Ficha Técnica Contractual

Documento aprobado · Código de verificación SIGFIC-C1BE39B280D59A25

1. Identificación

Número interno	FT-2026-00002	**Versión**	18
Nombre / objeto	RENOVACIÓN DE ARANDA SERVICE MANAGEMENT Y COMPONENTES ASOCIADOS		
Estado	**Aprobada · disponible para contratación**	**Ámbito tecnológico (TI)**	Sí
Proyecto de adquisición	PRY-2026-0008 · RENOVACIÓN DE ARANDA Y COMPONENTES ASOCIADOS 36M		

2. Contenido de la ficha

Plazo estimado	Treinta y seis (36) meses, contados a partir del cumplimiento de los requisitos de ejecución y de la activación de las suscripciones correspondientes.
Ámbito	Tecnológico (TI)
Norma aplicable	Ley 80 de 1993
Objeto de la contratación	Renovar por treinta y seis (36) meses las suscripciones, licenciamiento, mantenimiento y soporte de la solución Aranda actualmente utilizada por la Procuraduría General de la Nación – PGN, incluyendo Aranda Service Management Suite – ASMS, Aranda CMDB Enterprise, Aranda Device Management – Client Management + Patch Solution, Agente Virtual integrado con Microsoft Teams y Aranda Mirroring Database, así como la renovación de una solución que complemente esta suite para evaluación continua de cumplimiento de seguridad, asegurando continuidad operativa, actualización de versiones, soporte especializado, conservación de configuraciones e historial y cumplimiento de los Acuerdos de Nivel de Servicio – ANS definidos en la presente ficha.
Alcance	La contratación comprende la renovación y continuidad de la solución Aranda actualmente utilizada por la Procuraduría General de la Nación durante un periodo de treinta y seis (36) meses continuos, garantizando la permanencia de las configuraciones, información, integraciones y capacidades actualmente operativas. El alcance comprende como mínimo: • Mantener vigente el derecho de uso de los componentes licenciados durante treinta y seis (36) meses continuos, sin interrupción entre la vigencia actual y la renovación, acreditado mediante certificación del fabricante por la totalidad del término. • Conservar las configuraciones, catálogos, flujos, reglas, integraciones, históricos, base de conocimiento, usuarios, roles, CIs y demás información existente en la plataforma, verificable frente al acta de línea base. • Proveer acceso a actualizaciones, correcciones, nuevas versiones compatibles y soporte técnico especializado durante toda la vigencia, para la totalidad de los componentes contratados. • Mantener la operación en modalidad Cloud/SaaS de los componentes que actualmente se prestan bajo dicha modalidad. • Renovar una solución que evalúe la postura de seguridad de los dispositivos que operan en la Entidad. • Garantizar la atención de incidentes y requerimientos de soporte conforme con los ANS mínimos y las reglas de medición definidas. • Entregar reportes periódicos de soporte, disponibilidad y cumplimiento de ANS. • Realizar acompañamiento para garantizar la continuidad y aprovechamiento de la solución. • Mantener la información, configuración e históricos existentes sin

	pérdida atribuible al proceso de renovación. • Garantizar escalamiento hacia el fabricante cuando la atención del incidente lo requiera. • Permitir la exportación de información e históricos al finalizar la vigencia, cuando la PGN lo requiera, en las condiciones de formato, medio y plazos definidas.
Modalidad	Electrónica
Paso Actual	6
Entregables	Renovación, implementación y activación por treinta y seis (36) meses continuos de las suscripciones y licencias de la plataforma Aranda Service Management y sus componentes asociados, y de la solución de cumplimiento normativo para la seguridad de la información, de acuerdo con las cantidades definidas en la ficha técnica. El contratista deberá entregar: certificación del fabricante que acredite la activación y vigencia del licenciamiento por treinta y seis (36) meses continuos; inventario de licenciamiento; plan de soporte y escalamiento; acta de línea base; informe de activación y pruebas de continuidad; informes mensuales de servicio con el cálculo de disponibilidad, el cumplimiento de ANS y los registros de los canales de atención; documentación de actualización por evento, e informe final. Asimismo, deberá garantizar la continuidad de la configuración e información existente y disponer los servicios de soporte, actualización y escalamiento técnico durante el plazo contractual.
Obligaciones técnicas	Garantizar la continuidad operativa de la plataforma durante la vigencia contractual; mantener activas las licencias, suscripciones, soporte y actualizaciones de la totalidad de los componentes; suscribir el acta de línea base y ejecutar las pruebas mínimas de continuidad; atender y gestionar incidentes y requerimientos técnicos de acuerdo con los ANS y las reglas de medición definidas; escalar al fabricante los casos que lo requieran y efectuar seguimiento hasta su solución, respondiendo frente a la PGN por los tiempos de atención; preservar la integridad, disponibilidad y configuración de la información existente; mantener la réplica de Aranda Mirroring Database hacia el repositorio administrado por la PGN; informar previamente mantenimientos programados; entregar reportes periódicos sobre disponibilidad, incidentes, cumplimiento de ANS y actividades de soporte, con los registros sin edición de los canales de atención; realizar transferencia de conocimiento ante cambios relevantes, y apoyar al cierre la exportación de la información e históricos en las condiciones definidas.
Justificación de la necesidad	La Procuraduría General de la Nación requiere asegurar la continuidad y sostenibilidad de la plataforma Aranda utilizada para la gestión y control de los servicios tecnológicos institucionales. La solución permite centralizar y dar trazabilidad a incidentes, requerimientos y demás casos de servicio; administrar acuerdos de nivel de servicio; mantener catálogo de servicios y base de conocimiento; relacionar elementos de configuración mediante la CMDB; y gestionar de forma centralizada los equipos de usuario final y su ciclo de actualización. La renovación proyectada comprende 53 usuarios concurrentes y 12 usuarios nombrados de Aranda Service Management Suite, Aranda CMDB Enterprise con capacidad para 10.000 CIs y cinco (5) consolas, Aranda Device Management para 4.950 dispositivos, el Agente Virtual integrado con Microsoft Teams, Aranda Mirroring Database y la solución complementaria para evaluación continua de cumplimiento de seguridad sobre 4.950 dispositivos, por un término de treinta y seis (36) meses. Desde la perspectiva tecnológica, la renovación no corresponde únicamente al mantenimiento de licencias, sino a la preservación de una capacidad institucional de gestión de servicios de TI. Mantener la plataforma vigente permite conservar configuraciones, flujos, catálogos, históricos, reglas de atención, información de activos y relaciones de configuración, así como continuar midiendo tiempos de respuesta y solución. De igual forma, las capacidades de inventario, administración remota y gestión de parches sobre los dispositivos contribuyen a una operación más controlada, trazable y segura del parque tecnológico de la Entidad. La necesidad se encuentra alineada con el Plan Estratégico Institucional – PEI 2025-2028, particularmente con el eje de Fortalecimiento Institucional y su orientación hacia la transformación digital y la

