Clasificación del bien o servicio	81111500	Ingeniería de Software o Hardware
	81111600	Programadores de Computador
	81111800	Servicios de Sistemas y Administración de Componentes de Sistemas
	81112200	Mantenimiento y Soporte de Software
	81112500	Servicios de Alquiler o Arrendamiento de Licencias de Software de Computador
	43231500	Software Funcional Específico de la Empresa
	43232300	Software de Consultas y Gestión de Datos
	43232304	Software de Sistemas de Manejo de Base de Datos
	43232800	Software de Administración de Redes
	43232801	Software de Monitoreo de Red
	43233700	Software de Administración de Sistemas
	43233701	Software de Manejo de Sistemas de Empresas
Nombre Comercial del Bien o Servicio	SOLUCIÓN DE OBSERVABILIDAD PARA LA INFRAESTRUCTURA TECNOLÓGICA DE LA FISCALÍA GENERAL DE LA NACIÓN	
Calidad	La solución de Observabilidad deberá cumplir la normativa vigente sobre la transferencia internacional, almacenamiento y tratamiento de datos personales, de conformidad con la Circular Externa No. 008 de 2017 de la Superintendencia de Industria y Comercio (SIC), en concordancia con el artículo 26 de la Ley 1581 de 2012, garantizando que la información se almacene y procese únicamente en países con nivel adecuado de protección de datos reconocido por la SIC o cobijados por excepciones legales, siendo admisibles los mecanismos previstos en el artículo 26 de la Ley 1581 de 2012 y en la Circular Externa 008 de 2017 de la SIC (cláusulas contractuales, normas corporativas vinculantes u otros reconocidos por la SIC), debiendo el proveedor informar y documentar la ubicación de los centros de datos y los mecanismos técnicos, organizacionales y contractuales que aseguren su cumplimiento durante toda la vigencia del contrato. El servicio deberá operar bajo un Sistema de Gestión de Seguridad de la Información alineado con los controles y buenas prácticas del estándar ISO/IEC 27001, lo cual el proponente acreditará mediante declaración suscrita por su representante legal en la que describa las políticas, controles y procedimientos de seguridad de la información adoptados para la prestación del servicio SaaS. Asimismo, el proponente deberá declarar la adopción de las prácticas del marco COBIT 2019 en sus procesos de gestión del servicio. En ningún caso se exigirá certificación del producto, del fabricante ni del proveedor del servicio en dichos estándares.	

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Generalidades	La fiscalía general de la Nación requiere una solución integral de Observabilidad de TI de un único fabricante que permita contar con una visibilidad unificada, análisis en tiempo real y de extremo a extremo sobre el estado, desempeño, disponibilidad, seguridad y costos de la infraestructura tecnológica y de los servicios digitales institucionales, soportada en métricas, logs y trazas, y alineada con ANS (SLA, SLO y SLI). La arquitectura requerida es híbrida: la plataforma (procesamiento, almacenamiento, analítica y consola) se exige en modelo SaaS/PaaS, y los componentes de recolección (colectores, gateways y agentes) se despliegan en la infraestructura de la Entidad conforme al numeral 1.5, con hardware, software y licenciamiento a cargo del contratista. El modelo SaaS/PaaS se exige para la plataforma, no para los componentes de recolección. La solución deberá tener como alcance mínimo: • 955 Switches HP. • Dos dispositivos SD-WAN (Aruba EdgeConnect). • Dos dispositivos de balanceo AlteonOS. • Ecosistema de seguridad FORTINET en aproximadamente 28 dispositivos (14 por nodo principal – Bogotá/Cali). • Radware WAF / DDoS. • Ecosistema Symantec en aproximadamente 18 dispositivos / 24.000 End Point. • VMware en 34 servidores. • 272 servidores físicos de los cuales 23 corresponden a Windows Server - IIS. • 684 servidores virtuales de los cuales 193 corresponden a Windows Server - IIS • Ambientes Windows Server: 2003, 2008, 2012, 2016, 2019, 2022 • Ambientes UNIX/LINUX: Linux red hat, LINUX IBM, AIX, Oracle SOLARIS, SVOS, Unity XT, Storage Center, COMMANS VIEW, NETAPP, ROCKY, Virtual Storage Platform (VSP), Storage Virtualization Operating System, IBM Storage Virtualize, QTS LINUX, BeyondRAID) • 5 aplicaciones soportadas en: PHP, JAVASCRIPT, ASP Classic / javascript 3, javascript/HTML, ANGULAR JS, DELPHI, JAVA 1.8, NODE JS, REACT, .NET, INFORMIX D4GL, Microsoft Classic ASP/ javascript 3.0, javascript/HTML, BPMS BPMS, SQL, VIEU, VUE, C# HTML CSS, C# JavaScript, Oracle Database Enterprise Edition, NestJS, Api Web Desarrollada en

