PROGRAMA DE APOYO A LA MODERNIZACIÓN DE LA
DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES -
DIAN

CONTRATO DE PRÉSTAMO BID 5148/OC-CO

SOLICITUD DE INFORMACIÓN (RFI)

SERVICIO DE GESTIÓN DE IDENTIDAD Y ACCESO (IAM) PARA USUARIOS Y APLICACIONES DIAN

JULIO 2024

I. TERMINOS Y SIGLAS

TERMINO SIGLA	DESCRIPCION
ABAC	Attribute-based Access Control. Los permisos se otorgan en función de un conjunto de atributos que posee un usuario o recurso.
Alianza FIDO	Es una asociación de industria abierta que produce estándares de autenticación y certificaciones para escenarios sin contraseña.
API	Application Programming Interface. Es un conjunto de reglas que definen la forma en que aplicaciones o dispositivos pueden conectarse y comunicarse entre sí.
API REST API RESTful	Es una API que se ajusta a los principios de diseño de REST.
APM	Application Perfomance Monitor: Es un conjunto de software de monitoreo que comprende monitoreo de experiencia digital (DEM), descubrimiento, seguimiento y diagnóstico de aplicaciones, e inteligencia artificial diseñada específicamente para operaciones de TI
AuthN	Autenticación
AuthZ	Autorización
B2B	Business-to-Business
B2C	Business-to-Consumer
B2G	Business-To-Government
CDN	Content delivery network: es un grupo de servidores distribuidos geográficamente que almacena en caché el contenido cerca de los usuarios finales. Una CDN permite la transferencia rápida de recursos necesarios para cargar contenido de Internet, incluidas páginas HTML, archivos JavaScript, hojas de estilo, imágenes y videos.
CIAM	Customer Identity and Access Management CIAM se centra en la gestión de identidades y el acceso de los clientes que interactúan con una empresa o plataforma en línea.
Contenerización	La contenerización es el empaquetado de código de software con solo las bibliotecas de sistema operativo (SO) y las dependencias necesarias para ejecutar el código para crear un único ejecutable ligero, denominado contenedor, que se ejecuta de manera coherente en cualquier infraestructura.
COTS	Commercial Off The Shelf Software (Software comercial listo para usar)

DIAN	Dirección de Impuestos y Aduanas Nacionales
Ecosistema MUISCA	Conjunto de aplicativos que comparten la arquitectura MUISCA (DIAN), desarrollo propio basado en JEE
FIDO2	Es un estándar de autenticación FIDO (Fast Identity Online) creado por la Alianza FIDO.
GraphQL	Es un lenguaje de consulta y manipulación de datos para APIs, y un entorno de ejecución para realizar consultas con datos existentes.
gRPC	Es un sistema de llamada a procedimiento remoto (RPC) de código abierto desarrollado inicialmente en Google.
HTTPS	Protocolo de transferencia de hipertexto seguro
IaaS	Infraestructura como servicio.
IAM	Gestión de identidades y accesos, por sus siglas en inglés, Identity and Access Management.
Identidad	Identidad es la herramienta de autenticación y autorización (IAM-CIAM) que reconoce y habilita a una persona, servicio, recurso o componente a acceder a otros servicios y componentes. Gobierna el acceso a recursos en las condiciones y momento correcto. Establece las relaciones de confianza entre componentes o usuarios y es parte fundamental de los sistemas de seguridad.
Identity Fabric	Enfoque integral para administrar Identidades en varias plataformas, aplicaciones y dispositivos. Marco para integrar varias soluciones de IAM.
IdP	Proveedor de Identidad. Servicio o sistema que crea, administra y verifica las identidades de los usuarios para permitir un acceso seguro y fluido a diversos servicios, aplicaciones y plataformas.
ISO 27001	Es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI)
JSON	JavaScript Object Notation: Es un formato de texto sencillo para el intercambio de datos.
MFA	Multi factor authentication: La autenticación multifactor combina dos o más credenciales independientes
Microsoft Entra ID	Antiguo Azure Active Directory.
OAuth 2.0	Open Authorization: Es un estándar diseñado para permitir que un sitio web o una aplicación accedan a recursos alojados por otras aplicaciones web en nombre de un usuario.
OnPremises	El software local se instala y ejecuta en computadoras en las instalaciones de la persona u organización que utiliza el software.
Open Source	Open-source software. Es el software cuyo código fuente y otros

	derechos que normalmente son exclusivos para quienes poseen los derechos de autor, son publicados bajo una licencia de código abierto o forman parte del dominio público
OpenID Connect (OIDC)	Es un protocolo de identidad que utiliza los mecanismos de autorización y autenticación de OAuth 2.0
PaaS	Plataforma como servicio.
PBAC	Policy-Based Access Control. PBAC determina los privilegios de acceso de forma dinámica según reglas y políticas.
PWA	Aplicación Web Progresiva
RBAC	Role-based Access Control
ReBAC	Relationship-based Access Control.
REST	Representational State Transfer. Es un tipo de arquitectura de desarrollo web que se apoya totalmente en el estándar HTTP
RFI	Request For Information (Solicitud de Información)
RUB	Registro Único de Beneficiarios (Aplicativo DIAN)
RUT	Registro Único Tributario (Aplicativo DIAN)
SaaS	Software como servicio.
SAML	Security Assertion Markup Language: Es un estándar de código abierto basado en XML que permite intercambiar información de autentificación y autorización.
Serverless computing	Computación sin servidor: Es un modelo de ejecución de computación en la nube en el que el proveedor de los servicios en la nube destina por demanda recursos de las máquinas virtuales
Servicios Conexos	Son los servicios de desarrollo e implementación, migración, capacitación, entrenamiento, mantenimiento y soporte
Sidecar pattern	Es un patrón de diseño que se centra en ampliar la funcionalidad de un servicio principal adjuntándole un contenedor auxiliar, conocido como «sidecar». Este contenedor sidecar se ejecuta en el mismo contexto que el servicio principal y mejora sus capacidades sin necesidad de modificar el código del servicio. Proporciona funcionalidades de apoyo, como registro, monitorización, descubrimiento de servicios, seguridad, etc.
SIEM	Security Information and Event Management. combina la gestión de información de seguridad (SIM) y la gestión de eventos de seguridad (SEM) en un solo sistema de gestión de seguridad. La tecnología SIEM recopila datos de registro de eventos de una variedad de fuentes, identifica la actividad que se desvía de la norma con análisis en tiempo real y toma las medidas adecuadas.

SOC 2	System and Organization Controls 2: es una norma de cumplimiento voluntario establecido por el Instituto Americano de Contadores Públicos Certificados (AICPA) para organizaciones de servicios, y establece pautas sobre cómo deben gestionar los datos de sus clientes.
Solución IAM para la DIAN	Gestión de Identidad y Acceso (IAM-CIAM) incluido para usuarios internos (funcionarios) y externos (ciudadanos/clientes).
SPA	Single-Page Application: Es un tipo de aplicación web que ejecuta todo su contenido en una sola página.
SSL	Secure Sockets Layer: Es un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.
SSL offloading	Es el proceso de eliminar el cifrado basado en SSL del tráfico entrante para aliviar al servidor web de la carga de procesamiento de descifrar y/o cifrar el tráfico enviado a través de SSL.
SSO	Single Sign On: Inicio de sesión unificado
WAF	Web application firewall: Un WAF crea un escudo entre una aplicación web e Internet; este escudo puede ayudar a mitigar muchos de los ataques habituales.
WebAuthn	Web Authentication. Es un estándar web publicado por el Consorcio WWW (W3C). WebAuthn es un componente fundamental del proyecto FIDO2
WSO2	WSO2 Identity Server: Proveedor de identidad (DIAN – On-Premise).
XML	Extensible Markup Language: ES una especificación de W3C como lenguaje de marcado de propósito general

II. OBJETIVO DEL RFI

Recopilar información detallada y relevante sobre productos, servicios y Soluciones de Gestión de Identidad y Acceso (IAM), disponibles en el mercado para suplir las necesidades de la DIAN.
La Entidad busca identificar y comprender mejor las capacidades, características, estándares, servicios, costos y otros aspectos importantes de diferentes proveedores y soluciones que se puedan ofrecer, teniendo en cuenta: el entorno, las características, necesidades y evolución continua propias de la Entidad.

III. ALCANCE DEL RFI

La DIAN requiere conocer las condiciones comerciales, técnicas y financieras para contar con una Solución para la Gestión de Identidad y Acceso, y de servicios complementarios.

IV. CRONOGRAMA

El siguiente cronograma lista las actividades y fechas para llevar a cabo el RFI.

Actividad	Fecha
Publicación y lanzamiento del RFI	5 de julio de 2024
Plazo para la presentación de observaciones y aclaraciones al RFI por parte del proveedor	12 de julio de 2024
Plazo para envío de respuestas a las observaciones del RFI por parte de la DIAN	19 de julio 12 de julio de 2024
Plazo para la presentación del DEMO del producto/solución propuesta y costos por parte de los proveedores	26 de julio de 2024
Plazo para envío de respuestas al RFI por parte de los proveedores.	02 de agosto de 2024

La DIAN se reserva el derecho de analizar las respuestas de los interesados al RFI y de solicitar las aclaraciones que a su juicio se requieran.

V. FORMA DE PRESENTACIÓN DE RESPUESTAS AL RFI

El RFI se remitirá a través del correo electrónico *adquisiciones@fondodian.gov.co* que es gestionado por la Unidad de Coordinación del Programa (UCP) de apoyo a la modernización de la DIAN, de tal manera que se centralice la información. Todas las interacciones entre la DIAN y los interesados en participar en este requerimiento se deben realizar utilizando el correo mencionado.

No se aceptarán respuestas al RFI que se entreguen por un medio diferente o que se entreguen en papel en las dependencias de la DIAN.

Para efectos de cualquier comunicación, se debe relacionar el texto: ***Respuesta RFI- Solución IAM y servicios complementarios 2024.*** La respuesta debe darse en idioma español o en su defecto en inglés; la documentación a remitir deberá ser en formato PDF y Word adjuntos al correo, sin que éste supere los 20MB.

VI. FORMA DE PRESENTACIÓN DEL DEMO

Para conocer las soluciones que podrán ser ofertadas, de manera previa a recibir las respuestas al RFI se realizará una reunión en modalidad virtual en donde las firmas interesadas que cuenten con una solución tecnológica que responda a las necesidades planteadas por la DIAN, podrán realizar una demostración de la solución que pueden ofertar y darán respuestas frente a las inquietudes que se planteen.