	modernización de las capacidades tecnológicas. Asimismo, se articula con el Plan Estratégico de Tecnologías de la Información – PETI 2026-2028, que concibe la tecnología como habilitador estratégico de la misión institucional y prioriza la sostenibilidad de los servicios tecnológicos, la seguridad digital, la gestión de información y el uso y apropiación de las soluciones. En este contexto, la continuidad de la plataforma de gestión de servicios constituye un componente transversal para operar, medir y mejorar los servicios de TI que soportan los procesos institucionales. La no renovación generaría riesgos relevantes para la operación de TI, entre ellos la pérdida de continuidad en el licenciamiento, soporte y actualizaciones; limitaciones para la gestión centralizada y trazable de incidentes y solicitudes; afectación de la medición de los niveles de servicio; debilitamiento de la gestión de configuración e inventario; y reducción de las capacidades de administración y parchado de los dispositivos cubiertos. Adicionalmente, una interrupción de la plataforma podría generar dispersión de solicitudes, pérdida de trazabilidad operativa y mayores tiempos de atención. Por lo anterior, la renovación por treinta y seis (36) meses, acompañada de Acuerdos de Nivel de Servicio – ANS verificables, de una línea base que permita comprobar la conservación de la información y de reglas objetivas de medición, resulta necesaria para asegurar continuidad, control, disponibilidad y calidad en la gestión de los servicios tecnológicos de la PGN.
Tipo de necesidad	Prestación de servicios
Lugar de ejecución	Procuraduría General de la Nación, Bogotá D. C., con cobertura para las sedes y usuarios de la Entidad a nivel nacional. Por tratarse de una solución en modalidad Cloud, la prestación del servicio y el soporte podrán ejecutarse de manera remota, sin perjuicio de las actividades presenciales que sean requeridas y previamente coordinadas con la supervisión del contrato.
Especificaciones técnicas mínimas	La solución deberá contemplar la renovación por treinta y seis (36) meses continuos de Aranda Service Management y sus componentes asociados, incluyendo como mínimo: 53 usuarios concurrentes de Aranda Service Management Suite – Suscripción Cloud; 12 usuarios nombrados de Aranda Service Management Suite – Suscripción Cloud; 1 Aranda CMDB Enterprise, con cinco (5) consolas y capacidad de hasta 10.000 CIs; 1 Agente Virtual – Aranda Service Management, integrado con Microsoft Teams; 1 Aranda Mirroring Database; 4.950 dispositivos cubiertos con Aranda Device Management – Client Management + Patch Solution, y 4.950 dispositivos cubiertos por la solución de cumplimiento normativo para seguridad de la información, de la misma marca de la solución de administración de dispositivos. La renovación deberá garantizar: continuidad sin interrupción, acreditada con certificación del fabricante por treinta y seis (36) meses continuos; conservación de información y configuraciones, verificada mediante acta de línea base y pruebas mínimas de continuidad; actualizaciones; hotfixes; parches; versiones soportadas; soporte técnico para la totalidad de los componentes; escalamiento al fabricante; documentación; transferencia de conocimiento cuando existan cambios relevantes; disponibilidad mensual mínima del servicio Cloud de 99,5 %, medida con la fórmula definida en la ficha; atención de incidentes críticos con respuesta máxima de 30 minutos, con canales de radicación 7×24 y reglas objetivas de cómputo; continuidad de la réplica de Aranda Mirroring Database hacia el repositorio administrado por la PGN; exportación de la información al cierre en formatos técnicamente utilizables; y mantenimiento de las capacidades actuales de gestión de servicios, activos, configuración, endpoints, parches y cumplimiento de seguridad.
Tipo de contratación	Selección abreviada

3. Contenido técnico

1. ALCANCE

1.1. Mantener vigente el derecho de uso de los componentes licenciados durante treinta y seis (36) meses continuos, sin interrupción entre la vigencia actual y la renovación.

1.2. Conservar las configuraciones, catálogos, flujos, reglas, integraciones, históricos, base de conocimiento, usuarios, roles, CIs y demás información existente en la plataforma.

