Ficha Técnica Contractual

Documento aprobado · Código de verificación SIGFIC-914B5BB04B204F4C

1. Identificación

Número interno	FT-2026-00002	**Versión**	17
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, 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, sin interrupción entre la vigencia actual y la renovación. Conservar las configuraciones, catálogos, flujos, reglas, integraciones, históricos, base de conocimiento, usuarios, roles, CIs y demás información existente en la plataforma. Proveer acceso a actualizaciones, correcciones, nuevas versiones compatibles y soporte técnico especializado durante toda la vigencia. Mantener la operación en modalidad Cloud/SaaS de los componentes que actualmente se suministran 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 definidos. 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.

Modalidad	Electrónica
Paso Actual	0
Entregables	Renovación, implementación y activación por treinta y seis (36) meses de las suscripciones y licencias de la plataforma Aranda Service Management y sus componentes asociados, de acuerdo con las cantidades definidas en la ficha técnica. El contratista deberá entregar certificación de activación y vigencia del licenciamiento, 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; atender y gestionar incidentes técnicos de acuerdo con los ANS definidos; escalar al fabricante los casos que lo requieran y efectuar seguimiento hasta su solución; preservar la integridad, disponibilidad y configuración de la información existente; informar previamente mantenimientos programados; y entregar reportes periódicos sobre disponibilidad, incidentes, cumplimiento de ANS y actividades de soporte.
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, resulta necesaria para asegurar

Documento generado el 2026-11-05 20:18 · Verificable en línea con el código SIGFIC-914B5BB04B204F4C

	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 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. 4.950 dispositivos cubiertos por la solución de cumplimiento normativo para seguridad de la información. La renovación deberá garantizar: continuidad sin interrupción; conservación de información y configuraciones; actualizaciones; hotfixes; parches; versiones soportadas; soporte técnico; escalamiento al fabricante; documentación; transferencia de conocimiento cuando existan cambios relevantes; disponibilidad mensual mínima del servicio Cloud de 99,5 %; atención de incidentes críticos con respuesta máxima de 30 minutos; 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

ALCANCE

· Mantener vigente el derecho de uso de los componentes licenciados durante 36 meses, sin interrupción entre la vigencia actual y la renovación.

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

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

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

· Complementar la renovación de soporte y de una solución de auditoría y cumplimiento de postura de seguridad en los dispositivos de la entidad

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

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

COMPONENTES Y CANTIDADES A RENOVAR

Ítem	Tipo	Componente / requerimiento	Cantidad	Vigencia (meses)

Documento generado el 2026-11-05 20:18 · Verificable en línea con el código SIGFIC-914B5BB04B204F4C

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

COMPONENTES Y CANTIDADES PARA RENOVAR

Ítem	Tipo	Componente / requerimiento	Cantidad	Vigencia (meses)
1	Usuario	Solución de cumplimiento normativo para la seguridad de la información	4950	36

REQUERIMIENTOS FUNCIONALES Y TÉCNICOS MÍNIMOS

Aranda Service Management Suite (ASMS)

· Plataforma de Enterprise Service Management / IT Service Management para gestionar, integrar y automatizar procesos de soporte y entrega de servicios.

· Mesa de ayuda multicanal con registro y gestión de casos mediante portal de autoservicio web, correo electrónico y canales integrados.

· Gestión de incidentes, solicitudes/requerimientos, problemas, cambios y niveles de servicio.

· Configuración y medición de SLA/ANS, OLA y contratos de soporte (UC), con tiempos por prioridad, calendarios hábiles y reglas de escalamiento.

· Catálogo de servicios y base de conocimiento para publicación de servicios y artículos de autoayuda.

· Consola de especialistas para gestionar, escalar, documentar y solucionar solicitudes, con trazabilidad e historial.

· Licenciamiento mínimo: 53 usuarios concurrentes y 12 usuarios nombrados durante los 36 meses.

Aranda CMDB Enterprise

Documento generado el 2026-11-05 20:18 · Verificable en línea con el código SIGFIC-914B5BB04B204F4C

· Capacidad para administrar hasta 10.000 Elementos de Configuración (CIs) y cinco (5) consolas de gestión.

· Repositorio centralizado de CIs de hardware, software, servicios, contratos y demás elementos administrados por la PGN.

· Mapeo de relaciones y dependencias entre CIs y servicios, permitiendo análisis de impacto.

· Integración con ASMS para asociar CIs con incidentes, solicitudes y cambios.

· Gestión de información de contratos, garantías, proveedores, costos y ciclo de vida de activos, de acuerdo con las capacidades licenciadas.

Aranda Device Management

· Cobertura mínima para 4.950 dispositivos durante 36 meses.

· Descubrimiento e inventario automático de hardware y software mediante agente.