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	nest js, App Web Desarrollada en react js versión 1.4.10, HTML con Materialize CSS. • Nube AZURE (33 node pools, Linux) • Nube ORACLE OCI. • Para efectos del dimensionamiento, el proponente deberá contemplar un crecimiento estimado de activos del treinta por ciento (30%) durante la vigencia del contrato, adicional al alcance mínimo aquí descrito. • La observación de los clústeres de contenedores en Azure (AKS) y OCI se realizará mediante el operador nativo de Kubernetes de la solución, cubriendo la totalidad de los nodos activos de los 33 node pools, incluidos los ambientes no productivos; el dimensionamiento deberá contemplar el autoescalado configurado.
Requisitos generales	La solución debe cubrir de forma integral la observabilidad con una solución de un mismo fabricante en arquitecturas SaaS/PaaS con el licenciamiento correspondiente y que soporte como mínimo: 1. **Recolección de Telemetría.** La solución debe permitir la recolección continua y automatizada de telemetría (métricas, logs, eventos y trazas) mediante agentes, colectores o mecanismos sin agente, soportando estándares abiertos como mínimo: OpenTelemetry o equivalentes, SNMP, NetFlow, Syslog y APIs nativas de nube. 2. **Requisitos específicos de Observabilidad.** La solución debe proveer observabilidad de aplicaciones (APM), infraestructura, redes, bases de datos y contenedores, permitiendo análisis de latencia, errores, saturación, dependencias y trazabilidad extremo a extremo de los servicios. 3. **Analítica y Alertamiento.** La solución debe incorporar capacidades de analítica avanzada y AIOps para detección de anomalías, correlación de eventos, reducción de ruido, análisis de causa raíz y predicción de fallas y capacidad. 4. **Visualización y Gestión.** La solución debe ofrecer dashboards personalizables, mapas de servicios, visualización de topologías y reportes ejecutivos y técnicos, incluyendo seguimiento de SLA, SLO y SLI. La solución debe permitir generar reportes de asignación y distribución de costos por servicio, área o unidad organizacional, construidos a partir del consumo de recursos efectivamente observado y exportables a los sistemas financieros y administrativos de la Entidad. La solución no deberá operar como motor de facturación. 5. **Integración y Seguridad.** La solución debe integrarse con la solución de ITSM y CMDB de la Entidad. Así como con las herramientas de seguridad institucionales y canales de atención,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

garantizando cifrado de datos, control de accesos, trazabilidad, auditoría y cumplimiento de cadena de custodia.

6. **Solución de un único fabricante**. La totalidad de las funcionalidades exigidas en la presente ficha debe ser cubierta por módulos, componentes o capacidades del portafolio propio de un mismo fabricante, bajo una misma plataforma nativamente integrada y una única consola de visualización, análisis y alertamiento.

   No se aceptan soluciones conformadas por la agregación de productos de fabricantes distintos, ni el uso de componentes de terceros para cubrir alguna de las funcionalidades requeridas. Lo anterior sin perjuicio del uso de agentes, colectores, exportadores y estándares abiertos (como mínimo OpenTelemetry, SNMP, NetFlow, Syslog, Prometheus u OpenMetrics), ni de las integraciones exigidas con las soluciones institucionales de la Entidad (ITSM, CMDB, Directorio Activo, MFA, SIEM, SOAR y las demás aplicaciones de la Entidad).

   El requisito integraciones aquí admitidas sobre la plataforma de Observabilidad (módulos funcionales, motor de analítica, alertamiento y consola); los dispositivos de red y seguridad de la Entidad (Fortinet, Radware, AlteonOS, Aruba EdgeConnect) no deben ser del fabricante de la solución y su telemetría se recolecta mediante los estándares abiertos e integraciones aquí admitidos.

   El empleo de agentes, colectores y exportadores de estándares abiertos, incluso de código abierto, no constituye incumplimiento, siempre que las funcionalidades de procesamiento, analítica, alertamiento y visualización sean del portafolio del fabricante.

   Se entiende por “única consola” una experiencia de usuario unificada del mismo fabricante, que admite módulos especializados nativamente integrados que compartan autenticación, modelo de datos y correlación, sin que ello constituya agregación de fabricantes distintos.

Por lo anterior, la solución a adquirir debe cumplir con los siguientes requerimientos:

ÍTEM	TABLA DE CONTENIDO
O1.	Recolección de telemetría.
O2.	Requisitos específicos de 4bservabilidad.
O3.	Analítica y alertamiento.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	O4. Visualización y gestión. O5. Integración y seguridad. O6. Gestión de datos. O7. Implementación y soporte.