1.3. Proveer acceso a actualizaciones, correcciones, nuevas versiones compatibles y soporte técnico especializado durante toda la vigencia.

1.4. Mantener la operación en modalidad Cloud/SaaS de los componentes que actualmente se prestan bajo dicha modalidad.

1.5. Complementar la renovación de soporte con la renovación de una solución de auditoría y cumplimiento de postura de seguridad en los dispositivos de la Entidad.

1.6. Garantizar la atención de incidentes y requerimientos de soporte conforme con los ANS mínimos definidos en este documento.

1.7. Entregar reportes periódicos de soporte, disponibilidad y cumplimiento de ANS, y realizar acompañamiento para la continuidad y aprovechamiento de la solución.

2. COMPONENTES Y CANTIDADES

2.1. Componentes y cantidades a renovar

Ítem	Tipo	Componente / requerimiento	Cantidad	Vigencia (meses)
1	Usuario	Aranda Service Management Suite – Usuario concurrente – Suscripción Cloud	53	36
2	Usuario	Aranda Service Management Suite – Usuario nombrado – Suscripción Cloud	12	36
3	Servidor/CI	Aranda CMDB Enterprise – 5 consolas – hasta 10.000 CIs	1	36
4	Suscripción	Agente Virtual – Aranda Service Management – Conector con Microsoft Teams – Suscripción Cloud	1	36
5	Base de datos	Aranda Mirroring Database	1	36
6	Dispositivo	Aranda Device Management (Client Management + Patch Solution)	4.950	36

2.2. Componentes y cantidades para renovar – solución de cumplimiento

Ítem	Tipo	Componente / requerimiento	Cantidad	Vigencia (meses)
1	Usuario	Solución de cumplimiento normativo para la seguridad de la información	4.950	36

2.3. La vigencia de treinta y seis (36) meses se cuenta a partir de la fecha de activación certificada por el fabricante, la cual no podrá ser posterior al vencimiento de la suscripción vigente.

3. REQUERIMIENTOS FUNCIONALES Y TÉCNICOS MÍNIMOS

3.1. Aranda Service Management Suite (ASMS)

Código	Requerimiento mínimo
ASMS-01	Plataforma de Enterprise Service Management / IT Service Management para gestionar, integrar y automatizar procesos de soporte y entrega de servicios.
ASMS-02	Mesa de ayuda multicanal con registro y gestión de casos mediante portal de autoservicio web, correo electrónico y canales integrados.

Documento generado el 2026-11-19 14:05 · Verificable en línea con el código SIGFIC-C1BE39B280D59A25

ASMS-03	Gestión de incidentes, solicitudes/requerimientos, problemas, cambios y niveles de servicio.
ASMS-04	Configuración y medición de SLA/ANS, OLA y contratos de soporte (UC), con tiempos por prioridad, calendarios hábiles y reglas de escalamiento.
ASMS-05	Catálogo de servicios y base de conocimiento para publicación de servicios y artículos de autoayuda.
ASMS-06	Consola de especialistas para gestionar, escalar, documentar y solucionar solicitudes, con trazabilidad e historial.
ASMS-07	Licenciamiento mínimo: 53 usuarios concurrentes y 12 usuarios nombrados durante los treinta y seis (36) meses.

3.2. Aranda CMDB Enterprise

Código	Requerimiento mínimo
CMDB-01	Capacidad para administrar hasta 10.000 Elementos de Configuración (CIs) y cinco (5) consolas de gestión.
CMDB-02	Repositorio centralizado de CIs de hardware, software, servicios, contratos y demás elementos administrados por la PGN.
CMDB-03	Mapeo de relaciones y dependencias entre CIs y servicios, permitiendo análisis de impacto.
CMDB-04	Integración con ASMS para asociar CIs con incidentes, solicitudes y cambios.
CMDB-05	Gestión de información de contratos, garantías, proveedores, costos y ciclo de vida de activos, de acuerdo con las capacidades licenciadas.

3.3. Aranda Device Management (ADM)

Código	Requerimiento mínimo
ADM-01	Cobertura mínima para 4.950 dispositivos durante treinta y seis (36) meses.
ADM-02	Descubrimiento e inventario automático de hardware y software mediante agente.
ADM-03	Distribución e instalación/desinstalación remota de software y paquetes de configuración.
ADM-04	Control y asistencia remota sobre estaciones de trabajo para diagnóstico y soporte.
ADM-05	Gestión de políticas y capacidades de administración de endpoints.
ADM-06	Gestión automatizada de parches para sistemas operativos y software de terceros, programación de ventanas de mantenimiento y reportes de cumplimiento.

Documento generado el 2026-11-19 14:05 · Verificable en línea con el código SIGFIC-C1BE39B280D59A25

3.4. Agente Virtual para Microsoft Teams

Código	Requerimiento mínimo
AVT-01	Conector vigente con Microsoft Teams durante treinta y seis (36) meses.
AVT-02	Creación y seguimiento de tickets desde Teams.
AVT-03	Autogestión mediante respuestas automáticas y consulta de artículos de conocimiento.
AVT-04	Notificaciones al usuario sobre creación, avance, actualización y cierre de solicitudes, de acuerdo con las capacidades del producto.