· Distribución e instalación/desinstalación remota de software y paquetes de configuración.

· Control y asistencia remota sobre estaciones de trabajo para diagnóstico y soporte.

· Gestión de políticas y capacidades de administración de endpoints.

· Gestión automatizada de parches para sistemas operativos y software de terceros, programación de ventanas de mantenimiento y reportes de cumplimiento.

Agente Virtual para Microsoft Teams

· Conector vigente con Microsoft Teams durante 36 meses.

· Creación y seguimiento de tickets desde Teams.

· Autogestión mediante respuestas automáticas y consulta de artículos de conocimiento.

· Notificaciones al usuario sobre creación, avance, actualización y cierre de solicitudes, de acuerdo con las capacidades del producto.

Aranda Mirroring Database

· Servicio de réplica o copia espejo de la base de datos operativa de Aranda Cloud hacia un repositorio secundario de consulta.

· Habilitación de consultas para analítica y reportería sin afectar de manera significativa la carga transaccional del ambiente productivo.

· Disponibilidad de información para herramientas de analítica/BI y consultas autorizadas, bajo controles de seguridad y acceso definidos por la PGN.

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
- La solución debe contar con un único agente que se instale en las estaciones para todas las funciones del producto
- La solución deberá contar con información acerca de la cantidad de dispositivos donde se encuentra el agente desplegado.

- La solución deberá contar con información acerca de la cantidad de dispositivos que tienen política aplicada.
- La solución deberá contar con información detallada de los dispositivos que tienen/no tienen política aplicada.
- La solución deberá contar con información de cantidad de máquinas que cumplen/no cumplen con la política aplicada.
- La solución deberá contar con información detallada de las máquinas que cumplen/no cumplen con la política aplicada.
- La solución deberá contar con información acerca de la cantidad de políticas activas.
- La solución deberá contar con información acerca de la cantidad de las políticas activas en cumplimiento/no cumplimiento.
- La solución deberá contar con información detallada de las políticas activas en cumplimiento/no cumplimiento.
- La solución debe permitir la definición de distintos roles en el sistema, cada rol implica determinados permisos y privilegios en el sistema.
- La solución deberá permitir el despliegue de agente mediante línea de comandos.
- La solución deberá poder permitir la creación de grupos de máquinas, para sectorizar la política a aplicar según la necesidad del negocio.
- La solución deberá contar con un módulo para gestión de políticas que incluya visualización de cumplimiento de política, dispositivos alcanzados, descripción, fecha de creación, activo/no activo.
- La solución deberá permitir la creación de políticas de cumplimiento para los Navegadores Web
- La solución deberá permitir la creación de políticas de cumplimiento para software Antiphishing
- La solución deberá permitir la creación de políticas de cumplimiento para software Antimalware
- La solución deberá permitir la creación de políticas de cumplimiento para software Firewall
- La solución deberá permitir la creación de políticas de cumplimiento para software de Endpoint Encryption
- La solución deberá permitir la creación de políticas de cumplimiento para software VPN Client
- La solución deberá permitir la creación de políticas de cumplimiento para software de Backup
- La solución deberá permitir la creación de políticas de cumplimiento para herramientas de almacenamiento en la nube
- La solución deberá permitir la creación de políticas de cumplimiento para herramientas de comunicación
- La solución deberá permitir la creación de políticas de cumplimiento para Health Agent
- La solución deberá permitir la creación de políticas de cumplimiento para software de Control Remoto
- La solución deberá permitir la creación de políticas de cumplimiento para Virtual Machine
- La solución deberá permitir la creación de políticas de cumplimiento para software de Data Loss Prevention
- La solución deberá permitir la creación de políticas que puedan combinar los diferentes criterios a partir de las diferentes categorías de software que maneja la solución.
- La solución deberá permitir modificar el tiempo de monitoreo, definido como la frecuencia en la que se realizarán las validaciones de cumplimiento en las máquinas.
- La solución deberá permitir la asociación de una política en diferentes grupos de dispositivos.
- La solución deberá permitir la validación de múltiples criterios de configuración del software, incluyendo, como requisito mínimo, la validación de la instalación.