Requisitos específicos

ÍTEM	TABLA DE CONTENIDO
O1.	**Recolección de telemetría.** Se requiere la recolección de métricas de la plataforma tecnológica de la Fiscalía General de la Nación, en cuanto a:
1.1.	Se requiere que la solución recolecte datos de la plataforma tecnológica institucional por medio de mínimo: - **Recolección de telemetría:** La solución debe permitir la recolección, ingesta y procesamiento continuo y automatizado de telemetría en términos de métricas, LOGs, eventos y trazas de los componentes de la Plataforma Tecnológica Institucional. - **Uso de Agentes:** Recolección por medio de agentes utilizados en Sistema operativos, máquinas virtuales, nodos de contenedores o entornos equivalentes. Estos agentes deben operar a nivel de sistema operativo y/o a nivel de kernel, minimizando el impacto en desempeño, seguridad en la captura de datos de ambientes físicos, virtuales y conectados, (como mínimo Agentes eBPF/OS o equivalentes). - **Exportación de métricas:** La solución debe soportar la recolección de métricas expuestas de sistemas operativos, aplicaciones, bases de datos, plataformas de contenedores, componentes de red y demás componentes de la plataforma institucional, mediante exportes o mecanismos equivalentes, que publiquen información en formatos estándar y abiertos (como mínimo OpenTelemetry, Prometheus y/o OpenMetrics o formatos compatibles) - **Colectores de telemetría para plataformas de red, seguridad y nube.** La solución debe incluir o integrarse con colectores de telemetría que permita la ingesta de información proveniente de la plataforma tecnológica institucional, como mínimo para: ○ **Plataformas de red y seguridad**, mediante protocolos y estándares como SNMP, NetFlow, sFlow, IPFIX, o equivalentes.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		○ **Plataformas SD-WAN,** soluciones de conexión de órbita baja y SASE, mediante los protocolos y APIs que dichas plataformas expongan (SNMP, NetFlow/IPFIX, API REST del orquestador SD-WAN o del proveedor LEO/SASE), bajo modelo sin agente, permitiendo la recolección de métricas de desempeño, calidad de enlace, latencia, jitter, pérdida de paquetes y rutas. El proponente deberá acreditar la integración vía API genérica cuando no exista conector nativo. ○ **Plataformas que generan logs**, mediante Syslog o mecanismos de acceso compatibles. ○ **Plataformas de nube pública o privada,** mediante el consumo de APIs de proveedores de servicios en la nube (como mínimo Azure, Oracle Cloud Infrastructure), bajo un modelo sin agente cuando aplique. ○ **APIs personalizados** de acuerdo con las necesidades de observabilidad. ○ **Parametrización** de acuerdo con las necesidades de la Entidad, entre ellos, SLA, SLO y SLI. ○ Se debe documentar la personalización de la solución, de acuerdo con las necesidades de la Entidad. ○ Se requiere la implementación de los componentes de recolección con transmisiones seguras. ○ En caso de requerirse, se debe realizar la normalización de formatos y de correlación. La ingesta de telemetría de estándares abiertos (OpenTelemetry, Syslog, SNMP) deberá procesarse con las capacidades nativas de la plataforma del fabricante (transformación, filtrado y enmascaramiento de datos sensibles en ingesta).
	1.2.	Se requiere que la solución soporte como mínimo la captura de datos de la plataforma tecnológica institucional con respecto a: - **Trazas, eventos y alarmas.** Orientadas al comportamiento y causalidad de posibles fallos, con base mínimo en: ○ Recorrido completo de una solicitud incluyendo aplicaciones, microservicios, APIs, componentes de red y bases de datos. ○ Eventos como reinicios, despliegues, cambios de configuración, caídas, failovers y cambios de estado.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		○ Alarmas en cuanto umbrales, anomalías o reglas configuradas. - **Monitoreo de experiencia de usuario (Real user monitoring - RUM).** En términos de validación de interacción de usuario final con aplicaciones institucionales para observar como mínimo: ○ Tiempos de cargas reales. ○ Errores recibidos por el usuario. ○ Comportamientos por ubicación, navegadores, dispositivos, tipo de red. - **Configuraciones y posturas.** Entendidas como la detección de cambios de configuración y de desviaciones respecto de la línea base de comportamiento de los componentes observados (servidores, red, nube y aplicaciones), y su correlación con eventos de desempeño y disponibilidad, sin exigir un módulo independiente de gestión de cumplimiento normativo (GRC) ni de postura de seguridad (CSPM). - **Monitoreo sintético.** En cuanto a ejecución proactiva y controlada de transacciones para medir como mínimo disponibilidad, latencia, tiempos de respuesta, cumplimiento de SLA.
	1.3.	**LOGs de la plataforma tecnológica.** Se requiere la ingesta de los LOGs generados en los diferentes componentes de la plataforma tecnológica institucional (estructurado o no estructurados), mínimo con respecto a: • Servidores, equipos de red y de seguridad. • Aplicaciones institucionales. • SIEM de la Entidad. • SOAR de la Entidad.
	1.4.	**Trazas efectuadas en la plataforma tecnológica.** Se requiere que la solución permita identificar la trazabilidad de extremo a extremo en mínimo: • Ver cada salto de los componentes que intervienen en un servicio. • Ubicar posibles fuentes de fallo. • Propagar el contexto para identificar la traza.
	1.5.	Los componentes de recolección de datos se deben instalar en sitio para obtener datos de cada uno de los componentes de la plataforma tecnológica descrita en los requisitos