Para participar en esta sesión, las firmas interesadas remitirán un correo a la siguiente dirección adquisiciones@fondodian.gov.co, en donde deberán manifestar su interés en participar en la misma y en el que informen el nombre y el correo electrónico de las personas que participarán. En repuesta se remitirá la fecha y hora de la sesión con el protocolo de esta.

La finalidad de la sesión de DEMO es adoptar las decisiones, comparar productos, teniendo en cuenta las necesidades explicitas de la DIAN y las posibilidades que brinda el mercado. Por medio de la demostración del producto, el proveedor podrá resaltar las características de la solución.

La sesión debe contemplar 2 bloques, el primero de carácter técnico abarcando los temas de: Arquitectura, Autorización de usuarios y aplicativos, microservicios (OnPremises y Cloud) y Auditoria; y el segundo bloque, licenciamiento, aprovisionamiento y metodología en general del proyecto.

Nota: *Todo lo anterior respecto del estado actual de el o los productos que pudieran conformar la solución ofertada*.

La presentación del DEMO se desarrollará en una sesión virtual, con una duración máxima de 2 horas, de acuerdo con la programación establecida por la DIAN.

VII. ANTECEDENTES

La Dirección de Impuestos y Aduanas Nacionales es una Unidad Administrativa Especial del orden nacional, de carácter eminentemente técnico y especializado, con personería jurídica, autonomía administrativa y presupuestal y con patrimonio propio, adscrita al Ministerio de Hacienda y Crédito Público. Tiene a su cargo un servicio público esencial (parágrafo artículo 53 de la Ley 633 de 2000), su objetivo es coadyuvar a garantizar la seguridad fiscal del Estado colombiano y la protección del

orden público económico nacional, mediante la administración y control al debido cumplimiento de las obligaciones tributarias, aduaneras y cambiarias, y la facilitación de las operaciones de comercio exterior en condiciones de equidad, transparencia y legalidad.

El Plan Nacional de Desarrollo 2018-2022 incluyó dentro de sus objetivos fortalecer la capacidad técnica e institucional de la DIAN, y en ese marco se ha estructurado el Programa de Apoyo a la Modernización de la DIAN que tiene el propósito de mejorar la eficacia y la eficiencia de la gestión tributaria y aduanera de la Entidad y así incrementar la recaudación del Gobierno Nacional.

En ese sentido, en junio de 2020 fue aprobado el Documento CONPES 3993 "Concepto favorable al patrimonio autónomo Fondo DIAN para Colombia para la contratación de operaciones de crédito con la Banca Multilateral (…) y declaración de importancia estratégica que la Nación proyecta realizar al Programa de Apoyo a la Modernización de la DIAN". Dicho CONPES señala que en términos de modernización tecnológica, la DIAN ha adelantado esfuerzos para poner al día los sistemas de información y servicios digitales ante los cambios normativos; sin embargo, en los últimos 15 años no se ha realizado una renovación de sus soluciones frente a posibilidades que brindan actualmente las tecnologías digitales, además cuenta con deficiencias relacionadas con gobierno de datos, seguridad de la información, escalabilidad de las soluciones tecnológicas, baja adopción de tecnologías emergentes y estandarización de componentes tecnológicos, lo cual dificulta el desarrollo y despliegue de nuevas funcionalidades, incrementa costos por pagos de soportes a CONSULTORES exclusivos de tecnología, limita el escalamiento tanto vertical como horizontal, e incrementa los problemas de disponibilidad en el servicio.

El 24 de diciembre de 2020, el Fondo DIAN para Colombia y el Banco Interamericano de Desarrollo (BID), suscribieron el Contrato de Préstamo BID 5148/OC-CO, con el objeto de contribuir a la financiación y ejecución de la primera operación de un programa multifase de Apoyo a la Modernización de la DIAN cuyo objetivo general es mejorar la eficacia y eficiencia de la gestión tributaria, aduanera y cambiaria de la DIAN y cuyos objetivos específicos se han orientado a: Mejorar el modelo de gobernanza institucional para el fortalecimiento de la planificación estratégica y la estructura institucional y la actualización del modelo de gestión de talento humano.

Optimizar procesos de gestión tributaria, aduanera y cambiaria para el aumento de su eficiencia en términos de mayor recaudo y mejor gestión de riesgo.

Mejorar la eficiencia de la gestión tecnológica, los datos y la seguridad de la información para optimizar la toma de decisiones y proteger la información.

Para alcanzar los objetivos indicados, el Programa comprende tres componentes:

- Organización Institucional y Recursos Humanos (RR.HH.).
- Control y cumplimiento tributario, aduanero y cambiario.
- Plataforma Tecnológica (PT), datos y seguridad de la información.

De acuerdo con lo anterior, y con el propósito de mejorar la experiencia de los usuarios, lograr una mayor digitalización de los servicios y adicionalmente facilitar el intercambio de información con

diferentes actores, se hace necesario diseñar e implementar los siguientes componentes transversales:

Plataforma Digital de Integración de Servicios, es un grupo de componentes transversales que permiten lograr una mayor digitalización de los servicios, mejorar la experiencia de los usuarios y facilitar el intercambio de información con los diferentes actores.
Aplicaciones para la Gestión Corporativa, consiste en una plataforma tecnológica de procesos e información diseñada para facilitar y controlar de manera eficiente tres (3) procesos: i) gestión del talento humano; ii) gestión de asuntos disciplinarios; iii) gestión de logística e inventarios.

Aplicaciones para la Gestión Tributaria, es una plataforma tecnológica de procesos e información diseñada por la DIAN para facilitar y controlar de manera eficiente los procesos tributarios de recaudación de impuestos y derechos, control cambiario y fiscalización.

Aplicaciones para la Gestión Aduanera, es una plataforma tecnológica de procesos e información diseñada por la DIAN en el que se pretende reflejar la visión de un ecosistema eficiente, en el que la DIAN sea el habilitador de condiciones propicias para robustecer la actividad económica, articulando los esfuerzos de los actores del comercio exterior en Colombia.

Repositorio único de datos (Data-R), que permitirá contar con una sola fuente de datos e información que facilite la gestión y el aprovechamiento de estos en los distintos sistemas transaccionales, así como en los procesos analíticos.

Seguridad, establecerá un marco conceptual y normativo de seguridad de la información que incluye: (I) preparación de diagnóstico de la situación actual, diseño de la situación futura y período de transición, y propuesta de un nuevo marco consistente con el PETI; (II) desarrollo de los manuales de política de seguridad; (III) implantación del marco incluyendo campañas de concientización; y (IV) difusión de los instrumentos de seguridad de la información y ciberseguridad.

Multinube híbrida, servicio de nube híbrida (pública y privada basada en contenedores) para toda la plataforma de aplicaciones y servicios institucionales y para el Data-R, incluyendo almacenamiento, comunicación, seguridad, procesamiento de las aplicaciones, licencias de software, actualizaciones y soporte.

Es importante mencionar que dentro del ecosistema de la DIAN se encuentran aplicativos, componentes de software, servicios, integraciones de la DIAN, desarrollados a la medida, otros de tipo COTS, SaaS, PaaS y open source desplegados en diferentes infraestructuras como OnPremises, nube publica (Azure o AWS) o nubes públicas de terceros y sirve a más de veinte millones (20.000.000) de usuarios tanto internos como externos que pueden tener acceso a estos componentes.

Por lo anterior, la DIAN requiere una Solución de Gestión de Identidad y Acceso centralizada.

VIII. ALCANCE DE LA SOLUCIÓN

En el marco de su estrategia de modernización, la Dirección de Impuestos y Aduanas Nacionales (DIAN) requiere contar con una solución de Gestión de Identidad y Acceso (IAM), que cubra la Autenticación, Autorización y Auditoria para usuarios internos y externos incluyendo Control de Acceso a servicios y aplicaciones, alineados con las iniciativas institucionales, las políticas de seguridad y la normatividad aplicable; se espera del mismo modo, que se brinden los servicios conexos de diseño, desarrollo, implementación, migración, capacitación y transferencia de conocimiento, mantenimiento y soporte.

a. Solución Requerida

La DIAN busca adquirir una Solución de Gestión de Identidad y Acceso (IAM), centralizada que permita gestionar, controlar, monitorear, mantener trazabilidad de los accesos de los usuarios internos y externos a todos los aplicativos, componentes de software y servicios de la DIAN.

Este enfoque tiene como objetivo centralizar la identidad de los usuarios y permitir el acceso a los diferentes servicios de la DIAN a través de un único usuario y contraseña (Single SignOn) mejorando la experiencia del usuario, facilitando la administración de las identidades y brindando acceso seguro solo a los usuarios autorizados y exclusivamente a los aplicativos, componentes de software y servicios de la DIAN a los que está autorizado.

La solución de Gestión de Identidad y Acceso (IAM), debe gestionar la autenticación y autorización de los usuarios externos (ciudadanos-clientes), aproximadamente veinte millones (20.000.000), de los cuales se encuentran activos mensualmente cerca de dos millones; y usuarios internos (funcionarios), aproximadamente veinte mil (20.000), que participan en los procesos misionales y de apoyo de la DIAN.

Actualmente, el modelo de autorización de la DIAN para las aplicaciones y servicios se basa en roles y permisos, conformados por cerca de 1.300 roles con jerarquías y 10.150 funcionalidades aproximadamente. Se espera que la nueva solución de identidad optimice la gestión de acceso mediante el uso de roles, atributos, políticas y relaciones entre roles.

Se requiere que el proveedor presente y ejecute la estrategia de implementación para centralizar la gestión de identidades en la DIAN.

b. Escenarios de Autenticación y Autorización de la DIAN

La Solución de Gestión de Identidad y Acceso (IAM), se deberá personalizar y adaptar para que cumpla con los escenarios que se explican a continuación:

1. Se deberá implementar por lo menos los siguientes escenarios de ingreso a los sistemas de la DIAN:

- **A nombre propio.** Una persona natural se autentica para realizar sus trámites, servicios y consultas ante la DIAN. Esta persona puede ser un contribuyente o un funcionario actuando como contribuyente ante la DIAN.

- **A nombre de un tercero:** Una persona natural se autentica para realizar trámites, servicios y consultas a nombre de una persona natural o jurídica. Por ejemplo, el usuario ingresa como representante legal de una empresa para tramitar asuntos de la empresa.

- **Servidor DIAN:** Es un funcionario que se autentica para atender trámites y gestionar sus responsabilidades ante la Entidad.

