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

CONTRATO DE PRÉSTAMO BID 5148/OC-CO

ESTUDIO DE MERCADO

CONSULTORÍA ESPECIALIZADA EN DISEÑO E IMPLEMENTACIÓN DEL MODELO OPERATIVO DE GOBIERNO DE IDENTIDADES Y ACCESOS (IAM)

FEBRERO 2026

Contenido

GLOSARIO Y REFERENCIAS

- IAM: Identity and Access Management
- IGA: Identity Governance and Administration
- PAM: Privileged Access Management
- AM: Access Management
- OSI: Oficina de Seguridad de la Información
- MSPI/SGSPI: Modelos de Seguridad y Privacidad de la Información
- PETD: Proyectos Estratégicos de Transformación Digital
- NSGT – Nuevo Sistema de gestión Tributaria
- NSGA - Nuevo Sistema de gestión Aduanera
- NSGC - Nuevo Sistema de gestión Corporativa
- NSGDEA - Nuevo Sistema de gestión Documental
- SoD: Segregation of Duties
- Joiner-Mover-Leaver: Ciclo de vida del usuario (ingreso, cambio, retiro)

INTRODUCCION

En el marco de su proceso de modernización tecnológica y transformación digital, la Dirección de Impuestos y Aduanas Nacionales (DIAN) ha identificado la necesidad de evolucionar su gestión de identidades hacia un modelo de gobierno unificado y eficiente. El objetivo es alinear la administración de accesos con la estructura de procesos de la Entidad, garantizando que los permisos otorgados correspondan estrictamente a las necesidades del negocio bajo la premisa de Zero Trust

Con este propósito, la Entidad busca integrar mejores prácticas de industria que permitan optimizar el ciclo de vida de los usuarios, fortalecer los mecanismos de control y facilitar la auditoría sobre los sistemas de información. Para lograrlo, se requiere contar con servicios de consultoría especializada que apoyen el diseño de una estrategia de gobierno de identidades integral, la definición de roles funcionales y el establecimiento de lineamientos claros para su implementación en las nuevas plataformas tecnológicas.

Por lo anterior, la DIAN adelanta el presente estudio de mercado con el fin de identificar empresas con experiencia en la definición de modelos de gobierno de identidades (IGA) y minería de roles. En ese sentido, la recepción de información técnica y económica derivada de este ejercicio tiene como único propósito estimar el presupuesto oficial y analizar la oferta del sector. De conformidad con las políticas del Banco Interamericano de Desarrollo (BID), en especial la GN-2350-15, se aclara que este documento no constituye una solicitud de propuesta, no es vinculante, no forma parte de un proceso de selección activo y no genera obligación contractual alguna para la Entidad.

OBJETIVO

Obtener información sobre las condiciones comerciales, técnicas y financieras de los servicios de consultoría disponibles en el mercado para el diseño e implementación de un Modelo de Gobierno y Operativo de Identidades y control de Accesos. Esto incluye el entendimiento de la situación actual, la definición del catálogo de roles de negocio por procesos y el acompañamiento técnico-conceptual orientado a apoyar su adopción y alineación con los sistemas de información de la Entidad.

CRONOGRAMA

A continuación, se relacionan las fechas estimadas para las etapas del estudio de mercado:

Actividad	Fecha Estimada
Fecha de lanzamiento del Estudio de Mercado	23/02/2026
Fecha máxima para presentar observaciones	02/03/2026
Fecha máxima para respuesta a las observaciones	09/03/2026
Fecha límite para envío de cotizaciones	19/03/2026

La DIAN podrá solicitar aclaraciones sobre la información enviada si lo considera necesario.

El presente documento se publicará en el sitio web del Fondo DIAN (https://www.dian.gov.co/dian/Paginas/Fondo-DIAN.aspx) para centralizar la información.

Toda comunicación, consulta o envío de propuestas relacionado con este estudio debe realizarse exclusivamente a través del correo electrónico a**dquisiciones@fondodian.gov.co**. No se recibirán documentos físicos ni por otros medios.

Al enviar sus observaciones o cotizaciones, por favor indique en el asunto del correo el siguiente texto: **Estudio de mercado – Gobierno de Identidades (IAM)**.

I. ANTECEDENTES Y JUSTIFICACION

La Dirección de Impuestos y Aduanas Nacionales – DIAN, en cumplimiento de su misión de garantizar la seguridad fiscal del Estado colombiano y la protección del orden público económico nacional, ha emprendido un proceso integral de transformación digital y fortalecimiento institucional, sustentado en el Programa de Apoyo a la Modernización de la DIAN (BID 5148/OC-CO). Este programa busca optimizar la eficiencia de la gestión tributaria, aduanera y cambiaria mediante la modernización tecnológica, la gobernanza de datos y la consolidación de una infraestructura segura, interoperable y resiliente.

En este marco, la Oficina de Seguridad de la Información (OSI), creada mediante el Decreto 1742 de 2020, tiene entre sus funciones la de “generar el gobierno de identidades (roles y responsabilidades) y monitorear las directrices relacionadas con el control y asignación de permisos para el acceso a las instalaciones, áreas seguras y sistemas de información de la entidad”. Esta disposición constituye la base legal para el desarrollo de un modelo formal de Gobierno de Identidades y Accesos (IAM), que permita ejercer un control efectivo sobre los privilegios otorgados en los sistemas misionales, operativos y administrativos de la entidad.

Durante el análisis institucional y técnico realizado por la Oficina de Seguridad de la Información (OSI), se identificaron oportunidades de fortalecimiento en el modelo de gestión de identidades y accesos, asociadas al proceso de evolución y madurez institucional, entre las cuales se destacan:

1. La necesidad de consolidar un mapeo integral y estandarizado de roles y perfiles funcionales por área y proceso.
2. La coexistencia de prácticas heterogéneas en la provisión y administración de accesos, que requieren mayor formalización y alineación con el principio de mínimo privilegio.
3. La conveniencia de establecer criterios institucionales documentados para la asignación, modificación y revocación de accesos a los sistemas de información.
4. El fortalecimiento de lineamientos transversales y mecanismos de trazabilidad que permitan a la OSI ejercer de manera más efectiva sus funciones de monitoreo y seguimiento sobre la gestión de permisos en los distintos entornos tecnológicos.

Estas brechas han derivado en una administración fragmentada, dependiente de las áreas operativas y sin gobierno ni mecanismos de validación centralizada, lo que genera riesgos de acceso indebido, incumplimiento normativo y pérdida de control sobre la información institucional.

A nivel tecnológico, la entidad enfrenta un entorno heterogéneo caracterizado por la coexistencia de múltiples repositorios de autenticación (LDAP, Entra ID, IBM Security, entre otros), lo que configura un ecosistema fragmentado de identidades digitales. Esta dispersión impide la aplicación consistente de principios de mínimo privilegio, necesidad de saber y segregación de funciones, establecidos en los estándares internacionales ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701 y en la Arquitectura de Confianza Cero (Zero Trust Architecture) del NIST.

El fortalecimiento del Gobierno de Identidades resulta indispensable para garantizar la seguridad de la información, la continuidad operativa y la confianza digital, asegurando múltiples métodos de autenticación, como la aplicación móvil para dispositivos Apple y Android, gestionando la seguridad íntegramente. En consecuencia, la OSI ha definido la necesidad de una consultoría especializada que diseñe, documente y formalice el Modelo Operativo de Gobierno de Identidades y Accesos (IAM), para enfrentar los diversos desafíos que operan bajo las estrictas regulaciones y requiere un rendimiento consistentemente de alto para poder aprovechar la productividad de la seguridad informática de la entidad, incluyendo la estructuración del catálogo de roles, la definición de responsabilidades institucionales, la formalización normativa mediante un anexo técnico, y la transferencia de conocimiento que permita su aplicación transversal en toda la entidad.

Este proyecto se constituye como un componente esencial de la estrategia de modernización tecnológica y de seguridad digital de la DIAN, asegurando que la gestión de accesos esté alineada con los proyectos PETD (NSGT, NSGA, NSGC, NSGDEA), la Plataforma Digital de Integración (PDI), y demás soluciones del programa de modernización, así como del Marco de Confianza y Seguridad Digital (CONPES 3995 de 2020).

Mejorando la productividad y la eficiencia para aprovechar de manera integral la gestión de identidades y accesos (IAM) para todos los tipos de identidad y casos de uso previstos para brindar servicios digitales integrales para clientes, ciudadanos, personal vinculado y casos de uso de la entidad.

La gestión de identidades y accesos (IAM) desempeña un papel fundamental al extender el acceso seguro a usuarios externos a gran escala, manteniendo el control, el cumplimiento normativo y una excelente experiencia de usuario (UX). La IAM acelera y permite la administración delegada segura, garantizando que las personas adecuadas tengan el acceso correcto en el momento preciso.

En esencia, la consultoría de IAM actúa como un puente de control y habilitador que asegura que la modernización tecnológica (la migración a una plataforma Multi-nube, el desarrollo de nuevos sistemas misionales y la adopción de tecnologías emergentes) se realice sobre una base de seguridad, gobernanza, transparencia y eficiencia en el acceso a la información.

II. OBJETO, ALCANCE Y MARCO DE LA CONSULTORÍA

a. Objeto del Contrato (Mandato Estratégico y Operativo)

El objetivo de la contratación de la consultoría IAM (Gestión de Identidades y Accesos) y Gobierno de Identidades, describe el proceso de fortalecimiento ligado a la estrategia de modernización institucional, la mitigación de riesgos de seguridad crítica y el cumplimiento normativo de la DIAN, según se detalla en los documentos estratégicos (PETI, PESI y TDR).

El presente proceso tiene por objeto la contratación de los servicios de consultoría especializada para realizar el diagnóstico, diseño y definición del Modelo de Gobierno de Identidades y Accesos (IAM) y la minería de roles, así como brindar el acompañamiento técnico consultivo para su adopción temprana.

El alcance integral incluye el entendimiento de la situación actual, el establecimiento del Modelo Operativo de Gobernanza, la estrategia de centralización, la construcción del Catálogo de Roles de Negocio y la asesoría experta para analizar conceptualmente la alineación técnica de la implementación tecnológica. El propósito fundamental es dotar a la Oficina de Seguridad de la Información (OSI) de los instrumentos normativos, técnicos y estratégicos necesarios para ejercer su función de control, monitoreo y seguimiento sobre la asignación de permisos, contando con la transferencia de conocimiento del Consultor, sin que este asuma funciones de supervisión contractual o interventoría.
Esta acción estratégica es indispensable para pasar de un estado de vulnerabilidad y administración fragmentada a un modelo de Gobierno de Identidades centralizado, seguro y auditable, permitiendo a la OSI ejercer su función de control efectivo y asegurando que la transformación digital de la DIAN se construya sobre una base de seguridad robusta y cumplimiento normativo.

b. Alcance del Servicio y Dominios IAM

El alcance de la consultoría será holístico y transversal a toda la organización y sus sistemas de información, incluyendo los niveles: central, seccional y delegados. No se limita a una herramienta tecnológica específica, sino que se centra en el diseño institucional de gobernanza y control de acceso, aplicable a los siguientes dominios:

- Identity Governance & Administration (IGA): Diseño del Catálogo de Roles por proceso, Ciclo de Vida (*Joiner-Mover-Leaver*), Certificación de Accesos y Auditoría de Cumplimiento.
- Privileged Access Management (PAM): Definición de políticas de acceso privilegiado, gestión segura de credenciales, y monitoreo de sesiones administrativas.
- Access Management (AM): Estrategia para Single Sign-On (SSO), Multi-Factor Authentication (MFA) y Autenticación Adaptativa, integrando los mecanismos de la PDI-IAM.

La realización de una consultoría especializada en la Gestión de Identidades y Accesos (Identity and Access Management - IAM) y el Gobierno de Identidades es fundamental para la Dirección de Impuestos y Aduanas Nacionales (DIAN) debido a que busca solucionar problemáticas estructurales, mitigar riesgos de seguridad y habilitar la transformación digital integral de la entidad.

Esta consultoría se justifica como un componente esencial para la modernización institucional, especialmente dentro del marco del Programa de Apoyo a la Modernización de la DIAN (BID 5148/OC-CO).

Para efectos de estimación presupuestal, el plazo estimado de ejecución de la consultoría se proyecta entre seis (6) y ocho (8) meses, sujeto a la estructuración definitiva del proceso de selección.

A continuación, se presenta la justificación detallada indicando los procesos y habilitantes claves:

III. JUSTIFICACIÓN TÉCNICA Y BENEFICIOS INSTITUCIONALES

a. Fortalecimiento de la Seguridad de la Información y Gestión de Accesos

El principal motor de la consultoría IAM es fortalecer la seguridad y el control de accesos, sin sustituir ni detallar el alcance propio de los proyectos tecnológicos en curso, sino estableciendo los lineamientos de gobierno, roles y controles de acceso que deberán ser observados en su implementación. Lo anterior es crítico dado que la entidad maneja información pública, clasificada, reservada y datos personales sensibles en materia tributaria, aduanera y cambiaria.

- *Gobierno de Identidades y Control de Accesos:* La Oficina de Seguridad de la Información (OSI) tiene la función de generar el gobierno de identidades y monitorear las directrices relacionadas con el control y la asignación de permisos para el acceso a sistemas de información. La consultoría es necesaria para diseñar e implementar estos sistemas de control de identidad y acceso para toda la DIAN.
- *Mitigación de Riesgos y Fragmentación:* El entorno institucional presenta un alto grado de heterogeneidad en los mecanismos de gestión de identidades y autenticación, lo cual requiere procesos de armonización y fortalecimiento de la gobernanza. El modelo IAM propuesto se orienta a la consolidación de directrices, roles y controles de acceso bajo un enfoque centralizado, con el fin de reducir la exposición a riesgos de acceso no autorizado y fortalecer el cumplimiento normativo, sin perjuicio de las particularidades operativas de los distintos sistemas y plataformas.
- *Adopción de Principios de Seguridad:* La consultoría asegurará la aplicación consistente de principios de seguridad críticos, como el Principio de Mínimo Privilegio, la Necesidad de Saber y la Segregación de Funciones (SoD).
- *Alineación Normativa y Arquitectónica de Seguridad:* El diseño se sustentará en estándares internacionales como ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, y la Arquitectura de Confianza Cero (Zero Trust Architecture) del NIST, adoptando políticas de "Privacidad por Diseño" en todos los componentes de la arquitectura objetivo.

b. Procesos y Habilitantes que Fortalecen la Institución

La consultoría aborda dominios clave que garantizan la madurez operativa y la eficiencia interna:

Proceso/Habilitante	Justificación y Fortalecimiento Institucional
Identity Governance & Administration (IGA)	Se diseñará el Catálogo de Roles de Negocio por proceso y el Ciclo de Vida de las Identidades (Joiner-Mover-Leaver), que incluye la certificación de accesos y la revisión de cumplimiento. Esto formaliza los criterios para la asignación, modificación y revocación de accesos, lo cual es inexistente o fragmentado actualmente.
Access Management (AM)	Se definirá la estrategia para la implementación de Single Sign-On (SSO) y Multi-Factor Authentication (MFA), incluyendo autenticación adaptativa. Esto es crucial para mejorar la seguridad y la experiencia de usuario (UX).
Privileged Access Management (PAM)	Se definirán políticas de acceso privilegiado y la gestión segura de credenciales, junto con el monitoreo de sesiones administrativas.
Mapeo y Monitoreo	Se diseñarán los mecanismos de monitoreo y seguimiento periódico, incluyendo la Matriz de Verificación de Controles y KPIs, para que la OSI pueda supervisar de forma continua la adherencia al Modelo de Gobierno de Identidades.

La Gestión de Identidades y Accesos (IAM) está diseñada para mejorar la productividad y la eficiencia, ofreciendo servicios digitales integrales tanto para clientes, ciudadanos como para el personal vinculado, asegurando que las personas adecuadas tengan el acceso correcto en el momento preciso.

c. Articulación con Grupos de Interés y Gestión del Conocimiento

La consultoría tiene un enfoque fuerte en la dimensión humana y la transferencia de habilidades, esenciales para que la transformación sea sostenible.

- *Gestión del Conocimiento (GDCt)*: Un objetivo clave es la transferencia de capacidades y conocimiento a los equipos institucionales. El plan incluye un rol específico de Líder de Gestión del Conocimiento para diseñar el modelo de transferencia y crear un repositorio de conocimiento.
- *Gestión del Cambio (GDC)*: Se diseñará e implementará un Plan de Gestión del Cambio y Transferencia de Conocimiento para mitigar la resistencia y asegurar la apropiación del nuevo modelo por parte de los dueños de procesos. Esto es vital para que las áreas funcionales se apropien del Catálogo de Roles.
- *Articulación Transversal:* El modelo de entrega de valor de la DGIT promueve el Trabajo Transversal por las Áreas, estableciendo Centros de Excelencia (COE) y Núcleos de Especialización (incluyendo Ciberseguridad) para promover mejores prácticas y compartición de conocimiento.

- *Visibilidad Externa:* La Oficina de Seguridad de la Información (OSI) tiene iniciativas estratégicas para visibilizar la gestión de seguridad y privacidad ante grupos de interés externos, tales como gremios empresariales, la academia, aliados (ColCERT, MINTIC, DAFP) y usuarios (aduaneros, tributarios y cambiarios), fortaleciendo la confianza ciudadana.

d. Arquitectura Empresarial y Arquitectura de Datos

La consultoría IAM se articula directamente con los habilitadores tecnológicos de la entidad.

- *Arquitectura Empresarial:* El diseño del modelo IAM debe alinearse con el Plan Estratégico de Tecnología e Información (PETI) y el Marco de Referencia de Arquitectura Empresarial. La Arquitectura Objetivo incluye una Arquitectura de Seguridad con elementos de Identidad (Autenticación y Autorización).
- *Transformación Digital (PETD):* El proyecto es esencial para la implementación de los Proyectos Estratégicos de Transformación Digital (PETD) en curso, incluyendo el Nuevo Sistema de Gestión Tributaria (NSGT), el Nuevo Sistema de Gestión Aduanera (NSGA), el Nuevo Sistema de Gestión Corporativa (NSGC), y la Plataforma Digital de Integración (PDI-IAM) sin sustituir ni detallar el alcance propio de dichos proyectos, sino estableciendo los lineamientos de gobierno, roles y controles de acceso que deberán ser observados en su implementación.
- *Arquitectura de Datos:* La implementación de IAM es crucial para la gestión basada en información oportuna y de calidad. En la Fase II, el diseño del modelo de gobernanza IAM deberá definir los lineamientos conceptuales para la centralización y administración unificada de identidades. Además, se valorará la protección de bases de datos sensibles, aplicando el principio de mínimo privilegio y asegurando una estricta trazabilidad al activo de información más valioso.

e. Marco de actuación institucional

La ejecución de la consultoría deberá articularse con:

- El Plan Estratégico de Tecnología e Información (PETI) y el Programa de Modernización de la DIAN (BID 5148/OC-CO).
- El Modelo y Sistema de Gestión de Seguridad y Privacidad de la Información (MSPI – SGSPI) administrados por la OSI.
- Los Proyectos de Transformación Digital (PETD) en curso: NSGT, NSGA, NSGC, NSGDEA y la PDI-IAM, entre otros
- Las directrices de la Dirección de Gestión de Innovación y Tecnología (DGIT), responsable de la arquitectura tecnológica institucional.

IV. ESPECIFICACIONES TÉCNICAS Y FUNDAMENTO NORMATIVO

a. Fundamentación normativa y técnica

El desarrollo del modelo de Gestión de Identidades y Accesos (IAM) se sustentará en el marco legal y técnico vigente, estructurado bajo la siguiente jerarquía normativa:

Marco Legal (Leyes)

- **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- **Ley 1581 de 2012:** Ley Estatutaria para la Protección de Datos Personales y sus decretos reglamentarios.

Marco Reglamentario (Decretos)

- **Decreto 1742 de 2020 (Artículo 10, Numeral 3):** Por el cual se definen las funciones de la Oficina de Seguridad de la Información de la DIAN, específicamente en lo relacionado con la generación del gobierno de identidades y el monitoreo de la asignación de permisos.

Instrumentos de Política Pública (CONPES)

- **CONPES 4144 de 2025:** Política Nacional de Inteligencia Artificial.
- **CONPES 3995 de 2020:** Política Nacional de Confianza y Seguridad Digital.
- **CONPES 3920 de 2018:** Política Nacional de Explotación de Datos (Big Data).

Estándares Internacionales y Modelos Sectoriales

- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, v.2021).
- **ISO/IEC 27001:2022:** Estándar internacional para los Sistemas de Gestión de Seguridad de la Información (SGSI).
- **ISO/IEC 27002:2022:** Código de prácticas para controles de seguridad de la información.
- **ISO/IEC 27701:2019:** Extensión de la ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad de la información.

b. Objetivos específicos

- Diagnosticar el estado actual de la gestión de identidades y accesos.
- Definir principios rectores y lineamientos institucionales de gobierno de identidades.
- Diseñar el Modelo Operativo de Gobierno Centralizado IAM.
- Construir el Catálogo de Roles por proceso y el Ciclo de Vida de las Identidades.
- Formalizar el modelo en un Anexo Técnico Normativo OSI.
- Transferir capacidades y conocimiento a los equipos institucionales.
- Diseñar los mecanismos de monitoreo y seguimiento periódico.
- Garantizar la documentación formal y trazable de los productos y lineamientos definidos, para su adopción y sostenibilidad institucional.

V. DESARROLLO METODOLÓGICO Y FASES DE EJECUCIÓN

La consultoría se ejecutará siguiendo un modelo de gestión por fases, adaptado a la transformación digital de la entidad:

Fase	Objeto de la Fase
Fase I: Diagnóstico (As-Is) y Arqueología de Roles	Determinar el Nivel de Madurez de Gobernanza y el estado actual de dispersión de identidades, realizando la Minería de Roles de acuerdo con su geolocalización en el territorio (Seccionales) así como la caracterización del modelo actual de gestión de accesos y ciclo de vida de usuarios.
Fase II: Diseño del Modelo de Gobernanza (To-Be)	Diseñar el Modelo Operativo de Gobierno Centralizado y construcción del Catálogo de Roles de Negocio por proceso y casos de uso, así como los lineamientos para su operación y administración institucional.
Fase III: Formalización Normativa OSI y Transferencia	Creación y documentación del Anexo Técnico de Gobierno de Identidades y su integración con el Manual de Políticas y Lineamientos de la OSI (MN-IIT-0072 - Última versión), incluyendo lineamientos, procedimientos y herramientas que permitan su adopción institucional y transferencia de conocimiento.
Fase IV: Acompañamiento técnico a la función de monitoreo de la OSI	Brindar acompañamiento técnico-conceptual a la Oficina de Seguridad de la Información (OSI) para analizar conceptualmente la alineación del Modelo de Gobierno de Identidades con la implementación de la solución PDI-IAM y del Catálogo de Roles en los proyectos PETD (NSGT, NSGA, NSGC, NSGDEA), conforme a los cronogramas institucionales.

FASE I: Diagnóstico y Arqueología de Roles (As-Is)

El objetivo es establecer el punto de partida real, incluyendo la realidad operativa regional.

Actividades Clave	Productos/Entregables (Orientación IAM/OSI)
1.1. Evaluación de Madurez y Modelo de Gobernanza: Analizar el nivel actual de la gestión de identidades y accesos y definir el Modelo de Madurez de Gobernanza (MCM) deseado a 3-5 años (Ej. Nivel 3/4 Gestionado u Optimizado).	**Informe de Evaluación de Madurez IAM (**As-Is): incluyendo brechas, riesgos y definición del Modelo de Madurez deseado.
1.2. Arqueología de Roles en el Territorio: Realizar el **levantamiento en Seccionales** clave para mapear los procesos reales y la desviación entre la operación central y territorial.	**Mapa de actores, procesos y estructura actual de asignación de roles (incluye caracterización territorial).** **Propuesta Preliminar del Catálogo de Roles Base por proceso.**

FASE II: Diseño del Modelo Operativo de Gobierno (To-Be)

Esta fase define el modelo de gobernanza orientado a la centralización de las directrices de identidad.

Actividades Clave	Productos/Entregables (Orientación IAM/OSI)
2.1. Diseño del Modelo Operativo de Gobierno Centralizado: Definir la estrategia de centralización y formalizar el rol de la OSI como la entidad rectora. Se debe definir el modelo de responsabilidades para que los dueños de los procesos se apropien del rol.	**Documento del Modelo Operativo de Gobierno IAM (To-Be):** Incluyendo arquitectura conceptual de referencia y principios de seguridad.
2.2. Catálogo de Roles Final y Casos de Uso: Diseño del catálogo de Roles Funcionales y de Negocio (SoD, Mínimo Privilegio). Entrega del diseño de roles de negocio **por proceso** y los casos de uso listos para ser implementados por el área de Tecnología.	**Catálogo de Roles Detallado y Casos de Uso** (Incluye Reglas de Asignación y Control - SoD).