3.5. Aranda Mirroring Database

Código	Requerimiento mínimo
MDB-01	Servicio de réplica o copia espejo de la base de datos operativa de Aranda Cloud hacia un repositorio secundario de consulta.
MDB-02	Habilitación de consultas para analítica y reportería sin afectar de manera significativa la carga transaccional del ambiente productivo.
MDB-03	Disponibilidad de información para herramientas de analítica/BI y consultas autorizadas, bajo controles de seguridad y acceso definidos por la PGN.
MDB-04	El repositorio secundario de destino es administrado por la PGN, la cual dispone de la infraestructura y del licenciamiento de base de datos correspondientes. La oferta no incluye infraestructura ni licencias para dicho repositorio.
MDB-05	El contratista mantiene activa la suscripción, la configuración de la réplica, su frecuencia de sincronización vigente y el monitoreo del servicio durante los treinta y seis (36) meses.
MDB-06	El informe mensual de servicio incluye, para este componente: fecha y hora de la última sincronización exitosa de cada día del periodo, fallas de sincronización con su causa y solución, y prueba de conteo de registros de las tablas de casos entre la base operativa y la réplica.

3.6. Solución de cumplimiento normativo para la seguridad de la información

La solución deberá contar con capacidades de evaluación continua de cumplimiento de seguridad, incluyendo definición de políticas, detección de desviaciones, ejecución de remediaciones automáticas, monitoreo permanente, generación de evidencias para auditoría e integración con herramientas de gestión de dispositivos y servicios, permitiendo una gestión proactiva del riesgo y cumplimiento normativo. Para garantizar homogeneidad en la administración de las herramientas, la solución ofertada deberá ser de la misma marca de la solución de administración de dispositivos – Aranda Software.

3.6.1. Requerimientos funcionales

Código	Requerimiento mínimo
SC-01	Único agente que se instale en las estaciones para todas las funciones del producto.
SC-02	Información acerca de la cantidad de dispositivos donde se encuentra el agente desplegado.
SC-03	Información acerca de la cantidad de dispositivos que tienen política aplicada.
SC-04	Información detallada de los dispositivos que tienen/no tienen política aplicada.

Documento generado el 2026-11-19 14:05 · Verificable en línea con el código SIGFIC-C1BE39B280D59A25

SC-05	Información de cantidad de máquinas que cumplen/no cumplen con la política aplicada.
SC-06	Información detallada de las máquinas que cumplen/no cumplen con la política aplicada.
SC-07	Información acerca de la cantidad de políticas activas.
SC-08	Información acerca de la cantidad de las políticas activas en cumplimiento/no cumplimiento.
SC-09	Información detallada de las políticas activas en cumplimiento/no cumplimiento.
SC-10	Definición de distintos roles en el sistema; cada rol implica determinados permisos y privilegios.
SC-11	Despliegue de agente mediante línea de comandos.
SC-12	Creación de grupos de máquinas, para sectorizar la política a aplicar según la necesidad del negocio.
SC-13	Módulo para gestión de políticas que incluya visualización de cumplimiento de política, dispositivos alcanzados, descripción, fecha de creación, activo/no activo.
SC-14	Creación de políticas de cumplimiento para navegadores web.
SC-15	Creación de políticas de cumplimiento para software antiphishing.
SC-16	Creación de políticas de cumplimiento para software antimalware.
SC-17	Creación de políticas de cumplimiento para software firewall.
SC-18	Creación de políticas de cumplimiento para software de endpoint encryption.
SC-19	Creación de políticas de cumplimiento para software VPN client.
SC-20	Creación de políticas de cumplimiento para software de backup.
SC-21	Creación de políticas de cumplimiento para herramientas de almacenamiento en la nube.
SC-22	Creación de políticas de cumplimiento para herramientas de comunicación.
SC-23	Creación de políticas de cumplimiento para Health Agent.
SC-24	Creación de políticas de cumplimiento para software de control remoto.
SC-25	Creación de políticas de cumplimiento para Virtual Machine.
SC-26	Creación de políticas de cumplimiento para software de Data Loss Prevention.
SC-27	Creación de políticas que puedan combinar los diferentes criterios a partir de las diferentes categorías de software que maneja la solución.
SC-28	Modificación del tiempo de monitoreo, definido como la frecuencia en la que se realizan las verificaciones de cumplimiento en las máquinas.
SC-29	Asociación de una política en diferentes grupos de dispositivos.
SC-30	Verificación de múltiples criterios de configuración del software, incluyendo, como requisito mínimo, la verificación de la instalación.

APROBADO

SC-31	Exportación de información en formato Excel asociada a las políticas (SO, descripción, fecha de creación, cantidad de dispositivos, activo/no activo, estado de cumplimiento).
SC-32	Filtro por dispositivo, que permita identificar grupo, políticas y vulnerabilidades asociadas al equipo.
SC-33	Módulo para identificación de vulnerabilidades.
SC-34	Presentación de la información de la vulnerabilidad con descripción (incluye código CVE), software afectado y la cantidad de dispositivos que registran la misma.
SC-35	Categorización de las vulnerabilidades por nivel de criticidad.
SC-36	Visualización de la cantidad de vulnerabilidades asociadas a cada nivel de criticidad.
SC-37	Visualización de información detallada acerca de las vulnerabilidades asociadas al nivel de criticidad (descripción, incluye código CVE, software afectado y cantidad de dispositivos que registran la misma).
SC-38	Marca de la solución: la misma de la solución de administración de dispositivos – Aranda Software.