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		generales. En caso de requerirse servidores físicos o virtuales, el contratista debe proveer el hardware, software y licenciamiento necesario sin costo adicional para la Entidad en modelo de servicio. Para los componentes cuyo sistema operativo o entorno de ejecución no cuente con soporte vigente del fabricante de la solución para la instalación de agentes, se aceptará la recolección de telemetría mediante mecanismos sin agente (SNMP, WMI, SSH, Syslog, API o equivalentes), con alcance de disponibilidad, desempeño e indicadores de sistema operativo. El proponente deberá declarar en su oferta el tratamiento previsto para cada tecnología del alcance. Los componentes con soporte vigente deberán observarse con agente y trazabilidad completa. El proponente deberá declarar expresamente si su modelo de logs requiere indexación previa, filtros de retención, rehidratación o restauración desde archivo para consultar información histórica, así como las unidades de cobro aplicables. Durante la vigencia del contrato no se generarán costos variables para la Entidad por ingesta, consulta o retención.
	O2.	**Requisitos específicos de observabilidad.**
	2.1.	**Observabilidad general de la plataforma tecnológica.** Se requiere el monitoreo de la plataforma institucional, mínimo de: • Indicadores de tráfico. • Flujo de red. • Indicadores de desempeño de servidores físicos y virtuales, contenedores, almacenamiento, seguridad y Redes. • Indicadores en bases de datos en cuanto a monitoreo de queries, desempeño, locks, deadlocks, métricas de entrada y salida, aspectos de correlación con las aplicaciones. • Indicadores de uso de ancho de banda en los enlaces de las redes de datos de la Entidad.
	2.2.	Observabilidad de aplicaciones (APM). Se requiere como mínimo las siguientes funcionalidades: • Monitoreo de transacciones. • Identificación de cuellos de botella. • Análisis de código. • Perfilamiento de aplicaciones.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		• Monitoreo de dependencias. La instrumentación APM con agente (monitoreo de transacciones, análisis de código y perfilamiento) aplica a las tecnologías con soporte vigente del fabricante (Java, .NET, Node.js, PHP, JavaScript). Las aplicaciones en Delphi, ASP clásico, Informix 4GL y BPMS se observarán mediante monitoreo sintético, RUM cuando expongan interfaz web, observabilidad de infraestructura (servidor, IIS, base de datos) y trazabilidad de sus dependencias. El proponente deberá declarar en su oferta el tratamiento previsto para cada aplicación. Indicadores requeridos: • Latencia. • Desempeño. • Tasa de errores. • Saturación.
	2.3.	Observabilidad de infraestructura. La solución debe soportar como mínimo: • Descubrimiento automático • Monitoreo de capacidad • Monitoreo de disponibilidad • Gestión de eventos.
	2.4.	Observabilidad de red. La solución debe soportar como mínimo: • Análisis de tráfico. • Monitoreo de latencia. • Pérdida de paquetes. • Mapas de topología de red, que representen con actualización automática las dependencias y rutas de comunicación entre los componentes observados y los servicios institucionales, así como la relación de los dispositivos de red monitoreados con dichos servicios. El descubrimiento de topología física de capas 2 y 3 podrá acreditarse mediante integración con la plataforma de gestión de red de la Entidad.
	2.5.	Observabilidad de bases de datos. La solución debe realizar como mínimo: • Monitoreo de consultas.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		• Análisis de tendencias de queries. • Identificación de Deadlocks. • Monitoreo de índices. • Correlación con aplicaciones.
	2.6.	Observabilidad de contenedores. La solución debe realizar como mínimo: • Monitoreo de PODs • Monitoreo de cluster. • Trazabilidad de servicios. • Análisis de recursos de contenedores.
	2.7.	Trazabilidad de la gestión de cambios. La solución debe realizar como mínimo: • Integrarse con la solución de ITSM/CMDB implementada en la Entidad. • Identificación de la línea base de comportamiento normal (ambientes de QA y de producción). • Identificación de dependencias asociadas al cambio. • Identificación y priorización de riesgos técnicos y operativos; de posibles impactos en el servicio o funcionamiento de la plataforma que se va a modificar. • Monitoreo del impacto del cambio en tiempo real en términos mínimos de errores, latencia y fallos. • Generación de alertas. • Generación de Ticket en la herramienta de ITSM implementada en la Entidad.
	O3.	**Analítica y alertamiento.**
	3.1.	Se requiere el análisis para mínimo: • Predicción de saturación. • Degradación progresiva. • Detectar anomalías (observabilidad full-stack o equivalente). • Detección de patrones de comportamiento de la plataforma institucional. • Cambios en el comportamiento de la plataforma institucional. • Picos de carga. • Realizar análisis exploratorio.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		• Realizar análisis predictivo. La solución debe contar con capacidades propias de inteligencia artificial y aprendizaje automático, bajo un modelo que garantice el aislamiento lógico de la información de la Entidad, que los datos institucionales no sean empleados para el entrenamiento de modelos del fabricante ni de terceros, y que su procesamiento se efectúe en las regiones permitidas conforme al acápite Calidad de esta ficha. No se exige infraestructura físicamente dedicada: es admisible el aislamiento lógico del tenant con compromiso contractual del fabricante. Las capacidades de IA deben ser nativas del fabricante e incluidas en el valor del contrato; no se admite trasladar a la Entidad la provisión de modelos de lenguaje o claves (BYOLLM/BYOK). El motor de IA debe cubrir la totalidad del alcance observado (infraestructura, red, nube, aplicaciones, bases de datos y contenedores) con análisis de causa raíz automático. La solución debe aprender de forma automática y continua el comportamiento de la infraestructura y los servicios, mantener líneas base por servicio sin definición manual de umbrales, derivar el alertamiento de dichas líneas base de manera trazable al dato observado y realizar el análisis de causa raíz apoyado en el mapa de dependencias descubierto por la plataforma, consolidando las alertas sintomáticas en un único evento con la causa identificada y su evidencia. El proponente deberá aportar documentación oficial del fabricante que respalde cada una de estas capacidades. El proponente deberá dimensionar y declarar en su oferta el volumen de uso de las capacidades de IA y del asistente conversacional incluido en el licenciamiento, suficiente para la operación descrita en esta ficha. Durante la vigencia del contrato no se generarán cobros adicionales para la Entidad por consulta, investigación, evento procesado o consumo, y el contratista garantizará la continuidad del servicio sin costo si dicho volumen se agotara. La solución debe cumplir como mínimo: • Detección automática de anomalías. • Correlación automática de eventos. • Reducción de ruido de alertas. • Predicción de fallas. • Análisis de causa raíz. • Análisis predictivo de capacidad.
	3.2.	La solución debe soportar la gestión de alertas con mínimo: • Motor de alertas configurable.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		• Alertas basadas en umbrales. • Alertas basadas en anomalías. • Supresión de alertas duplicadas. • Escalamiento automático.
	3.3.	Se requiere una capacidad de analítica y detección, como mínimo de: • Ubicación de componente de fallo. • Detección de anomalías en tiempo real. • Detección de errores intermitentes. • Fallas en cadena de servicios. • Prospectivas de prevención de fallas detectadas bajo datos históricos. • Identificar dependencias. • Visualizar flujos de producto de la detección realizada. Para esto se requiere el uso de aprendizaje automático (ML) para la detección de anomalías y el establecimiento de líneas base de comportamiento de las plataformas y servicios tecnológicos. Se considera deseable, sin constituir requisito excluyente, que la solución incorpore capacidades de análisis de comportamiento de usuarios y entidades (UEBA) o permita alimentarlas mediante la integración con el SIEM de la Entidad.
	3.4.	La solución debe como mínimo: • Generar alertas automáticas y definir umbrales de alertamiento. • Reducir el ruido por alertas duplicadas o irrelevantes. • Escalamiento para la gestión de eventos y alertas. • Generación de alarmas de cumplimiento de SLA, SLO, SLI. • Configuración de bots de operación, entendidos como la automatización de respuestas ante alertas (ejecución de acciones o flujos predefinidos, notificaciones y creación de tickets en la herramienta ITSM) mediante las capacidades nativas de automatización de la plataforma, sin exigir un motor RPA independiente.
	O4.	**Visualización y gestión.**
	4.1.	La solución debe permitir como mínimo: • Filtrados dinámicos. • Correlación entre telemetría capturada.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		• Análisis de LOGs. • Análisis exploratorio. • Análisis histórico.
	4.2.	Se requiere la representación de: • Topología y dependencias. • Topologías de flujos de servicios. • Exploración de trazas • Llamado de servicios. • Visualización de degradación de servicios. • Identificación de servicios críticos.
	4.3.	Personalización de Dashboard para contar con observabilidad de mínimo: • Anchos de banda de los enlaces de transmisión de datos soportados por la red WAN y LAN de las redes de la Entidad. • Plataformas tecnológicas implementadas en diferentes nubes como Azure y Oracle. • Calidad de los servicios tecnológicos soportados por la Plataforma tecnológica de la Fiscalía General de la Nación. • La solución debe permitir la generación mínima de 20 Dashboards.
	4.4.	Visualizar el cumplimiento de los SLA, SLO y SLI establecidos en la Entidad. Esta capacidad podrá acreditarse mediante tableros, alertas de umbral y reportes configurables sobre las métricas observadas, sin exigir un módulo con esa denominación comercial, siempre que permita definir objetivos por servicio, medir su cumplimiento en periodos configurables y generar alertas ante su incumplimiento.
	4.5.	Asistente conversacional de la solución. La solución debe contar con un asistente conversacional nativo del fabricante que permita a la mesa de ayuda y a los funcionarios designados por la Entidad formular consultas en lenguaje natural y obtener respuestas sobre la telemetría recolectada, el estado y desempeño de los servicios, las alertas generadas y los incidentes y análisis previamente registrados en la plataforma, incluyendo resúmenes y orientación sobre eventos ya diagnosticados. El licenciamiento y uso de esta capacidad debe estar incluido en el valor del contrato, sin cargos variables por consulta, investigación o consumo adicional para la Entidad. El proponente deberá dimensionar y declarar en su oferta el volumen de uso incluido, suficiente para la operación descrita;

