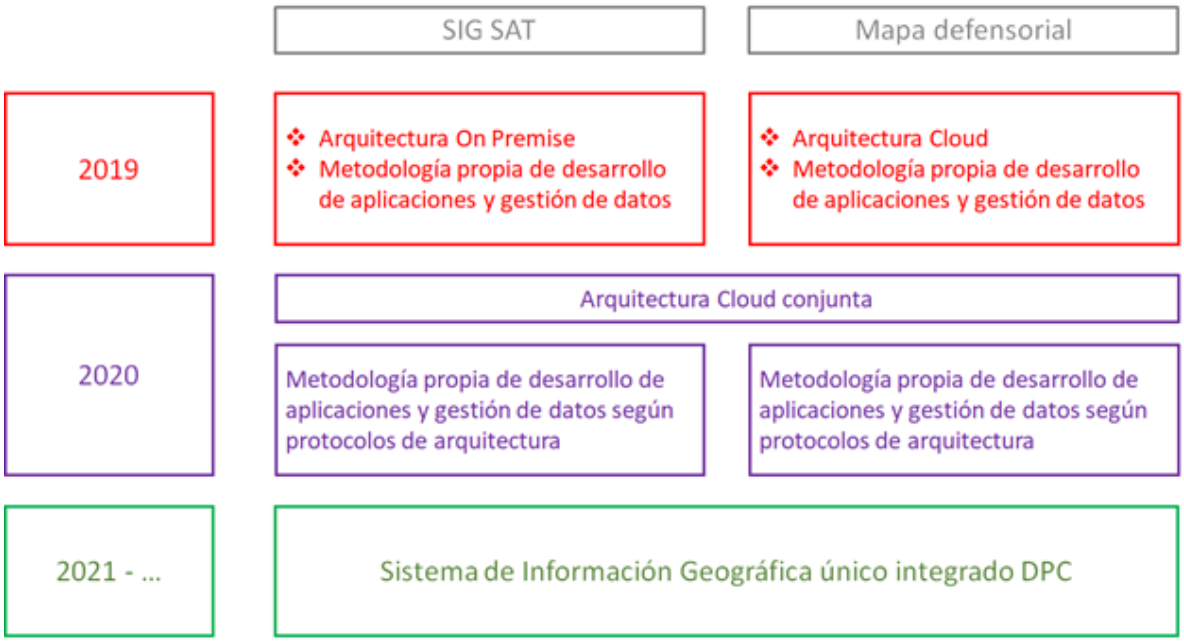
En la Defensoría se venía manejando una arquitectura de 1 solo nivel en un servidor *On-premise*, esto bajo una base de datos PostgreSQL y un licenciamiento de ArcGIS de la empresa ESRI para la administración y publicación de datos, esto complementado con una suscripción de ArcGIS Online para el desarrollo de aplicaciones mediante las plantillas de Web AppBuilder las cuales pueden ser descargadas y editadas para ser publicadas directamente desde el servidor mencionado. Esta arquitectura estaba desplegada con el objetivo de soportar la información geográfica que se administra desde el grupo de Sistema de Alertas Tempranas (SAT).

Con el proyecto del BID se realizó una reestructuración que permitiera mejorar el rendimiento y la administración de las diferentes aplicaciones geográficas y a su vez incorporar el otro desarrollo principal que se va a implementar en la Defensoría que corresponde al Mapa Defensorial; asimismo esta arquitectura permitirá unificar a mediano plazo un único grupo centralizado de Sistemas de Información Geográfica de la Defensoría del Pueblo.

