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

CONTRATO DE PRÉSTAMO BID 5148/OC-CO

ANEXO 1 - CAPÍTULO TÉCNICO ESTUDIO DE MERCADO PARA SERVICIOS ADMINISTRADOS DE NUBE

MARZO DE 2026

CONTENIDO

1. OBJETO DEL CAPÍTULO TÉCNICO

Este documento establece el alcance, las condiciones, los entregables y los supuestos mínimos para cotizar los Servicios Administrados de Nube requeridos por la DIAN. Su propósito es describir, con el nivel suficiente para el estudio de mercado, los servicios base que integran la operación continua de la Multinube, los servicios opcionales que pueden contratarse de forma independiente y los servicios especializados por demanda.

El anexo está orientado a la necesidad de la DIAN de contratar un servicio de administración de nubes que asuma la operación técnica, la gestión del servicio, la seguridad operativa, la continuidad, la automatización y la mejora continua del ecosistema Multinube, preservando la gobernanza institucional en cabeza de la DIAN.

2. CATEGORIAS DE SERVICIOS DE ADMINISTRACIÓN DE NUBE

i. ALCANCE

Los servicios se han estructurado y agrupado en tres (3) categorías y dominios así:

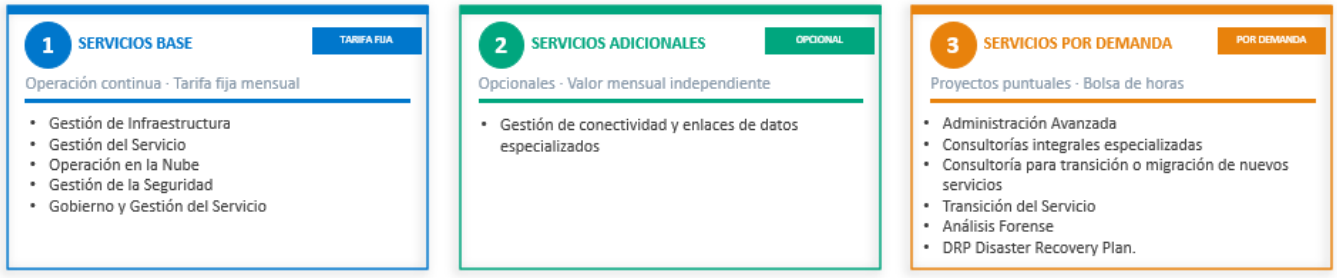


Figura 1 – Servicios requeridos por la Entidad

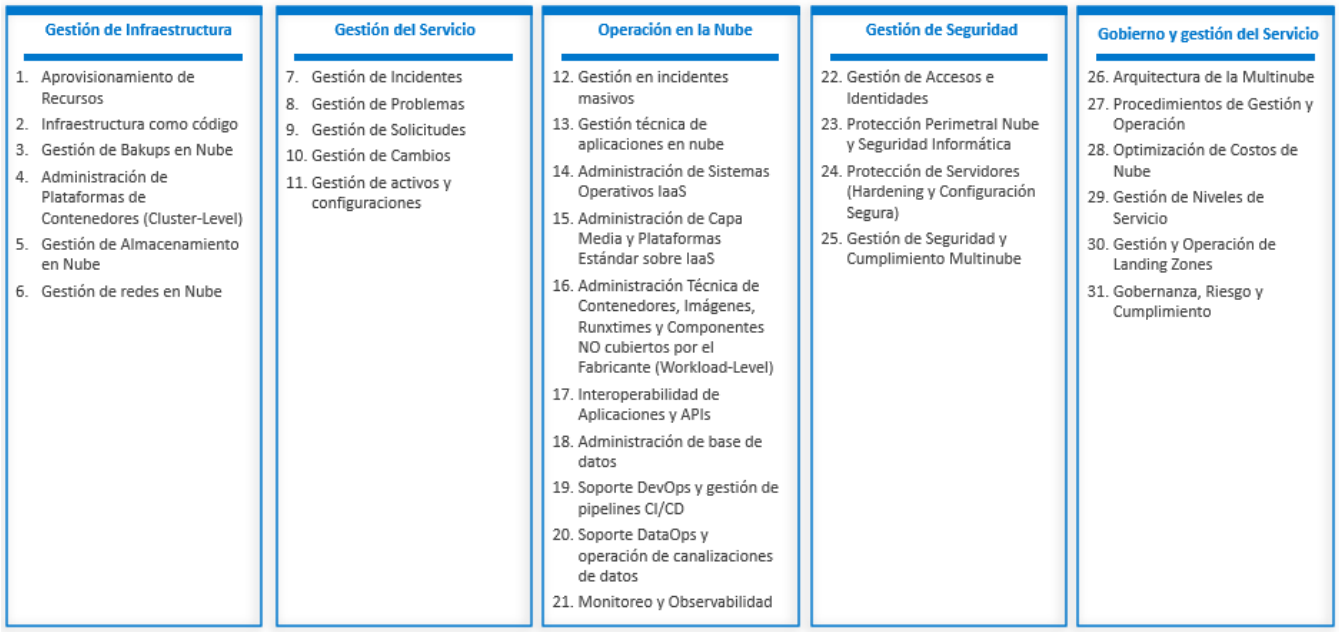
ii. SERVICIOS BASE

Los servicios base constituyen el núcleo obligatorio del servicio y se prestan de forma continua, con costo fijo mensual, deberán prestarse sobre el stack tecnológico y las herramientas institucionales definidas por la DIAN, sin imponer a la Entidad plataformas que dupliquen capacidades ya existentes salvo justificación técnica y económica aprobada.

Los Servicios Base deberán cubrir como mínimo la operación recurrente del ecosistema multinube definido por la DIAN. Dentro de este alcance no podrán incluirse actividades recurrentes derivadas de los servicios adicionales o por demanda, que ya hayan sido

contratados y pagados por la DIAN. La operación de dichos servicios deberá ser asumida como parte de la prestación de los Servicios Base, sin generar costos adicionales para la DIAN.

En este capítulo, se describen los dominios que forman parte de los servicios base, mencionando de carácter enunciativo y no limitativo el alcance de cada servicio. .



En consecuencia, el proveedor deberá ejecutar todas las tareas complementarias, conexas o necesarias para asegurar la correcta prestación del servicio, aun cuando no estén expresamente descritas, siempre que guarden relación directa con el objeto contractual y los niveles de servicio establecidos por la DIAN.

Del mismo modo, las actividades indicadas como “No incluye” corresponden a aquellas que, por su naturaleza o responsabilidad, no hacen parte de las obligaciones del proveedor dentro del presente servicio.

1.1.1. Gestión de la infraestructura

1.1.1.1. Aprovisionamiento de recursos

Esta actividad se centra en el aprovisionamiento o desaprovisionamiento de recursos de nube en modelo de recursos individuales que requieren los entornos de las aplicaciones actuales y los nuevos proyectos de transformación digital. DIAN puede solicitar el aprovisionamiento de recursos durante toda la ejecución del servicio. El proveedor debe realizar el levantamiento de requerimientos y aprovisionar/desaprovisionar los recursos siguiendo las políticas de nombrado y etiquetado establecidas por DIAN para cada una de las nubes. Como parte del

aprovisionamiento el proveedor debe etiquetar cada uno de los subcomponentes y recursos para poder llevar un efectivo control interno para fines de facturación e inventario.

A. Actividades excluidas del alcance

- Diseño o desarrollo de arquitectura de aplicaciones
- Decisiones sobre cambios en la arquitectura de referencia o en el diseño aprobado por DIAN, manteniéndose la responsabilidad del proveedor de emitir conceptos y recomendaciones técnicas documentadas sobre la implementación de nuevos servicios o componentes, incluyendo análisis de costo-beneficio, desempeño, seguridad y mantenibilidad. La aprobación final corresponderá al equipo de arquitectura de DIAN.

B. Condiciones de prestación del servicio

- La prestación del servicio se hará en horario laboral, salvo las excepciones que se presenten de acuerdo con las necesidades del servicio, entre ellas, un cambio programado fuera de hora pico o en horario nocturno o un cambio de emergencia o un incidente de seguridad los cuales deben quedar cubiertos con el servicio solicitado 7x24.
- Cuando exista una plantilla IaC aprobada para el recurso solicitado, el aprovisionamiento deberá realizarse utilizando dicha plantilla, aplicando los ANS establecidos en este servicio.
- Cuando no exista una plantilla IaC para el recurso, y la DIAN determine que el recurso debe gestionarse mediante IaC, el proveedor deberá crear o ajustar la plantilla IaC bajo los ANS del servicio “Infraestructura como Código (IaC)”.

1.1.1.2. Infraestructura como Código

Mantener la gestión automatizada de la infraestructura en las nubes de la DIAN mediante el uso de plantillas de Infraestructura como Código (IaC), garantizando consistencia, estandarización y trazabilidad en el aprovisionamiento y despliegue de recursos. Implica la utilización de un repositorio de control de versiones mediante la integración con los flujos de trabajo DevOps. El proveedor debe mantener el catálogo de plantillas para los aprovisionamientos que realice. Estas plantillas deben mantenerse actualizadas siempre que haya cambios en los recursos o grupos de recursos.

A. Condiciones de prestación del servicio

- El proveedor deberá mantener sincronizados los repositorios y pipelines entre Azure DevOps, GitHub Enterprise y Argo CD durante toda la vigencia del servicio.
- Cualquier migración o cambio de herramienta dentro del ecosistema DevOps / GitOps no generará costos adicionales ni constituye cambio de alcance.
- Todas las plantillas IaC deberán utilizar repositorios bajo control de versiones, validaciones automáticas y revisión de seguridad.
- El uso de IaC es obligatorio para todo nuevo aprovisionamiento o despliegue.

- El proveedor deberá implementar mecanismos de detección de drift entre el estado real de la infraestructura y las definiciones IaC.

1.1.1.3. Gestión de backups en nube

Incluye la definición y ejecución de los procesos de copias de respaldo y restauración con base en las definiciones técnicas y de negocio específicas de las aplicaciones de DIAN teniendo en cuenta el tipo de información a respaldar, la frecuencia, la ubicación de las copias de respaldo y las consideraciones para su restauración. Las definiciones de los procesos de copia de respaldo y restauración deberán estar alineadas con el plan de recuperación de desastres y con el plan de continuidad de negocio.

A. Actividades fuera del alcance

- Definición de la política de retención de respaldos, incluyendo tiempos de conservación, número de versiones y ciclos de vida (responsabilidad exclusiva de DIAN).
- Determinación de qué datos, sistemas o componentes deben ser respaldados según necesidades funcionales de cada aplicación (definido por el área responsable de la aplicación).
- Validación funcional o lógica de los datos restaurados posterior a la recuperación (responsabilidad del área de pruebas o funcional).
- Análisis forense o recuperación de datos a nivel de aplicación, salvo en los casos específicos en lo que se presente una filtración de datos o ransomware, para lo cual se requeriría un análisis forense que determine el punto de afectación y el alcance de la brecha.

B. Condiciones del servicio

- Todos los respaldos deberán ejecutarse utilizando herramientas nativas de las nubes gestionadas o aquellas expresamente aprobadas por DIAN.
- Los respaldos deberán garantizar cifrado en tránsito y en reposo, así como replicación geográfica cuando aplique.
- Las pruebas de restauración deberán realizarse al menos una vez por semestre y documentarse en informe técnico. De igual forma, deberán incluir al menos una prueba trimestral de restauración de sistemas críticos.
- Los reportes mensuales deberán consolidar el porcentaje de respaldos exitosos, fallidos, restauraciones ejecutadas y capacidad utilizada.

1.1.1.4. Administración de Plataformas de Contenedores (Cluster-Level)

Garantizar la operación, estabilidad, seguridad, capacidad y continuidad de las plataformas de orquestación de contenedores utilizadas por la DIAN (incluyendo, entre otras, OpenShift/ARO, Azure Kubernetes Service – AKS y Amazon Elastic Kubernetes Service – EKS), abarcando los

componentes del plano de control y de datos del clúster, en coherencia con las responsabilidades de los fabricantes (Red Hat, Microsoft, AWS) y las políticas de gobernanza definidas por la entidad.

A. Actividades fuera del alcance:

- Administración de imágenes de contenedores, contenido de contenedores, runtimes, operadores de middleware o cualquier componente asociado a las cargas de trabajo de aplicación, los cuales se gestionan en el servicio de administración técnica de contenedores y workloads.
- Diseño, implementación o mantenimiento de arquitecturas de microservicios, modelos de integración o definiciones de APIs de las aplicaciones que se ejecutan en los clústeres.

B. Condiciones del servicio:

- El proveedor será responsable de la administración técnica a nivel de plataforma (cluster-level), en coordinación con los fabricantes (Red Hat, Microsoft, AWS) y aprovechando los servicios de soporte correspondientes, sin duplicar las funciones propias del fabricante.
- La responsabilidad sobre las cargas de trabajo, contenedores, imágenes, runtimes y operadores de aplicación será cubierta por el servicio específico de administración técnica de workloads y no por este servicio de plataforma.
- Los incidentes de plataforma que correspondan a fallas propias del servicio de nube deberán ser escalados y gestionados con el fabricante (Red Hat, Microsoft, AWS) según los canales de soporte vigentes, manteniendo a la DIAN informada del estado y los avances hasta la resolución de los incidentes.

1.1.1.5. Gestión de almacenamiento en nube

El proveedor deberá ejecutar todas las actividades técnicas, operativas y de control que garanticen la adecuada administración, monitoreo, disponibilidad, seguridad, continuidad y optimización de los servicios de almacenamiento de información en la nube que soportan las soluciones tecnológicas de la Entidad.

Este servicio abarca los servicios de almacenamiento estructurado y no estructurado a nivel de infraestructura en las nubes del servicio, incluyendo cuentas de almacenamiento y sus componentes (Blob/Object Storage, File Storage, Table Storage, colas de mensajería asociadas a las cuentas de almacenamiento), volúmenes/discos (Block Storage), repositorios de respaldo y recuperación (backups) y componentes de datalake utilizados por las soluciones de la DIAN en IaaS, PaaS y contenedores.

A. Excluye

- Diseño y operación de soluciones analíticas, data warehouse, data lakehouse y procesos ETL/ELT/DataOps que consuman la información almacenada. DIAN: SPD y equipos de analítica, junto con áreas de negocio.
- Gestión del contenido funcional o de negocio (clasificación funcional, depuración de registros, organización de carpetas, archivo regulatorio/histórico). DIAN: áreas de negocio y gestión documental/archivo.
- Proyectos de migración masiva o re-arquitectura de plataformas de almacenamiento (racionalización global de cuentas, rediseño de data lake), que se contratan como servicios/proyectos por demanda. DIAN: DGIT – Arquitectura/Infraestructura y áreas de negocio.

B. Condiciones del servicio

- La DIAN define lineamientos de arquitectura, seguridad, clasificación y ciclo de vida; el proveedor los implementa y mantiene técnicamente.
- Todo aprovisionamiento y cambio se gestiona vía ITSM, siguiendo estándares, plantillas y esquema de etiquetado aprobados por la DIAN.
- Cambios con impacto relevante en costos, seguridad o arquitectura requieren aprobación previa de la DIAN.
- El servicio se coordina con redes, identidades/accesos, administración de bases de datos y otros servicios que consuman almacenamiento.

1.1.1.6. Gestión de redes en nube

La gestión de redes en nube comprende las actividades necesarias para operar y asegurar los componentes de red virtual en las nubes gestionadas por el proveedor, garantizando conectividad segura y eficiente entre los entornos, cargas de trabajo y servicios de la DIAN. El proveedor debe asegurar la implementación del protocolo IPV6 de acuerdo con lo establecido con el Ministerio de Telecomunicaciones en coordinación con DIAN, administrar el direccionamiento, rangos o reservas y mantener una continua actualización sobre la asignación de cada uno.

A. Actividades fuera del alcance

- Análisis forense de red o captura avanzada de paquetes que requiera herramientas especializadas o servicios dedicados.
- Diseño e implementación de arquitecturas de red multinube completamente nuevas o rediseños integrales de la topología, que se consideran parte de los servicios de arquitectura y gobierno de nube.

1.1.2. Gestión del Servicio

A. Disposiciones comunes para la gestión del servicio

La DIAN cuenta con un modelo corporativo de gestión de incidentes, solicitudes, problemas y cambios autogestionado, a través de una plataforma ITSM institucional ya implementada.

La Gestión del Servicio se enfoca en actividades de coordinación, seguimiento de ANS y mejora continua, apoyándose en la plataforma ITSM corporativa y en los procesos institucionales existentes.

La atención técnica y resolución de los casos (incidentes, problemas, cambios y solicitudes) relacionados con la infraestructura y servicios de nube, incluyendo análisis, diagnóstico y ejecución de acciones técnicas, forma parte del alcance de los servicios de Operación de la Nube (SOC, NOC, administración de sistemas operativos, administración de plataformas, gestión de redes, gestión de backups y otros definidos en este documento), por lo que no deberá ser cotizada nuevamente dentro de la Gestión del Servicio.

El proveedor deberá registrar y mantener actualizada en la plataforma ITSM toda la información relacionada con los tickets asignados (clasificación, prioridad, actividades realizadas, responsables, tiempos y resultado), sin perjuicio del uso de otros medios (correo, chat, etc.) como canales de apoyo.

B. Alcance general de la responsabilidad del proveedor

El proveedor será responsable de la gestión técnica de los servicios de nube (infraestructura, sistemas operativos, capa media, bases de datos, plataformas de contenedores y servicios PaaS bajo su administración), incluyendo la atención de incidentes, problemas, solicitudes y cambios asociados a dichos componentes, de acuerdo con los servicios técnicos definidos para la prestación del servicio.

La DIAN, o los contratos que esta defina, serán responsables de la atención de usuarios finales, la definición de procesos de negocio, el soporte funcional de aplicaciones, la provisión y administración corporativa de la plataforma ITSM y la adquisición de nuevos servicios de nube y licenciamiento, entre otros aspectos de gobierno y negocio.