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		durante la vigencia del contrato no se generarán cobros adicionales por consulta, investigación o consumo, y el contratista garantizará la continuidad del servicio sin costo si dicho volumen se agotara.
	4.6.	Automatización de reportes o dashboard de los servicios prestados por parte de terceros.
	O5.	**Integración y seguridad.**
	5.1.	Se requiere la integración con las soluciones institucionales de: • Herramienta de ITSM (SaaS/PaaS). • Gestión de activos CMDB (SaaS/PaaS). • Directorio Activo (DA). • Control de acceso MFA.
	5.2.	Capa de seguridad. Se requiere contar con: • Auditabilidad y trazabilidad del uso de la solución. • Cifrado de datos sensibles. • Definición de perfiles y roles. • Debe incluir mecanismos, procedimientos o procesos de cumplimiento de cadena de custodia de datos, LOGs y reportes generados en el momento de requerirse.
	5.3.	Se requiere que la solución transmita datos de manera cifrada con mínimo las siguientes características: • Cola o mensajería intermedia cifrada, cuando la arquitectura ofertada la utilice (por ejemplo Kafka o AMQP). • Transmisión cifrada con TLS 1.2 o superior y certificados digitales en todos los componentes. • Autenticación mutua (mTLS) o mecanismo equivalente de autenticación de componentes cuando la arquitectura ofertada lo soporte. • Firma o mecanismo de verificación de integridad de la información transmitida y de las evidencias generadas.
	O6.	**Gestión de datos.**
	6.1.	Capa de almacenamiento. La solución debe contar con una capacidad de almacenamiento que permita la retención de la información de acuerdo con la línea base de la plataforma tecnológica descrita en el acápite Generalidades de esta ficha,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		garantizando la integridad, disponibilidad y confidencialidad de la información, con las siguientes retenciones mínimas diferenciadas por tipo de telemetría: (i) métricas agregadas e indicadores de ANS: por toda la ejecución del contrato, por cuanto soportan la medición oficial frente a los proveedores de la Entidad; (ii) trazas (iii) logs operativos (iv) logs de auditoría y seguridad durante la ejecución del contrato y entrega de históricos al finalizar.
	6.2.	Módulo de auditoría. La solución debe permitir como mínimo: - Traza de accesos realizados a la solución. - Acceso a los LOGS de la solución. - Generación de reportes. - Trazabilidad de los cambios de políticas, reglas de alertamiento, permisos y configuraciones de la plataforma, con registro de autor, fecha y valor anterior, exportable para fines de auditoría.
	O7.	**Implementación y soporte.**
	7.1.	Instalación y configuración. El contratista deberá realizar como mínimo las siguientes actividades: • Aprovisionamiento de todos los componentes (hardware, software, licenciamiento, servicios en la nube) necesarios para el correcto funcionamiento de la solución sin costo adicional para la Fiscalía General de la Nación. • Configuración de todos los componentes de la solución para soportar la funcionalidad requerida en esta ficha, sin costo adicional para la Entidad, conforme a los siguientes hitos verificables: (i) fase inicial de diseño y aprobación de la arquitectura de seguridad, zonas de gestión y políticas de acceso, previa al despliegue en producción, con duración no inferior a diez (10) ni superior a quince (15) días hábiles, que hace parte del primer hito; (ii) al término del primer mes, contado desde la entrega de accesos y la aprobación de la arquitectura de seguridad por la Entidad: despliegue de la plataforma, habilitación de la recolección e integraciones y cobertura de los servicios críticos que la Entidad priorice; (iii) al término del tercer mes: cobertura de la totalidad del alcance, de manera concurrente con el acompañamiento del numeral 7.4. Los plazos se suspenderán durante el