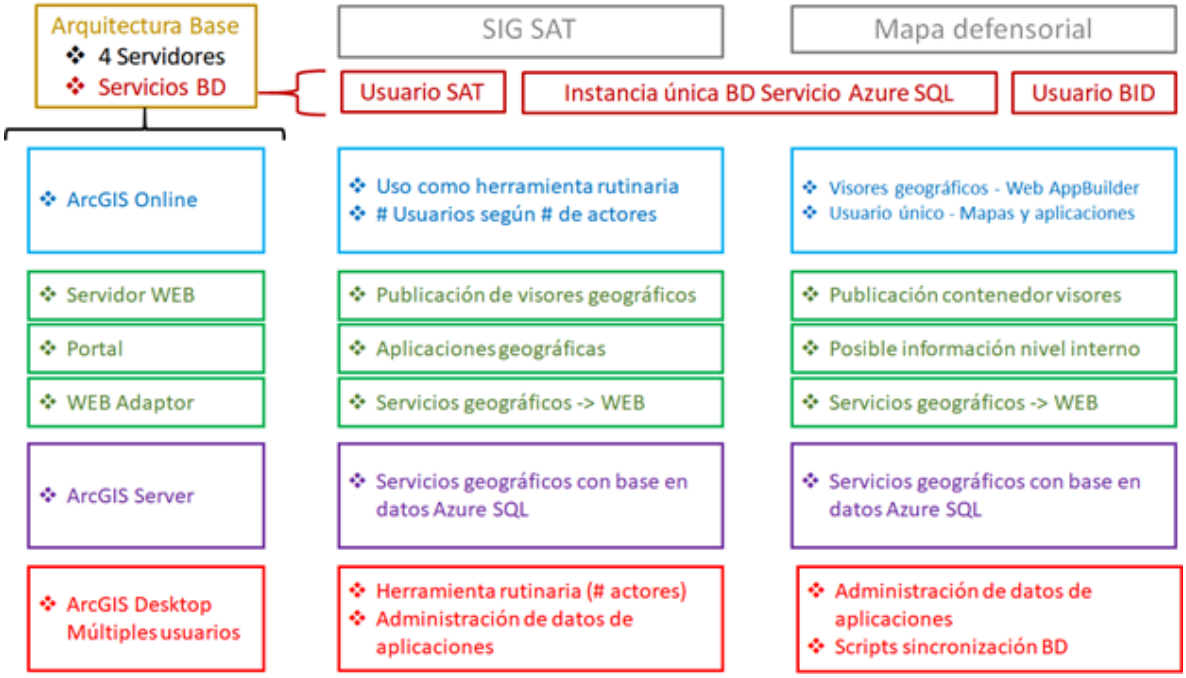
Esta nueva arquitectura está compuesta por 5 niveles, uno soportado por la suscripción de ArcGIS Online para la configuración de aplicaciones mediante Web AppBuilder, los otros 4 niveles en un ambiente total de nube Azure y que corresponden a los siguientes aspectos:

- **Almacenamiento de datos**: Servicio de SQL Azure.
- **Servidor WEB**: Publicación de aplicaciones a medida, componente Portal for ArcGIS, Web adaptor para publicación WEB de servicios geográficos desplegados.
- **Servidor ArcGIS Server**: Servicios geográficos.
- **Administración y estructuración de datos**: A través de la licencia ArcGIS Desktop que permite adicionalmente administrar los servicios geográficos y ejecución de scripts en Python como tareas programadas.

En el siguiente diagrama se muestran los pasos generales en el tiempo para la implementación de la arquitectura de SIG definitiva orientada a consolidar un grupo integrado para la administración de datos geográficos en la Defensoría, el cual soportará el desarrollo de la plataforma del Mapa Defensorial:



En el siguiente diagrama se muestra la nueva arquitectura implementada a la fecha con los 5 niveles descritos anteriormente:



3.8.1 Almacenamiento de datos

Bajo una única instancia se deben gestionar los diferentes esquemas/usuarios para administrar los diferentes grupos de datos temáticos, los datos almacenados en estos esquemas están orientados a soportar los servicios WEB. A la fecha existen dos esquemas, uno para la información temática del Mapa Defensorial y otra para la del grupo del SAT.

Tanto las tablas como los Feature Classes no deben tener ningún tipo de relación de base de datos, esto para facilitar el uso de los servicios geográficos desde las aplicaciones WEB. La relación entre tablas se debe manejar mediante Scripts de sincronización, desarrollados en Python (usando principalmente la función arcpy.ArcSDESQLExecute) y que se ejecutan como tareas programadas del sistema con una periodicidad definida desde los servidores dónde se encuentren instaladas las licencias de ArcGIS Desktop.

La sincronización se realiza principalmente desde la base de datos alfanumérica que soporta el componente de *Diseño e implementación de un Modelo de Inteligencia de Negocios y Analític*a del BID, ya que esa base de datos consolida automáticamente la información desde los diferentes repositorios de datos de la Defensoría. Para esto se deben definir unos identificadores únicos por entidad que permiten la asociación de los atributos desde la base datos alfanumérica a hacia las entidades geográficas de la geodatabase.

Debe existir un archivo integral con el inventario de cada elemento de la geodatabase y la descripción de cada uno de sus atributos (campos), asimismo la relación entre los elementos que son objeto de sincronización identificando los campos origen y destino.

Las tablas de los elementos deben cumplir los procesos de estandarización necesarios, éstos comprenden entre otros, el uso de campos con Dominios, la homogenización de los datos como por ejemplo el uso de texto tipo oración para los respectivos campos (primera letra en mayúscula y demás en minúscula) y el nombramiento de campos que debe ser de máximo de 10 caracteres usando solamente mayúsculas y el signo de raya al piso, sin espacios, tildes ni caracteres especiales, esto para garantizar una correcta exportación a archivos tipo Shapefile (.SHP).