C. Condiciones generales de prestación del servicio

La atención de incidentes, problemas, solicitudes y cambios se realizará de acuerdo con los horarios de operación, niveles de severidad/prioridad y catálogos de servicios definidos por la DIAN, garantizando en todos los casos la trazabilidad completa del ciclo de vida de cada ticket en la plataforma ITSM, así como la vinculación entre incidentes, problemas, solicitudes y cambios cuando exista relación entre ellos.

El proveedor de la nube deberá garantizar los más altos estándares en protección de información en reposo y en tránsito entre sus distintas componentes o nodos, según las políticas, lineamientos del SGSPI de la Entidad, que es basado en ISO27001 y mejores prácticas del mercado.

Cuando la naturaleza del incidente o problema lo requiera, el proveedor deberá escalar los casos a los contratos de soporte de fabricante existentes (por ejemplo, Soporte Unificado y Misión Crítica de Microsoft, soporte de fábrica de Red Hat), siguiendo los lineamientos de la DIAN, gestionando la interacción técnica con dichos fabricantes y manteniendo el caso actualizado en la plataforma ITSM hasta su cierre, de igual manera deberá escalar cualquier alarma o evento anómalo en integración con el modelo operativo del SOC y la gestión de incidentes de la DIAN

Los acuerdos de nivel de servicio (ANS) específicos de cada proceso se consolidarán en un Anexo de Niveles de Servicio, en el que se definirán los tiempos objetivo de registro, atención inicial, resolución y calidad del registro para cada tipo de ticket y severidad.

D. Exclusiones generales

Salvo que se indique expresamente lo contrario en alguno de los procesos específicos, se consideran excluidas de los servicios de Gestión de incidentes, problemas, solicitudes y cambios, por corresponder a la DIAN u otros contratos:

- La provisión, licenciamiento, administración y soporte corporativo de la plataforma ITSM.
- El soporte técnico o funcional de primer nivel a usuarios finales (funcionarios o contribuyentes).
- La atención de requerimientos funcionales de negocio o de aplicación (cambios en reglas de negocio, formularios, reportes funcionales, parametrizaciones), así como el desarrollo o despliegue de nuevas funcionalidades o correcciones de código.
- La gestión de tickets (incidentes, problemas, solicitudes) relativos a equipos de usuario final, redes locales, centros de datos on-premise u otra infraestructura fuera de la nube administrada, salvo apoyos puntuales de coordinación o diagnóstico que solicite la DIAN.
- La gestión de tickets (incidentes, problemas) asociados exclusivamente a procesos de negocio sin impacto técnico en la infraestructura o plataformas de nube administradas por el proveedor.
- La comunicación directa con usuarios finales sobre el estado, impacto o contenido de las solicitudes, incidentes o problemas cuando esta sea responsabilidad de la mesa de servicios u otras áreas designadas por la DIAN.

Las exclusiones anteriores no liberan al proveedor de atender, analizar y gestionar los tickets de naturaleza técnica cuya causa raíz o tratamiento se relacione con infraestructura, sistemas operativos, capa media, bases de datos, plataformas de contenedores o servicios PaaS bajo su administración.

Cuando un requerimiento combine aspectos técnicos y funcionales, el proveedor será responsable de la parte técnica que le corresponda, en coordinación con los equipos funcionales y de negocio de la DIAN.

1.1.2.1. Gestión de incidentes

La gestión de incidentes tiene como finalidad restablecer la operación normal de los servicios de nube en el menor tiempo posible, minimizando el impacto en la operación de la DIAN y cumpliendo los niveles de servicio definidos.

A. Objetivo

Garantizar que los incidentes que afecten los servicios de nube (IaaS, PaaS, contenedores, servicios gestionados y conectividad asociada) se gestionen de forma oportuna, estandarizada y trazable, desde su registro hasta su cierre, coordinando las acciones técnicas necesarias y los escalamientos requeridos, de conformidad con las disposiciones comunes de Gestión del Servicio. Los incidentes pueden ser detectados por el proveedor a través de sus propios mecanismos de monitoreo o por el personal administrativo de DIAN. En cualquier caso, el proveedor debe registrar el incidente en el momento en que suceda con los datos de referencia necesarios para identificar la falla y notificar al administrador del contrato u operador correspondiente de acuerdo con el procedimiento establecido en la Entidad.

B. Actividades fuera del alcance

Aplican las exclusiones generales definidas en el numeral para la Gestión del Servicio y Exclusiones transversales del servicio.

1.1.2.2. Gestión de problemas

Son las actividades para identificar y comprender las causas subyacentes de toda alteración, real o potencial de los servicios en el entorno Multinube y en determinar el mejor método para solucionarlas y eliminar el origen de estos problemas. Si se adopta una solución alternativa para un incidente reportado, se detiene el cálculo de ANS, pero el proveedor debe actuar de manera ininterrumpida para la solución definitiva bajo un tratamiento de gestión de problemas

A. Objetivo

Asegurar que los problemas que afecten a los servicios de nube (IaaS, PaaS, contenedores, servicios gestionados y conectividad asociada) se gestionen de forma sistemática y trazable, desde su identificación hasta la definición e implementación de acciones correctivas y preventivas, contribuyendo a la reducción de incidentes recurrentes y a la mejora continua del servicio.

B. Actividades fuera del alcance:

Aplican las exclusiones generales definidas en el numeral para la Gestión del Servicio.

C. Condiciones de prestación del servicio

- La gestión de problemas deberá realizarse en coordinación con la Gestión de Incidentes y la Gestión de Cambios, abarcando tanto problemas reactivos (derivados de incidentes) como problemas identificados de manera proactiva.
- Los problemas asociados a servicios catalogados como críticos o de misión crítica deberán tratarse con prioridad, conforme a los criterios y plazos que defina la DIAN.
- Los análisis de causa raíz deberán quedar documentados en la herramienta ITSM o en los repositorios que defina la DIAN, vinculados al registro de problema y a los incidentes asociados.
- Las acciones correctivas o preventivas que impliquen cambios en la infraestructura o en las plataformas de nube deberán gestionarse mediante el proceso de Gestión de Cambios, respetando los flujos de aprobación y ventanas definidos por la DIAN.
- El proveedor deberá apoyar activamente los procesos de mejora continua, proponiendo acciones técnicas que reduzcan la recurrencia de incidentes y problemas en los servicios administrados.

1.1.2.3. Gestión de solicitudes

Son las actividades para la comunicación entre los solicitantes de los servicios de nube y sus prestadores de servicio con el fin de asegurar la atención y cumplimiento de los requerimientos los cuales deben ser de bajo costo, de bajo riesgo y de solicitud frecuente. Por el cumplimiento de requerimientos también se gestiona y/o se apoya las solicitudes de información, la atención de quejas, comentarios y agradecimientos de los usuarios.

A. Objetivo

Garantizar que las solicitudes de servicio relacionadas con los entornos de nube (IaaS, PaaS, contenedores, servicios gestionados y conectividad asociada) se gestionen de forma estandarizada, oportuna y trazable, de acuerdo con el catálogo de servicios y los niveles de servicio definidos por la DIAN.

B. Actividades fuera del alcance:

- La gestión de solicitudes asociadas a procesos de negocio que no tengan impacto o relación con la capa técnica de infraestructura o plataforma de nube gestionada por el proveedor.
- Aplican las exclusiones generales definidas en el numeral para la Gestión del Servicio y Exclusiones transversales del servicio

C. Condiciones de prestación del servicio

- La gestión de solicitudes se prestará en los horarios de operación definidos para los servicios de nube, diferenciando cuando aplique entre solicitudes prioritarias y solicitudes estándar.
- La DIAN definirá y mantendrá el catálogo de servicios y tipos de solicitud aplicables a este servicio; el proveedor deberá ajustarse a dicho catálogo y proponer mejoras cuando identifique oportunidades (por ejemplo, estandarización o automatización de solicitudes recurrentes).
- Las solicitudes que impliquen cambios relevantes en configuración, arquitectura o parámetros de los servicios de nube deberán canalizarse, cuando corresponda, mediante el proceso de Gestión de Cambios y sus flujos de aprobación.
- El proveedor deberá asegurar la trazabilidad completa de las solicitudes, incluyendo su relación con incidentes, problemas y cambios cuando exista vínculo entre ellos.

1.1.2.4. Gestión de cambios

La gestión de cambios tiene como finalidad controlar, evaluar y ejecutar de manera ordenada los cambios técnicos sobre la infraestructura y servicios de nube administrados, minimizando el riesgo de incidentes y afectaciones al negocio y asegurando trazabilidad y alineación con los lineamientos de arquitectura y seguridad incluidos en el SGSPI de la DIAN.

A. Objetivo

Garantizar que los cambios que afecten los servicios de nube (IaaS, PaaS, contenedores, servicios gestionados y conectividad asociada) se gestionen de forma planificada, autorizada y trazable, desde su solicitud hasta su cierre, de conformidad con las disposiciones comunes de Gestión del Servicio y con las políticas de cambio definidas por la DIAN.

B. Excluye

- Para la Gestión de cambios aplican las exclusiones generales definidas en las disposiciones comunes de Gestión del Servicio, en especial:
    - La definición de la política corporativa de Gestión de Cambios de la DIAN (normas generales, roles organizacionales, cambios de negocio), que será responsabilidad de la Entidad.
    - La aprobación de cambios de negocio o funcionales que no involucren componentes técnicos de la nube administrada por el proveedor.
- Estas exclusiones no liberan al proveedor de su responsabilidad sobre la gestión técnica de los cambios que afecten la infraestructura y servicios de nube bajo su administración.

C. Condiciones del servicio

- No se permitirá la ejecución de cambios no autorizados (“cambios directos” o no registrados), salvo en situaciones de emergencia debidamente justificadas, las cuales deberán registrarse y regularizarse posteriormente conforme a los lineamientos de la DIAN.
- Las ventanas de mantenimiento, niveles de aprobación requeridos y criterios para cambios estándar, normales y de emergencia serán definidos por la DIAN, y el proveedor deberá ajustarse a dichos lineamientos.

1.1.2.5. Gestión de activos y configuraciones

La gestión de activos y configuraciones comprende las actividades necesarias para mantener un inventario actualizado de los recursos en nube (Azure y AWS) bajo el servicio, así como un modelo básico de relaciones y atributos que permita apoyar la gestión de costos, capacidad, seguridad y continuidad de los servicios de TI en la nube.

A. Objetivo

Asegurar que los activos y configuraciones de los recursos de nube (IaaS, PaaS, contenedores y servicios asociados) bajo administración del proveedor se encuentren identificados, registrados, controlados y conciliados de forma periódica, permitiendo conocer qué existe, cómo está configurado y cómo se relaciona a un nivel básico, para soportar la gestión técnica y financiera de la nube.

Este servicio no tiene como objetivo implementar una CMDB corporativa completa ni modelar todos los elementos de configuración de TI de la DIAN. Su alcance se limita a los recursos de nube gestionados por el servicio y a los servicios y aplicaciones críticos definidos por la Entidad, utilizando principalmente capacidades nativas de Azure y AWS y herramientas estándar de mercado.

B. Actividades fuera del alcance

- La implementación, administración o soporte funcional de la herramienta ITSM o CMDB corporativa de la DIAN (Aranda u otras).
- La modelación detallada de elementos de configuración fuera de las nubes gestionadas (infraestructura on-premises, estaciones de trabajo, impresoras, etc.).
- La automatización completa de la asociación de incidentes, problemas o cambios a elementos de configuración.

C. Condiciones del servicio

- El esquema de atributos mínimos y de etiquetado será definido y aprobado por la DIAN y revisado de forma conjunta cuando sea necesario.

- Los mecanismos de exportación y consulta de la información deberán utilizar formatos abiertos o APIs documentadas, compatibles con las herramientas corporativas de la DIAN.
- El proveedor garantizará la confidencialidad y protección de la información de inventario y configuraciones según las políticas de seguridad de la DIAN.
- El proveedor deberá realizar una toma de control de la gestión existente, evitando proponer como requisito la reconstrucción total del inventario salvo decisión expresa de la DIAN.
- La DIAN definirá los lineamientos de gobierno del inventario y configuraciones, y el proveedor deberá ajustarse a ellos y proponer mejoras cuando identifique oportunidades.
- La gestión de activos y configuraciones deberá mantenerse alineada con los procesos de aprovisionamiento, gestión de cambios y gestión de costos, para reflejar oportunamente las altas, bajas y modificaciones en la infraestructura de nube.

1.1.3. Operación de la nube

1.1.3.1. Gestión de incidentes masivos

A. **Objetivo del servicio**
Gestionar de forma coordinada los incidentes de alto impacto que afecten servicios en nube de la DIAN (infraestructura, plataformas y, cuando aplique, aplicaciones en alcance), minimizando el impacto en la operación misional y restableciendo el servicio en el menor tiempo posible, en articulación con el NOC y el proceso de Gestión de Incidentes del ITSM corporativo.

B. Actividades fuera del alcance

Quedan fuera del alcance de este servicio:

- La corrección funcional o evolutiva de aplicaciones o cambios en la lógica de negocio, salvo cuando la causa raíz se relacione directamente con la infraestructura o servicios de nube administrados en el servicio prestado.
- El RCA sobre procesos de negocio de la DIAN o sobre infraestructura on-premises ajena al alcance del servicio, más allá de la coordinación técnica que sea requerida.
- La gestión de comunicaciones hacia usuarios finales, medios de comunicación u otras entidades externas, que es responsabilidad de la DIAN.
- La implementación de cambios permanentes que correspondan a otros contratos, áreas o proveedores, más allá de las recomendaciones y coordinación técnica del proveedor.

C. Condiciones del servicio

- La Gestión de incidentes masivos se presta en esquema 7x24x365, alineado con la operación del NOC y la criticidad de los servicios en nube.
- El proveedor utilizará la plataforma ITSM corporativa de la DIAN para el registro, seguimiento, clasificación y cierre de los incidentes masivos, siguiendo los flujos definidos por la Entidad.
- La activación de la condición de incidente masivo se realizará con base en criterios acordados con la DIAN y podrá ser solicitada por el NOC o por las áreas responsables de la Entidad.
- El proveedor mantendrá procedimientos documentados y actualizados, alineados con buenas prácticas de ITIL/ITSM y con los lineamientos de gobierno de nube de la DIAN.
- Se debe garantizar la trazabilidad completa del incidente (eventos, evidencias técnicas, comunicaciones y línea de tiempo) y ponerla a disposición de la DIAN cuando sea requerida.

1.1.3.2. Gestión técnica de aplicaciones en nube

A. Objetivo del servicio

Asegurar la operación técnica de las aplicaciones y servicios misionales o de soporte que funcionan en la Multinube híbrida de la DIAN, brindando apoyo tanto en la operación diaria, despliegues, requerimientos de capacidad, monitoreo y respaldo, sobre infraestructura de nube ya aprovisionada, en coordinación con los servicios especializados de infraestructura.

B. Actividades fuera del alcance – Excluye

Quedan explícitamente fuera del alcance de este servicio (sin perjuicio de su coordinación con otros servicios sí incluidos):

- Ejecución de pruebas funcionales o de negocio, diseño de casos de prueba funcionales y pruebas de soporte funcional.
- Diagnóstico y resolución de errores de lógica de negocio, reglas de negocio, flujos internos, modelos de datos o estructuras internas de las aplicaciones.
- Planeación y gestión de proyectos de desarrollo o evolución funcional de aplicaciones, definición de roadmaps funcionales o decisiones de producto.

C. Condiciones de prestación del servicio

- Servicio prestado como parte de la operación continua de la Multinube, articulado con el NOC y los demás servicios base.
- Aplica a las aplicaciones incluidas en el Anexo de cargas de trabajo y a las que la DIAN incorpore formalmente al ámbito gestionado durante la vigencia del servicio.

- El proveedor se enfoca en la operación técnica sobre la nube; el desarrollo, soporte funcional y definición de negocio son responsabilidad de la DIAN y sus fábricas de software.
- Este servicio no reemplaza los servicios especializados de Administración de sistemas operativos, Administración de capa media y plataformas estándar, Administración de bases de datos y almacenamiento, Gestión de redes en nube, Interoperabilidad de Aplicaciones y APIs, DataOps, DevSecOps ni Monitoreo y observabilidad/NOC; sus actividades se limitan a la coordinación, solicitud y apoyo operativo específico por aplicación, apoyándose en dichas capacidades especializadas.
- Todas las actividades se gestionan a través de la plataforma ITSM corporativa y siguen la arquitectura de referencia, el stack tecnológico y los lineamientos de seguridad, DevSecOps, DataOps, redes e interoperabilidad definidos por la DIAN.

1.1.3.3. Administración de Sistemas Operativos (IaaS)

Asegurar la operación, mantenimiento, actualización y continuidad de los sistemas operativos Windows y Linux instalados en máquinas virtuales (IaaS) de las nubes públicas utilizadas por la DIAN, garantizando su disponibilidad, seguridad y alineamiento con las políticas técnicas y de gobierno definidas por la entidad.

A. Actividades fuera del alcance:

- Actividades de hardening avanzado, auditorías de seguridad especializadas o cumplimiento normativo que excedan la línea base de configuración definida por la DIAN.
- Migraciones funcionales de aplicaciones que requieran intervención de equipos de desarrollo, fabricantes de aplicaciones o terceros especializados.
- Administración integral de sistemas operativos en máquinas virtuales unidas/matriculadas al dominio corporativo de la DIAN, cuando estas sean gestionadas directamente por los equipos internos de la entidad. En estos casos, el proveedor únicamente prestará apoyo técnico bajo solicitud expresa de la DIAN, sin asumir la responsabilidad primaria sobre su operación.

B. Condiciones del servicio:

- Todas las actividades se deben ejecutar de acuerdo con las políticas de seguridad, gobierno, cambio y operación definidas por la DIAN, incluyendo la obligatoriedad de usar las ventanas de mantenimiento aprobadas para cambios que impacten la disponibilidad.
- La responsabilidad del proveedor se limita al componente técnico de sistema operativo; la correcta operación funcional de las aplicaciones corresponde a las áreas propietarias y/o equipos de desarrollo.