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		tiempo que demande la aprobación institucional de ventanas de mantenimiento. • El recibo de la implementación se acreditará mediante un protocolo de pruebas de aceptación funcional por cada ítem de los requisitos específicos, ejecutado durante la puesta en funcionamiento (numeral 7.4) y verificado por la supervisión, con lista de verificación firmada, como criterio objetivo de recibo de la implementación y de inicio de la fase de acompañamiento. Para las capacidades de IA/ML, correlación, análisis de causa raíz y predicción, el proponente deberá aportar documentación oficial del fabricante que respalde cada capacidad y demostrar su funcionamiento sobre los servicios de la Entidad en dicha fase.
	7.2.	Se requiere el licenciamiento de la solución, expedido por un mismo fabricante y que cubra la totalidad de los módulos y funcionalidades exigidas en esta ficha, para realizar la observabilidad de mínimo lo descrito de acuerdo con la línea base de la plataforma tecnológica descrita en el acápite Generalidades de esta ficha. Los licenciamientos deberán ser generados a nombre de la Fiscalía General de la Nación.
	7.3.	El contratista debe proveer el hardware, software, firmware y licenciamiento necesario para el correcto funcionamiento de la solución sin costo adicional para la Entidad.
	7.4.	Puesta en funcionamiento. Se requiere por espacio de tres meses el acompañamiento en la puesta en funcionamiento de la solución con la configuración inicial de: • Recolección de métricas. • Análisis y construcción de dashboard.
	7.5.	Soporte del funcionamiento de la solución. Se requiere un soporte en la operación de la solución por mínimo doce (12) meses con mínimo: - Identificación de problemas o incidentes de operación. - Elaboración de informes mensuales de incidentes de operación detectados y de las soluciones aplicadas. - Implementación de recolección de métricas requeridas.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