Documento generado el 2026-11-05 20:18 · Verificable en línea con el código SIGFIC-914B5BB04B204F4C

- La solución deberá contar con opción de exportar información en formato Excel asociada de las políticas (SO, descripción, fecha de creación, cantidad de dispositivos, activo/no activo, estado de cumplimiento)
- La solución deberá contar con opción de filtro por dispositivo, que permita identificar grupo, políticas y vulnerabilidades asociadas al equipo.
- La solución deberá contar con un módulo para identificación de vulnerabilidades.
- La solución deberá presentar la información de la vulnerabilidad con descripción (Incluye código CVE), software afectado y la cantidad de dispositivos que registran la misma.
- La solución deberá permitir la categorización de las vulnerabilidades por nivel de criticidad.
- La solución deberá permitir mostrar la cantidad de vulnerabilidades asociadas a cada nivel de criticidad.
- 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
- La solución deberá permitir mostrar información detallada acerca de las vulnerabilidades asociadas al nivel de criticidad. (descripción (Incluye código CVE), software afectado y la cantidad de dispositivos que registran la misma)
- La solución deberá permitir al menos las siguientes actividades:

Ø Evaluación continua de cumplimiento (Compliance Assessment)

• Ejecución automatizada de evaluaciones de cumplimiento sobre endpoints y servidores.• Validación contra políticas de seguridad corporativas y estándares definidos.• Identificación de desviaciones en configuraciones de seguridad.

Ø 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.

Ø 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.

Ø 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.

Ø 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.

Ø Gestión de auditorías y evidencias

Documento generado el 2026-11-05 20:18 · Verificable en línea con el código SIGFIC-914B5BB04B204F4C

- Generación automática de evidencias de cumplimiento.
- Trazabilidad completa de evaluaciones y remediaciones.
- Soporte a auditorías internas, externas y regulatorias.

Ø Reportes y dashboards de cumplimiento

- Visualización en tiempo real del nivel de cumplimiento.
- Indicadores clave: porcentaje de cumplimiento, brechas abiertas, tendencias.
- Reportes ejecutivos y técnicos para toma de decisiones.

Ø Automatización de controles de seguridad

- Programación de evaluaciones periódicas.
- Automatización de respuestas ante incumplimientos.
- Reducción de intervención manual en procesos de compliance.

Ø 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.

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.
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.
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	

APROBADO

	El contratista deberá suministrar 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.

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.

Prioridad	Criterio	Cobertura	Respuesta	Diagnóstico / contención	Restablecimiento / solución
Crítica – P1	Indisponibilidad total del servicio o afectación generalizada que impida la operación de la mesa de servicios, sin alternativa viable.	7x24	≤ 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.	7x24	≤ 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

APROBADO

Documento generado el 2026-11-05 20:18 · Verificable en línea con el código SIGFIC-914B5BB04B204F4C

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

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.

Medición y cumplimiento de ANS

· El tiempo de respuesta se medirá desde la radicación del caso por un canal autorizado hasta la primera atención efectiva del contratista.

· El tiempo de restablecimiento se medirá hasta recuperar el servicio o disponer de una solución temporal aceptable que permita restablecer la operación.

· El reloj del ANS solo podrá suspenderse cuando exista una dependencia documentada de información o acción de la PGN; la suspensión deberá quedar registrada y ser trazable.

· El contratista deberá entregar mensualmente un informe de casos, prioridades, tiempos, cumplimiento de ANS, disponibilidad, causas, incidentes recurrentes, casos escalados a fabricante y acciones de mejora.

· El incumplimiento de ANS será gestionado conforme a las condiciones del contrato y a los mecanismos de seguimiento definidos por la supervisión.

SEGURIDAD, PRIVACIDAD Y GESTIÓN DE LA INFORMACIÓN

· 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.

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

· 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.

Documento generado el 2026-11-05 20:18 · Verificable en línea con el código SIGFIC-914B5BB04B204F4C

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

· 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.

ENTREGABLES MÍNIMOS

No.	Entregable	Contenido mínimo	Periodicidad / plazo
1	Certificación o evidencia de renovación	Documento del fabricante o canal autorizado que acredite la vigencia por 24 meses, componentes y cantidades contratadas.	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, matriz de escalamiento y procedimiento para P1/P2.	Dentro de los primeros 5 días hábiles
4	Informe mensual de servicio	Casos, disponibilidad, cumplimiento de ANS, escalados al fabricante, problemas recurrentes y acciones de mejora.	Mensual
5	Documentación de actualización	Notas de versión, cambios relevantes, riesgos, recomendaciones 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

CRITERIOS DE RECIBO Y ACEPTACIÓN

· Verificación de las cantidades, componentes y vigencia contratada.

· Validación de que los accesos, usuarios, configuraciones, integraciones, histórico e información se mantienen disponibles.

· Validación de acceso a los canales de soporte y escalamiento.

· Entrega de las certificaciones y documentos requeridos.

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

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

OBLIGACIONES TÉCNICAS ESPECÍFICAS DEL CONTRATISTA

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

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

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

· 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.

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

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

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

CONSIDERACIONES DE CONTINUIDAD Y SALIDA

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.

4. Anexos de la ficha

La ficha no relaciona anexos.

Elaboró	Revisó	Aprobó

Verificación de autenticidad

Código: **SIGFIC-914B5BB04B204F4C**

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

APROBADO