- Para los ambientes productivos se prestará atención 7x24 a incidentes críticos; para ambientes no productivos (dev/test/preprod) la atención se realizará en horario laboral, salvo que se establezca lo contrario por escrito.

1.1.3.4. Administración de Capa Media y Plataformas Estándar sobre IaaS

Garantizar la operación técnica, la actualización y el mantenimiento de la capa media (middleware) y de las plataformas estándar instaladas sobre servidores IaaS, de forma que se mantengan en versiones soportadas por el fabricante, seguras y estables para las aplicaciones de la DIAN que dependen de ellas.

A. Actividades fuera del alcance

- Cambios en contenido, estructura funcional, apariencia o configuración de negocio de las Plataformas Estándar (por ejemplo, administración de contenidos en WordPress o Moodle).
- Instalación, actualización o configuración de *plugins*, módulos, temas o extensiones personalizados no considerados estándar ni definidos dentro del alcance técnico por la DIAN.

B. Condiciones del servicio

- El proveedor será responsable únicamente del componente técnico (servicios, binarios, configuración técnica), mientras que las áreas funcionales y de desarrollo serán responsables de la correcta operación funcional y del contenido.
- El proveedor deberá coordinar con la DIAN y con otros equipos involucrados (por ejemplo, desarrollo o seguridad) las actividades que puedan tener impacto transversal sobre las aplicaciones.

1.1.3.5. Administración Técnica de Contenedores, Imágenes, Runtimes y Componentes NO cubiertos por el Fabricante (Workload-Level)

Administrar la capa técnica de las cargas de trabajo que se ejecutan en los clústeres de contenedores de la DIAN (workloads), incluyendo contenedores, imágenes, runtimes y ciertos componentes complementarios, exclusivamente en aquellos aspectos que no están cubiertos por los fabricantes Red Hat, Microsoft o AWS, garantizando su disponibilidad, compatibilidad con las plataformas de contenedores y actualización técnica conforme a las políticas de la entidad.

A. Actividades fuera del alcance

- Migraciones entre tecnologías o plataformas de middleware (por ejemplo, migrar de un stack Kafka a otro completamente distinto) que impliquen rediseño funcional o de arquitectura.
- Configuración técnica y funcional de las herramientas de autenticación/autorización (por ejemplo, definición de realms, roles, flujos de autenticación en Keycloak).

B. Condiciones del servicio

- El proveedor administrará únicamente los componentes y actividades que no están cubiertos por el soporte del fabricante (Red Hat, Microsoft, AWS) en lo referente a workloads, contenedores, imágenes, runtimes y componentes complementarios, evitando duplicidades con el soporte de la plataforma o de las imágenes base certificadas.
- La responsabilidad funcional de las aplicaciones desplegadas -comportamiento de negocio, lógica funcional, modelos de datos y pruebas funcionales-. permanecerá a cargo de las áreas propietarias y en los equipos de desarrollo de la DIAN, o terceros que ésta designe.
- Cuando se identifiquen problemas cuyo origen esté en la plataforma de contenedores o componentes cubiertos por el fabricante, el proveedor deberá coordinar el escalamiento con Red Hat, Microsoft o AWS, según corresponda, e informará a la DIAN del avance hasta la resolución de los problemas.

1.1.3.6. Interoperabilidad de Aplicaciones y APIs

La interoperabilidad de aplicaciones y APIs comprende las actividades necesarias para operar y soportar las plataformas de integración y gestión de APIs en las nubes públicas de la DIAN, garantizando el intercambio seguro y confiable de información entre aplicaciones en nube, sistemas on-premise y entidades externas, de acuerdo con los lineamientos de arquitectura, seguridad, gobierno y el stack tecnológico de nube del Anexo 1.

Estas actividades se realizan sobre las plataformas de gestión de APIs e integraciones definidas en el stack tecnológico de la DIAN -entre ellas Azure API Management o Red Hat 3scale-, y servicios de integración relacionados.

A. Excluye

- Gobernabilidad funcional o comercial de las APIs incluyendomodelos de monetización, planes de consumo, catálogos externos.
- El diseño avanzado o comercial de portales de desarrolladores.
- Las transformaciones complejas de datos, orquestaciones avanzadas o flujos de integración que constituyan proyectos específicos de integración, que se atenderán como servicios por demanda o proyectos independientes.

- Definición de arquitectura empresarial, modelo corporativo de gobierno de APIs y datos , y/o políticas institucionales de interoperabilidad, a cargo de la DIAN.

B. Condiciones del servicio – Interoperabilidad de Aplicaciones y APIs

- La operación en ambientes productivos se presta en modo de operación continua (24/7), con atención de incidentes críticos según ANS y sujeta a las ventanas de mantenimiento programado acordadas con la DIAN.
- La atención de requerimientos y ajustes en ambientes no productivos se realiza principalmente en horario hábil, salvo acuerdo expreso con la DIAN.
- La criticidad de APIs e integraciones será definida por la DIAN y se usará para priorización y aplicación de ANS.
- Las actividades se ejecutan sobre las plataformas y servicios de integración definidos en el stack tecnológico de la DIAN, respetando arquitectura, segmentación y políticas de seguridad.
- El proveedor utilizará las herramientas corporativas de la DIAN (ITSM, monitoreo, observabilidad) y coordinará con otros proveedores cuando los incidentes involucren sistemas fuera del alcance del servicio, manteniendo trazabilidad.
- Cuando los incidentes involucren sistemas fuera del alcance del servicio, el proveedor coordinará con los proveedores responsables, manteniendo trazabilidad completa del caso.
- El proveedor mantendrá actualizada la documentación técnica operativa mínima de las APIs e integraciones gestionadas, conforme a los estándares y plantillas definidos por la DIAN..

1.1.3.7. Administración de bases de datos

Servicio de operación continua para la administración técnica de bases de datos en nube y del almacenamiento directamente asociado (datos, logs y backups), sobre dos tipos de despligue:

- Servicios gestionados (PaaS/DBaaS): PostgreSQL, MySQL Cosmos DB, MongoDB gestionado, Redis gestionado, DynamoDB y otros.
- Motores instalados en IaaS (VM): PostgreSQL, MySQL, MongoDB.

Las actividades avanzadas -tuning profundo, migraciones complejas, cargas históricas, proyectos-. se atienden mediante el servicio por demanda de “Administración avanzada de bases de datos en nube”.

A. Excluye

- Procesos ETL (Extract, Transform, Load) complejas, pipelines de integración de datos, migraciones masivas y transformaciones estructurales complejas.
- Migraciones masivas de datos o migraciones funcionales entre motores que impliquen el rediseño del modelo de datos.

- Diseño o rediseño del modelo de datos y definición de políticas institucionales de retención de datos, a cargo de la DIAN.
- Instalación inicial de motores de base de datos en IaaS, upgrades mayores de versión, tuning profundo y cargas históricas, los cuales se atienden mediante el servicio por demanda *"Administración avanzada de bases de datos en nube"*.

B. Condiciones del servicio

- El proveedor es responsable de la operación técnica del motor de base de datos y el almacenamiento asociado. La responsabilidad sobre los modelos de datos, la lógica de negocio y las pruebas funcionales corresponde a la DIAN.
- SQL Server y Oracle, permanecen bajo la responsabilidad principal del grupo de bases de datos de la DIAN. Cualquier intervención del proveedor sobre estos motores se realizará de forma coordinada con el grupo de bases de datos y dentro del alcance que la DIAN defina explicitamente.
- En despliegues IaaS, la administración del sistema operativo (SO) está cubierta porel servicio de sistemas operativos; en el presente servicio se atiende exclusivamente el motor de base de datos.
- Las actividades avanzadas -instalación, upgrades mayores de versión, tuning profundo, migraciones, cargas históricas- se canalizan mediante el servicio por por demanda.

1.1.3.8. Soporte DevOps y gestión de pipelines CI/CD

A. Objetivo del servicio

Garantizar la operación técnica, administración, continuidad y evolución controlada de las plataformas, herramientas y flujos DevOps actualmente implementadas en la nube de la DIAN. Su proposito es que los equipos de desarrollo puedan construir, probar y desplegar aplicaciones sobre el *stack tecnológico institucional,* que incluye – entre otras – herramientas comoAzure DevOps, GitHub, pipelines CI/CD, Tekton, Argo CD, Terraform, etc.), así como la administración de las herramientas utilizadas en DevOps, sin que el proveedor asuma actividades de desarrollo de software ni diseño funcional de las soluciones.

B. Fuera del alcance

Se excluyen expresamente, entre otras, las siguientes actividades:

- La definición de la estrategia DevOps, políticas de seguridad, matrices de roles o estándares de arquitectura, que corresponde a la Oficina de Seguridad de la información (OSI), al equipo DevSecOps y a las áreas de arquitectura de la DIAN.
- La operación de un Centro de Operaciones de Seguridad (SOC) o monitoreo de seguridad centralizado.

- La administración de la infraestructura on-premise de la DIAN (solo se reportan fallos de pipelines que despliegan hacia esos entornos).
- La adquisición o financiación de licencias de herramientas DevOps y deseguridad, las cuales sonprovistas por la DIAN.

C. Condiciones del servicio

- El servicio se prestará sobre el stack tecnológico y herramientas definidos por la DIAN. Cualquier cambio sobre herramientas, versiones o configuraciones base deberá ser aprobado formalmente por la Entidad conforme a su proceso de gestión de Cambios.
- La DIAN, a tráves de su proceso de Gestión de cambios, definirá para qué tipos de despliegues y ambientes se requiere registro y aprobación formal en el ITSM.
- El uso de credenciales y secretos en pipelines se realizará exclusivamente mediante los mecanismos corporativos de gestión de identidades y secretos definidos por la DIAN, conforme a las politicas de seguridad vigentes.
- El proveedor implementará y operará técnicamente, en las herramientas y pipelines, los lineamientos y controles definidos por la OSI y el equipo DevSecOps, y entregará a dichos equipos reportes técnicos necesarios.

1.1.3.9. Soporte DataOps y operación de canalizaciones de datos

A. Objetivo del servicio

El proveedor será responsable de la operación técnica de las canalizaciones de datos sobre las plataformas de orquestación y procesamiento definidas por la DIAN -por ejemplo, Azure Data Factory, Synapse Pipelines, Databricks, Glue u otras que la DIAN incorpore formalmente al stack tecnológico durante la vigencia del contrato-, respetando:

- La arquitectura y lineamientos establecidos por el equipo de Arquitectura de Nube y Datos de la Dirección de Gestión de Innovación y Tecnología (DGIT).
- Los requerimientos de explotación de información y las ventanas de procesamiento definidos por la Subdirección de Procesamiento de Datos (SPD) y demás áreas usuarias de datos.
- Las políticas y controles de seguridad definidos por la OSI.

El servicio abarcaa tanto canalizaciones existentes como nuevas canalizaciones que el que el proveedor implemente, conforme a las prioridades, planes de trabajo y aprobaciones definidos por la DIAN.

B. Excluye

- La defínción de modelos de datos corporativos, diccionarios de datos, dominios de información o taxonomías institucionales, correspondientes al nivel de gobierno del dato a cargo de la DIAN.
- El diseño de la arquitectura de datos institucional, el modelamiento técnico de bases de datos y/o los esquemas de integración corporativos.
- El desarrollo o implementación modelos de analítica avanzada, inteligencia artificial (incluyendo machine learning) sobre los datos procesados.
- La definición de reglas de calidad funcional de los datos y de políticas institucionales de retención, a cargo de la SPD y las áreas de nesgocio de la DIAN.

C. Condiciones del servicio

- El alcance se limita a la operación técnica de las canalizaciones y a la calidad técnica de los datos. La definición de reglas de negocio, calidad funcional de la información y modelos de datos corporativos es responsabilidad de SPD, arquitectura y las áreas de negocio de la DIAN.
- En los procesos ETL(Extract, Transform, Load) y ELT(Extract, Load, Transform), el proveedor es responsable de la correcta ejecución técnica de las cargas según el diseño aprobado; la validación funcional y de negocio corresponde a la DIAN.
- Los cambios estructurales en las canalizaciones – entendidos como aquellos que alteran su lógico de procesamiento, fuentes de datos o destinos- se gestionarán a través del proceso de gestión de cambios institucional y requerirán aprobación de SPD, el equipo de arquitectura, Seguridad y dueños funcionales de los datos.
- La operación de DataOps se integrará con la plataforma ITSM institucional para el registro, seguimiento y cierre de incidentes, problemas, requerimientos y cambios asociados a las canalizaciones de datos.

1.1.3.10. Monitoreo y observabilidad

Es el conjunto de estrategias y prácticas que permiten recopilar, correlacionar, agregar y analizar las telemetrías de la nube para gestionar el estado, el rendimiento, la disponibilidad y la seguridad de la infraestructura y las aplicaciones desplegadas en el ecosistema Multinube. El proveedor deberá configurar, implementar, operar y mantener las plataformas nativas de monitoreo y observabilidad de las nubes (Azure Monitor, Log Analytics, Application Insights, AWS CloudWatch, CloudTrail, X-Ray u otras aprobadas por la DIAN), integrando fuentes de telemetría, métricas y trazas provenientes de los recursos de infraestructura, servicios PaaS, contenedores y aplicaciones desplegadas en los entornos de nube, conforme con las políticas técnicas, de seguridad y gobernanza establecidas por la DIAN.

A nivel de APM (Application Performance Monitoring)

El proveedor deberá implementar y operar herramientas de APM dentro del ecosistema Multinube, garantizando la visibilidad del desempeño, la disponibilidad y la salud operativa de las aplicaciones desplegadas.

A. Actividades fuera del alcance:

- El monitoreo de componentes completamente externos o no integrados al ecosistema Multinube de la DIAN, tales como infraestructuras o aplicaciones de terceros sin conexión con los servicios gestionados.
- La Ejecuciónde actividades de correlación de ciberseguridad, análisis forense, las cuales son gestionadas por el SOC y el Sistema de Gestión de Información y Eventos de Seguridad (SIEM) institucional.
- Implementación de modelos de analítica avanzada o machine learning que excedan las capacidades nativas de las herramientas de observabilidad.
- El desarrollo de dashboards o reportes personalizados de alta complejidad que constituyen proyectos independientes; estos se canalizarán como servicios por demandas.

B. Condiciones de prestación del servicio

- El servicio deberá operar de forma continua, disponibilidad de la plataforma de monitoreo: 7x24x365, garantizando la generación oportuna de métricas y alertas conforme a los umbrales y tiempos de respuesta definidos en las ANS.
- Las herramientas de monitoreo deberán permanecer integradas con la plataforma ITSM, el NOC, de modo que el proveedor asegure la trazabilidad correlación de eventos entre ambas plataformas.
- El proveedor deberá mantener los accesos, configuraciones y controles de seguridad necesarios para la administración y operación de las plataformas, cumpliendo las políticas de la Oficina de Seguridad de la Información (OSI), las cuales son de carácter vinculante para este servicio.
- La gestión de alertas – incluyendo canales de notificación, tiempos de respuesta y procedimientos de escalamiento- se realizará conforme a lo establecido en el ANS y los procedimientos operativos acordados con la DIAN.

1.1.4. Gestión de seguridad en la multinube

A. Objetivo

Definir el modelo de gestión de seguridad en la Multinube de la DIAN bajo este servicio, de forma que los servicios y recursos en las nubes en alcance se operen con controles adecuados de confidencialidad, integridad, disponibilidad y trazabilidad, aplicando los lineamientos de la OSI y la DGIT y articulándose con los servicios de accesos, perímetro, hardening y operación de nube.

B. Alcance

La gestión de seguridad en la Multinube aplica a:

- Los recursos y servicios en las nubes en alcance (IaaS, PaaS y servicios gestionados) administrados por el proveedor e inventariados en el servicio.
- Las actividades de seguridad asociadas a los servicios definidos (gestión de accesos e identidades, protección perimetral en nube, protección de servidores y hardening, entre otros).
- La aplicación de las políticas y lineamientos de seguridad de la información emitidos por la OSI sobre dichos recursos.

Quedan fuera del alcance directo: la infraestructura on-premise y sistemas legacy, la definición de políticas corporativas y gobierno de datos, y la operación de SOC, SIEM, XDR/CSPM y otros servicios de seguridad avanzados que se gestionen por otros contratos o dependencias.

C. Marco normativo y lineamientos OSI / MSPI

La prestación de los servicios de seguridad en la Multinube deberá alinearse, como mínimo, con:

- El Manual MN-IIT-0072, en especial el numeral 5.23 “Seguridad de la información para el uso de servicios en la nube”.
- El Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma NTC ISO/IEC 27001.
- La normatividad de protección de datos y acceso a la información,Manual de Protección de Datos Personales MN-IIT-0062 (Ley 1581 de 2012, Ley 1712 de 2014 y demás disposiciones aplicables).
- Las guías de computación en la nube de MinTIC y referencias técnicas (por ejemplo, lineamientos de Arquitectura Zero Trust).
- Las políticas, estándares y procedimientos de la OSI en clasificación de información, gestión de riesgos de acuerdo con la Cartilla CT-IIT-0132, uso de criptografía, gestión de incidentes e integración con identidades, SIEM ,SOC y cualquier otra solución tecnológica que apoye la vigilancia, detección y mitigación de amenazas.

La DIAN mantiene el rol de definir y gobernar la seguridad de la información; el proveedor debe aplicar y evidenciar el cumplimiento de estos lineamientos en los servicios de nube que administra.