<table>
<tr><td></td><td></td><td>En caso de presentarse fallas o necesidades de integración el contratista debe suministrar el personal técnico especializado para atender los requerimientos de soporte.</td></tr>
<tr><td></td><td>7.6.</td><td>Soporte.

Se requiere de personal en modalidad 5x8 durante el periodo de soporte requerido de manera virtual (el contratista debe proveer los equipos e infraestructura necesaria sin costo adicional para la entidad), con los siguientes roles (la experiencia mínima de dos (2) años exigida podrá acreditarse de forma acumulada en uno o varios contratos, y las certificaciones exigidas son las vigentes del fabricante de la solución ofertada, en implementación o configuración para el operador y en uso u operación para el analista):

• Un (1) operador.

<table><tr><th>PERFIL PROFESIONAL</th><th>EXPERIENCIA</th></tr><tr><td>Un (1) tecnólogo o ingeniero (Electrónico, sistemas, industrial, telecomunicaciones o a fines)</td><td>Experiencia profesional de dos (2) años a partir de la expedición de la tarjeta profesional.

Experiencia mínima de dos (2) años implementando o configurando la solución de observabilidad del fabricante ofertado.

Certificación vigente expedida por el fabricante de la solución ofrecida, en implementación o configuración de dicha solución.</td></tr></table>
<table><tr><th>FUNCIONES</th></tr><tr><td>• Implementar la solución de Observabilidad alineada con las mejores prácticas de administración de este tipo de soluciones.
• Gestionar recursos necesarios para el correcto funcionamiento de la solución.
• Realizar las integraciones requeridas por la Entidad.
• Participar en reuniones de entendimiento de necesidades de observabilidad y realizar la conexión a los dispositivos a observar que requiera la Entidad.
• Personalizar la herramienta Observabilidad de acuerdo con los requerimientos mínimos exigidos en esta ficha.</td></tr></table></td></tr>
</table>

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

- Colaborar con equipos multidisciplinarios para asegurar la correcta adopción y uso de la herramienta implementada.
- Documentar procesos y configuraciones realizadas para facilitar la transferencia de conocimiento y soporte técnico.
- Monitorear el desempeño de la solución implementada y proponer mejoras continuas basadas en métricas clave (KPI).
- Garantizar el cumplimiento de estándares de calidad y seguridad en la implementación y operación de la solución.