Las capas geográficas que lo ameriten deben ser generalizadas en su geometría para optimizar el rendimiento de carga y publicación de servicios geográficos. Se deben mantener disponibles las capas originales.

3.8.2 Servidor WEB

En este componente está incluido el Web Adaptor que permite exponer en internet los servicios WEB geográficos desplegados en el componente de ArcGIS Server que a su vez está federado con el componente de Portal for ArcGIS, éste último usado principalmente para la configuración de aplicaciones WEB a través de los servicios y uso de capas alojadas para ciertos componentes como Survey 123, también para datos alojados que se deseen administrar solamente nivel interno.

En el momento existe un solo servidor de ArcGIS server con 4 *cores*, el Web Adaptor debe ser escalable para poder configurar *cores* adicionales que se requieran en el futuro según las necesidades del negocio.

Para el componente de Portal for ArcGIS, en la carpeta arcgisportal se almacena toda la información relacionada y alojada en este componente, ésta se encuentra ubicada en un disco secundario de este servidor.

En este servidor también se alojan todas las aplicaciones hechas a la medida en la carpeta C:\inetpub\wwwroot\, asimismo se alojan en esta ubicación, los reportes (imágenes por ejemplo) que se usan como un servicio que es consumido por otras aplicaciones correspondientes a módulos del proyecto BID, estos reportes o imágenes se generan a través de Scripts de Python con la periodicidad que el servicio requiera a través de tareas programadas del sistema, la información debe ser almacenada en este servidor y ejecutada automáticamente desde el servidor donde se encuentra la licencia de ArcGIS Desktop.

3.8.3 Servidor ArcGIS Server

Está incluido todo el componente de publicación de servicios geográficos que está federado a su vez con el componente Portal for ArcGIS, los servicios pueden ser administrados desde las licencias ArcGIS Desktop o directamente desde el servidor a nivel interno o a través de internet con el uso de las respectivas credenciales.

Los servicios geográficos dinámicos deben ser publicados con información que provenga directamente desde la geodatabase empresarial. Se cuenta también con un disco secundario en el cual se localiza alojada toda la información relacionada con el *DataStore*, que contiene la información que se publica como estática (imágenes, capas de referencia).
Debe existir un archivo integral de relación entre los servicios geográficos y cada una de las entidades de la geodatabase asociadas a cada uno, y a su vez la relación de las aplicaciones Web geográficas que consumen cada uno de los servicios.

3.8.4 Administración y estructuración de datos

A través de las licencias ArcGIS Desktop se administrarán y estructurarán los datos, los datos ubicados en la geodatabase estarán allí con el propósito de ser publicados, cualquier otra información de trabajo debe estar ubicada en *File Geodatabases* locales, la información susceptible de ser estructurada en lotes deberá crearse de forma local y luego subirse a la geodatabase; para la información que deba ser editada directamente en la geodatabase empresarial, deberán definirse los protocolos necesarios para permitir el correcto uso de las aplicaciones.

Desde este componente también pueden ser publicados y administrados los servicios a través de la conexión con el servidor de ArcGIS Server.

Los Scripts de Python deberán ser ubicados en estos servidores y los que requieran ejecutarse como tarea programada deben establecerse en este mismo y hacer las conexiones necesarias con los demás servidores para llevar a cabo las tareas necesarias.

En el momento, existe un servidor por cada dos licencias de ArcGIS Desktop, a estos servidores se pueden conectar dos usuarios al mismo tiempo para hacer uso de cada una de estas licencias. A la fecha hay dos servidores desplegados, se debe permitir la escalabilidad para futuros usuarios usando este esquema.

Por cada licencia de ArcGIS Desktop existe una licencia de ArcGIS Pro que es utilizada con el mismo fin, estas licencias están asociadas a los diferentes actores analistas de SIG de la Defensoría y pueden ser usadas ya sea en los servidores asociados o en computadores locales mediante el proceso de autenticación.

3.8.5 Suscripción ArcGIS Online

Se puede usar como el componente Portal for ArcGIS (pero a un nivel de nube suministrada por ESRI) para la configuración de aplicaciones (Story Maps, Web AppBuilder, entre otras), alojamiento de capas, etc. Desde allí se administran las licencias de ArcGIS Pro a través de usuarios autenticados.

3.8.6 Desarrollo de aplicaciones WEB geográficas

Las aplicaciones deben ser desarrolladas en su mayoría a través de la última versión *ArcGIS API for JavaScript* y alojadas en el servidor WEB, estas aplicaciones deberán usar todas las funcionalidades necesarias para la configuración de capas de servicios y widgets y a su vez los elementos DOM necesarios para permitir el apropiado funcionamiento según las necesidades de los usuarios. Existirán algunos casos que se puedan configurar las aplicaciones, mapas o servicios desde ArcGIS Online o que existan aplicaciones híbridas, que usen algunos componentes de ArcGIS Online y otros del API de ArcGIS.