D. Requisitos transversales de seguridad de la información para el uso de servicios en la nube

El proveedor deberá prestar todos los servicios cumpliendo el numeral 5.23 del MN-IIT-0072, el MSPI y la normatividad aplicable, y como mínimo:

- Aplicar principios de seguridad y privacidad en todos los servicios en nube:
  - Privacy by design en el diseño y operación de soluciones.
  - Principios de Arquitectura Zero Trust (verificación explícita y mínimo privilegio).
  - Uso de protocolos seguros y cifrado en reposo y en tránsito según lineamientos de la OSI.
- Respetar la segregación de ambientes y roles, manteniendo separación entre desarrollo, pruebas, preproducción y producción, y separación de funciones en accesos y permisos.
- Garantizar la pertinencia del acceso y uso de la información para usuarios internos y externos, según la clasificación y reglas definidas por la DIAN.
- Validar la seguridad antes del paso a producción, utilizando listas de verificación o revisiones técnicas acordadas con la DIAN y dejando evidencia trazable en ITSM u otros mecanismos formales.
- Coordinar con OSI y DGIT la evaluación de riesgos digitales en los servicios en nube en alcance y aplicar las remediaciones que sean responsabilidad del proveedor, incluyendo controles temporales cuando se acuerde.
- Incorporar prácticas de seguridad, cuando el proveedor gestione plataformas de desarrollo e integración (repositorios, pipelines CI/CD, herramientas DevOps en nube), incluyendo:
  - Controles de seguridad automatizados en los pipelines (escaneo de código, dependencias, configuración e infraestructura como código, gestión de secretos).
  - Integración de hallazgos y eventos de seguridad de repositorios y pipelines CI/CD con las plataformas de gestión de incidentes de la DIAN (ITSM y, cuando aplique, SIEM/SOC) para asegurar trazabilidad y tratamiento oportuno.

La definición de políticas, clasificación de datos, gobierno de la información y gestión de riesgos organizacionales seguirá siendo responsabilidad de la DIAN; el proveedor debe aplicar estos requisitos en los servicios de nube que administra y suministrar evidencias para auditoría y gobierno.

1.1.4.1. Gestión de accesos e identidades

A. Objetivo

Brindar servicios de autenticación y autorización en las nubes en alcance, permitiendo autenticar a usuarios y aplicaciones, autorizar el acceso a recursos de nube pública con base en privilegios asignados, grupos de recursos y registrar la trazabilidad de las acciones realizadas, mediante un único servicio para la Multinube y herramientas que soporten evidencias con validez probatoria para las actuaciones administrativas de la DIAN.

B. Excluye

- Gestión corporativa de identidades y accesos: administración y operación del sistema de Identidad Digital DIAN (ID), gestión del ciclo de vida de empleados y usuarios finales de negocio (altas, bajas, cambios), gestión de identidades de contribuyentes, MDM, biometría y otros mecanismos avanzados de autenticación institucional. (DIAN)
- Plataformas corporativas de seguridad e identidad: implementación y operación de soluciones IAM/IDM/IGA de alcance institucional para toda la DIAN, así como SOC y otros servicios de seguridad centralizados. (DIAN o terceros fuera de este servicio).

C. Condiciones del servicio

- El servicio aplica únicamente a los recursos y plataformas en nube en alcance del servicio e inventariados en la gestión de activos y configuraciones.
- Toda creación, modificación o revocación de accesos se realiza mediante solicitudes registradas y aprobadas en la herramienta ITSM corporativa de la DIAN.
- La gestión de accesos se realiza bajo el principio de mínimo privilegio y conforme a los lineamientos de seguridad y segregación de funciones definidos por la DIAN.
- Cuando las identidades se originen en servicios on-premise (AD, LDAP u otros sistemas locales), su creación y administración es responsabilidad de la DIAN; el proveedor solo administra los permisos y roles en la nube asociados a dichas identidades.
- Se debe garantizar la trazabilidad y registro de las acciones sobre accesos y permisos, manteniendo evidencias consultables para auditorías y actuaciones administrativas.
- El proveedor mantendrá procedimientos documentados para la gestión del ciclo de vida de accesos, revisiones de permisos y control de licencias/suscripciones asociadas.

1.1.4.2. Protección Perimetral Nube y Seguridad Informática

A. Objetivo

Implementar, operar, administrar y mantener los mecanismos de protección lógica de los recursos en las nubes en alcance (WAF, DDoS, firewalls, balanceadores, VPN, bastión, entre otros), incluyendo el monitoreo del tráfico de red y los controles necesarios para detección y prevención de ataques, de forma que se cumplan los esquemas de seguridad definidos por la DIAN en la Multinube.

Realizar la gestión de seguridad informática de acuerdo con las directrices establecidas por DIAN, cumpliendo con los principios de confidencialidad, integridad y disponibilidad de la información. El proveedor deberá validar la seguridad implementada en los servicios de nube antes de ponerlos en producción.

B. Excluye del alcance de este servicio

- Firewalls y controles no nativos / on-premise

- Administración de reglas de firewalls no nativos y de controles perimetrales en centros de datos on-premise. (DIAN – SITO / otros servicios)
- Configuración de balanceadores físicos y gestión de balanceo para aplicaciones no cloud. (DIAN / terceros)

- Servicios especializados de seguridad de la información
  - Actividades de análisis forense, pentesting, análisis de código fuente, auditoría de seguridad de aplicaciones, validación activa y remediación de vulnerabilidades, diseño de arquitecturas de seguridad de aplicaciones y protección de infraestructura on-premise. (DIAN / servicios de seguridad especializados)

C. Condiciones del servicio

- Aplica únicamente a controles en las nubes en alcance del servicio y a las soluciones que la DIAN defina explícitamente dentro de este.
- La operación se alinea con la arquitectura de referencia de seguridad en nube y los lineamientos del área de seguridad de la información.
- La atención de incidentes de seguridad que involucren estos componentes se realiza en coordinación con el SOC y equipos de seguridad de la DIAN.

1.1.4.3. Protección de Servidores (Hardening y Configuración Segura)

El proveedor debe realizar la gestión de seguridad de los sistemas operativos en los entornos de nube en alcance, principalmente sobre recursos IaaS y los servicios PaaS asociados, ejecutando las actividades de administración y control necesarias para garantizar la protección, estabilidad y cumplimiento normativo de los sistemas que soportan los servicios desplegados.

Esto incluye la gestión integral de parches y actualizaciones de seguridad mediante procedimientos automatizados y controlados para evaluar, probar y desplegar correcciones críticas y mitigaciones frente a vulnerabilidades, minimizando el riesgo sobre la operación. Así mismo, contempla el hardening de la infraestructura de aplicaciones, bases de datos y almacenamiento en nube, manteniendo expuestos únicamente los puertos y servicios necesarios para su funcionamiento adecuado.

A. Actividades fuera del alcance:

- Servicios avanzados de seguridad: pentesting/ethical hacking, análisis forense, gestión integral de vulnerabilidades. (DIAN / servicios especializados)
- Herramientas de seguridad no nativas: configuración de CSPM, XDR u otras plataformas de fabricantes como Trend Micro cuando su operación esté a cargo de terceros. (Terceros / otros servicios)

- Seguridad fuera del ámbito cloud gestionado: hardening a nivel de código, guías o frameworks de seguridad propios, sistemas legacy no soportados, sistemas on-premises no conectados y dispositivos de usuario final. (DIAN)

B. Condiciones del servicio

- Aplica a servidores, sistemas operativos y servicios IaaS/PaaS en nube dentro del alcance del servicio e inventariados.
- Los ciclos de parcheo siguen ventanas de mantenimiento y gestión de cambios definidos por la DIAN.
- Los estándares de hardening y configuración segura se basan en lineamientos de la DIAN y de fabricantes; el proveedor los aplica y mantiene.
- Se deben mantener procedimientos documentados para parchado, hardening, validación de cumplimiento y corrección de desviaciones.

1.1.4.4. Gestión de seguridad y cumplimiento multinube

A. Objetivo

Garantizar que las nubes en alcance mantengan una postura de seguridad adecuada, aplicando y vigilando las configuraciones y controles definidos por la DIAN, analizando y gestionando las vulnerabilidades, usando las herramientas nativas de seguridad (Microsoft Defender for Cloud, Azure Policy, AWS Security Hub, AWS Config, etc.), avaladas por el grupo de seguridad de la Subdirección de Infraestructura Tecnológica y de Operaciones de la DIAN, alineándose con los lineamientos de la OSI y marcos de referencia (ISO 27001, ISO/IEC 27017, entre otras NIST, CIS).

B. Excluye

- Definición o aprobación de políticas de seguridad institucional, gobierno de datos o marcos de referencia. (DIAN)
- Operación del SIEM, SOC y análisis avanzado de seguridad (correlación de eventos, casos de uso, hunting, forense, etc.). (DIAN / terceros)

C. Condiciones del servicio

- Aplica a las suscripciones, cuentas y recursos de nube en alcance que estén bajo administración del proveedor y hagan parte del inventario de activos gestionados en nube definido para este servicio.
- La DIAN define las políticas y criterios de cumplimiento; el proveedor las aplica, monitorea y evidencia en los entornos de nube administrados.
- Los hallazgos críticos se gestionan mediante la herramienta ITSM y en coordinación con la OSI cuando corresponda.

- Los cambios de configuración de seguridad en ambientes productivos deben tramitarse a través del proceso de Gestión de Cambios definido por la DIAN.

1.1.5. Gobierno y Gestión del Servicio

1.1.5.1. Arquitectura de la Multinube (Servicio base – operación continua)

A. Objetivo del servicio

Asegurar que los servicios y plataformas en nube cubiertos por el servicio se implementen y operen de acuerdo con la arquitectura de referencia y las políticas definidas por el equipo de arquitectura de la DIAN, garantizando coherencia técnica, seguridad, desempeño y control de costos en su evolución.

B. Alcance

Se centra en el gobierno arquitectural operativo de la multinube dentro del servicio.
El proveedor no define la arquitectura corporativa, sino que aplica los lineamientos y estándares emitidos por el equipo de arquitectura de la DIAN (SITO-SDD-SPD), revisa el alineamiento de los despliegues y documenta la arquitectura efectiva de los servicios administrados, incluyendo los diagramas de despliegue en nube a nivel de infraestructura.

C. Excluye

- Definición de la arquitectura de referencia corporativa de la DIAN y de las políticas de arquitectura, seguridad, datos o integración; estas son responsabilidad exclusiva del equipo de arquitectura de la DIAN.
- Diseño detallado de arquitecturas de aplicaciones de negocio específicas (modelo de datos, capas funcionales, UX, lógica de negocio), que corresponde a los proyectos y/o fábricas de software de la DIAN u otros servicios.

D. Condiciones del servicio

- El equipo de arquitectura de la DIAN (SITO-SDD-SPD) entregará al proveedor los lineamientos, artefactos de arquitectura de referencia y políticas vigentes, y notificará los cambios estructurales que los afecten.
- Las recomendaciones que impliquen cambios significativos de arquitectura (nuevos dominios, cambios relevantes de segmentación, adopción de tecnologías clave, modificación de patrones transversales) deberán ser validadas por el equipo de arquitectura de la DIAN (SITO-SDD-SPD) antes de su implementación.

- La documentación de arquitectura de nube y los diagramas de despliegue relacionados con el servicio deberán mantenerse versionados, actualizados y disponibles en los repositorios y herramientas que la DIAN defina, siguiendo las convenciones de documentación institucional.
- Los equipos de proyectos y/o fábricas de software deberán suministrar al proveedor la información técnica mínima necesaria (recursos utilizados, topología, dependencias, ambientes) para la elaboración y actualización de los diagramas de despliegue.
- Las decisiones arquitecturales con impacto relevante en costos, seguridad, continuidad o cumplimiento se tratarán en los comités de gobierno que la DIAN disponga; el proveedor actúa como soporte técnico y no como instancia de decisión.

1.1.5.2. Procedimientos de gestión y operación

El proveedor debe seguir los procedimientos de gestión y operación de la Multinube y mantenerlos actualizados, como mínimo: gestión de incidentes, gestión de problemas, gestión de cambios, gestión de activos y configuraciones, gestión de conocimiento, gestión de DevOps/DataOps, gestión de despliegues, gestión de gobernanza, pruebas y validación de servicio, observabilidad, centro de operaciones de red y monitoreo, enlaces de comunicaciones a nube, gestión de eventos, gestión de solicitudes, gestión de incidentes de seguridad, gestión de niveles de servicio, gestión y operaciones de la nube, continuidad del servicio, plan de disponibilidad, acceso a recursos, aprovisionamiento de recursos. Adicionalmente, debe mantener actualizadas las fichas de los procedimientos con las actividades, responsabilidades, entradas y salidas y realizar la medición de indicadores de gestión y tableros de control. Lo anterior debe estar alineado con las políticas de seguridad de la información, las políticas de gobierno y calidad de datos de la entidad y las políticas de protección de datos personales, de gobierno digital y demás políticas y regulaciones colombianas en la materia.

A. Actividades fuera del alcance

- Diseño, creación o modificación de las políticas de seguridad de la información, las políticas de gobierno y calidad de datos, las políticas de protección de datos personales, de gobierno digital y demás políticas y regulaciones colombianas.

1.1.5.3. Optimización de costos de nube (Servicio base – operación continua)

A. Objetivo del servicio

Realizar la gestión operativa de costos y consumo de nube de los servicios cubiertos por el servicio, aplicando prácticas básicas de optimización inspiradas en FinOps para dar visibilidad, control y recomendaciones a la DIAN..

B. Alcance del servicio

Incluye el seguimiento periódico de consumo y costos, la generación de reportes y la identificación de oportunidades de optimización que puedan ejecutarse dentro de la operación normal del servicio.

- Detectar y proponer la optimización del uso de recursos (Right-sizing) para Ajuste de tamaño, eliminación de recursos huérfanos y apagado programado si es posible.
- Evaluar y sugerir modelos de contratación y descuentos en torno a planes de ahorro y reservas e instancias Spot.
- Revisar el almacenamiento y transferencia de datos configurados respecto los ciclos de vida del almacenamiento y el control de transferencia (Egress)
- Informar alertas de presupuesto y autoescalado de infraestructura.
- creación de tableros y alertas

Todo esto enmarcado en un informe periódico, para que la Entidad defina las acciones de mejora.

C. Excluye

- Diseño e implementación de proyectos de consultoría financiera, diseño de un marco FinOps institucional ni decisiones presupuestales o contractuales de la DIAN.
- Creación y operación de una oficina FinOps o equipo dedicado exclusivamente a costos de TI de toda la Entidad.
- Adquisición e implementación de herramientas especializadas de terceros para FinOps no incluidas en el servicio base.

D. Condiciones del servicio

- La calidad del análisis dependerá de la información disponible (consumo, facturación, tags) y del cumplimiento de las políticas de etiquetado acordadas.
- Cualquier cambio en configuraciones de recursos para optimización (apagado, redimensionamiento, cambio de SKU) se realizará solo con aprobación de la DIAN, siguiendo los procesos de gestión de cambios.

1.1.5.4. Gestión de niveles de servicio

Son las actividades para supervisar la calidad de los servicios de nube ofrecidos con respecto a los niveles de servicio requeridos por la entidad y debe tener en cuenta la forma de entrega y las especificaciones relacionadas (fuente de información, formato de entrega, medio de entrega, tiempo de respuesta, horarios de servicio, etc.). El proveedor deberá entregar el cálculo de los niveles de servicio y, en conjunto con la interventoría y la supervisión, establecerá la compensación que debe aplicarse por el incumplimiento del que pudiera haber sido objeto, de forma que esta compensación se asuma por el proveedor de servicios administrados de nube en la facturación correspondiente.

A. Actividades fuera del alcance

- Definición unilateral o modificación de los niveles de servicio (ANS) sin acuerdo escrito entre las partes.
- Responsabilidad y compensaciones por el incumplimiento de los ANS causado por factores fuera del control del proveedor como:
    - Fallas en infraestructura o servicios no gestionados por el proveedor
    - Problemas en la red o conectividad externos al entorno gestionado
    - Interrupciones por parte de los proveedores de servicios de nube no atribuibles a la gestión propia del proveedor
    - Cambios no coordinados realizados por DIAN o terceros
    - Eventos de fuerza mayor o caso fortuito
    - Mantenimientos programados y aprobados
    - Fallas de los servicios de los proveedores de servicios de nube.
- Penalizaciones acumulativas por un mismo incidente que afecte a múltiples servicios o métricas.
- Compensaciones que excedan el 10% del valor mensual de los servicios base afectados.
- Aplicación de penalizaciones durante el período de estabilización inicial de 3 meses.
- Compensaciones por incidentes en los que DIAN no haya seguido los procedimientos acordados o recomendaciones del proveedor.
- Aplicación retroactiva de nuevos ANS o cambios en la medición.
- Compensaciones por eventos donde DIAN no pueda demostrar un impacto real en sus operaciones.
- Cálculo o definición de compensaciones basadas en criterios subjetivos o no especificados explícitamente en el servicio.
- Descuentos por incumplimiento de los niveles de servicio por parte de los proveedores de nube.

1.1.5.5. Gestión y operación de Landing Zones

La gestión y operación de Landing Zones comprende las actividades necesarias para mantener, operar y evolucionar las zonas de aterrizaje establecidas en las nubes públicas de la DIAN, asegurando que cumplan con los estándares de estabilidad, seguridad, cumplimiento normativo, trazabilidad, gobernanza y alineación con los lineamientos técnicos y de arquitectura definidos por la Entidad.

Este servicio se enfoca en la operación técnica y continua del modelo de Landing Zone ya definido por la DIAN, utilizando de forma prioritaria las capacidades nativas de Azure y AWS (por ejemplo: Azure Management Groups, suscripciones, Azure Policy, blueprints/CAF Landing Zones, AWS Organizations, cuentas, AWS Control Tower, AWS Config y servicios equivalentes) y evitando la adquisición de plataformas adicionales que solo repliquen estas funcionalidades.

A. Actividades fuera del alcance

- Administración funcional de herramientas externas de gobierno, seguridad o monitoreo no integradas a la arquitectura actual; el proveedor solo soportará su integración técnica cuando sea requerido por la DIAN y se encuentre dentro del alcance del servicio.
- La adquisición y licenciamiento de plataformas de terceros cuya única finalidad sea gestionar estructuras de cuentas, suscripciones, políticas o controles que ya puedan definirse mediante capacidades nativas de Azure y AWS, salvo aprobación explícita de la DIAN y cotización independiente como servicio adicional.

B. Condiciones del servicio

- Los cambios significativos en estructura, segmentación o configuración base de una Landing Zone deberán gestionarse mediante el proceso formal de gestión de cambios y con la correspondiente actualización de la documentación asociada.
- La DIAN mantendrá el control de los accesos privilegiados a nivel de directorio e identidad corporativa on-premise; el proveedor gestionará únicamente los permisos sobre recursos de nube dentro del alcance de las Landing Zones, conforme a los lineamientos de identidad y acceso definidos por la DIAN.
- Se realizará, como mínimo, una reunión técnica mensual para revisar:
    - El estado y la evolución de las Landing Zones.
    - Incidentes relevantes y desviaciones de políticas.
    - El avance de los planes de acción y mejoras aprobadas.

1.1.5.6. Gobernanza, riesgo y cumplimiento

El proveedor debe proponer el conjunto de políticas, reglas o marcos que se utilizan para alcanzar los objetivos planteados en el servicio, gestionar los riesgos, incluidos los financieros, legales, estratégicos y de seguridad y asegurar el cumplimiento de las reglas, las leyes y las regulaciones incluyendo las políticas corporativas internas y los requisitos legales y regulatorios establecidos por los organismos externos que aplican a la entidad.

A. Actividades fuera del alcance

- Desarrollo de marcos de gobierno corporativo globales.
- Gestión de cumplimiento normativo corporativo fuera del alcance de la infraestructura en la nube.
- Gestión de riesgos empresariales fuera del alcance de la infraestructura y servicios de nube.
- Gestión de relaciones con proveedores que no estén directamente relacionados con la infraestructura o servicios de nube.
- Gestión de riesgos legales o financieros fuera del ámbito de la infraestructura en la nube.
- Gestión de compliance o auditorías internas fuera del alcance de la infraestructura tecnológica.

iii. SERVICIOS ADICIONALES

1.1.1. Gestión de conectividad y enlaces de datos

Garantizar la conectividad privada, segura y de alto desempeño entre los centros de datos de la DIAN y las nubes pública primaria y secundaria (Azure y AWS), mediante la gestión integral, monitoreo y soporte de los enlaces dedicados, servicios nativos de conectividad, alta disponibilidad y recuperación ante desastres, conforme a las políticas técnicas y de seguridad establecidas por la entidad.

A. Actividades comprendidas dentro del alcance

- Contratación, administración y pago de los enlaces de datos dedicados requeridos para la conectividad entre los centros de datos de la DIAN y las nubes primaria y secundaria (Azure ExpressRoute y AWS Direct Connect), actualmente provistos a través de carriers como Megaport e Internexa.
- Aprovisionamiento, configuración, monitoreo y mantenimiento operativo de dichos enlaces, garantizando la disponibilidad, redundancia y rendimiento definidos por la DIAN.
- Gestión técnica y operativa con los proveedores de telecomunicaciones para la instalación, mantenimiento o resolución de incidentes que involucren tramos físicos o peering con las nubes.
- Monitoreo continuo (24x7x365) de disponibilidad, latencia, jitter, pérdida de paquetes y utilización del ancho de banda de los enlaces.
- Gestión de configuraciones nativas de conectividad en la nube (failover, redundancia, resiliencia y gateways).
- Documentación técnica actualizada de topologías, configuraciones y cambios realizados en la conectividad multinube. Participación en pruebas de continuidad o DRP que involucren los mecanismos de failover o replicación de red.

B. Actividades fuera del alcance

- Pago o contratación de nuevos enlaces no contemplados en el alcance contractual o no autorizados por la DIAN.
- Diseño, adquisición o mantenimiento de infraestructura física de red (routers, switches, firewalls u otros equipos) en los centros de datos de la DIAN.
- Gestión o soporte de servicios de telecomunicaciones subyacentes (MPLS, SD-WAN, etc.) fuera del alcance de los enlaces dedicados.
- Optimización de ancho de banda o QoS dentro de la red interna de la DIAN.
- Implementación o gestión de soluciones de balanceo no nativas de la nube.
- Soporte a nivel de conectividad de aplicación.

C. Condiciones del servicio

- Los costos de los enlaces dedicados (ExpressRoute y Direct Connect) serán asumidos por el proveedor y deberán estar incluidos en la propuesta económica del servicio adicional en caso de contratarse.
- El proveedor deberá mantener los enlaces activos, operativos y con un SLA mínimo del 99,5 % de disponibilidad mensual.
- Toda modificación, ampliación o sustitución de enlaces deberá contar con autorización previa de la DIAN.
- Se deberán generar reportes mensuales de desempeño y disponibilidad con evidencia de monitoreo, gestión proactiva e incidentes atendidos.
- El proveedor deberá garantizar trazabilidad completa de las contrataciones, incidentes y mantenimientos realizados sobre los enlaces.
- Los servicios deberán mantenerse operativos durante mantenimientos o cambios de carrier, asegurando continuidad mediante configuraciones redundantes.

1.1.2. Centro de operaciones de nube (NOC)

A. Objetivo

Operar un Centro de Operaciones de Nube (NOC) 24x7x365 en instalaciones del proveedor, encargado de la vigilancia, atención y coordinación de eventos e incidentes de la infraestructura y servicios de nube, usando las herramientas de monitoreo, observabilidad (incluyendo APM) e ITSM definidas por la DIAN, y apoyándose, cuando la Entidad lo contrate, en la Plataforma de correlación y analítica avanzada de eventos de nube (AIOps), para mantener la estabilidad y disponibilidad de los servicios multinube.

El NOC se enfoca en operación y coordinación técnica, articulado con Monitoreo y observabilidad, Administración de infraestructura, Soporte DevOps, mesa de servicio, OSI/DevSecOps y soportes de fabricante.

B. Actividades comprendidas dentro del alcance:

- Operación 24x7x365 del NOC para monitoreo y atención de alertas e incidentes de infraestructura y plataformas en nube.
- Recepción, verificación, clasificación y registro en ITSM de eventos y alertas provenientes de las herramientas de monitoreo/observabilidad (incluyendo APM) y de la mesa de servicio.
- Gestión de incidentes técnicos: análisis inicial, priorización y escalamiento según matriz de responsabilidades (infra, DevOps, aplicaciones).
- Ejecución de runbooks operativos autorizados (reinicios controlados, conmutación a componentes redundantes, acciones básicas de mitigación), coordinando con Administración de infraestructura y Gestión de cambios cuando aplique.
- Uso operativo de dashboards, métricas, logs y trazas definidos en el servicio de Monitoreo y observabilidad para el diagnóstico inicial y la clasificación de incidentes.

- Correlación básica y análisis proactivo de eventos, utilizando las capacidades estándar de las herramientas de monitoreo/observabilidad de la DIAN para identificar patrones y recurrencias y proponer acciones preventivas. La correlación avanzada, reducción de ruido de alertas, priorización inteligente y analítica AIOps se realizará mediante el Servicio adicional: Plataforma de correlación y analítica avanzada de eventos de nube (AIOps), cuando la DIAN lo contrate.
- Mantenimiento de dashboards operativos de estado (incidentes activos, alertas críticas, disponibilidad) y reportes periódicos de estado operativo (por ejemplo, diarios y consolidados).
- Análisis de tendencias e insumos para Gestión de problemas, así como la coordinación de la resolución de incidentes y escalamiento a soportes de fabricante (apertura, seguimiento y cierre técnico de casos).

C. Excluye

- Configuración, administración e instrumentación de herramientas de monitoreo, observabilidad y APM, así como de la plataforma AIOps, que se realiza en los servicios de Monitoreo y observabilidad y Plataforma de correlación y analítica avanzada de eventos de nube (AIOps).
- Operación de SOC, correlación de eventos de seguridad institucional y respuesta a incidentes de seguridad (responsabilidad de la OSI y servicios de seguridad).
- Gestión de NSG, firewalls y componentes de red, cubierta en Gestión de redes / Administración de infraestructura.
- Soporte funcional de aplicaciones de negocio, soporte a usuarios finales y operación de la mesa de servicio de primer nivel.
- Gestión de infraestructura on-premise fuera del alcance del servicio y monitoreo de sistemas o aplicaciones no migradas a nube.
- Diagnóstico o solución de errores de aplicación a nivel de código o lógica de negocio, más allá de la identificación y escalamiento al equipo de aplicación.

D. Condiciones del servicio

- El NOC usará la plataforma ITSM corporativa para registrar, seguir y cerrar eventos/incidentes, conforme a los procesos de Gestión de incidentes, problemas y cambios de la DIAN.
- Deberá estar integrado con las herramientas de monitoreo y observabilidad que la DIAN disponga (nativas de nube y/o corporativas, incluyendo APM).
- La adquisición y operación de la Plataforma de correlación y analítica avanzada de eventos de nube (AIOps) se realizará como servicio adicional. Cuando la DIAN la contrate, el NOC deberá:
    - Usar la plataforma AIOps como fuente principal para correlación avanzada, reducción de ruido y priorización de alertas.

- Gestionar y hacer seguimiento a los tickets generados/actualizados automáticamente en ITSM por la plataforma AIOps.
- El NOC se coordinará con la OSI y el equipo DevSecOps cuando se identifiquen posibles implicaciones de seguridad.

iv. SERVICIOS POR DEMANDA (ACTIVABLES SEGÚN NECESIDAD)

Los servicios por demanda complementan la operación base y se activan a solicitud de la DIAN mediante orden de trabajo, previa validación técnica y económica:

1.1.1. Respuesta a incidentes de seguridad y análisis forense (DFIR / Threat Hunting)

A. Objetivo

Atender requerimientos puntuales de **respuesta especializada** ante incidentes de ciberseguridad en entornos multinube, mediante actividades de contención, análisis técnico, recolección/preservación de evidencias, análisis de causa raíz y definición de plan de remediación, bajo orden de servicio aprobada por la DIAN.

B. Actividades comprendidas dentro del alcance

- Activación de célula DFIR y coordinación con las áreas de seguridad de la DIAN (p. ej., OSI/CSIRT) y equipos técnicos de nube cuando aplique y siguiendo el procedimiento de incidentes y protocolos de crisis definidos en la DIAN.
- Recolección y preservación de evidencias según lineamientos definidos por la DIAN (logs, *snapshots*, artefactos, registros de auditoría, configuraciones relevantes).
- Análisis técnico del incidente: línea de tiempo, vector de ataque, alcance, activos impactados, indicadores de compromiso (IoC) y evaluación de impacto.
- Recomendaciones y ejecución controlada (previa autorización) de acciones de contención/erradicación: aislamiento, bloqueo, hardening puntual, revocación/rotación de credenciales, entre otros, garantizando un trabajo alineado y conjunto con el modelo operativo definido en el servicio gestionado del SOC.
- Informe preliminar y reporte final con hallazgos, causa raíz, acciones ejecutadas y plan de remediación priorizado.
- Acompañamiento y remediación, según corresponda, en mesas técnicas conjuntas con DIAN y cualquier otro proveedor involucrado, durante el manejo del incidente (war room) según severidad y criticidad.

C. Excluye

- Cambios evolutivos mayores, rediseños de arquitectura o modernizaciones de gran alcance posteriores al incidente (se tratan como proyectos/servicios por demanda).
- Desarrollo o refactorización de código de aplicaciones.

D. Condiciones del servicio

- Se ejecuta únicamente mediante orden de servicio aprobada por la DIAN, con alcance, severidad, recursos objetivo, canales de coordinación y responsables definidos.
- Requiere accesos, permisos y habilitaciones necesarias para recolección de evidencias y análisis (conforme a políticas de la DIAN).
- La preservación de evidencias y cadena de custodia se realizará según el procedimiento que defina la DIAN.
- Las acciones de contención/erradicación se ejecutan solo con autorización expresa de la DIAN y bajo control de cambios cuando aplique.

1.1.2. Transición del Servicio

La transición de los Servicios Administrados de Nube es una fase crítica que requiere un enfoque metódico y altamente especializado para garantizar la continuidad operativa y minimizar impactos en el servicio. El proveedor deberá llevar a cabo una fase de transición que cumpla con al menos los siguientes requisitos:

A. Metodología y Organización

- Aplicación de una metodología estructurada de transición específica para entornos multinube críticos.
- Equipo dedicado exclusivamente a la transición, separado del equipo de operación regular, con roles claramente diferenciados.
- Modelo de gobernanza que incluya comités de seguimiento a tres niveles: estratégico, táctico y operativo.
- Experiencia previa en transiciones de complejidad similar en entornos con requisitos de disponibilidad comparables a los de DIAN.

B. Actividades comprendidas dentro del alcance

- Elaboración de un plan detallado de transición con cronograma, recursos, riesgos y estrategias de mitigación, sujeto a aprobación por parte de DIAN.
- Ejecución de la transición por fases o componentes tecnológicos, priorizando la estabilidad operativa sobre la velocidad de implementación.
- Documentación exhaustiva del estado actual de la infraestructura y servicios de las nubes gestionadas, incluyendo recomendaciones y planes de mejoramiento de las arquitecturas actuales, utilizando artefactos y formatos estandarizados.

- Transferencia de conocimiento bidireccional sobre los aspectos particulares de las configuraciones implementadas en las nubes gestionadas, con evaluación formal de efectividad.
- Implementación de un modelo de operación paralela durante un período de hasta 45 días para servicios críticos, con matriz RACI detallada que defina responsabilidades específicas durante el período de coexistencia.
- Validación conjunta de procedimientos operativos y protocolos de respuesta a incidentes con simulacros documentados.
- Configuración y calibración de herramientas de gestión y monitoreo según los parámetros actuales de operación, con evidencia de pruebas y aceptación.
- Ejecución de hasta 3 simulacros de continuidad para componentes críticos identificados por DIAN, con medición de RTO y RPO reales.
- Establecimiento de un "war room" virtual permanente durante la fase crítica de transición con presencia obligatoria de especialistas de todas las áreas involucradas.

C. Actividades fuera del alcance

- Rediseño o modificación de la arquitectura durante la fase de transición, salvo acuerdo explícito entre las partes.
- Migración de datos o aplicaciones entre nubes o entornos no contemplados en el alcance original.
- Integración con sistemas o herramientas no incluidos en el inventario oficial proporcionado por DIAN.

D. Consideraciones Adicionales

- El proveedor deberá asignar recursos exclusivos para la transición, sin afectar la operación regular de la infraestructura de DIAN.
- El equipo de transición deberá contar con experiencia específica en servicios similares y entornos multinube.
- El plan de transición debe incluir un modelo de gestión del cambio organizacional para minimizar el impacto en los usuarios y equipos técnicos de DIAN.
- Se deberá presentar una matriz de dependencias y prerrequisitos con puntos de control y criterios de éxito medibles para cada fase de la transición.
- El proveedor deberá incluir una estrategia documentada de "*rollback*" para cada componente crítico en caso de problemas no resueltos durante la transición.
- Todos los costos asociados a la fase de transición deberán estar incluidos en este servicio de la oferta económica presentada para los Servicios Administrados de Nube.

1.1.3. Administración avanzada de bases de datos en nube

A. Objetivo

Prestar servicios especializados bajo demanda para actividades avanzadas de administración de bases de datos en nube que van más allá de la operación continua: *tuning* de rendimiento, migraciones técnicas, cargas históricas y configuraciones avanzadas, en servicios gestionados (PaaS/DBaaS) y en motores sobre IaaS (VM).

B. Alcance

Aplica a bases de datos en nube dentro del servicio, incluyendo, entre otras: Azure SQL, Azure SQL MI, AWS RDS (SQL Server, Oracle, PostgreSQL, MySQL), Cosmos DB, MongoDB gestionado, Redis gestionado, DynamoDB y motores en IaaS como PostgreSQL, MySQL, MongoDB, Redis, SQL Server y Oracle, cuando la DIAN los incluya explícitamente.

C. Actividades comprendidas dentro del alcance

- Tuning avanzado de rendimiento: análisis de planes de ejecución, recomendaciones de particionamiento y parámetros avanzados del motor, apoyo a pruebas de carga.
- Ajustes técnicos de esquema orientados a performance, conservando el modelo de datos funcional definido por la DIAN (particionamiento de tablas grandes, cambios estructurales menores).
- Migraciones técnicas de bases de datos entre instancias IaaS, entre IaaS y PaaS/DBaaS o entre servicios gestionados, cuando el modelo destino ya esté definido.
- Ejecución técnica de cargas históricas o masivas, según reglas definidas por la DIAN (jobs, scripts, monitoreo y validaciones técnicas básicas).
- Instalación y configuración técnica de motores en IaaS (PostgreSQL, MySQL, MongoDB, Redis, SQL Server, Oracle, etc.).
- Soporte técnico especializado para problemas de performance que requieran ajustes profundos

D. Excluye

- Proyectos de transformación/modernización de bases de datos que impliquen rediseño profundo de modelos o cambio de motor a nivel funcional.
- Actividades rutinarias ya cubiertas por el servicio de Administración de bases de datos y almacenamiento en nube (monitoreo diario, parches, backups básicos, gestión estándar de capacidad).

E. Condiciones y cobro

- Servicio prestado exclusivamente por demanda, con precio unitario por hora de especialista según anexo económico.
- Cada solicitud se formaliza mediante orden de servicio, con objetivo, alcance, ambientes y tope máximo de horas aprobado por la DIAN.
- El proveedor registra actividades y horas efectivas, no puede superar el tope sin autorización previa y solo factura las horas validadas por la DIAN.

- Para instancias de SQL Server y Oracle, las actividades se coordinan siempre con el grupo de bases de datos de la DIAN (SITO).

1.1.4. Consultoría integral en DevSecOps

A. Objetivo

Brindar asesoría especializada en DevSecOps a la OSI, al equipo DevSecOps y a otros equipos de la DIAN, en todos los temas relacionados con seguridad, calidad y operación del ciclo de vida de desarrollo, integración, despliegue y operación de soluciones tecnológicas, cuando la Entidad requiera apoyo adicional al equipo interno.