- **Autorizaciones o poderes:** Una persona natural ingresa al sistema para realizar un trámite a nombre de una persona jurídica o natural que le ha concedido poder o autorización para ello. Tal es el caso de una empresa dedicada a realizar trámites de aduanas para varias organizaciones. Una persona puede delegar algunos de sus roles a otra persona en un rango de tiempo determinado para que ingrese al sistema en su nombre.

  La solución IAM debe garantizar la gestión de permisos delegados. En detalle, una organización puede delegar permisos a otra organización o persona en un periodo de tiempo. La organización que recibe la delegación puede asignar permisos a sus empleados en representación del delegante.

- **Organización no obligada a RUT.** organizaciones o asociaciones sin ánimo de lucro o sociedades extranjeras que no realizan actividades económicas gravables o que no tiene establecimiento permanente en Colombia.

- **Ciudadanos no obligados a RUT**: Personas naturales o extranjeras que son enrolados por funcionarios, persona jurídica o que se autogestionan.

- **Aplicaciones - B2B**: Se conceden autorizaciones a aplicaciones de terceros.

2. La asignación de roles y autorizaciones se deberá realizar en función de atributos u otras características que **son gestionadas por las aplicaciones de negocio** que se deben sincronizar automáticamente en la Solución de Identidad, entre ellas:

- **RUT:** Obligaciones del contribuyente, representantes y delegados de la sociedad, calidades aduaneras con que cuenta o su estado en el RUT.
- **Recursos Humanos:** La situación administrativa de un funcionario, ubicación geográfica, dependencia a la que pertenece y su estado.
- **RUB:** Asignar y cambiar el administrador de una Estructura sin personería jurídica, vigencia

del patrimonio autónomo y estado.

- **MUISCA - Autorizaciones y delegaciones:** Flujos de trabajo para la autorización de usuarios y la delegación de usuarios.
- **Gestión de Roles de aplicativos para funcionarios.**
  La solución IAM debe integrarse con las aplicaciones de negocio que realizan y gestionan el enrolamiento en la identidad de los usuarios, como por ejemplo las aplicaciones: RUT, Recursos Humanos, RUB y gestión de permisos delegados. Es de anotar que las aplicaciones de negocio registran características cambiantes de los usuarios y estas son insumo para la gestión de permisos.

3. Se requiere garantizar que las soluciones IAM y de Firma Electrónica de la DIAN utilicen una única contraseña.

4. Se deberá integrar la autenticación y autorización hasta con cinco (5) servicios elegidos por la DIAN (nube, OnPremises, SaaS), para definir, implementar y aplicar las mejores prácticas (frontend/backend), estableciendo pautas y directrices para que sean utilizadas por otras soluciones y sus proveedores.

c. Fases propuestas del Proyecto

La DIAN para la implementación de la Solución IAM, identifica de forma preliminar las siguientes fases, que se deben implementar de acuerdo con las Premisas, Requerimientos y demás necesidades expresadas por la Entidad, en el tiempo esperado de ejecución del proyecto **(6 meses):**

- **Planeación:** Planificación detallada del proyecto proporcionando y alineando metodología, tiempos y recursos a las necesidades específicas que la DIAN solicita para la implementación de la Solución IAM, así como los Servicios Conexos.

- **Entendimiento y Diseño:** Recopilación, inventario de información e insumos para la definición, refinamiento y diseño de estrategias, arquitecturas, componentes y subcomponentes requeridos para que la Solución IAM cumpla con los requerimientos funcionales y técnicos solicitados por la DIAN.

- **Instalación y habilitación de la Solución IAM:** Aprovisionamiento, instalación y habilitación de las capacidades de la Solución IAM y sus componentes en los distintos ambientes de trabajo (Desarrollo y Pruebas).

- **Configuración, construcción y pruebas de Escenarios de Autenticación y Autorización:** Actividades de configuración, personalización, desarrollo, integraciones para cumplir con los escenarios de autenticación y autorización de la DIAN (*numeral b de esta sección*). Los tipos de pruebas esperadas incluyen: pruebas unitarias, funcionales, de seguridad, estrés, de carga, entre otras.

- **Migración y puesta en Producción:** Proceso de migración de los usuarios, contraseñas y demás atributos necesarios a la nueva Solución de IAM, así como la puesta en Producción de toda la Solución IAM.

- **Capacitaciones y Transferencia de Conocimiento:** Entrenamiento para los usuarios técnicos, administradores y operadores de la Solución, con el fin de lograr un conocimiento profundo de la herramienta y sus personalizaciones, para que los funcionarios de la DIAN estén en capacidad de administrar, soportar y evolucionar la Solución IAM.

- **Soporte y Mantenimiento:** *Servicio de Soporte* de la Solución IAM en horario 7x24 los 365 días del año, el soporte incluye aplicación de parches, actualización de nuevas versiones, atención de incidentes, vulnerabilidades, monitoreo y revisiones periódicas de seguridad, el Proveedor debe contar con el respaldo y servicio de soporte vigente por parte del fabricante para garantizar la disponibilidad y estabilidad de la Solución IAM a adquirir. *Servicio de Mantenimiento* de la Solución IAM que incluye mantenimiento evolutivo y correctivo de las personalizaciones, extensión de la funcionalidades e integraciones de la Solución realizadas para la DIAN

  Nota: *La Fase de Soporte y Mantenimiento se iniciará al finalizar la implementación de la Solución IAM (6 meses), se espera que este servicio se preste hasta por 3 años.*

IX. TIEMPO DE IMPLEMENTACIÓN DEL PROYECTO

El tiempo esperado para la implementación de la Solución IAM (diseño, instalación, configuración, desarrollo, pruebas, despliegue en producción, capacitación) es de máximo 6 meses.

X. PREMISAS DE OBLIGATORIO CUMPLIMIENTO

- La DIAN implementará aplicativos de misión crítica bajo la arquitectura de referencia establecida en el numeral *Arquitectura de Referencia de la DIAN* de la sección de Anexos de este documento.

- La DIAN desarrollará y adquirirá aplicativos de misión crítica y de apoyo que cumplan con lo especificado en el numeral *Requisitos mínimos que deben cumplir las aplicaciones de la DIAN,* de la sección de Anexos de este documento.

- La Solución IAM debe ofrecer los servicios de autenticación y autorización para todos los aplicativos, componentes de software, servicios e integraciones de la DIAN, y esto incluye los aplicativos de misión crítica, transversales y de apoyo, en cuyos procesos intervienen diferentes tipos de usuarios (i) usuarios internos (funcionarios) y (ii) usuarios externos (ciudadanos, contribuyentes, usuarios aduaneros) de manera centralizada.

- Los aplicativos, componentes de software, servicios, microservicios e integraciones de la DIAN se encuentran desplegados en diferentes infraestructuras (OnPremises, nube pública (Azure y AWS), nubes privadas o públicas de terceros) y estos pueden ser desarrollados a la medida o pueden ser de tipo COTS, Open Source o propietarios que operen bajo modelos SaaS/PaaS/IaaS/OnPremises, la DIAN busca que todos ellos se puedan integrar con la Solución IAM.

- Todos los escenarios B2B, B2C y B2G de la DIAN deben hacer uso de la Solución IAM.

- La Solución IAM debe permitir desacoplar los permisos (autenticación y autorización) y el código, de los componentes de software (aplicaciones, microservicios, integraciones), que se encuentren desplegados en la nube de Azure o AWS de la DIAN, OnPremises y SaaS en los casos en que aplique.

- La DIAN cuenta con un API Management y un API Gateway en las nubes de Azure y AWS respectivamente y el Proveedor de Identidad (IdP) ofrecido por la Solución deberá estar integrado con estos.

- La Solución IAM debe contar como mínimo con logs de trazabilidad de auditoría de la Solución de Identidad (autorización y autenticación) de la totalidad de los eventos ocurridos.

  La solución IAM debe mantener la trazabilidad de auditoría a lo largo de cada una de las transacciones realizadas a través del servicio de identidad, de tal manera que sea posible identificar las acciones de autorización y de autenticación, como: quien, cuando, desde donde, que permisos tenía en una determinada fecha un usuario, cuando se autenticó el usuario, cambios en la asignación y revocación de roles.

- La solución IAM debe integrarse con la solución de SIEM de la DIAN.

- La solución IAM es una solución de misión crítica que debe contar con esquemas de alta disponibilidad (99.999%), ya que este es el principal punto de acceso a todos los aplicativos y servicios tecnológicos de la DIAN.

- La Solución IAM debe estar disponible en ambiente de desarrollo, pruebas y producción, estos ambientes deben estar aislados y debe permitir la promoción de la solución entre cada uno de estos ambientes.

- La Solución IAM debe exponer APIs REST para los servicios de autorización y autenticación de tal manera que permita la integración con otros sistemas y extender su funcionalidad.

- La Solución IAM debe permitir crear y personalizar flujos para autenticación y autorización. Dentro de los flujos debe ser posible invocar APIs construidos en la DIAN o de terceros.

- La Solución IAM debe permitir gestionar los usuarios y roles para los usuarios administradores, auditores y entes de control.

- La Solución IAM debe permitir la integración con Microsoft ENTRA ID / Active Directory para usuarios internos.

- La Solución IAM debe permitir la integración con LDAP IBM (OnPremises) para usuarios externos mientras la transición y reemplazo con la nueva Solución de Identidad.

- EL proveedor debe garantizar que la implementación de los requerimientos y necesidades de la DIAN no obstaculice a la Entidad para la actualización de los productos de acuerdo con el roadmap del fabricante.

- El código fuente y la propiedad intelectual de las personalizaciones, integraciones o extensión de funcionalidades realizadas para la DIAN serán de propiedad de la DIAN.

- El servicio de soporte e implementación de la Solución IAM deberá ser provisto en idioma español con especialistas certificados disponibles en el huso horario de Colombia.

XI. SOLICITUD DE INFORMACIÓN (RFI)

Por favor responda las siguientes preguntas.