Además de aplicaciones se deben desarrollar los servicios necesarios a través de URL parametrizadas que pueden ser consumidas desde otras aplicaciones de la defensoría.

Las aplicaciones desarrolladas pueden ser invocadas desde un componente externo el cual hará el enlace a la página de inicio de la respectiva aplicación, pero además debe existir una plataforma central de mapas que es la base del Mapa Defensorial y que permitirá interactuar de la mejor forma posible con los usuarios en términos de rendimiento, usabilidad, apariencia y diseño, entre otros; esta plataforma debe ser interoperable con los demás sistemas que se requieran de la Defensoría y debe incluir búsquedas interactivas, reconocimiento de voz, etc.

4 PORTAFOLIO DE PROYECTOS

Teniendo en cuenta la arquitectura objetivo y el punto de partida establecido en la arquitectura de línea base, se identifican los siguientes proyectos en cada dominio:

Estos proyectos son:

Dominio	Proyecto	Alcance	Misional/Transversal/Apoyo
Negocio	Herramienta de monitoreo, análisis y seguimiento a alertas y recomendaciones diseñada e implementada	Visibilizar y gestionar las Alertas tempranas.	Misional
Negocio	Plataforma integrada para la gestión defensorial y un instrumento de reportes internos y externos diseñada e implementada.	Plataforma nueva de gestión defensorial.	Misional
Negocio	Interoperabilidad con Procuraduría General de la Nación (PGN) y las personerías diseñado e implementado	Apoyo de cooperación con entidades relacionadas en el seguimiento de requerimientos.	Misional
Negocio	Diseño e implementación de un sistema de relacionamiento con los ciudadanos con diversos canales de acceso.	Funciones generales de CRM orientadas a la Defensoría.	Misional
Negocio	Gestión del Conocimiento	Integrar orígenes de datos con la Gestión de Conocimienot	Misional
Negocio	Firma Electrónica	Fortalecer plataforma existente de Firma Electrónica.	Transversal
Aplicaciones	Automatización de procesos	(Servicios de DPA. Capacidades PDA-Wide Capacidades PDA-Deep)	Apoyo
Aplicaciones	Carpeta Electrónica	Centralización y visibilización de procesos.	Apoyo

Dominio	Proyecto	Alcance	Misional/Transversal/Apoyo
Interoperabilidad	X-Road	Integración MinTic	Transversal
Interoperabilidad	Agenda	Coordinación de actividades, tareas y esfuerzo.	Transversal
Análisis	Plataforma Analítica	Configuración y construcción de la infraestructura de analítica.	Transversal

5 GLOSARIO/DEFINICIONES.

- ✓ PDA/DPA - Automatización Digital de procesos por su sigla en inglés (Process Digital Automation): es un concepto que describe la automatización, a través de software, de los procedimientos y procesos de una organización. DPA es un concepto genérico y no define tecnologías concretas, aunque sí da pistas sobre cuáles utilizar, ya que da especial relevancia a determinados aspectos dentro de la automatización

- ✓ API Gateway: es la pieza encargada de unificar la publicación de APIs para que sean consumidas por otras aplicaciones o por los desarrolladores. Dentro de algunos de las funciones: permite crear, implementar y administrar una interfaz de programación de aplicaciones (API).

- ✓ Eventos de negocio:

- ✓ Data streaming: son datos que se generan constantemente a partir de miles de fuentes de datos, que normalmente envían los registros de datos simultáneamente en conjuntos de tamaño pequeño. Los datos de streaming incluyen diversos tipos de datos, como archivos de registros generados por los clientes que utilizan sus aplicaciones móviles o web, compras electrónicas, actividades de los jugadores en un juego, información de redes sociales, operaciones bursátiles o servicios geoespaciales, así como telemetría de dispositivos conectados o instrumentación en centros de datos.

- ✓ ETL: es el proceso que permite a las organizaciones mover datos desde múltiples fuentes, reformatearlos y limpiarlos, y cargarlos en otra *base de datos, data mart, o data warehouse* para analizar, o en otro sistema operacional para apoyar un *proceso de negocio*. Los procesos ETL también se pueden utilizar para la integración con *sistemas heredados*.

- ✓ Mensajes push: son mensajes instantáneos que recibes en tus dispositivos. Los mensajes de WhatsApps, por ejemplo, son mensajes push. También lo son los SMS de promociones, las notificaciones que recibes en tu navegador web o las notificaciones de aviso de un nuevo email.