3.6.2. Capacidades mínimas

Capacidad	Actividades mínimas
Evaluación continua de cumplimiento (Compliance Assessment)	Ejecución automatizada de evaluaciones de cumplimiento sobre endpoints y servidores. Verificación contra políticas de seguridad corporativas y estándares definidos. Identificación de desviaciones en configuraciones de seguridad.
Definición y administración de políticas de seguridad	Creación y gestión de políticas basadas en buenas prácticas (hardening). Parametrización por tipo de activo, rol de usuario o criticidad. Versionamiento y trazabilidad de cambios en políticas.
Detección de brechas y vulnerabilidades de configuración	Identificación de configuraciones inseguras (misconfigurations). Detección de software no autorizado o fuera de estándar. Evaluación de cumplimiento frente a benchmarks definidos.
Remediación automatizada de incumplimientos	Ejecución de acciones correctivas de forma automática o asistida. Aplicación de configuraciones seguras en dispositivos. Integración con capacidades de parcheo (ADM) para cierre de brechas.
Monitoreo continuo y alertamiento	Supervisión permanente del estado de cumplimiento. Generación de alertas ante desviaciones o incumplimientos. Seguimiento de activos en riesgo o fuera de norma.
Gestión de auditorías y evidencias	Generación automática de evidencias de cumplimiento. Trazabilidad completa de evaluaciones y remediaciones. Soporte a auditorías internas, externas y regulatorias.
Reportes y dashboards de cumplimiento	Visualización en tiempo real del nivel de cumplimiento.

Documento generado el 2026-11-19 14:05 · Verificable en línea con el código SIGFIC-C1BE39B280D59A25

	Indicadores clave: porcentaje de cumplimiento, brechas abiertas, tendencias. Reportes ejecutivos y técnicos para toma de decisiones.
Automatización de controles de seguridad	Programación de evaluaciones periódicas. Automatización de respuestas ante incumplimientos. Reducción de intervención manual en procesos de compliance.
Enfoque basado en riesgo	Priorización de brechas según criticidad del activo. Apoyo a la gestión de riesgos de TI. Base para planes de tratamiento y mejora continua.

4. CONDICIONES MÍNIMAS DE LA RENOVACIÓN Y SOPORTE

Condición	Requerimiento mínimo
Continuidad	La renovación deberá iniciar sin interrupción del servicio ni pérdida de derecho de uso respecto de la vigencia actual.
Certificación de vigencia	Certificación expedida por el fabricante Aranda Software, dirigida a la PGN, que acredite la renovación y activación de la totalidad de las suscripciones y licencias por treinta y seis (36) meses continuos. No se acepta la acreditación por periodos anuales ni la certificación expedida únicamente por el canal o distribuidor.
Conservación	No se admitirán pérdidas de configuraciones, tickets, históricos, artículos, catálogos, reglas, integraciones, roles, CIs o información existente atribuibles al proceso de renovación.
Actualizaciones	El contratista deberá garantizar acceso a actualizaciones, hotfixes, parches y versiones soportadas disponibles para los componentes licenciados, sin costo adicional diferente al contratado.
Compatibilidad	Las actualizaciones deberán conservar la compatibilidad con las configuraciones e integraciones existentes o contar con un plan de actualización previamente aprobado por la supervisión, que incluya evidencia de respaldo emitida por el fabricante y procedimiento de reversión.
Soporte	Debe incluir mesa/canal de soporte del contratista y escalamiento al fabricante cuando el caso lo requiera.
Escalamiento	Los incidentes cuya solución dependa del fabricante deberán ser escalados oportunamente y permanecer bajo seguimiento del contratista hasta su cierre.
Documentación	El contratista deberá entregar documentación técnica y funcional aplicable, notas de versión y recomendaciones de actualización cuando corresponda.
Transferencia	Cuando se introduzcan cambios relevantes por actualización, deberá realizarse sesión de transferencia de conocimiento a los administradores designados por la PGN.

5. LÍNEA BASE Y PRUEBAS DE CONTINUIDAD

5.1. **Acta de línea base.** Dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de inicio, el contratista y la supervisión suscribirán un acta de línea base que registrará: versión de cada componente; número de usuarios, roles y perfiles; número de tickets históricos, artículos de la base de conocimiento, servicios del catálogo y CIs; flujos, reglas e integraciones activos; número de dispositivos con agente ADM y con agente de la solución de cumplimiento reportando. El acta se soportará en reportes exportados y capturas generadas desde la propia herramienta.

5.2. **Pruebas mínimas de continuidad.** Efectuada la activación, el contratista ejecutará con la supervisión, como mínimo, las siguientes pruebas:

Documento generado el 2026-11-19 14:05 · Verificable en línea con el código SIGFIC-C1BE39B280D59A25

No.	Prueba
1	Acceso de usuarios concurrentes y nombrados a la consola de especialistas y de usuarios finales al portal de autoservicio.
2	Creación, asignación, escalamiento y cierre de un caso por cada canal habilitado (portal, correo electrónico y Microsoft Teams), con medición de ANS.
3	Consulta de históricos, base de conocimiento, catálogo y CIs, contrastada con las cifras del acta de línea base.
4	Reporte de inventario y de cumplimiento de parches de ADM, y reporte de cumplimiento de políticas de la solución de cumplimiento.
5	Sincronización y consulta de la réplica de Aranda Mirroring Database.

5.3. **Respaldo y reversión.** La activación se realiza sobre la misma instancia en operación. Toda actualización de versión durante la vigencia estará precedida del plan de actualización aprobado por la supervisión, con evidencia de respaldo emitida por el fabricante y procedimiento de reversión.

5.4. **Incidentes preexistentes.** Las fallas consignadas en el acta de línea base no son imputables al proceso de renovación. A partir del inicio de la vigencia se gestionan como casos de soporte, con la prioridad y los ANS de esta ficha.