1. Información del interesado

1.0 Nombre (razón social):

1.1 Identificación tributaria:

1.2 Dirección/ciudad/país:

1.3 ¿Tiene oficinas o representación en Colombia? (Sí / No) ___

1.4 Información de la persona de contacto.

- Nombre:
- Cargo:
- Teléfono:
- e-mail:

1.5 Actividad principal (Fabricante, partner, integrador, otro). ¿Cual?

1.6 Número de empleados _____

1.7 ¿Es el fabricante de la Solución IAM? (Si/No) ___

1.8 ¿Si no es el fabricante, es representante oficial del fabricante? (Si/No) ___

1.9 Enliste y describa su experiencia relacionada con la implementación de soluciones de gestión de control de acceso (autorización como servicio o solución de autorización escalable)

- Descripción de la implementación
- Alcance de la implementación
- Fecha de implementación
- Cantidad de usuarios activos (desglosar por aplicaciones)
- Cantidad de roles, atributos, políticas y relaciones
- Tecnología (productos, arquitectura)
- Duración del proyecto (meses)
- Sector (público/privado)
- Cliente
- Valor del proyecto

1.10 Liste y describa su experiencia en implementación de CIAM

- Descripción de la implementación
- Alcance de la implementación
- Fecha de implementación
- Cantidad de usuarios activos
- Volumen de peticiones por API
- Cantidad promedio de validaciones de acceso por hora
- Tecnología (productos, arquitectura)
- Duración del proyecto (meses)
- Sector (público/privado)
- Cliente
- Valor del proyecto

1.11 Describa cómo se presentaría a un eventual proceso de contratación en Colombia (directamente, unión temporal, consorcio, subcontratista, otra).

2. Información general de la Solución de identidad

2.1 Nombre de la Solución IAM:

2.2 Página web:

2.3 Descripción:

2.4 Describa las características técnicas de la Solución IAM y cada uno de sus componentes.

2.5 ¿Cuáles Modelos de implementación de la Solución IAM ofrecida soporta?

- IaaS __
- SaaS __

- PaaS __
- OnPremises ___

2.6 En caso de que la Solución IAM sea SaaS en que nube opera la Solución.

2.7 Por favor indique si la Solución de Autenticación para la DIAN puede operar en los siguientes ambientes (Si la solución la integran varios productos discrimine la información por producto):

- Nube Azure
- Nube AWS
- OnPremises
- Otro. ¿Cuál?

2.8 Por favor indique si la Solución de Autorización para la DIAN puede operar en los siguientes ambientes (Si la solución la integran varios productos discrimine la información por producto):

- Nube Azure
- Nube AWS
- OnPremises
- Otro ¿Cuál?

2.9 Indique que productos de su Solución IAM para la DIAN están disponibles en los Marketplaces de los proveedores de servicios de nube y enumérelos.

2.10 La solución tiene componentes open-source (SI/No): ____ Por favor enumérelos.

2.11 Indique ¿cuál es la estrategia que ha implementado en proyectos similares a la necesidad de la DIAN?

3. Modelo de Licenciamiento

3.1 Describa los modelos de licenciamiento que ofrecen de la Solución IAM (como se costea la solución ofrecida). Si la solución la integran varios productos discrimine la información por producto, por favor detalle los costos asociados en el anexo de Costos.

- Por servicio o transacción.
- Por usuario (desglose por categoría).
- Por tipo (concurrente, nombrada, flotante).
- Escalas de licenciamiento (indique los rangos que ofrece).
- Licenciamiento ilimitado.
- Por suscripción.
- A perpetuidad.

- Otro. Indique Cuál.

3.2 Describa el modelo bajo solución de código abierto (si aplica).

3.3 En caso de que el licenciamiento sea en la Nube, indique si los costos incluyen el consumo propio de la plataforma.

3.4 Si la Solución IAM o los componentes que la conforman, requiere otro tipo de licenciamiento por favor indíquelo.

3.5 Indique las condiciones de renovación del licenciamiento en el tiempo por producto y otras condiciones comerciales aplicables.

4. Cobertura de la Solución IAM

4.1 Por favor responda con la cobertura de la Solución IAM ofrecida. En el archivo *excel* "*Anexo A. Requerimientos técnicos RFI Solución IAM.xlsx*" se listan los requerimientos de alto nivel requeridos por la DIAN, por favor responda sobre este archivo teniendo en cuenta las siguientes instrucciones:

✓ En la columna "**Cumple**", el interesado debe ingresar de qué manera la Solución IAM cubre el requerimiento técnico solicitado por la DIAN.

- **Totalmente disponible.** La solución IAM cubre el requerimiento técnico mediante una funcionalidad o componente existente sin requerir desarrollo o parametrización de la solución.
- **Requiere parametrización.** La solución IAM cubre parcialmente el requerimiento técnico y requiere parametrización de la funcionalidad o componente existente.
- **Requiere desarrollo.** La solución IAM cubre parcialmente el requerimiento técnico y requiere un desarrollo a la medida para extender la funcionalidad existente para que se adapte al requerimiento de la DIAN en el corto plazo (durante la implementación del proyecto).
- **No Disponible.** El requerimiento no está disponible en la solución IAM.

✓ En la columna "**Cómo**" indique como a través de las capacidades de la solución IAM puede cubrir el requerimiento técnico.

✓ En la columna "**Producto o Componente de la arquitectura propuesta**" indique que componente, funcionalidad o producto de la solución IAM ofrece las capacidades descritas para cubrir el requerimiento técnico.

5. Arquitectura de la Solución

5.1 Incluya un diagrama de Arquitectura de alto nivel para la Solución IAM ofrecida para la DIAN (On-premises, Nube Azure DIAN, Nube AWS DIAN, IaaS DIAN).

4.1 Tenga en cuenta la arquitectura presentada en el numeral Arquitectura de Referencia de la DIAN de la sección de Anexos y los escenarios de autenticación y autorización descritos en la sección “VIII Alcance de la Solución/ b Escenarios de autenticación y autorización de la DIAN”

5.2 Describa detalladamente la arquitectura de la solución IAM, describa los principales componentes (almacenamiento, servicios, agentes, software, bases de datos, etc.) y adjunte la documentación que considere relevante.

5.3 Indique si la Solución IAM soporta un modelo hibrido, es decir, para el caso de autorización puede funcionar para aplicaciones OnPremises y en la Nube, en caso de que sea afirmativo ¿cuáles características mínimas deben cumplir esas aplicaciones?

5.4 Describa de forma textual y gráfica cómo está estructurado el modelo de autorización de forma que se indique la jerarquía y sea posible entender el nivel de granularidad de los roles y las autorizaciones que maneja la Solución IAM.

5.5 ¿Cómo se garantiza el rendimiento y los tiempos de respuesta de acuerdo con las necesidades de la DIAN, basados en el número de usuarios externos e internos y la cantidad de aplicaciones de la Entidad?

6. Estándares y Certificaciones

6.1 Indique los estándares que cumple la Solución IAM (por ejemplo: OPEN ID Connect, SAML, OAuth, entre otros).

6.2 Indique las certificaciones de seguridad con que cuenta el Fabricante (por ejemplo: SOC 2, ISO 27001, CSA Star, HIPAA/HITECH entre otras).

6.3 Indique las certificaciones de seguridad con que cuenta el Proveedor (por ejemplo: SOC 2, ISO 27001, CSA Star, HIPAA/HITECH entre otras).

6.4 Indique las certificaciones de desarrollo y gestión con que cuenta el Proveedor (por ejemplo: CMMI, nivel de partner, entre otras).

6.5 ¿La Solución ofrecida responde al Framework de Identity Fabric y cómo lo implementa?

7. Capacidades de la Solución

7.1 La DIAN permite que un usuario pertenezca a varias organizaciones, para cada organización el usuario tiene permisos diferentes. ¿La Solución IAM cubre este escenario? Por favor describa e ilustre como soluciona este caso de uso.

7.2 La DIAN permite la gestión de permisos delegados. En detalle, una organización puede delegar permisos a otra organización o persona en un periodo de tiempo. La organización que recibe la delegación puede asignar permisos a sus empleados en representación del delegante. Por favor describa e ilustre como soluciona este caso de uso.

7.3 Por favor indique los escenarios de enrolamiento de usuarios que ofrece la solución.

7.4 Indique cómo puede implementar la gestión de roles planteada por la DIAN en el *numeral VIII - subnumeral b* de este documento.

7.5 ¿Cuál es el nivel de granularidad de los roles y permisos que gestiona la Solución IAM?

7.6 Indique el número máximo de usuarios, roles, políticas y permisos que soporta la IAM.

7.7 Indique si la solución ofrecida tiene alguna limitante para soportar la operación de los volúmenes de usuarios de la DIAN.

7.8 Indique el número máximo de peticiones o transacciones concurrentes por segundo que soporta la Solución IAM.

7.9 ¿Cuál es el porcentaje de disponibilidad que puede garantizar para la Solución IAM ofrecida?

7.10 ¿Cómo escala la solución? (gestión de accesos y picos en los volúmenes de usuarios)

7.11 ¿Cuáles son los mecanismos de backup de la información que gestiona la Solución IAM? Indique detalladamente cual es la política para cada tipo de información (parametrización, de operación, logs, etc.)

7.12 ¿Cuál es el tiempo de retención de los logs que gestiona la Solución IAM?

8. Migración de las identidades actuales a la Solución IAM

8.1 ¿Qué estrategia de migración ha implementado en proyectos similares a la necesidad de la DIAN? Detalle la estrategia de migración para una configuración hibrida (aplicaciones on-

premises, en la nube, saas), como la descrita para la DIAN.

8.2 ¿Qué insumos requiere para la migración de identidades a la Solución IAM propuesta?

8.3 ¿Cuáles estrategias ha implementado para la migración y transición de soluciones IAM hasta la puesta en producción?

8.4 En su experiencia, ¿cuánto tiempo tardó el proceso de migración de identidades a una nueva solución?

8.5 En su experiencia, ¿cuánto tiempo tardó el proceso de transición de identidades a una nueva solución (convivencia de la solución actual con la nueva solución IAM implementada)?

9. Mapa de ruta de la Solución IAM

9.1 Indique el mapa de ruta para la evolución de sus productos en el corto, mediano y largo plazo, indicando horizonte de tiempo, nuevas funcionalidades, capacidades o mejoras.

9.2 ¿Cuál ha sido el histórico de periodicidad de Versionamiento y evolución de la solución?

10. Servicio de capacitación

10.1 Indique cuales son las características de servicio de capacitación y transferencia de conocimiento para los usuarios técnicos, administradores y operadores de la Solución IAM

10.2 Indique si ofrece programas de certificación de conocimiento y capacitación.

10.3 Indique si los manuales de los productos están disponibles en internet.

10.4 Indique si cuenta con una plataforma de entrenamiento para la realización de las capacitaciones y describa las capacidades de esta herramienta.

11. Mantenimiento, Soporte y Garantía

11.1 Garantía de la solución IAM (No. de meses de garantía luego de la aceptación del proyecto y alcance de esta).

11.2 Indique, ¿cuáles son las características del servicio de mantenimiento?

11.3 ¿Cómo gestiona los mantenimientos programados para minimizar el impacto en la operación de sus clientes?