B. Actividades comprendidas dentro del alcance

Se contrata solo cuando la DIAN lo solicite e incluye, por ejemplo:

- Acompañamiento en el diseño o ajuste de lineamientos y modelos DevSecOps (código, repositorios, pipelines CI/CD, artefactos, IaC, observabilidad y gestión de incidentes desde la perspectiva DevOps).
- Asesoría en mejores prácticas de DevOps/DevSecOps: automatización, trazabilidad, control de cambios, seguridad en el ciclo de vida, gestión de secretos, gestión de configuraciones, gestión de dependencias e imágenes.
- Soporte en la definición de gobierno DevSecOps (roles, flujos de aprobación, criterios de cumplimiento, integración con procesos de desarrollo, pruebas, cambios y seguridad).
- Evaluación técnica de nuevas capacidades o herramientas relacionadas con DevOps/DevSecOps (SAST/DAST/SCA, gestión de artefactos, firmas, escáneres de IaC, observabilidad, etc.) sobre el stack existente.

C. Excluye

- La operación diaria de herramientas y pipelines CI/CD (cubierta por el servicio base de Soporte DevOps).
- La ejecución de cambios técnicos recurrentes en herramientas/pipelines (este servicio está incluidoen los servicios base).
- Las responsabilidades propias de la OSI y del equipo DevSecOps como dueños de políticas, decisiones de riesgo y aprobación de lineamientos.
- Servicios de SOC o monitoreo de seguridad 24x7.

D. Condiciones

- Cada intervención se definirá caso a caso (alcance, temas a tratar, horas, entregables) según solicitud expresa de la DIAN.

- No podrá utilizarse para re-etiquetar tareas operativas recurrentes que ya estén cubiertas por los servicios base de operación de nube, administración de infraestructura o Soporte DevOps.

1.1.5. Estudios y consultoría en Arquitectura de la Multinube

A. Objetivo

Brindar a la DIAN apoyo especializado en arquitectura de la multinube para proyectos o decisiones estratégicas y excepcionales (modernizaciones grandes, cambios estructurales, nuevas estrategias tecnológicas), siempre bajo los lineamientos del equipo de arquitectura de la DIAN.

B. Alcance

Se contrata por orden de servicio y aplica solo cuando la DIAN requiera estudios o rediseños de carácter estructural, que van más allá del gobierno arquitectural operativo cubierto por el servicio base.

C. Actividades comprendidas dentro del alcance

Según cada orden de servicio, podrá abarcar, por ejemplo:

- Rediseños mayores de la arquitectura de la multinube aplicada al servicio (nuevos modelos de segmentación, seguridad, integración o despliegue a nivel global del servicio).
- Estudios de arquitectura para proyectos estratégicos o modernizaciones masivas (consolidación de plataformas, nuevas zonas o dominios arquitecturales, cambios de tecnología base en un dominio completo).
- Evaluación comparativa de alternativas de arquitectura para decisiones tecnológicas de alto impacto (nuevas tecnologías core, nuevos proveedores, nuevos patrones estándar).
- Diseño y acompañamiento de pilotos/POC estratégicos cuyo resultado se use para definir estándares de arquitectura para varios sistemas o dominios.

D. Excluye

- Todas las actividades de arquitectura de operación continua que ya están definidas en el servicio base.
- La definición de la arquitectura de referencia institucional y políticas de arquitectura, que es responsabilidad del equipo de arquitectura de la DIAN.

E. Condiciones del servicio

- Cada intervención debe formalizarse mediante orden de servicio con alcance, objetivos y entregables definidos.
- Toda recomendación que implique cambios estructurales deberá ser analizada y aprobada por el equipo de arquitectura de la DIAN antes de volverse estándar o aplicarse al servicio.

1.1.6. Consultoría y proyectos FinOps para optimización avanzada de costos de nube

A. Objetivo

Prestar a la DIAN servicios especializados de consultoría y proyectos FinOps para el diseño e implementación de prácticas avanzadas de gestión de costos de nube y la ejecución de iniciativas de optimización profunda sobre dominios, plataformas o servicios específicos.

B. Alcance del servicio

Se activa por demanda y previa orden de servicio. Cubre actividades de análisis avanzado, diseño y acompañamiento que van más allá de la gestión operativa de costos incluida en el servicio base de optimización de costos de nube, e incluye tanto el marco FinOps institucional como proyectos de optimización para cargas de trabajo concretas.

C. Actividades comprendidas dentro del alcance

De acuerdo con cada orden de servicio, podrá contemplar, entre otros:

- Definición o ajuste del marco FinOps corporativo de la DIAN: roles, procesos, niveles de madurez, modelo de gobierno y relacionamiento entre áreas técnicas, financieras y de contratación.
- Diseño del modelo de gobierno de costos de nube: políticas de uso, lineamientos de etiquetado extendidos, esquemas de showback/chargeback y mecanismos de revisión y decisión sobre costos.
- Proyectos avanzados de optimización de costos para dominios o plataformas específicas: análisis detallado de consumo, cuantificación de oportunidades de ahorro, definición de planes de optimización y acompañamiento en su implementación.
- Apoyo técnico a negociaciones relevantes con proveedores de nube, aportando escenarios de consumo, alternativas técnicas y análisis de impacto económico.
- Diseño y/o configuración de tableros y reportes FinOps avanzados usando herramientas nativas de nube y/o soluciones corporativas que defina la DIAN.
- Talleres y jornadas de formación FinOps para equipos técnicos, financieros y de contratación de la DIAN.

D. Excluye

- La gestión operativa recurrente de costos de nube (reportes mensuales, monitoreo básico y recomendaciones de bajo esfuerzo), que está cubierta por el servicio base de optimización de costos.
- La adquisición e implementación de herramientas de terceros para FinOps no contempladas en el servicio base, que deberán definirse y contratarse explícitamente si la DIAN lo requiere.

E. Condiciones del servicio

- Cada intervención requerirá una orden de servicio con alcance, objetivos, entregables y duración definidos.
- La DIAN debe garantizar el acceso a la información de consumo y facturación, y la participación de los actores clave (tecnología, finanzas, contratación).
- Las recomendaciones que impliquen cambios técnicos o contractuales deberán ser revisadas y aprobadas por la DIAN, siguiendo sus procesos de gestión de cambios y de contratación.

1.1.7. Gestión de Continuidad y Recuperación (Exclusivamente DRP Disaster Recovery Plan)

La gestión del Plan de Recuperación ante Desastres comprende las actividades necesarias para mantener, probar y ejecutar cuando sea necesario los procedimientos de recuperación que garanticen la continuidad de los servicios críticos ante eventos disruptivos.

A. Actividades comprendidas dentro del alcance

- Mantenimiento y actualización de la infraestructura de nube dedicada a la recuperación ante desastres, según la arquitectura actual documentada.
- Implementación y configuración de los mecanismos de replicación entre la nube primaria y secundaria para los servicios catalogados como críticos, con un máximo de 50 cargas de trabajo críticas.
- Configuración y mantenimiento de los mecanismos de respaldo y replicación de datos según las políticas definidas por DIAN.
- Actualización de la documentación técnica del DRP cuando se produzcan cambios en la arquitectura o configuración de los servicios cubiertos.
- Ejecución de pruebas controladas del DRP según el calendario aprobado por DIAN, con un máximo de dos (2) pruebas completas anuales y cuatro (4) pruebas parciales anuales.
- Elaboración de informes detallados tras cada prueba, incluyendo hallazgos, tiempos de recuperación logrados y recomendaciones de mejora.
- Soporte técnico en la ejecución del DRP en caso de un evento real de desastre, limitado a la infraestructura de nube gestionada.
- Monitoreo periódico del estado de los mecanismos de replicación y la integridad de los respaldos críticos para recuperación.

- Mantenimiento de los *runbooks* técnicos de recuperación para cada uno de los servicios críticos cubiertos.
- Revisión trimestral de la alineación entre los RTO (tiempo objetivo de recuperación) y RPO (punto objetivo de recuperación) definidos y la capacidad real de recuperación.

B. Actividades fuera del alcance:

- Definición de la estrategia de continuidad de negocio de DIAN.
- Determinación de RTO, RPO y clasificación de criticidad de aplicaciones y servicios.
- Desarrollo de procedimientos no técnicos como notificaciones, escalamientos y coordinación de equipos de respuesta.
- Recuperación de servicios o aplicaciones no incluidos explícitamente en el alcance del DRP.
- Desarrollo o mantenimiento del Plan de Continuidad de Negocio (BCP) más allá de los aspectos técnicos.
- Recuperación de datos no cubiertos por las políticas de respaldo o replicación acordadas.
- Análisis de impacto de negocio (BIA) o evaluaciones de riesgo organizacional.

C. Condiciones del servicio:

- Las pruebas completas del DRP se realizarán en horarios no hábiles y deberán ser planificadas con al menos 30 días de anticipación.
- Se mantendrá la infraestructura de recuperación con una capacidad del 70% respecto a la infraestructura principal para las aplicaciones críticas definidas.
- La activación del DRP en caso de evento real requerirá autorización formal del comité de crisis de DIAN.
- El alcance del DRP se limitará a los servicios y componentes explícitamente documentados en el catálogo de servicios críticos, que será revisado semestralmente.
- Cualquier modificación significativa en la estrategia o arquitectura de recuperación requerirá un proceso formal de gestión de cambios y podrá implicar costos adicionales.
- La inclusión de nuevos servicios en el alcance del DRP requerirá un proceso de *onboarding* específico y puede generar costos adicionales.
- El proveedor no será responsable por fallos en la recuperación causados por modificaciones no documentadas en aplicaciones o infraestructura realizadas por DIAN o terceros.
- Los tiempos de recuperación (RTO) se medirán exclusivamente para la capa de infraestructura, no incluyen la validación funcional de las aplicaciones.

v. CONDICIONES TRANSVERSALES DE LOS SERVICIOS DE ADMINISTRACIÓN DE NUBE (BASE, ADICIONALES Y/O POR DEMANDA)

Las siguientes condiciones aplican a todos los servicios del catálogo (Servicios Base, Servicios Opcionales y Servicios por Demanda), salvo que un servicio indique expresamente una condición específica diferente:

- **Canal oficial y trazabilidad:** Toda solicitud, incidente, problema, cambio, actividad y entrega del proveedor deberá registrarse y gestionarse mediante la herramienta ITSM definida por la DIAN. Los canales informales (correo, chat, llamadas) serán complementarios y no sustituyen el registro oficial.
- **Inicio de atención:** La atención iniciará cuando el caso esté debidamente radicado, categorizado y cuente con la información mínima requerida, así como con las aprobaciones y ventanas aplicables.
- **Habilitación de cambios:** Las actividades que impliquen cambios de configuración, seguridad, conectividad, despliegues o afectación de componentes críticos se tramitarán mediante el proceso de Habilitación de Cambios definido por la DIAN, incluyendo evaluación de impacto, plan de reversa y aprobación correspondiente.
- **Alcance por inventario:** La prestación del servicio se realizará sobre recursos y componentes incluidos en el alcance del servicio y, cuando aplique, inventariados o gestionados bajo los mecanismos definidos por la DIAN (repositorios, listas de activos, suscripciones/cuentas, clústeres, etc.).
- **Cumplimiento de lineamientos DIAN:** Todas las actividades se ejecutarán conforme a la arquitectura de referencia, lineamientos y políticas de seguridad[1] de la información, gestión de vulnerabilidades, gobierno, continuidad, operación, protección de datos, etiquetado y normatividad aplicable definidos por la DIAN. Cualquier excepción deberá gestionarse mediante el mecanismo formal de aprobación establecido por la Entidad.
- **Ventanas operativas y coordinación:** Las acciones se ejecutarán respetando ventanas de mantenimiento/operaciones definidas por la DIAN, coordinando con las áreas involucradas y minimizando el impacto sobre los servicios misionales.
- **Trazabilidad integral:** El proveedor mantendrá la trazabilidad entre incidentes, problemas, cambios, solicitudes, vulnerabilidades y entregables relacionados, garantizando evidencias y decisiones registradas en ITSM.
- **Dependencias con terceros:** Cuando la atención dependa de terceros (fabricantes, carriers, otros proveedores o áreas internas), el proveedor deberá coordinar, escalar y hacer seguimiento a requerimientos, incidentes tecnológicos o de seguridad, registrando en ITSM los números de caso, comunicaciones, evidencias, informes y aplicando acciones de contención o alternativas técnicas cuando sea posible.
- **Documentación y evidencias:** El proveedor deberá mantener documentación técnica actualizada, todo ajuste relevante deberá reflejarse en la documentación operativa

[1] Se aclara que cada vez que se haga referencia a las políticas de seguridad, debe ser bajo el SGSPI vigente.

(inventario, runbooks, diagramas, procedimientos, matrices de acceso, bitácoras de cambios) y en evidencias auditables, usando los repositorios definidos por la DIAN. También deberá atender oportunamente los requerimientos de los diferentes entes de control en coordinación con DIAN.

- **Interoperabilidad operativa:** El proveedor deberá integrarse al modelo operativo institucional definido por la DIAN (NOC institucional, ITSM, cualquier herramienta de seguridad y cualquier capacidad incluida en el SOC o SIEM, arquitectura, monitoreo y comités), manteniendo roles claros y evitando duplicidad de funciones.
- **Modelo económico y no duplicidad:** Los consumos de nube y los costos de licencias, suscripciones o soportes de terceros se manejarán conforme al modelo económico establecido en el documento. El proponente no deberá incluir costos ya cubiertos por contratos vigentes o licencias institucionales de DIAN, salvo contratación adicional explícita.
- **Servicios por demanda:** Los servicios por demanda se ejecutarán únicamente mediante orden de trabajo aprobada (alcance, entregables, perfiles/horas o unidad, fechas, hitos y aceptación de cierre), con seguimiento y cierre documentado en el mecanismo definido por la DIAN.

vi. EXCLUSIONES TRANSVERSALES DE LOS SERVICIOS DE ADMINISTRACIÓN DE NUBE (BASE, ADICIONALES Y/O POR DEMANDA)

Las siguientes exclusiones aplican de manera transversal a todos los servicios del catálogo, salvo que un servicio indique expresamente lo contrario:

- Se excluye el soporte funcional de negocio, la parametrización funcional, la definición o validación de reglas de negocio y requisitos con áreas usuarias.
- Se excluyen actividades de desarrollo, corrección o ajuste de código de aplicaciones, así como fábrica de software y mantenimiento evolutivo de aplicaciones.
- Se excluye la operación del SOC/SIEM institucional, la correlación avanzada de eventos de ciberseguridad, el threat hunting y el análisis forense, salvo que estas capacidades se contraten de forma explícita como un servicio especializado por demanda.
- Se excluye la administración u operación de infraestructura on-premise o de terceros, incluyendo hardware y plataformas fuera del perímetro multinube definido para el servicio.
- Se excluye la administración de dispositivos físicos y de infraestructura de telecomunicaciones, tales como routers, switches, firewalls, WAN, MPLS o SD-WAN, así como tramos fuera del punto de conexión con la nube, salvo lo definido en el servicio específico de conectividad y enlaces de datos cuando aplique.
- Se excluyen el licenciamiento y suscripción de herramientas de terceros, los cuales se cotizan como servicios adicionales o por demanda, o como rubros separados, conforme al modelo económico definido en el documento.
- Se excluye el monitoreo o la gestión de componentes completamente externos o no integrados al ecosistema multinube de la DIAN.

Se excluyen proyectos, rediseños integrales y evoluciones mayores, como topologías nuevas, rediseños completos o analítica avanzada no nativa, los cuales se atienden como servicios por demanda o mediante los servicios de arquitectura y gobierno, según

4. ARQUITECTURAS DE REFERENCIA

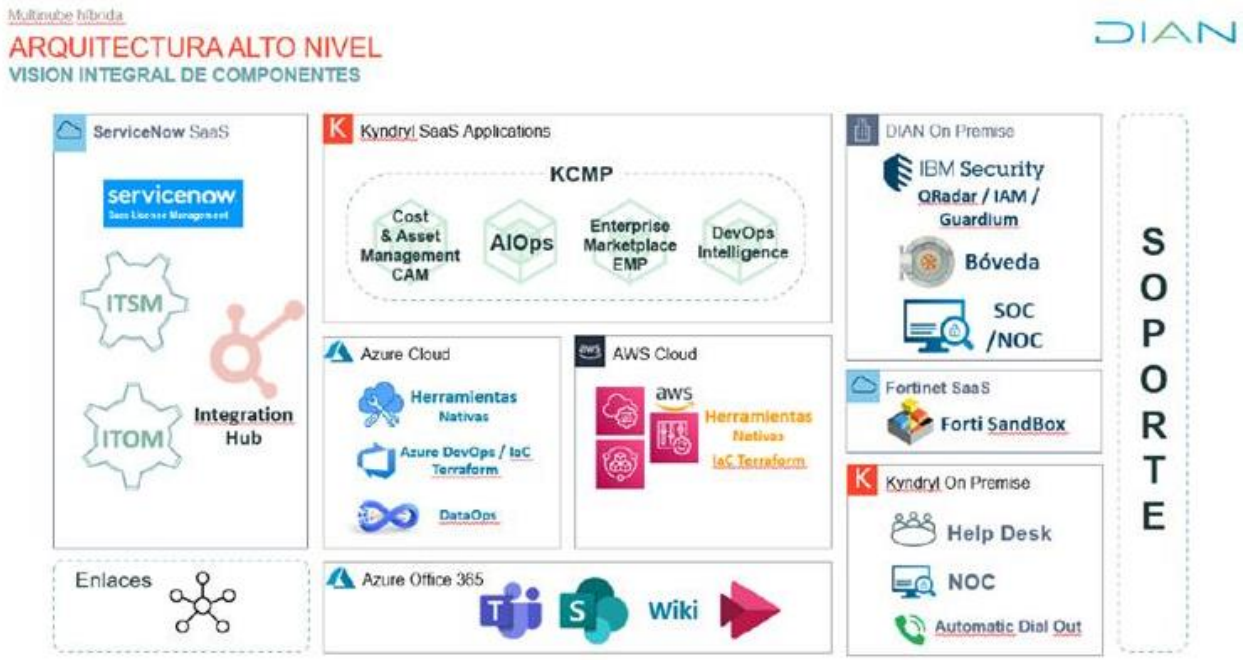


Figura 2 – Arquitectura de la Multinube DIAN. 2026.