2.3. Diagnostico para inclusión de herramienta IA: Análisis exploratorio de tendencias tecnológicas aplicables al modelo IAM.	**Informe de análisis de tendencias tecnológicas aplicables al modelo IAM** (incluye revisión exploratoria de herramientas del mercado)
2.4. Definición del Ciclo de Vida y Roadmap: Estructuración de los procedimientos de *Joiner-Mover-Leaver*, asegurando la desarticulación periódica de accesos excesivos y la gestión de salidas.	**Hoja de Ruta (Roadmap) IAM Detallada:** Cronograma de implementación realista, considerando los tiempos del BID.

FASE III: Formalización Normativa OSI y Transferencia

Documentar oficialmente el modelo para su adopción institucional.

Actividades Clave	**Productos/Entregables (Orientación IAM/OSI)**
3.1. Formalización Normativa OSI: Redacción del **Anexo Técnico de Gobierno de Identidades**, incluyendo lineamientos técnicos orientados a su adopción institucional por el área de Tecnología, que respalden los mecanismos de autogestión de accesos para servidores y contratistas, así como la definición de directrices para la inscripción y gestión de dispositivos tecnológicos..	**Anexo Técnico Normativo de Gobierno de Identidades.**
3.2. Integración al Manual de Políticas y Lineamientos de la OSI: Apoyo a la OSI para integrar los Lineamientos de Acceso y Gobierno en el Manual de Políticas y Lineamientos de Seguridad de la Información (MN-IIT-0072 - Última versión), actualizando las secciones pertinentes a la Segregación de Funciones y Gestión de Identidades.	**Documento actualizado del Manual de Políticas OSI (apartado de Gobierno de Identidades):** Apartado actualizado del Manual de Políticas y Lineamientos. Incluir políticas de autenticación adaptativas y basadas en el riesgo para equilibrar la seguridad y la productividad
3.3. Plan de Gestión del Cambio y Transferencia: Diseño de un plan que incorpore la gestión del tiempo y la gestión del conocimiento para lograr la apropiación del modelo por parte de los dueños de proceso, directores de gestión, directores seccionales y jefes de oficina	**Plan de Gestión del Cambio y Transferencia de Conocimiento** (enfocado en las tareas de monitoreo y auditoría de la OSI).

FASE IV: Acompañamiento técnico a la función de monitoreo de la OSI

Tiene como propósito brindar asistencia técnica experta a la Oficina de Seguridad de la Información (OSI) para interpretar, contrastar y analizar conceptualmente la alineación de la implementación tecnológica (realizada por terceros o in-house) con el Modelo de Gobierno de Identidades diseñado.

Actividades Clave	**Productos/Entregables (Orientación IAM/OSI)**
4.1. Acompañamiento técnico a la alineación de la solución IAM: Acompañar al equipo técnico de la DIAN en la revisión de los parámetros de configuración de la solución IAM, emitiendo conceptos técnicos sobre la alineación de dichos parámetros con el diseño de roles y privilegios definidos en la Fase III.**.**	Concepto Técnico de Alineación del Modelo IAM.
4.2. Revisión conceptual de Roles y Controles de Acceso en PETD (Según Cronograma): Acompañar técnicamente a la OSI en la revisión conceptual de la incorporación del Catálogo de Roles de Negocio en los proyectos PETD (NSGT, NSGA, NSGC, NSGDEA, entre otros), conforme a los cronogramas institucionales. El consultor emitirá recomendaciones técnicas sobre la consistencia entre los roles definidos y los casos de uso implementados, promoviendo la aplicación de los principios de mínimo privilegio y segregación de funciones (SoD), sin realizar funciones de supervisión contractual ni validación final de aceptación.	Matriz de Referencia y Recomendaciones de Alineación por PETD.
4.3. Monitoreo y seguimiento de Cumplimiento: Diseñar el Procedimiento de Monitoreo y seguimiento periódico incorporando controles técnicos, indicadores de cumplimiento (KPIs) y pruebas que permitan a la OSI evaluar de forma continua la adherencia al Modelo de Gobierno de Identidades. Este procedimiento permitirá a la OSI evaluar de manera continua la adherencia al modelo definido, incluyendo la aplicación de mecanismos de autenticación institucionales (MFA, OTP, autenticación adaptativa u otros habilitados por la entidad), sin intervenir directamente en su implementación tecnológica.	Procedimiento de Monitoreo y Seguimiento con indicadores (KPIs).

VI. PERFIL REFERENCIAL DEL EQUIPO CONSULTOR

Para efectos exclusivos del presente estudio de mercado, la Entidad presenta una descripción referencial de los perfiles técnicos que podrían ser requeridos para la ejecución de la consultoría, con el fin de orientar la estimación presupuestal del servicio por parte de los interesados.

La información relacionada con formación, experiencia y certificaciones tiene carácter indicativo y no constituye requisito habilitante ni criterio de evaluación en esta etapa. No se están solicitando hojas de vida, soportes, acreditaciones ni validaciones formales de idoneidad. Los interesados podrán proponer estructuras de equipo alternativas que garanticen el cumplimiento del objeto y alcance descritos.

La consultoría requerirá un enfoque integral y multidisciplinario, con experiencia en diseño estratégico, gobierno de identidades, arquitectura tecnológica, procesos organizacionales y gestión del cambio, considerando la complejidad institucional y el entorno tecnológico de la DIAN.

Rol	Descripción
Arquitecto de Ciberseguridad / IAM (Líder)	Perfil con experiencia en diseño de arquitecturas empresariales y modelos de gestión de identidades y accesos (IAM), incluyendo gobierno de identidades, principios de mínimo privilegio y enfoques de seguridad como Zero Trust. Será responsable del direccionamiento técnico integral del modelo y su alineación con la arquitectura institucional.
Especialista en Gobernanza de Identidades (IGA)	Perfil con experiencia en estructuración de catálogos de roles, ciclos de vida de identidad (Joiner-Mover-Leaver), certificación de accesos y segregación de funciones (SoD). Apoyará el diseño funcional del Modelo Operativo de Gobierno de Identidades.
Especialista en Procesos y Cumplimiento	Perfil con experiencia en modelado de procesos de negocio y articulación de controles de acceso con marcos normativos y de seguridad de la información. Contribuirá a la alineación del modelo IAM con la estructura organizacional y regulatoria de la Entidad.
Ingeniero de Integración y Seguridad	Perfil con experiencia en integración de sistemas, interoperabilidad, autenticación y mecanismos de seguridad técnica en entornos tecnológicos. Apoyará la coherencia del modelo IAM frente a las plataformas tecnológicas institucionales.
Gerente de Proyecto	Perfil con experiencia en dirección o coordinación de proyectos tecnológicos, responsable de la planeación, seguimiento de cronograma y articulación de los diferentes frentes de trabajo.
Especialista en Gestión del Cambio y Transferencia	Perfil con experiencia en estrategias de adopción organizacional, apropiación institucional y transferencia de conocimiento en proyectos de transformación digital. Apoyará la estructuración de planes de comunicación, apropiación y documentación del modelo.

Dedicación Referencial

Para efectos de estimación presupuestal, los interesados podrán presentar su propuesta indicando la dedicación estimada por rol en meses equivalentes, entendidos como el tiempo requerido para el cumplimiento de las actividades y entregables planteados.

La distribución de dedicación entre roles podrá ajustarse según el modelo de ejecución propuesto por cada interesado.

VII. FORMA DE PRESENTACIÓN DE COTIZACIONES

Para efectos del presente estudio de mercado, los interesados deberán presentar:

- Valor total estimado de la consultoría.
- Desglose del valor por entregables (Anexo No. 1).
- Estructura referencial del equipo y dedicación estimada (Anexo No. 2), únicamente como soporte técnico de la estimación económica.

El valor total de la consultoría corresponderá al consolidado de los entregables definidos en el Anexo No. 1. La información del equipo tiene carácter ilustrativo para sustentar la estructura de costos y no implica modalidad de pago por perfiles.

La modalidad de pago definitiva será establecida en el proceso de selección correspondiente.