11.4 Enumere los tipos del servicio de soporte, características y detalle el costo de cada uno en el anexo correspondiente (*Anexo B. Precios de Referencia Solución IAM*).

11.5 Indique si dispone de una comunidad de usuarios y foros, si demanda costo por favor especifíquelo en el *Anexo B. Precios de Referencia Solución IAM*.

11.6 Es necesario un Soporte remoto 7x24, indique ¿cuáles son los niveles de servicio (SLA) para las opciones ofrecidas? Detalle el costo de cada uno en el anexo correspondiente (*Anexo B. Precios de Referencia Solución IAM*).

11.7 Indique las condiciones del Mantenimiento Preventivo para cada una de las opciones que ofrece. Detalle el costo de cada uno en el anexo correspondiente (*Anexo B. Precios de Referencia Solución IAM*).

11.8 Indique las condiciones de Mantenimiento Correctivo para cada una de las opciones que ofrece. Detalle el costo de cada uno en el anexo correspondiente (*Anexo B. Precios de Referencia Solución IAM*).

11.9 Indique las condiciones de Mantenimiento Evolutivo para cada una de las opciones que ofrece. Detalle el costo de cada uno en el anexo correspondiente (*Anexo B. Precios de Referencia Solución IAM*).

12. Información de experiencia

Describa en el siguiente cuadro, las experiencias similares en la implementación de la Solución IAM ofrecida, considerando el porcentaje de participación en la experiencia aportada.

- Fecha Inicio (año/mes/día)
- Fecha Fin (año/mes/día)
- ¿Actualmente la Solución IAM implementada, se encuentra en producción? (Si/No)
- Indique la fecha de salida en producción (año/mes/día)
- Indique el modelo de despliegue (IaaS, SaaS, PaaS, OnPremises, Hibrido)
- País
- Descripción del proyecto y alcance de la solución
- % participación
- Valor del contrato/proyecto (USD)
    - Porcentaje del valor de licenciamiento o costos anuales del producto
    - Porcentaje del valor de servicios de personalizaciones y adecuaciones
    - Porcentaje de otros valores relevantes e indique cuales
- Entidad cliente (incluir información de contacto)

- Componentes y/o productos implantados para cumplir con el alcance del proyecto
- Tipo de licenciamiento (A perpetuidad, por suscripción, por transacción, otro)

Por favor diligencie esta información en el cuadro siguiente

Fecha Inicio (año/mes/día)	Fecha Fin (año/mes/día)	¿Actualmente la Solución IAM implementada, se encuentra en producción? (Si/No)	Indique la fecha de salida en producción (año/mes/día)	Indique el modelo de despliegue (IaaS, SaaS, PaaS, OnPremises, Hibrido)	País	Entidad cliente (incluir información de contacto)	Descripción del proyecto y alcance de la solución	% participación	Valor del contrato proyecto (USD)	Porcentaje del valor de licenciamiento o costos anuales del producto	Porcentaje del valor de servicios de personalizaciones y adecuaciones	Porcentaje de otros valores relevantes e indique cuales	Componentes y/o productos implantados para cumplir con el alcance del proyecto	Tipo de licenciamiento (A perpetuidad, por suscripción, por transacción, otro)

13. Cronograma estimado de implementación

Basado en su experiencia previa, ¿cuál es el cronograma típico de implementación de la solución (fases, hitos, duración) para un proyecto de esta magnitud? Adjuntar un cronograma típico estimado a alto nivel.

14. Equipo de trabajo

En el siguiente cuadro, describa el equipo de trabajo que considera se requiere para implementar, operar y mantener este tipo de soluciones indicando el perfil, cantidad, las responsabilidades principales, formación y experiencia mínima que se requiere. Tener en cuenta el alcance y tiempo esperado de implementación.

Perfil	Cantidad	Formación	Experiencia	Responsabilidades principales

15. Costos

Indique los costos estimados por producto y para los servicios conexos para la implementación en la DIAN. Por favor diligencie el cuadro en el *Anexo B - Precios de referencia Solución IAM.*

XII. ANEXOS

16. ARQUITECTURA DE REFERENCIA DE LA DIAN

La arquitectura de la DIAN se basa en un modelo de multinube híbrida que comprende varios componentes: una nube principal (Azure), una nube secundaria (AWS), la infraestructura en tierra (que incluye el DataCenter y/o Nube privada) y las nubes de terceros (soluciones SaaS como ERP, CRM, entre otros).

En esta infraestructura, las soluciones se organizan de manera que la nube principal alberga las soluciones misionales de la entidad. La comunicación entre estas soluciones se lleva a cabo exclusivamente a través de la Plataforma de Interoperabilidad (PdI) cuyo mecanismo predeterminado son las API basadas en REST, incluyendo Open Data y GraphQL como alternativas válidas (gRPC es también una alternativa en escenarios aprobados por la entidad). La representación de datos por defecto es el formato JSON, soportando otros esquemas (como XML) para sistemas legados o externos donde la organización no tenga injerencia.

El núcleo central para la habilitación de una plataforma unificada de servicios es la Identidad Digital DIAN (ID). Esta plataforma proporciona un esquema de inicio de sesión único (SSO) para toda la organización, centralizando la gestión de acceso y autorización para todos los servicios. Aquí es donde se administran los usuarios (incluyendo contribuyentes, funcionarios y aplicaciones) en aspectos relacionados con la autenticación, autorización y auditoría. Las aplicaciones dentro del ecosistema de la DIAN delegan la gestión de estos aspectos al servicio de Identidad Digital. El protocolo principal utilizado para la autenticación es OpenID Connect (OIDC) y la autorización utiliza un esquema basado en RBAC (Role Access Control), ABAC (Attribute-Based Access Control) y PBAC (Policy-Based Access Control).

A continuación, se presenta un diagrama general de la Arquitectura Digital de Referencia, que permite una visión global del ecosistema DIAN:

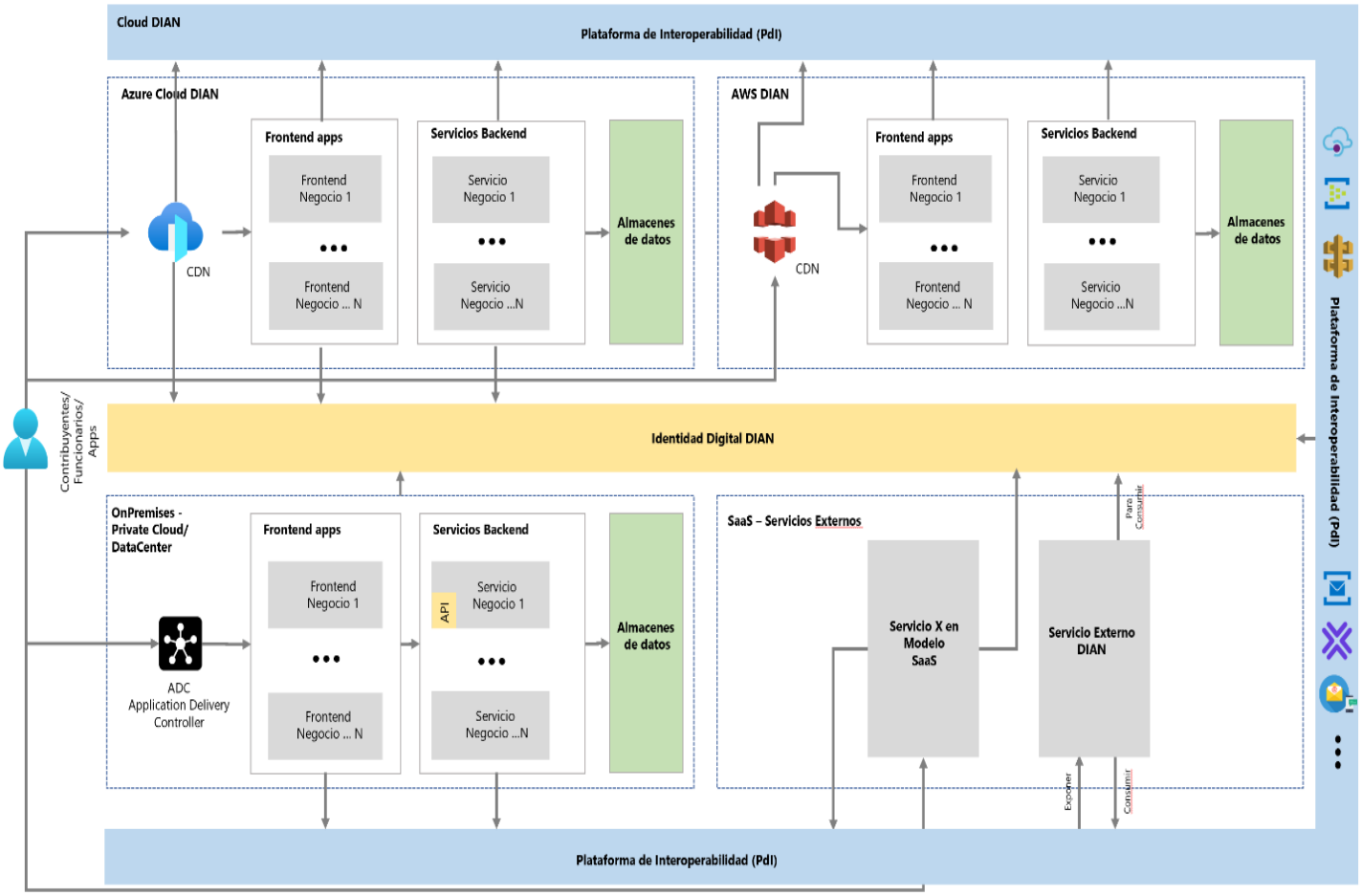


Ilustración 1. Diagrama general de Arquitectura Digital de Referencia

Las aplicaciones están organizadas según una arquitectura de servicios y microservicios. Esta estructura se fundamenta en:

- **Frontend:** Consiste en los elementos de la interfaz de usuario que siguen un esquema de Aplicaciones de Página Única (SPA), Microfrontends, Aplicaciones Web Progresivas (PWA) y Web basado en Angular.
- **Backend:** Engloba la lógica empresarial a través de la exposición de servicios y microservicios utilizando tecnologías serverless y de contenerización de aplicaciones. Los lenguajes de programación disponibles para la construcción son Java, Python y C#.
- **Acceso a datos:** Proporciona almacenes de datos SQL y NoSQL ofrecidos por los proveedores de nube para satisfacer los distintos escenarios empresariales requeridos en la organización.

Como se puede apreciar en el diagrama, todas las soluciones están conectadas tanto al servicio de Identidad Digital como a la Plataforma de Interoperabilidad, la cual también se integra con

Identidad Digital. Esta configuración posibilita que las soluciones puedan acceder a cualquier servicio, sin importar dónde estén alojadas y sin necesidad de realizar configuraciones específicas adicionales para lograrlo. En otras palabras, esta integración permite una interoperabilidad fluida entre las diferentes soluciones, simplificando significativamente el acceso a los servicios del ecosistema para todos los participantes.

La elección entre una infraestructura en la nube o local (OnPremises) influye en cómo las aplicaciones pueden aprovechar las capacidades nativas para agilizar y simplificar el desarrollo. Una arquitectura base detallada es definida por la DIAN para implementar soluciones, mediante la definición de directrices específicas para los ámbitos de aplicación.

Los datos juegan un papel crucial en toda la arquitectura, por lo que se prioriza el uso de almacenes especializados capaces de gestionar diversos tipos de información (SQL y NoSQL). La arquitectura cuenta con mecanismos detallados para aprovechar al máximo la información generada por las soluciones, así como la implementación de informes, indicadores y paneles de control tomando como base la definición de escenarios específicos para su implementación.

Las soluciones externas o SaaS, deben cumplir con un conjunto específico de requisitos para integrarse con éxito en el ecosistema de la organización. Estos requisitos incluyen la necesidad de integrarse con el servicio de Identidad Digital y utilizar la Plataforma de Interoperabilidad. En el caso de que la DIAN sea cliente de algún sistema externo, ya sean entidades nacionales o internacionales, públicas o privadas, la Plataforma de Interoperabilidad establece un modelo de Conectores. Este enfoque permite evitar el acoplamiento directo de los servicios de la DIAN con las tecnologías, protocolos, esquemas de seguridad, taxonomías y representaciones de terceros correspondientes a dichos servicios externos.

El acceso a todas las soluciones o APIs de la plataforma requiere obligatoriamente el paso a través de servicios que realizan tareas como balanceo de carga, enrutamiento de tráfico, SSL offloading, WAF y otros mecanismos diseñados para respaldar la redundancia, el manejo de fallos, el monitoreo y la analítica, entre otros aspectos. Ninguna solución de la DIAN puede exponer directamente sus servicios sin primero pasar por los correspondientes CDN y Gestor de API definidos en la Arquitectura Digital de Referencia. Estos servicios, a su vez, están integrados con el servicio de Identidad Digital para funcionar como la primera línea de validación de aspectos de acceso para cualquier solicitud.

Arquitectura de la Plataforma de Interoperabilidad (PDI)

La arquitectura de la plataforma de interoperabilidad en la nube híbrida de la DIAN está diseñada para facilitar la integración eficiente y segura de los servicios existentes y futuros disponibles en Azure, AWS, OnPremises y con servicios SaaS. Se basa en un conjunto de capacidades base en los que se incluyen ETL, Gestor de API, integraciones Event-driven, Pub/Sub y Colas, Orquestación de procesos, Canales (correo, SMS y WhatsApp, Push), Data Streaming y XROAD (Plataforma definida por MinTic). Todos estos servicios se implementan sobre un protocolo de seguridad robusto, OpenID Connect (OIDC), proporcionado por el servicio de Identidad Digital de la DIAN.

El mecanismo predeterminado para lograr la interoperabilidad son las API basadas en REST, las cuales incluyen gRPC, Open Data y GraphQL como alternativas válidas, junto con la representación en formato JSON. Aunque no se descarta completamente el uso de FTP y las interfaces basadas en archivos, su implementación solo será permitida con la aprobación del grupo de arquitectura, y exclusivamente para escenarios legados en los cuales la DIAN no tenga una participación tecnológica directa.

Otro componente fundamental de la Plataforma de Interoperabilidad (PdI) son los Conectores, los cuales desempeñan un papel crucial en la estandarización y el desacoplamiento de servicios externos, SaaS o legados. Su función es garantizar que estos servicios puedan ser consumidos por todos los servicios disponibles en el ecosistema de la DIAN. Los Conectores evitan que los sistemas internos se vean obligados a acoplarse con tecnologías, protocolos y estándares de seguridad que no están bajo el control de la DIAN. Esto se logra al consumir servicios que no están controlados por la entidad y cuyos lineamientos no están alineados con los de la DIAN.

A continuación, se presentan un diagrama general de la PdI y su rol dentro del ecosistema como intermediario entre todas las interacciones de los servicios dispuestos.

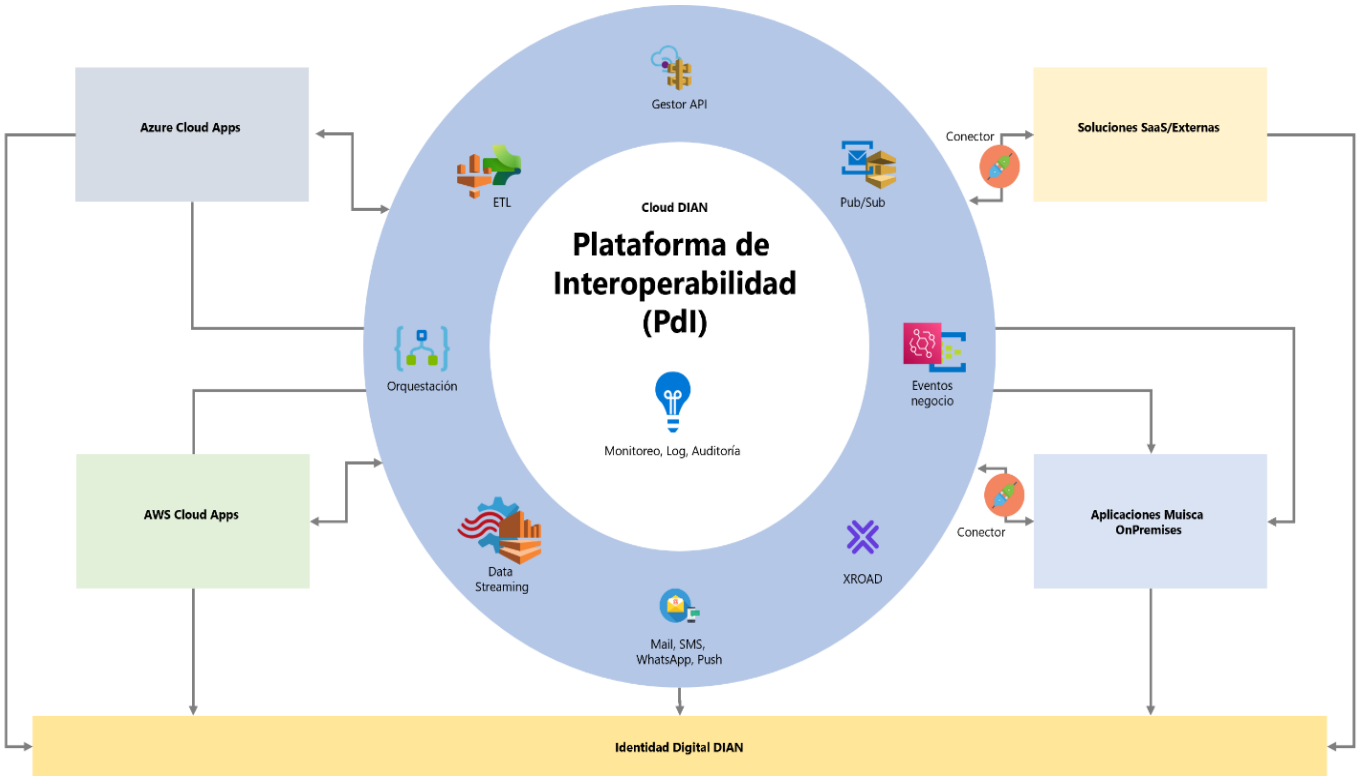


Ilustración 2. Diagrama General Plataforma Interoperabilidad

Como se observa en el diagrama anterior, la Plataforma de Interoperabilidad (PdI) aborda los

escenarios de interacción más comunes, evitando la implementación individualizada para cada solución. Esto conlleva a que las soluciones dentro del ecosistema utilicen exclusivamente los servicios proporcionados por la PdI para satisfacer todas sus necesidades de interacción. El uso de herramientas, librerías o servicios externos a los ofrecidos en la plataforma no es permitido, al igual que no seguir los parámetros de uso definidos para los mismos.

La plataforma refuerza la autenticación y autorización de los servicios expuestos al integrarse con el servicio de Identidad Digital de la DIAN. Es fundamental asegurar la seguridad de las APIs publicadas en la PdI mediante esta integración con el servicio de Identidad Digital. Este enfoque centralizado en el gobierno de la autorización no solo proporciona un mayor nivel de seguridad, sino que también facilita la gestión eficiente de los cambios y restricciones de recursos para todos los participantes de la plataforma.

Los conectores se implementan principalmente utilizando arquitectura Serverless o de contenedores, según sean las necesidades y tecnologías que se involucran para su implementación. Estos conectores deben responder a las necesidades no funcionales de la integración que pretender abstraer, por lo que también deben cumplir con lineamientos particulares para su construcción.

17. REQUISITOS MINIMOS QUE DEBEN CUMPLIR LAS APLICACIONES DE LA DIAN

Una de las directrices fundamentales para todas las aplicaciones dentro del ecosistema de la DIAN ya sean desarrolladas a la medida o adquiridas es la integración con su proveedor de identidad, este está encargado de gestionar la autenticación y autorización de los usuarios. El servicio de identidad de la DIAN se basa en los estándares OpenID Connect (OIDC)/WebAuth, compatibles con el estándar FIDO 2.0.

Entre los requisitos específicos que deberán soportar las aplicaciones desarrolladas a la medida o adquiridas para la integración con la Solución de Identidad de la DIAN, se encuentran los siguientes:

Autenticación

- Las aplicaciones deberán utilizar el protocolo OIDC/WebAuth para la autenticación de usuarios mediante la integración con el proveedor de identidad de la DIAN.
- Las aplicaciones deben soportar de estándares FIDO 2.0.
- La DIAN establece el proveedor de identidad (IdP).
- Las aplicaciones deberán ser compatibles con el perfil core de OpenID Connect.
- Las aplicaciones deberán soportar el uso de tokens de acceso y tokens de refresco.