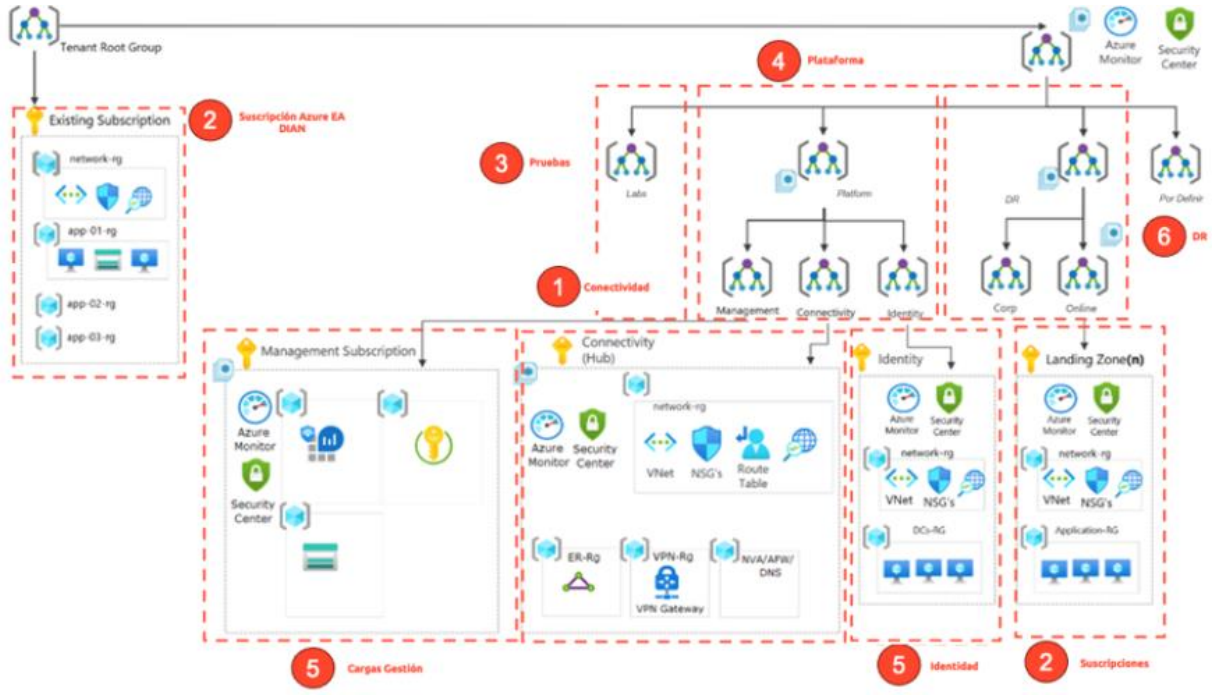


Figura 3 – Arquitectura de Referencia Azure Landing Zone. 2026.

5. STACK TECNOLÓGICO DIAN (Dic2026)

Stack tecnológico	Lenguajes de programación/Fabricante
Frontend	Angular en sus últimas versiones Visual Studio .NET, C# CSS para la gestión de estilos
Plataforma de gestión de contenidos (CMS)	WordPress como gestor de contenidos web (PHP), desplegado sobre servicios de aplicación en Azure e IAAS y bases de datos MySQL/Azure Database for MySQL
Backend	Java (spring boot, quarkus), C#
Mecanismos de integración	XROAD, API - REST, Servicios web, FTP, Stream, eventos, Apicurio Registry, Azure Logic Apps, Azure Functions, Azure Data Factory, AWS Lambda
Gestión de APIs	Azure API Management, Red Hat 3scale
Gestión de identidades y accesos	Microsoft Entra ID. Active Directory de Microsoft, Keycloak, WSO2 Identity Server, LDAP / OpenLDAP
Gestores de secretos	Azure Key Vault
Bases de datos relacionales	Oracle SqlServer (incl. Hyperscale, managed instance, dedicated SQL pool) Azure Database for MySQL/PostgreSQL flexible
Bases de datos no relacionales	CosmosDB MongoDB
Plataformas analítica	Azure Databricks, Azure Synapse Analytics, Azure Data Explorer (ADX), Power BI Embedded, Analysis Services
Almacenamiento en nube	Azure Storage (blobs, data lake, tablas, file shares) y AWS S3
Cache distribuido	Azure Redis Cache, Infinispan / Red Hat Data Grid
Centros de datos	On-premises Nube publica Azure Nube publica AWS
Contenerización	Kubernetes, Azure Red Hat OpenShift (ARO), AKS, EKS, Docker, Container registry / webhooks, Container App
Red y seguridad perimetral en nube	Virtual Network, Network Security Group, Route table, Azure Load Balancer, Application Gateway, Azure Front Door (incl. WAF), Azure Firewall y Firewall Policy, DDoS Protection, Azure Bastion, Private Endpoint, Private Link Service, Private DNS Zone, DNS Private Resolver, DNS forwarding ruleset, ExpressRoute, Virtual Network Gateway, Local Network Gateway, Network Watcher
Respaldo y continuidad de servicios	Azure Backup (Backup vault, Recovery Services vault), Restore Point Collection, snapshots de disco y base de datos, estrategias de alta disponibilidad y escalamiento en Azure SQL, Backup Database, AWS backup. Azure Data Factory (table storage)
Plataformas de monitoreo y observabilidad	Azure Monitor, Log Analytics, Application Insights, AWS CloudWatch, AWS CloudTrail, Prometheus, Grafana, Loki, Tempo, OpenTelemetry, Smart Detector y reglas de alerta.solarwinds para on-premise
Plataforma ITSM	Aranda (DIAN), Service Now (Contrato actual multinube)
CMDB	Aranda (DIAN)

Stack tecnológico	Lenguajes de programación/Fabricante
SIEM	Pruebas con Microsoft Sentinel.
Mensajería, streaming y eventos	AMQ Streams (Kafka + Zookeeper + Debezium), AMQ Broker, Event Hubs, Event Grid, Azure Storage Queues y Amazon SQS.
Herramientas de gestión	Azure DevOps, MS Project
Infraestructura como Código (IaC)	Terraform
Control de versiones y pruebas de código estático	GitHub y Azure DevOps Repos para control de versiones, CodeQL, Dependabot.
Integración y entrega continua (CI/CD y GitOps)	Azure DevOps para CI/CD, OpenShift Pipelines (Tekton), OpenShift GitOps (Argo CD), firma y verificación de artefactos de contenedor y análisis de SBOM basados en estándares (Sigstore, Notary v2, CycloneDX/SPDX)
Experiencia de desarrollador y modernización	Red Hat Developer Hub, Red Hat Dev Spaces, Podman Desktop, Migration Toolkit for Applications (MTA)
Automatización de pruebas	Selenium Nunit Microsoft Azure Load Testing y Microsoft Visual Studio Community 2022 (64-bit) - Version 17.7.5 JMeter 5.6.3 (pruebas de carga y estrés). pruebas automatizadas orquestadas desde Azure DevOps Pipelines
Servicios de IA y machine learning	Azure Machine Learning, Azure AI Services (incl. Computer Vision), Azure AI Foundry

6. CARGAS DE TRABAJO (Dic 2026)

Servicio	Descripción	Características	Fecha de ingreso
Pinpoint	Servicio de campañas masivas de correo interno y externo.	Solución PAAS en la nube de AWS.	13/Diciembre/2022
DataR - Preproductivo	Servicio de analítica y Big Data para el ambiente Preproductivo que se encarga de entregar nuevas vistas y nueva información a partir de las fuentes de datos misionales de DIAN.	Servicio PAAS nube de Azure.	10/Marzo/2023
DataR -Productivo	Servicio de analítica y big data para el ambiente de producción que se encarga de entregar nuevas vistas y nueva información a partir de las fuentes de datos misionales de DIAN.	Servicio PAAS nube de Azure.	21/Abril/2023
Canales de comunicación y AWS Direct Connect	Canales de comunicación principal y backup para conexión entre DIAN y la nube de AWS y servicio AWS Direct Connect.	Enlaces de Comunicaciones de 500Mbps redundante con AWS Direct Connect.	12/Septiembre/2023
Canales de comunicación y Azure ExpressRoute	Canales de comunicación principal y backup para conexión entre DIAN y la nube de Azure y servicio Azure ExpressRoute.	Enlaces de Comunicaciones de 2000Mbps redundante con ExpressRoute.	17/Octubre/2023
Facturación Electrónica	El Sistema de Factura Electrónica está compuesto por varias herramientas: El Catálogo, la Solución Gratuita, servicios de recepción de documentos electrónicos (factura electrónica, nómina electrónica, otros documentos electrónicos) y otras.	Servicio PAAS nube de Azure.	20/Octubre/2023
PQRDS	Solución de recepción y trámite de peticiones, quejas, reclamos, denuncias y solicitudes.	Solución PAAS y SAAS en la nube de Azure.	12/Febrero/2024
Notificaciones Electrónicas	Solución de apoyo para el envío de las notificaciones electrónicas a los contribuyentes.	Solución PAAS en la nube de Azure.	12/Febrero/2024
Importación Temporal Vehículos Turismo	Solución para el trámite de solicitudes de importación de vehículos de turismo.	Solución PAAS y SAAS en la nube de Azure.	07/Abril/2024
Portales Defensoría	Solución de publicación Web ajustado para la Defensoría.	Solución PAAS y SAAS en la nube de Azure.	07/Abril/2024
Sistema de Clasificación Arancelaria	Solución para radicación de solicitudes referentes a resoluciones de clasificación arancelaria y resoluciones anticipadas.	Solución PAAS y SAAS en la nube de Azure.	07/Abril/2024
Devoluciones de factura electrónica	Solución para consulta de información de facturas relacionadas en formatos de impuestos del SIE de devoluciones.	Solución PAAS y SAAS en la nube de Azure.	07/Abril/2024

Servicio	Descripción	Características	Fecha de ingreso
Proyecto RUT OCR	Solución que realiza el escaneo de las imágenes de documentos de identidad cargados en el registro de RUT para extracción de información de estos.	Solución PAAS y SAAS en la nube de Azure.	07/Abril/2024
OTP	Solución de generación y validación de códigos de un solo uso.	Solución PAAS y SAAS en la nube de Azure.	07/Abril/2024
Identidad	Solución para la consulta de información de usuarios en el proceso de acceso a sistemas de información.	Solución PAAS y SAAS en la nube de Azure.	07/Abril/2024
Comunicaciones	Solución para el envío de notificaciones a diferentes destinos desde las soluciones productivas de la entidad.	Solución PAAS y SAAS en la nube de Azure.	07/Abril/2024
Interoperabilidad	Solución para la consulta de datos a diferentes sistemas de información.	Solución PAAS y SAAS en la nube de Azure.	07/Abril/2024
DATAR Subdirección de Datos-Preproductivo	Entorno de analítica para la subdirección de datos, ambiente Preproductivo para el procesamiento de datos con Data Factory y DataBricks.	Integración de servicios PaaS en la nube de Azure.	Junio/2024
Micrositios	Solución para el alojamiento de los portales web de la entidad.	Solución PAAS y SAAS en la nube de Azure.	11/Abril/2024
Interoperabilidad registraduría	Solución para la interconexión y consulta de información de los contribuyentes en las bases de datos de la registraduría.	Solución PAAS y SAAS en la nube de Azure.	11/Abril/2024
Analítica Factura	Solución para extracción de datos del sistema de factura electrónica que brinda información detallada sobre valores asociados a tributos.	Solución PAAS y SAAS en la nube de Azure.	11/Abril/2024
Firma Electrónica	Solución de uso interno para la firma certificada de comunicaciones y documentos para envío a contribuyentes y entes de apoyo.	Solución PAAS y SAAS en la nube de Azure.	11/Abril/2024
Remates Virtuales	Solución para el trámite y agendamiento de sesiones y procesos de remates.	Solución PAAS y SAAS en la nube de Azure.	11/Abril/2024
SPD_Preproductivo	Servicio de analítica de datos para el ambiente PreProductivo que se encarga de realizar la extracción de data de fuentes de datos misionales de DIAN e integra el desarrollo bajo DEVOPS.	Solución IAAS y PAAS en la nube de Azure.	8/Abril/2024
SPD_Productivo	Servicio de analítica de datos para el ambiente PreProductivo que se encarga de realizar la extracción de data de fuentes de datos misionales	Solución IAAS y PAAS en la nube de Azure.	8/Abril/2024

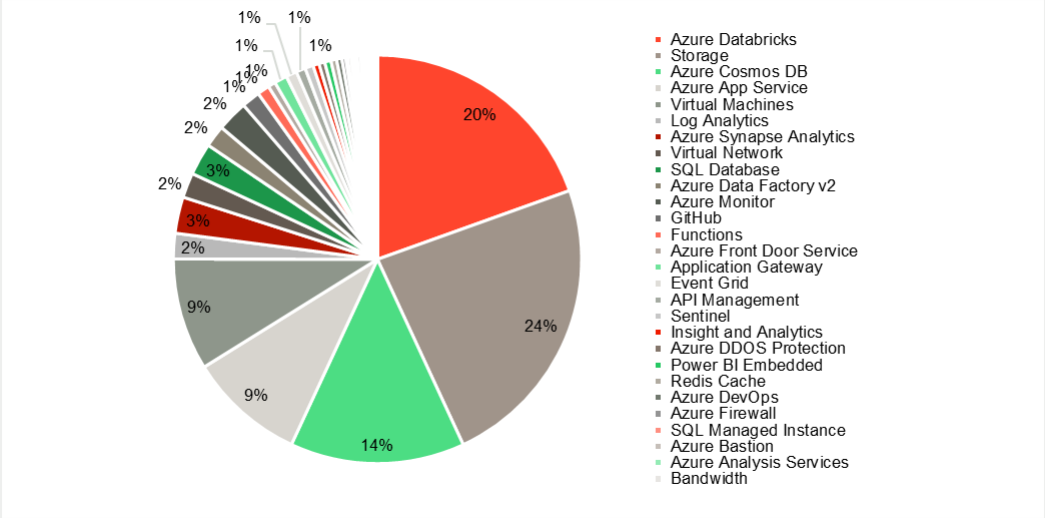
Servicio	Descripción	Características	Fecha de ingreso
	de DIAN e integra el desarrollo bajo DEVOPS.		
Selectividad LUCIA	LUCIA es una herramienta que usa algoritmos y técnicas de análisis de datos para identificar patrones y seleccionar casos que podrían requerir una revisión más detallada por parte de la DIAN. Características:	Solución PAAS en la nube de Azure.	8/Abril/2025
Interoperabilidad Exógena - BRMS	La App Exógena está diseñada para facilitar la carga y procesamiento de formatos específicos, permitiendo una gestión eficiente de los datos. Por otro lado, la App BRMS funciona como un motor de reglas de gestión empresarial, lo que permite a las organizaciones definir, implementar y gestionar reglas de negocio de manera ágil y efectiva, optimizando así la toma de decisiones y la operatividad.	Solución PAAS en la nube de Azure. AKS	8/junio/2025
ARO (Azure Red Hat OpenShift)	Plataforma de aplicaciones nativa de la nube gestionada conjuntamente por Microsoft y Red Hat. Es una versión de OpenShift, de Kubernetes empresarial, que se ejecuta en la infraestructura de Microsoft Azure.	Solución PAAS en la nube de Azure (ARO)	15/06/2025
Cadena	LACChain es una iniciativa de blockchain desarrollada por el Banco Interamericano de Desarrollo (BID) para fomentar la adopción de esta tecnología en América Latina y el Caribe. Su objetivo es crear un ecosistema de blockchain que sea accesible, seguro, transparente y escalable, con un enfoque particular en los sectores público y privado.	Servicio IaaS en la nube de Azure	
Procesos Jurídicos	Aplicación de la DIAN que permite registrar, gestionar y hacer seguimiento a los procesos judiciales y administrativos en los que la entidad es parte, incluyendo demandas, recursos, actuaciones y depósitos judiciales, con control de plazos, notificaciones y generación de reportes para la gestión jurídica institucional.	Solución PAAS en la nube de Azure.	
Administración Identidad	Permite que la DIAN verifique tu identidad de forma segura en línea, mediante un sistema de autenticación de dos factores (contraseña + código electrónico). Es la base para que	Solución PAAS en la nube de Azure.	

Servicio	Descripción	Características	Fecha de ingreso
	puedas firmar y llevar a cabo tus trámites tributarios y aduaneros digitalmente, con validez legal ante la entidad. Además, incluye mecanismos para renovar o recuperar el acceso de manera segura y controlada.		
Encuentas de satisfacción	Realiza encuesta de satisfacción usuarios que cumplieron su declaración de renta	Solución PAAS en la nube de Azure.	

7. CONSUMOS Y CANTIDAD DE RECURSOS EN LA NUBE (Referencia Dic2026)

i. Consumo general nube primaria

A continuación, se presenta el consumo histórico en la nube primaria Microsoft Azure en el segundo semestre de 2025, de junio a noviembre de 2025.