6. ALCANCE DEL SOPORTE POR COMPONENTE

6.1. El soporte técnico, la actualización y la atención conforme a los ANS cubren, durante los treinta y seis (36) meses, la totalidad de los componentes contratados: Aranda Service Management Suite, Aranda CMDB Enterprise, Aranda Device Management, Agente Virtual con conector Microsoft Teams, Aranda Mirroring Database y la solución de cumplimiento normativo para la seguridad de la información.

Actividad incluida	Descripción
Incidentes y requerimientos	Atención de prioridades P1 a P4, con diagnóstico, restablecimiento, solución definitiva y escalamiento al fabricante.
Actualización	Acceso, instalación y documentación de actualizaciones, hotfixes, parches y versiones soportadas.
Parametrización	Ajuste de la configuración existente sobre funcionalidades nativas de los productos licenciados: catálogos, flujos, reglas, formularios, ANS, perfiles, grupos de dispositivos, paquetes de distribución, políticas de cumplimiento y reportes. Se atienden como requerimientos P3 o P4.
Transferencia de conocimiento	Sesiones para los administradores designados por la PGN cuando se introduzcan cambios relevantes por actualización o cambios de configuración relevantes de la solución de cumplimiento.

6.2. No forman parte del alcance los desarrollos a la medida ni las integraciones nuevas con sistemas de terceros que no existan en la línea base o que no correspondan a funcionalidades nativas del producto.

7. ACUERDOS DE NIVEL DE SERVICIO (ANS) MÍNIMOS

Los siguientes ANS se establecen como requerimientos mínimos contractuales para la atención del servicio de soporte. El proponente podrá ofrecer niveles superiores. Para incidentes que dependan de corrección del fabricante, el contratista deberá demostrar el escalamiento, mantener seguimiento continuo y aplicar una solución temporal o alternativa cuando técnicamente sea posible.

7.1. Tiempos de atención por prioridad

Prioridad	Criterio	Cobertura	Respuesta	Diagnóstico / contención	Restablecimiento / solución

Documento generado el 2026-11-19 14:05 · Verificable en línea con el código SIGFIC-C1BE39B280D59A25

Crítica – P1	Indisponibilidad total del servicio o afectación generalizada que impida la operación de la mesa de servicios, sin alternativa viable.	7×24	≤ 30 min	≤ 2 h	≤ 4 h o solución temporal; seguimiento continuo hasta solución definitiva
Alta – P2	Degradación severa o afectación de una función crítica con impacto significativo en múltiples usuarios, con alternativa limitada.	7×24	≤ 1 h	≤ 4 h	≤ 8 h o solución temporal
Media – P3	Falla con impacto moderado o parcial, con alternativa operativa disponible; no impide la continuidad del servicio.	Horario hábil	≤ 4 h hábiles	≤ 1 día hábil	≤ 2 días hábiles
Baja – P4	Consulta, ajuste menor, solicitud de información o defecto cosmético sin impacto relevante en la operación.	Horario hábil	≤ 8 h hábiles	≤ 2 días hábiles	≤ 5 días hábiles

7.2. Disponibilidad del servicio Cloud

Indicador	Nivel mínimo	Regla de medición
Disponibilidad mensual de ASMS Cloud	≥ 99,5 %	Medición mensual sobre el tiempo total del mes, excluyendo ventanas de mantenimiento programadas informadas con mínimo 48 horas de anticipación y eventos de fuerza mayor debidamente soportados.
Notificación de mantenimiento programado	≥ 48 horas	El contratista deberá informar ventana, duración estimada, componentes afectados y medidas de contingencia.
Notificación de incidente crítico Cloud	≤ 30 minutos desde su identificación	Debe informar impacto, estado inicial y canal de seguimiento; posteriores actualizaciones mínimo cada 60 minutos mientras persista la indisponibilidad.

7.2.1. **Fórmula:** Disponibilidad (%) = [(TT − TE − TI) / (TT − TE)] × 100, donde TT es el tiempo total del mes en minutos; TE, el tiempo de exclusiones válidas (mantenimientos programados notificados con mínimo 48 horas de anticipación y eventos de fuerza mayor debidamente soportados), y TI, el tiempo de indisponibilidad no excluida.

7.2.2. **Fuente de medición:** reportes de disponibilidad del monitoreo del fabricante, presentados por el contratista en el informe mensual y contrastados con los casos radicados en el periodo. En caso de diferencia, se toma el mayor tiempo de indisponibilidad soportado.

7.2.3. **Mantenimiento que excede la ventana:** el tiempo que exceda la ventana notificada se computa como indisponibilidad (TI).

7.2.4. **Degradaciones parciales y fallas de integraciones:** las que cumplan el criterio de prioridad P1 se computan como indisponibilidad; las demás se gestionan y miden con los ANS de atención de la prioridad que corresponda.

7.2.5. **Periodos inferiores a un mes:** al inicio y al final de la vigencia, TT corresponde a los minutos efectivamente comprendidos dentro de la vigencia en ese mes.

7.2.6. **Componentes medidos:** ASMS Cloud y los módulos que operan sobre dicha plataforma: consola de especialistas, portal de autoservicio y CMDB.