Autorización

- Las aplicaciones deben utilizar el protocolo OpenID Connect para la autorización de usuarios.
- El proveedor de identidad de la DIAN actuará como Authorization Server (AS).
- Las aplicaciones deberán soportar el uso de modelos RBAC, ABAC, PBAC y ReBAC para

la gestión de roles de usuarios ofrecidos por el proveedor de identidad de la DIAN.

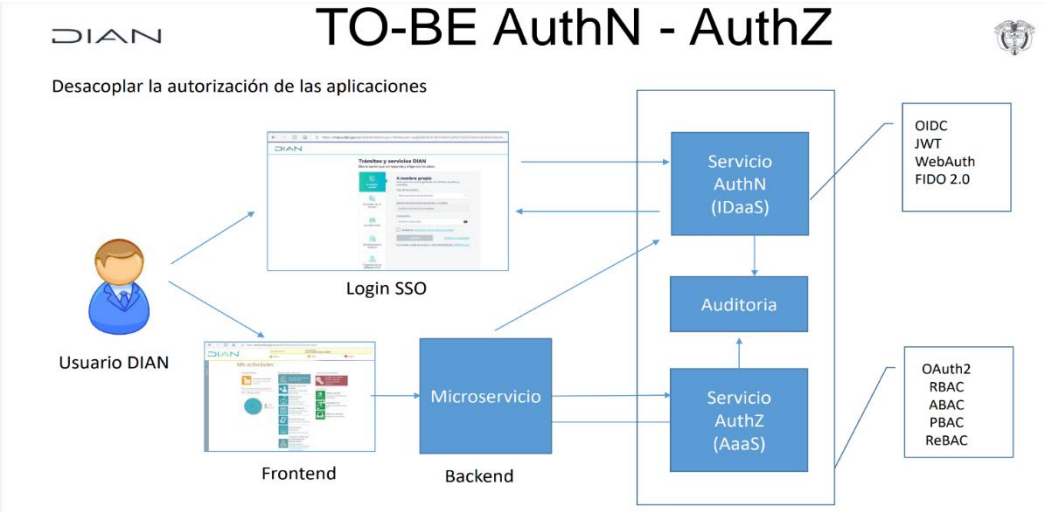
- Las aplicaciones deberán solicitar permisos para acceder a los recursos.

Otros requerimientos

- Las aplicaciones deberán utilizar HTTPS para la comunicación con el proveedor de identidad de la DIAN.
- Las APIs ofrecidas por la aplicación deberán estar aseguradas contra el proveedor de identidad de la DIAN.

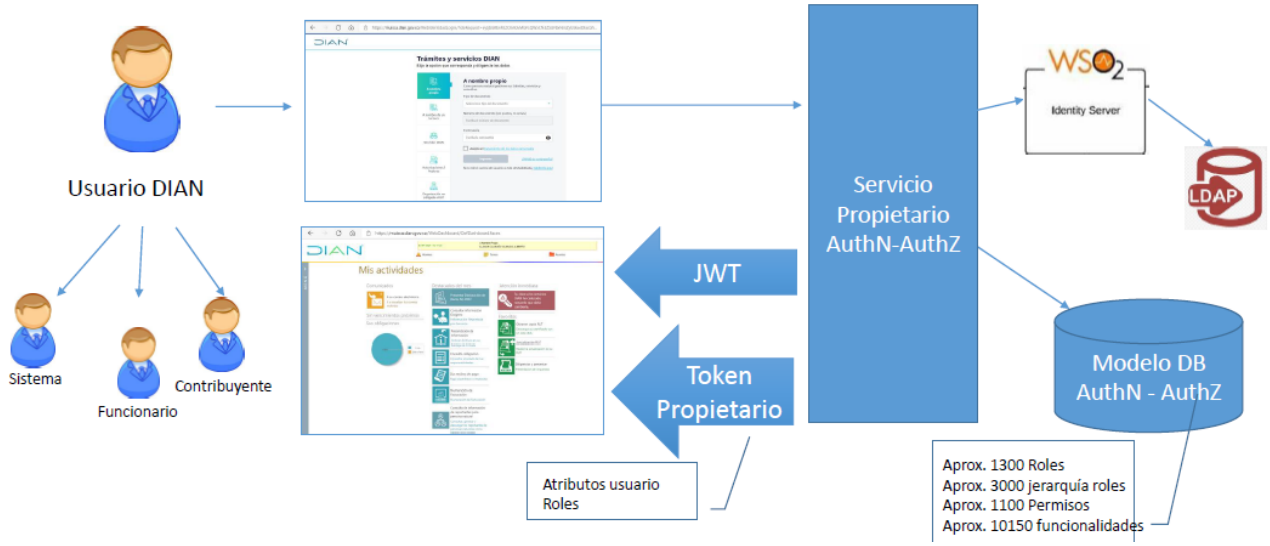
18. TO-BE AuthN – AuthZ

La solución de identidad debe permitir desacoplar los permisos de la lógica de las aplicaciones (microservicios)



19. AS-IS

AS-IS AuthN - AuthZ



AS-IS Autenticación

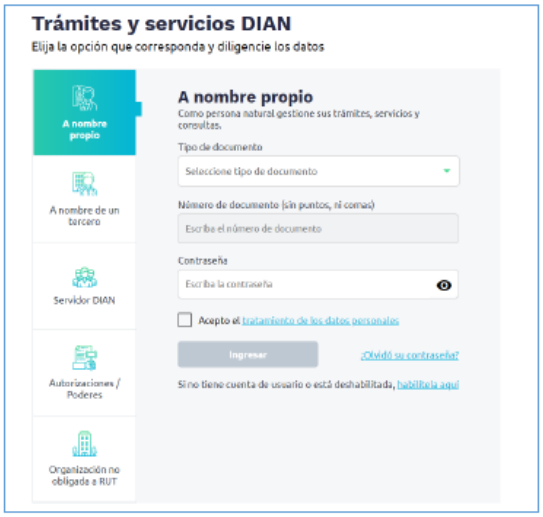
Definiciones

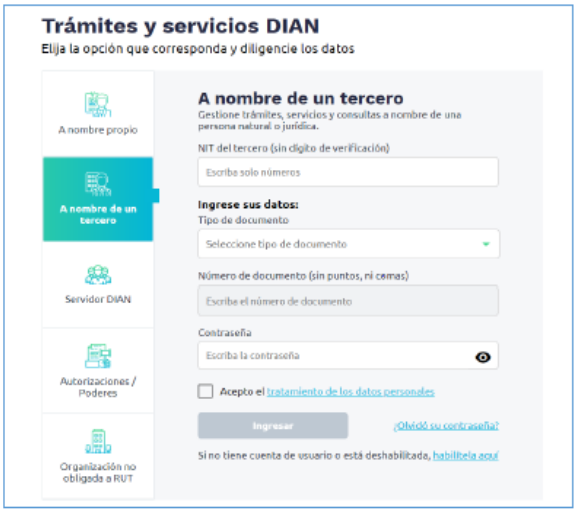
- Persona natural: ciudadano
- Persona jurídica: empresa, entidad del estado, etc.
- Registro Único Tributario (RUT) Permite identificar a los clientes de la DIAN (responsabilidades tributarias, calidades aduaneras, representantes., ubicación, correo, teléfonos, sucursales, socios, capital, etc.) y le asigna un número de identificación conocido como NIT.
- Para autenticarse en el sistema se requiere el NIT del contribuyente y el tipo y número de documento de la persona natural que lo representa.

AS-IS Autenticación

Nuestro Login SSO

Un usuario se puede autenticar de varias formas: como personal natural (a nombre propio), en representación otra persona u organización, como funcionario o como autorizado (delegación de roles). https://muisca.dian.gov.co.





AS-IS Autenticación

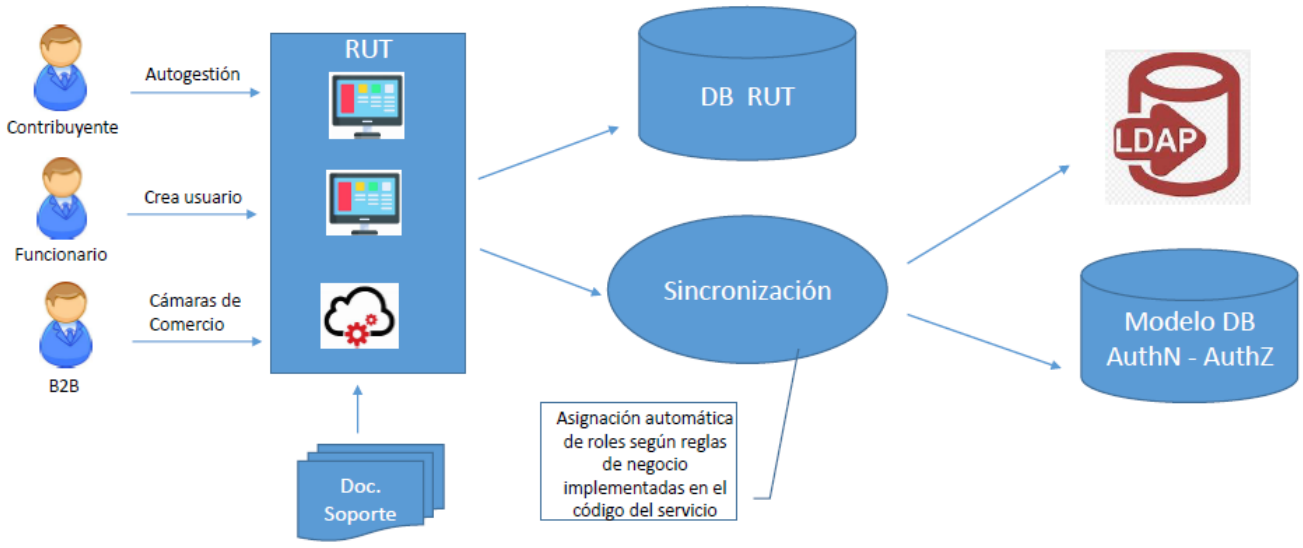
Casos de Uso de Enrolamiento

- Inscripción de personas (naturales y jurídicas) en el RUT (Registro Único Tributario)
- Inscripción de organizaciones no obligadas a RUT en el RUB(Registro Único de Beneficiarios
- Funcionarios por medio del sistema de administración de personal.
- Inscripción de personas no obligadas a RUT
- Auto inscripción de personas naturales no obligadas a RUT
- Inscripción de aplicaciones internas / externas