Cantidad total de recursos (DEV, TEST, PREPROD,PRO Y POC) Nube Primaria por tipo de recurso (Nov 2025)

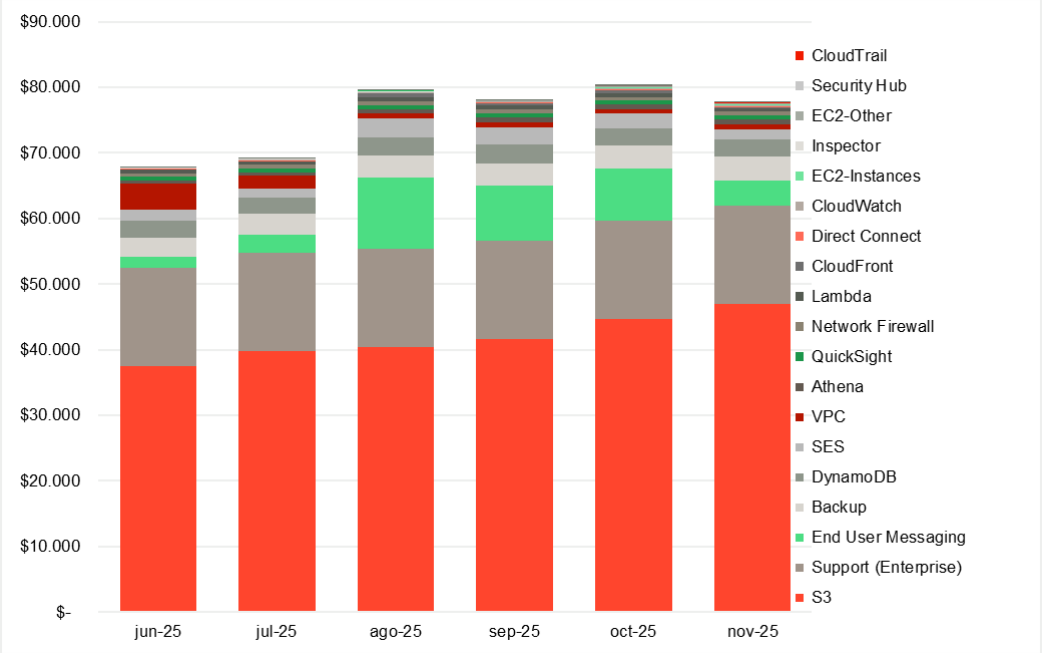
Servicio/Tipo	Total recursos
Compute	4303
Disk	2866
Virtual machine	1335
Restore Point Collection	47
Container registry	21
Virtual machine scale set	21

Servicio/Tipo	Total recursos
Snapshot	7
Image	2
Kubernetes service	2
VM image version	1
Container App	1
Networking	1802
Public IP address	1137
Private endpoint	418
Private DNS zone	156
Load balancer	25
Application gateway	24
Front Door and CDN profile	11
Bastion	10
Virtual network gateway	4
Front Door WAF policy	4
NAT gateway	3
Connection	3
DDoS protection plan	1
Firewall Policy	1
DNS forwarding ruleset	1
microsoft.network/dnsresolvers/outboundendpoints	1
ExpressRoute circuit	1
Firewall	1
microsoft.network/dnsresolvers/inboundendpoints	1
Management and Governance	1032
Metric alert rule	741
Log search alert rule	205
Log Analytics workspace	55
Action group	15
Recovery Services vault	14
Microsoft Purview account	1
Azure Monitor workspace	1
Web	587
App Service web app	312
App Service plan	151
App Service deployment slot	113
Static Web App	8
App Configuration	3
Storage	533
Storage account	527
Backup vault	6
Databases	147
SQL database	58
Cosmos DB account	33
Redis cache	20
SQL server	12
Azure Database for MySQL flexible server	9
Microsoft.Sql/longTermRetentionServers	5
SQL elastic pool	4
Azure Database for PostgreSQL flexible server	4
SQL managed instance	2

Servicio/Tipo	Total recursos
Security	82
Key vault	80
Defender for Cloud	2
Integration	63
Data factory (V2)	29
API Management service	9
Logic app	9
Event Grid extension topic	7
Automation account	4
Event Hubs namespace	3
Event Grid Topic	2
Analytics	36
Apache Spark pool	9
Synapse workspace	9
Azure Databricks Service	9
Power BI Embedded	3
Azure Managed Grafana	2
Dedicated SQL pool	2
Azure Data Explorer Cluster	1
Analysis Services server	1
Multicloud	27
Machine - Azure Arc	23
SQL Server - Azure Arc	4
AI and Machine Learning	5
Azure Machine Learning workspace	4
Azure AI services	1
Developer Tools	1
microsoft.visualstudio/organizations	1
Grand Total	8618

ii. Consumo general nube secundaria

A continuación, se presenta el consumo histórico en la nube secundaria Amazon AWS en los últimos cinco meses, de junio a noviembre de 2025.



Cantidad recursos nube AWS a noviembre de 2025 (914)

Servicio/Tipo	Cantidad de recursos AWS
Storage	445
AWS Backup	219
Amazon Simple Storage Service	203
Amazon Elastic Compute Cloud	23
Amazon Glacier	
Management and Governance	135
AmazonCloudWatch	135
AWS Config	
AWS Systems Manager	
AWS CloudTrail	
Security	77
Amazon Inspector	50
AWS Security Hub	26
AWS Network Firewall	1
Networking	58
Amazon Virtual Private Cloud	34
Amazon CloudFront	20
AWS Direct Connect	3
Amazon API Gateway	1
Compute	50
Amazon Elastic Compute Cloud	37
AWS Lambda	13

Servicio/Tipo	Cantidad de recursos AWS
AWS Step Functions	
Identity	43
AWS Key Management Service	42
AWS Secrets Manager	1
Integration	43
Amazon Simple Notification Service	29
Amazon Simple Queue Service	9
CloudWatch Events	5
Analytics	39
Amazon QuickSight	31
AWS Glue	3
Amazon Kinesis Firehose	3
Amazon Athena	2
Databases	17
Amazon DynamoDB	16
Amazon Relational Database Service	1
Business Applications	6
Amazon Simple Email Service	4
AWS End User Messaging	2
Developer Tools	1
AWS X-Ray	1
Other	
AWS Cost Explorer	
Mobile	
Amazon Location Service	
Grand Total	**914**

8. ESTADISTICAS CASOS INCIDENTES, REQUERIMIENTOS Y CAMBIOS

Estas son las estadísticas de los casos incidentes, requerimientos y cambios atendidos durante el servicio por parte del contratista actual, a noviembre del 2025

Incidentes	Cantidad de incidentes por Año			
Grupo Resolutor	**2023**	**2024**	**2025**	**Total general**
MN – Especialista Azure	22	156	144	322
MN - Monitoreo	4	4	241	249
MN – Administradores Multicloud		28	49	77
MN – Especialista AWS	20	6	11	37
MN – Especialista gobierno		3	2	5
MN – Especialista networking			5	5
MN – Agente nivel 1.5			3	3
MN – Especialista DevOps			1	1
Total general	46	197	456	699

Incidentes	Cantidad de incidentes por Año			
Nombre del Servicio	**2023**	**2024**	**2025**	**Total general**
Elementos no monitoreados			259	259
Degradación o falla de componentes o servicios de Azure		67	58	125
Aplicaciones	27	68		95
Errores técnicos		13	53	66
Caida o degradación del sistema		5	29	34
Incidentes no categorizados		21	6	27
Incidente de seguridad en Azure		6	6	12
Sistema operativo, almacenamiento, IaaS	8	4		12
Fallas automatizaciones			11	11
Degradación o falla de componentes o servicios de AWS			8	8
AWS	8			8
Falla en la integración de herramientas		3	4	7
Caida o degradación de canales			5	5
Falla en un pipeline			5	5
Servidores de aplicaciones, Bases de datos, PaaS	1	3		4
Azure		4		4
KCMP - Indisponibilidad o degradación del servicio			3	3
Caida o Degradación técnica del Sistema		1	1	2
Sandbox - Incidentes de correo			2	2
Accesos			2	2
Acceso a correo	2			2
Falla en el monitoreo y la gestión de eventos			2	2
Caida total solución DevOps			1	1
Falla en una configuración			1	1
Notificaciones Electrónicas - Caida o Degradación técnica del Sistema		1		1
Caida o Degradación técnica del Sistema - Factura Electrónica		1		1
Total general	**46**	**197**	**456**	**699**

Incidentes x Prioridad	Cantidad de incidentes por prioridad					
Nombre del Servicio	**1 - Crítica**	**2 - Alta**	**3 - Media**	**4 - Baja**	**5 - En planificación**	**Total general**
INFRAESTRUCTURA	454	9	63	8	70	604
Elementos no monitoreados	259					259
Degradación o falla de componentes o servicios de Azure	99		2		24	125
Aplicaciones	61	4	15	2	13	95
Incidentes no categorizados	2		2	3	20	27
Errores técnicos		3	18			21
Incidente de seguridad en Azure	6		6			12
Sistema operativo, almacenamiento, IaaS	10	2				12
Fallas automatizaciones			10		1	11

Incidentes x Prioridad	Cantidad de incidentes por prioridad					
Nombre del Servicio	1 - Crítica	2 - Alta	3 - Media	4 - Baja	5 - En planificación	Total general
Degradación o falla de componentes o servicios de AWS	3				5	8
AWS	2		6			8
Falla en la integración de herramientas	4			3		7
Caida o degradación de canales	4				1	5
Azure	4					4
Servidores de aplicaciones, Bases de datos, PaaS					4	4
Falla en el monitoreo y la gestión de eventos			2			2
Accesos			2			2
Acceso a correo					2	2
SISTEMAS DE INFORMACIÓN	30		55	1	7	93
Errores técnicos			44	1		45
Caida o degradación del sistema	29				5	34
Falla en un pipeline			5			5
KCMP - Indisponibilidad o degradación del servicio			3			3
Sandbox - Incidentes de correo			2			2
Notificaciones Electrónicas - Caida o Degradación técnica del Sistema					1	1
Caida total solución DevOps	1					1
Caida o Degradación técnica del Sistema - Factura Electrónica					1	1
Falla en una configuración			1			1
REPOSITORIO DE DATOS	1			1		2
Caida o Degradación técnica del Sistema	1			1		2
Total general	485	9	118	10	77	699

Requerimientos	Cantidad de requerimientos por Año			
Grupo Resolutor	2023	2024	2025	Total general
MN – Administradores Multicloud	27	559	1461	2047
MN – Especialista Azure	9	21	19	49
MN – Agente nivel 1.5	6	5	20	31
MN – Especialista networking			8	8
MN – Especialista AWS	1	3	3	7
MN – Especialista gobierno			4	4
Total general	43	588	1515	2146

Requerimientos	Cantidad de requerimientos por Año			
Nombre del Servicio	2023	2024	2025	Total general
DataR: modelos, servicios e integraciones		168	715	883
Operaciones transversales multinube		81	251	332
Gestión en nube de recursos y ambientes no productivos		101	186	287
Factura electrónica		28	145	173
DevOps		64	92	156
Gestión de usuarios	10	31		41
Comunicaciones		4	34	38
Notificaciones Electrónicas		28	1	29
Escritorios Virtuales de Nube		7	19	26
Operaciones de Nube	13	13		26
Pinpoint			24	24
Implementación de recursos en nube	9	13		22
Seguridad Forticloud		14	2	16
Analítica factura electronica		2	12	14
SARP - sistema clasificación arancelaria		2	8	10
Solicitudes de información	1	7		8
Identidad		3	4	7
KCMP		1	5	6
ServiceNow		3	2	5
Seguridad	2	2		4
RST - simuladores de formación		2	2	4
Devoluciones factura electrónica		1	3	4
DARN - devoluciones automáticas			4	4
Crear solicitud	3			3
Interoperabilidad		2	1	3
Micrositios		1	2	3
Firma electrónica		1	2	3
Dynamics 365 - PQSRD		2	1	3
Pasarela de Pagos		2		2
Backups y recuperación	2			2
Remates Virtuales		2		2
Contingencia aduana		2		2
Procesos Jurídicos		1		1
Logs y auditoria. Generar reportes de logs para ejercicios de auditoria	1			1
Provisionar recursos en nube primaria	1			1
Gestion de Accesos	1			1
Total general	43	588	1515	2146

Requerimientos	Prioridad		
Nombre del Servicio	4 - Baja	5 - En planificación	Total general
DataR: modelos, servicios e integraciones	926	1	927
Operaciones transversales multinube	368		368
Gestión en nube de recursos y ambientes no productivos	308		308
Factura electrónica	200	1	201
DevOps	179	1	180
Escritorios Virtuales de Nube	78		78
Comunicaciones	45		45
Gestión de usuarios	44		44
Notificaciones Electrónicas	39	1	40
Implementación de recursos en nube	32		32
Operaciones de Nube	31		31
Pinpoint	26	1	27
Seguridad Forticloud	18		18
Identidad	17		17
Analítica factura electronica	16		16
SARP - sistema clasificación arancelaria	14		14
RUT OCR	10		10
Dynamics 365 - PQSRD	10		10
Firma electrónica	9		9
Pasarela de Pagos	9		9
Solicitudes de información	9		9
Exógena	8		8
ServiceNow	8		8
Seguridad	7		7
Contingencia aduana	6		6
KCMP	6		6
Micrositios	5		5
Interoperabilidad	5		5
Micrositios renta	5		5
DARN - devoluciones automáticas	5		5
RST - simuladores de formación	4		4
Devoluciones factura electrónica	4		4
Remates Virtuales	4		4
Crear solicitud	3		3
Backups y recuperación	2		2
Procesos Jurídicos	2		2

Requerimientos	Prioridad		
Nombre del Servicio	**4 - Baja**	**5 - En planificación**	**Total general**
Numeración de facturación	2		2
Prevalidadores	2		2
Provisionar recursos en nube primaria	1		1
Logs y auditoria. Generar reportes de logs para ejercicios de auditoria	1		1
Gestion de Accesos	1		1
Operaciones de Desarrollo DevOps	1		1
OTP	1		1
Importación vehículos	1		1
Observabilidad	1		1
Gestión de roles	1		1
Total general	2474	5	2479

Cambios	Cantidad de cambios por Año			
Grupo de asignación	**2023**	**2024**	**2025**	**Total general**
MN – Especialista Azure	17	107	106	230
MN – Administradores Multicloud	2	11	87	100
MN – Especialista AWS	2	7	1	10
MN – Especialista networking		1		1
Total general	21	126	194	341

Cambios	Cantidad de cambios por Año			
Servicio Afectado	**2023**	**2024**	**2025**	**Total general**
Ajuste de Software	9	109	157	275
Actualización de versión	2	7	28	37
Ajuste de Hardware	8	6	9	23
Mantenimiento Proveedores	2	4		6
Total general	**21**	**126**	**194**	**341**

9. CONTRATOS DE SOPORTE – SERVICIOS MULTINUBE

La DIAN cuenta actualmente con contratos de soporte con fabricantes y/o terceros para algunos componentes del ecosistema multinube que hacen parte del alcance técnico del presente proceso. Estos contratos se mantienen y se utilizarán como mecanismo de escalamiento a fabricante, sin que ello sustituya la responsabilidad del futuro proveedor de Servicios Administrados de Nube respecto de la operación, diagnóstico, contención, remediación y cumplimiento de ANS.

En coherencia con las premisas del documento, los Servicios Base no incluyen costos de licenciamiento, suscripción o soporte de herramientas/plataformas de terceros, los cuales serán asumidos por la DIAN o por contratos específicos.

Así mismo, el proveedor deberá coordinar sus actividades con los demás proveedores/contratos vigentes de la Entidad, sin trasladar responsabilidades ni ANS de terceros.

iii. Inventario de contratos de soporte vigentes / en gestión

Ítem	Contrato / Soporte	Alcance principal	Componentes / servicios cubiertos	Estado	Cómo se usará en este servicio
1	Microsoft – Soporte Unificado (Azure Unified Support)	Soporte a servicios de nube Azure (plataforma y servicios nativos)	Servicios IaaS/PaaS/SaaS de Azure usados por DIAN	Vigente	Se usará para escalamiento a fabricante cuando aplique. El proveedor administrado debe realizar diagnóstico, evidencias, apertura y seguimiento de casos según el proceso acordado con DIAN.
2	Microsoft – Soporte de Misión Crítica (Factura Electrónica)	Soporte especializado para el servicio misional de Factura Electrónica	Componentes del servicio de Facturación Electrónica desplegados en Azure (según alcance del soporte)	Vigente	Se utilizará como canal prioritario de escalamiento para incidentes críticos del servicio misional. El proveedor deberá coordinar acciones, tiempos, comunicaciones y trazabilidad del caso.
3	Red Hat – Soporte ARO (Azure Red Hat OpenShift)	Soporte de fabricante sobre la plataforma ARO	Cluster(es) ARO: plataforma OpenShift administrada en Azure	Vigente	Se usará para incidentes/problemas de plataforma (cluster-level), upgrades/parches, y fallas atribuibles a OpenShift/ARO.
4	Soporte adicional para Operadores sobre ARO	Soporte para operadores (middleware/plataformas) desplegados sobre el cluster ARO	Operadores instalados en ARO (p. ej. operadores de integración/mensajería/observabilidad u otros que DIAN defina)	En contratación	Complementa el soporte del fabricante de ARO cuando el origen del incidente sea el operador o su producto.

5	IBM – Soporte para Bus BAMOE sobre ARO	Soporte de fabricante para el componente IBM BAMOE desplegado sobre ARO	IBM BAMOE (bus/motor) operando en ARO	En gestión	Se usará para escalamiento a IBM en fallas del producto, parches, recomendaciones y defectos, coordinado por el proveedor administrado bajo el proceso definido con DIAN.

Nota: Los números de contrato, vigencias, SLAs de fabricante, contactos y canales oficiales de apertura (portal/correo/teléfono) se entregarán al proveedor adjudicatario durante la transición y alistamiento del servicio, conforme a los controles de seguridad y acceso de la DIAN.

iv. Reglas de coordinación y uso del soporte de terceros

1. Responsabilidad del proveedor administrado: el proveedor es responsable de la gestión de incidentes extremo a extremo (registro, diagnóstico, contención, workaround, remediación, cierre y lecciones aprendidas), usando el soporte del fabricante como escalamiento cuando aplique.
2. Trazabilidad: toda interacción con fabricantes/terceros debe quedar registrada en ITSM (número de caso, fechas, evidencias, comunicaciones y resolución).
3. No duplicidad de cobros: el proponente no debe incluir en su tarifa costos ya cubiertos por estos contratos de soporte/licenciamiento, de acuerdo con las premisas del documento.
4. Coordinación inter-proveedores: el proveedor deberá coordinar acciones con Microsoft/Red Hat/IBM y demás contratos vigentes, sin trasladar responsabilidades ni ANS ajenos al alcance del contrato.
5. Alcance de escalamiento: se escalará a fabricante cuando el incidente/problema exceda capacidad de diagnóstico del proveedor, requiera hotfix/parche oficial, análisis de bug, o cuando el componente sea administrado por el fabricante (según aplique).
6. El reloj de ANS del proveedor NO se detiene por esperar respuesta del fabricante; el proveedor debe aplicar contención/workaround y gestionar escalamiento en paralelo.

----------FIN DEL DOCUMENTO----------