7.3. Reglas de medición y cumplimiento de ANS

Regla	Condición

Documento generado el 2026-11-19 14:05 · Verificable en línea con el código SIGFIC-C1BE39B280D59A25

Canales de radicación	Línea telefónica de atención, correo electrónico y herramienta de gestión de casos, habilitados 7×24×365 para la radicación de todas las prioridades. La atención de P3 y P4 se presta en horario hábil; la radicación no está restringida por horario.
Zona horaria	Hora legal de la República de Colombia (UTC-5).
Horario hábil (P3 y P4)	Lunes a viernes, de 7:00 a.m. a 7:00 p.m., excluidos los días festivos nacionales.
Tiempo de respuesta	Se mide desde la radicación del caso por un canal autorizado hasta la primera atención efectiva del contratista. El cómputo inicia en la marca de tiempo más temprana entre la recepción del correo, el registro de la llamada, la radicación en la herramienta o el reporte de la PGN por cualquier canal autorizado. El caso no radicado por causas imputables al contratista se computa desde el reporte de la PGN.
Primera atención efectiva	Intervención de un especialista del contratista sobre el caso, mediante contacto con el usuario reportante o acción técnica registrada. Los acuses de recibo automáticos, las respuestas genéricas y la sola asignación del caso no constituyen primera atención efectiva.
Incidente crítico Cloud	La hora de identificación es la más temprana entre el registro del monitoreo del fabricante, el del monitoreo del contratista, la publicación en el portal de estado del fabricante o el reporte de la PGN. El contratista radica el caso de inmediato con dicha hora.
Tiempo de restablecimiento	Se mide de manera continua hasta recuperar el servicio o disponer de una solución temporal aceptada por la supervisión o por el administrador de la plataforma designado por la OTITD, quien deja constancia en el caso.
Suspensión del reloj	Solo podrá suspenderse cuando exista una dependencia documentada de información o acción de la PGN; la suspensión deberá quedar registrada y ser trazable. La intervención del fabricante no suspende el cómputo del ANS.
Prioridad	La asigna la PGN al momento del reporte. El contratista no podrá reclasificarla sin aprobación previa y escrita de la supervisión.
Registros y prevalencia	Los registros de la herramienta de gestión de casos, del sistema telefónico y del correo electrónico se entregan sin edición con el informe mensual y, a solicitud de la supervisión, dentro de los dos (2) días hábiles siguientes. Ante ausencia, inconsistencia o falta de entrega oportuna de los registros del contratista, prevalecen los registros de la PGN.
Esquema de atención	Se admite disponibilidad o guardia remota bajo la exclusiva responsabilidad y riesgo del contratista; no constituye justificación para el incumplimiento de los tiempos. El personal de guardia y sus datos de contacto hacen parte del Plan de soporte y escalamiento.
Incumplimiento	El incumplimiento de ANS será gestionado conforme a las condiciones del contrato y a los mecanismos de seguimiento definidos por la supervisión.

7.4. Escalamiento al fabricante

Aspecto	Condición
Plazo de escalamiento	Dentro del tiempo de diagnóstico de la prioridad: P1 ≤ 2 h; P2 ≤ 4 h; P3 ≤ 1 día hábil; P4 ≤ 2 días hábiles.
Evidencias	Número de caso asignado por el fabricante, fecha y hora de radicación ante este y bitácora de seguimiento. En P1, informe de avance a la PGN mínimo cada sesenta (60) minutos mientras persista la afectación.

Documento generado el 2026-11-19 14:05 · Verificable en línea con el código SIGFIC-C1BE39B280D59A25

Responsabilidad	Frente a la PGN, el contratista responde por el cumplimiento de los ANS, incluidos los casos escalados al fabricante. Las evidencias de escalamiento oportuno se valoran en el procedimiento de incumplimiento previsto en el contrato, sin excluir la medición del ANS.

8. SEGURIDAD, PRIVACIDAD Y GESTIÓN DE LA INFORMACIÓN

8.1. La información registrada, procesada o generada por la PGN en la solución es propiedad de la Entidad. El contratista no podrá usarla para fines diferentes a la ejecución contractual.

8.2. El acceso del personal de soporte deberá aplicar mínimo privilegio, autenticación robusta y trazabilidad de las actividades realizadas.

8.3. Los incidentes de seguridad que puedan comprometer información o disponibilidad de la solución deberán ser notificados de manera inmediata a la PGN y gestionados conforme a los procedimientos institucionales.

8.4. El contratista deberá mantener confidencialidad sobre información, configuraciones, credenciales y datos conocidos durante la prestación del servicio.

8.5. A la terminación del contrato, la PGN deberá poder obtener exportación de la información e históricos en formatos técnicamente utilizables, sin impedir la continuidad o transferencia del servicio, conforme al numeral 13.

9. LUGAR DE EJECUCIÓN Y ACTIVIDADES PRESENCIALES

9.1. Procuraduría General de la Nación, Bogotá D. C., con cobertura para las sedes y usuarios de la Entidad a nivel nacional. Por tratarse de una solución en modalidad Cloud, la prestación del servicio y el soporte podrán ejecutarse de manera remota, sin perjuicio de las actividades presenciales que sean requeridas y previamente coordinadas con la supervisión del contrato.

9.2. **Actividades presenciales:** reunión de inicio, suscripción del acta de línea base, sesiones de transferencia de conocimiento, sesiones de verificación funcional de la solución de cumplimiento y comités de seguimiento convocados por la supervisión, en la sede central de la PGN (Carrera 5 No. 15-80) y demás sedes de la Entidad en Bogotá D.C., con convocatoria de la supervisión con una antelación mínima de dos (2) días hábiles.

10. ENTREGABLES MÍNIMOS

No.	Entregable	Contenido mínimo	Periodicidad / plazo
1	Certificación de renovación	Certificación del fabricante Aranda Software, dirigida a la PGN, que acredite la renovación y activación de la totalidad de las suscripciones y licencias por treinta y seis (36) meses continuos, con componente, cantidad, fecha de inicio y fecha de terminación. No se acepta por periodos anuales ni expedida únicamente por el canal.	Al inicio de la vigencia
2	Inventario de licenciamiento	Relación de productos, cantidades, fechas de inicio/fin y datos de soporte.	Dentro de los primeros 5 días hábiles
3	Plan de soporte y escalamiento	Canales, horarios, responsables, personal de guardia, matriz de escalamiento y procedimiento para P1/P2.	Dentro de los primeros 5 días hábiles
4	Informe mensual de servicio	Casos, prioridades, tiempos, disponibilidad con su cálculo, cumplimiento de ANS, escalados al fabricante, problemas recurrentes, acciones de mejora, registros sin edición de los canales y evidencias de sincronización de Mirroring.	Mensual
5	Documentación de actualización	Notas de versión, cambios relevantes, riesgos, recomendaciones, plan de actualización y evidencias de actualización cuando aplique.	Por evento
6	Informe final	Consolidado de licenciamiento, soporte, ANS, incidentes relevantes, actualizaciones y recomendaciones de continuidad.	Al cierre
7			

Documento generado el 2026-11-19 14:05 · Verificable en línea con el código SIGFIC-C1BE39B280D59A25

	Acta de línea base	Estado inicial de componentes, información e integraciones, conforme al numeral 5.1.	Dentro de los 5 días hábiles siguientes al acta de inicio
8	Informe de activación y pruebas de continuidad	Resultado de las pruebas mínimas del numeral 5.2, con evidencias.	Previo al recibo a satisfacción

11. CRITERIOS DE RECIBO Y ACEPTACIÓN

11.1. Verificación de las cantidades, componentes y vigencia contratada, frente a la certificación del fabricante por treinta y seis (36) meses continuos.

11.2. Verificación de que los accesos, usuarios, configuraciones, integraciones, histórico e información se mantienen disponibles, frente al acta de línea base.

11.3. Resultado satisfactorio de las pruebas mínimas de continuidad.

11.4. Verificación del acceso a los canales de soporte y escalamiento.

11.5. Entrega de las certificaciones y documentos requeridos.

11.6. Ausencia de afectaciones atribuibles a la renovación que impidan la operación normal de la herramienta.

11.7. Aprobación por parte de la supervisión contractual de los entregables correspondientes.

12. OBLIGACIONES TÉCNICAS ESPECÍFICAS DEL CONTRATISTA

12.1. Garantizar la continuidad del licenciamiento y soporte durante toda la vigencia contractual.

12.2. Mantener un único punto de contacto y una matriz de escalamiento actualizada.

12.3. Gestionar directamente con el fabricante los casos que requieran soporte de segundo o tercer nivel.

12.4. No realizar cambios en producción que puedan afectar el servicio sin coordinación y autorización previa de la PGN, salvo acciones urgentes de recuperación debidamente justificadas.

12.5. Informar oportunamente vulnerabilidades, fin de soporte, cambios de versión o condiciones que puedan afectar la operación de los componentes contratados.

12.6. Acompañar las actividades de prueba requeridas por la PGN ante cambios de versión o actualización relevante.

12.7. Suscribir el acta de línea base y ejecutar las pruebas mínimas de continuidad.

12.8. Mantener activa la réplica de Aranda Mirroring Database hacia el repositorio administrado por la PGN.

12.9. Entregar sin edición los registros de los canales de atención y aplicar las reglas de medición de ANS de esta ficha.

12.10. Cumplir los ANS, condiciones de seguridad y obligaciones de confidencialidad definidas en la presente ficha y en el contrato.

13. CONSIDERACIONES DE CONTINUIDAD Y SALIDA

13.1. Al finalizar la vigencia, y cuando la PGN lo requiera, el contratista deberá apoyar la entrega ordenada de la información técnica y operativa necesaria para asegurar la continuidad del servicio, incluyendo inventario de licencias, casos abiertos, configuraciones relevantes, documentación disponible y exportación de información que se encuentre bajo su control. Esta obligación no implica transferencia de propiedad intelectual del fabricante, pero sí debe evitar dependencia técnica injustificada sobre la información institucional.

Aspecto	Condición
Contenido	Tickets con su historial y bitácoras, adjuntos, catálogo de servicios, base de conocimiento, ANS configurados, usuarios, roles y perfiles, CIs de la CMDB con sus atributos y relaciones, inventario de ADM, y políticas y resultados de la solución de cumplimiento.
Formato	Archivos CSV o XLSX con diccionario de datos para la información estructurada; adjuntos en su formato original; copia de la base de datos en el formato nativo que permitan las herramientas del fabricante.
Medio de entrega	

	Canal cifrado SFTP o repositorio institucional que indique la OTITD, o unidad de almacenamiento cifrada entregada en la OTITD, con acta de entrega y suma de verificación (hash) de los archivos.
Plazos	Solicitud de la PGN con mínimo 60 días calendario de antelación al vencimiento; entrega dentro de los 15 días hábiles siguientes; revisión de la PGN en 10 días hábiles; corrección de inconsistencias en 5 días hábiles. Todo dentro de la vigencia de 36 meses.
Responsabilidades	Contratista: ejecuta la extracción y gestiona ante el fabricante lo que requiera su intervención. Fabricante: habilita, a través del contratista, las herramientas de exportación. PGN: designa el medio de recepción y revisa la información.

4. Anexos de la ficha

La ficha no relaciona anexos.

Elaboró	Revisó	Aprobó

Verificación de autenticidad

Código: **SIGFIC-C1BE39B280D59A25**

Escanee el código QR o consulte el código en el portal para validar el documento.

APROBADO