AS-IS Autenticación

Casos de Uso de Enrolamiento

Inscripción de personas en el RUT

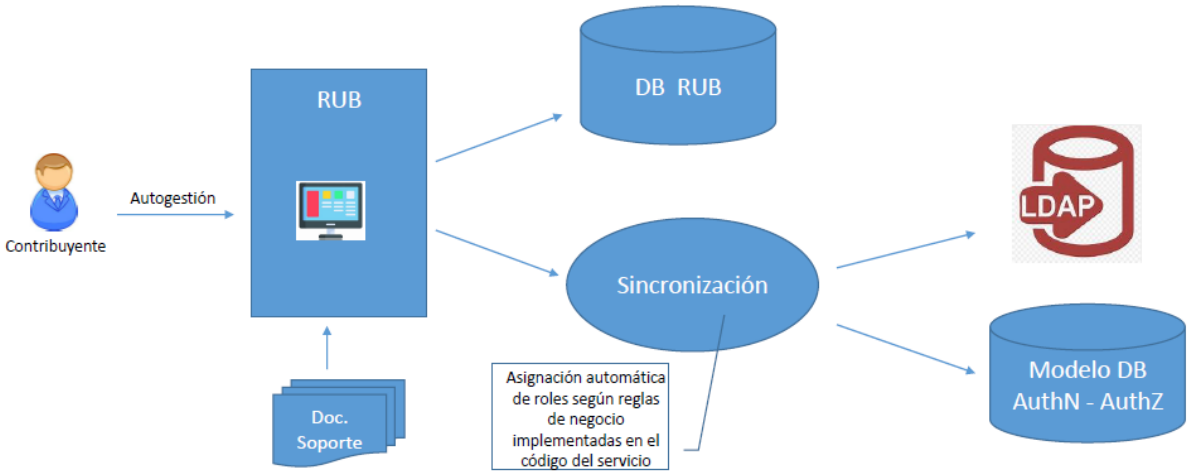


DIAN

AS-IS Autenticación

Casos de Uso de Enrolamiento

Inscripción de organizaciones no obligadas a RUT

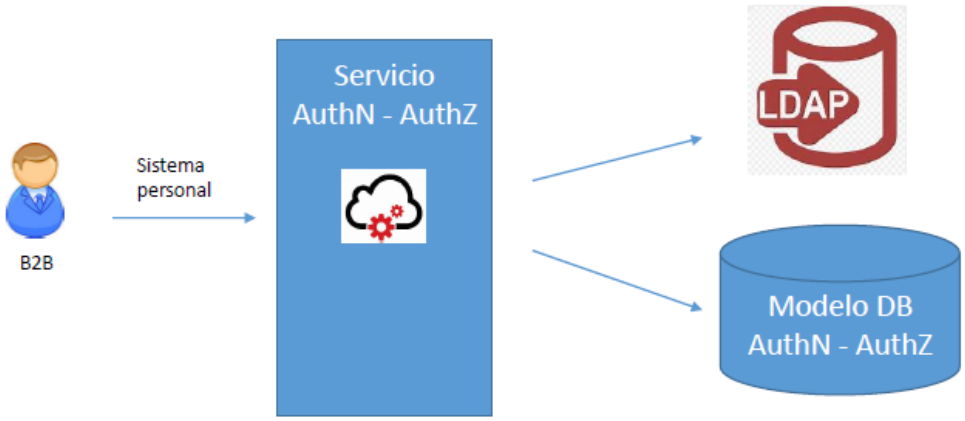


DIAN

AS-IS Autenticación

Casos de Uso de Enrolamiento

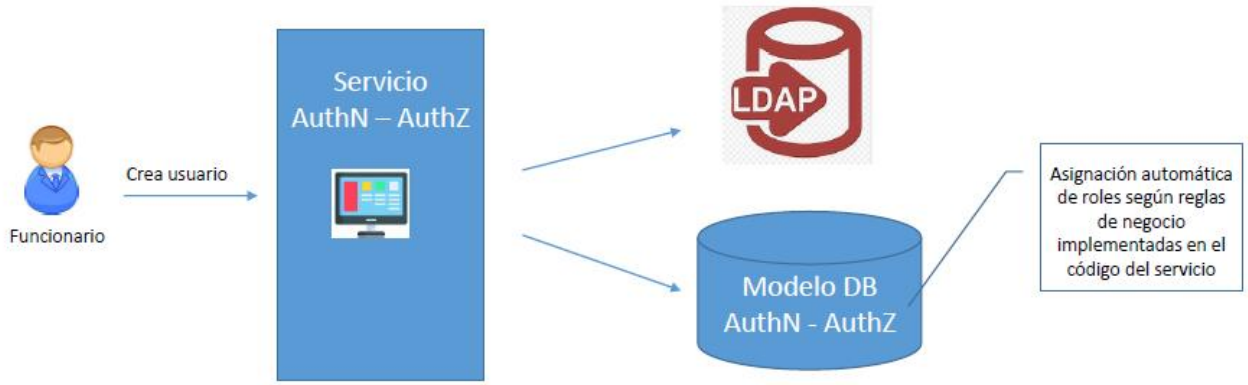
Funcionarios por medio del sistema de administración de personal



AS-IS Autenticación

Casos de Uso de Enrolamiento

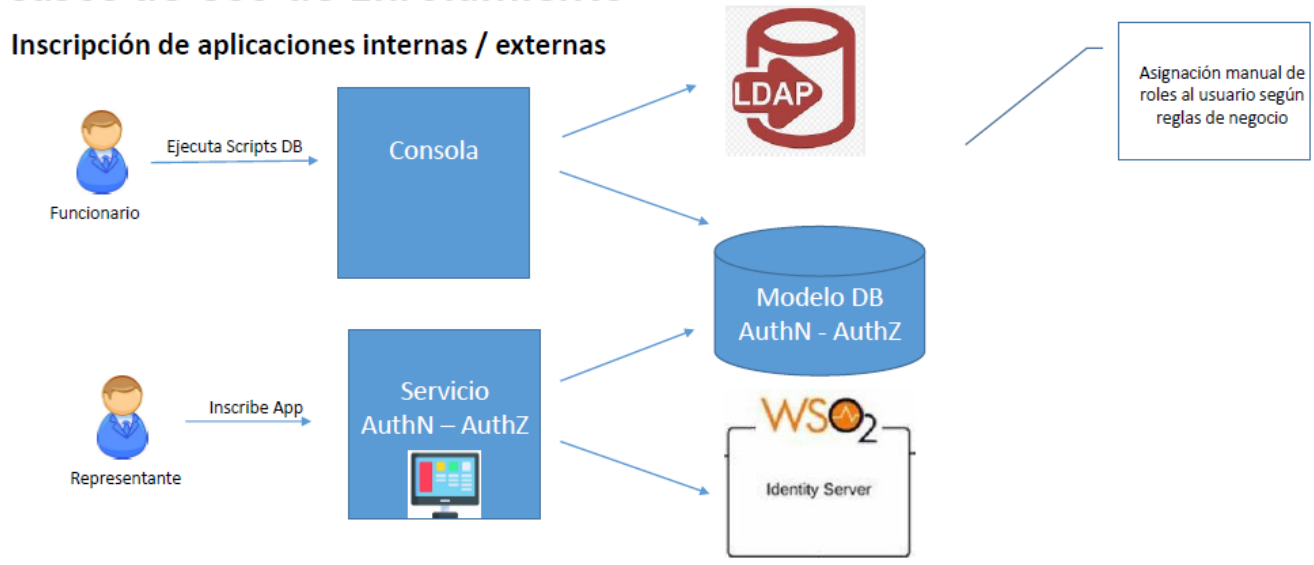
Inscripción de personas no obligadas a RUT



AS-IS Autenticación

Casos de Uso de Enrolamiento

Inscripción de aplicaciones internas / externas



AS-IS Autorización

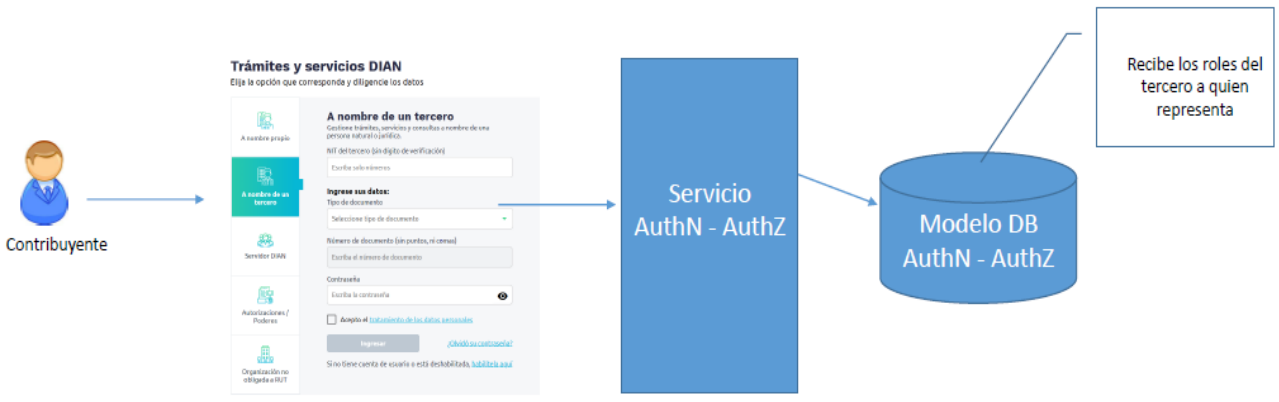
Definiciones

- Las aplicaciones usan un modelo RBAC centralizado para realizar el proceso de autorización.
- Las autorizaciones al consumo se los servicios se realiza mediante parametrización en base de datos del modelo propietario.
- En el registro de las personas jurídicas en el RUT se definen las personas naturales que actuaran como sus representantes. Ejemplo (Representante Legal, contador, Revisor fiscal, etc.)
- Según el tipo de representación y los atributos tributarios, aduaneros y cambiarios de las personas jurídicas en el RUT se realiza la (des)asignación automática de los roles al(los) representante(s).
- Una persona puede delegar algunos de sus roles a otra persona en un rango de tiempo determinado para que ingrese al sistema en su nombre.
- Una persona natural puede ser representante de miles de personas naturales, jurídicas y/o organizaciones no obligadas a RUT

AS-IS Autorización

Casos de Uso de Enrolamiento

Persona natural ingresa en representación de una persona u organización



Vista Login Terceros/Organizaciones

AS-IS Autorización

Casos de Uso de Enrolamiento

Persona natural o jurídica delega sus roles a otra persona natural y/o jurídica