- Un (1) Analista de observabilidad.

PERFIL PROFESIONAL	EXPERIENCIA
Un (1) ingeniero (Electrónico, sistemas, industrial, telecomunicaciones o a fines)	Experiencia profesional de dos (2) años a partir de la expedición de la tarjeta profesional. Experiencia mínima de dos (2) años en uso u operación de la solución de observabilidad del fabricante ofertado. Certificación vigente expedida por el fabricante de la solución ofrecida, en uso u operación de dicha solución.

FUNCIONES
• Configurar y personalizar tableros, acorde a las necesidades de la entidad. • Participar en reuniones de análisis y determinación de acciones correctivas para solucionar las posibles causas/raíz de casos de fallas o de requerimientos de la Entidad. • Apoyar en el análisis de requerimientos técnicos y presentar los informes mensuales de las actividades realizadas. • Colaborar con equipos multidisciplinarios para asegurar la correcta adopción y uso de la herramienta implementada. • Documentar procesos y configuraciones para facilitar la transferencia de conocimiento y soporte técnico. • Capacitar a usuarios finales y especialistas o gestores, en el uso adecuado de la solución. • Monitorear el desempeño de las automatizaciones implementadas.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

		• Garantizar el cumplimiento de estándares de calidad en el análisis y presentación de los resultados obtenidos con el uso de la solución.
	7.7.	**Acuerdos de niveles de servicio.** La prestación del servicio de soporte se realizará bajo los siguientes niveles de servicio (ANS). Los tiempos de diagnóstico y restauración aplican a los incidentes atribuibles al contratista (configuración, integraciones, componentes de recolección, agentes y servicios de su personal). La disponibilidad de la plataforma SaaS se regirá por el acuerdo de nivel de servicio publicado por el fabricante, el cual el contratista deberá acreditar en su oferta y gestionar ante el fabricante en favor de la Entidad, incluidas las compensaciones que procedan. La Entidad será responsable de la entrega oportuna de accesos y de la aprobación de las ventanas de mantenimiento requeridas; los tiempos se suspenderán mientras dichas condiciones estén pendientes por parte de la Entidad: Prioridad Alta: Se define cuando la plataforma o cualquiera de sus módulos quedan fuera de servicio. El incidente debe ser diagnosticado en un tiempo no mayor a 30 minutos y se contará a partir de la notificación por correo electrónico que defina el proveedor. Solución: La restauración del servicio no debe superar las dos (2) horas después del diagnóstico. Prioridad media: Se define cuando la plataforma o cualquiera de sus módulos presentan intermitencia. El incidente debe ser diagnosticado en un tiempo no mayor a 30 minutos y se contará a partir de la notificación por correo electrónico que defina el proveedor. Solución: La restauración del servicio no debe superar las cuatro (4) horas después del diagnóstico. Prioridad baja: Se define cuando la plataforma presenta fallas que no se consideren prioridad alta y media. El incidente debe ser diagnosticado en un tiempo no mayor a 30 minutos y se contará a partir de la notificación por correo electrónico que defina el proveedor. Solución: La restauración del servicio no debe superar las ocho (8) horas después del diagnóstico.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	7.8.	**Transferencia de conocimiento:** Se requiere la transferencia en la configuración y operación de la solución para los funcionarios de la Subdirección de Tecnología de la Información y las Comunicaciones y contratistas que requieran el uso de la plataforma, sin límite de usuarios, con una intensidad mínima de cuarenta (40) horas en modalidad mixta. En caso de que se requiera se deberán realizar capacitaciones en cualquier momento de acuerdo con las necesidades e implementaciones que se realicen en la ejecución del contrato. **Manuales de operación:** Se debe entregar un manual de operación de la solución para usuario final en donde se encuentre la administración de la plataforma. De igual manera se debe entregar los ejecutables, licenciamiento que se están usando bajo plataforma.
Empaque y rotulado	N/A	
Presentación y Unidad de Medida	N/A	

Elaboró	José Luis Daza Pérez	30/09/2026	
Aprobó	Eric Mauricio Vargas Forero	30/09/2026	

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada