1	REQUERIMIENTOS GENERALES	CUMPLE	NO CUMPLE
1.1	El contratista brindará servicios de soporte técnico especializado para los siguientes productos instalados en la infraestructura de la Policía Nacional: Sistema Operativo Linux: Red Hat Enterprise Linux versiones 7.x/8.x/9.x/10.x, Oracle Linux versiones 7.x/8.x/9.x/10.x, Ubuntu. Incluyendo Filesystems, Docker y Kubernetes. Virtualizadores: KVM versión 4.x o superior, Oracle Linux Virtualization Manager (OLVM). Bases de Datos: Oracle Database Enterprise Edition versiones 12c, 18c, 19c, 21c y 26ai; PostgreSQL. Herramientas y funcionalidades de Oracle: Diagnostics Pack, Database Lifecycle Management, Partitioning, Multitenant, Tuning Pack, Real Application Clusters (RAC) en contenedor Multitenant, High Availability (HA), RMAN (Recovery Manager), Automatic Storage Management (ASM), Backup and Recovery, Oracle Data Guard, Oracle Data Masking. Servicios de Aplicación: Identity and Access Management versión 11g, Oracle Unified Directory (OUD) versión 12c, WebLogic versiones 12c y 14c, Forms y Reports versión 12c, Business Intelligence (OBIEE) versión 12c, Red Hat JBoss Enterprise Application Platform versión 7.x. Servicios de Monitoreo: Oracle Enterprise Manager Cloud Control.		
1.2	El contratista garantiza la disponibilidad, estabilidad, seguridad y óptimo rendimiento de todos los productos y tecnologías indicados en el numeral 1.1 del presente anexo técnico, mediante la prestación de soporte técnico proactivo y correctivo según corresponda. Adicionalmente, documentará de manera detallada y oportuna todas las actividades realizadas, incluyendo diagnósticos, análisis de causa raíz, ajustes, actualizaciones, optimizaciones y recomendaciones técnicas. Dicha documentación deberá cumplir con los estándares de calidad, mejores prácticas de la industria y los requerimientos establecidos por la Policía Nacional. El servicio de soporte técnico especializado se prestará en modalidad remota o presencial, según la criticidad del evento reportado o por solicitud expresa del supervisor del contrato. Para la asistencia remota, el contratista deberá garantizar una conexión segura mediante el uso de herramientas tecnológicas debidamente licenciadas en origen y destino, asegurando la confidencialidad e integridad de la información. En ningún caso se permitirán conexiones remotas desatendidas o sin la presencia de un administrador de la Policía Nacional designado por el supervisor del contrato, quien será el responsable de autorizar y facilitar el acceso a los recursos tecnológicos necesarios. Esta medida asegurará el control y supervisión adecuados durante la ejecución de las actividades de soporte, manteniendo los estándares de seguridad y cumplimiento institucional.		
1.3	El contratista deberá prestar el servicio especializado de soporte técnico, actualización y afinamiento de las tecnologías mencionadas en el ítem 1.1 (Especificaciones Técnicas Mínimas) del presente anexo técnico, con personal debidamente certificado en las áreas correspondientes. Los servicios se llevarán a cabo en los siguientes sitios: Centro de Procesamiento de Datos Principal: Oficina de Tecnologías de la Información y las Comunicaciones de la Policía Nacional, ubicada en la carrera 59 # 26-21 CAN, Bogotá. Teléfonos: (601) 5159140 – (601) 5159489. Centro de Procesamiento de Datos Alterno: Carrera 106 # 15a-25, manzana 4, lote 38, Datacenter Zona Franca, Bogotá.		
1.4	El contratista garantiza la disponibilidad de personal calificado para atender las necesidades técnicas en los sitios descritos en el ítem 1.3, asegurando la correcta operación, optimización y mantenimiento de las tecnologías mencionadas. Adicionalmente, deberá coordinar con el supervisor del contrato para cumplir con los protocolos de acceso y seguridad establecidos por la Policía Nacional en cada uno de los centros de procesamiento de datos.		

1.5	El contratista ofrecerá una bolsa de 787 horas de servicios profesionales durante el plazo de ejecución del contrato, destinadas al soporte técnico especializado, actualización, afinamiento y mantenimiento de las tecnologías descritas en el Ítem 1.1 (Especificaciones Técnicas Mínimas) del presente anexo técnico. La cantidad de horas se distribuirá proporcionalmente por vigencia fiscal, correspondiendo 112 horas para la vigencia 2026 (1 mes) y 675 horas para la vigencia 2027 (6 meses).		
1.6	El contratista garantiza que las horas contratadas se utilicen de manera eficiente y efectiva, priorizando las necesidades críticas y los requerimientos expresados por el supervisor del contrato o quien haga sus veces.		
1.7	El contratista garantiza la disponibilidad continua de soporte técnico especializado las 24 horas del día, los 7 días de la semana (7x24), para atender los requerimientos que la Policía Nacional necesite, incluyendo el mantenimiento de la plataforma de Bases de Datos, servicios de capa media y sistemas operativos descritos en el ítem 1.1 del presente anexo técnico. Esto implica, la atención inmediata de incidencias, la aplicación de actualizaciones, parches y correcciones necesarias, así como la disponibilidad de personal técnico especializado y herramientas adecuadas para garantizar la operatividad y continuidad de los sistemas.		
1.8	El contratista debe cumplir con los tiempos de respuesta y niveles de servicio acordados en el SLA (*Service Level Agreement*), proporcionar reportes periódicos sobre el estado de los sistemas.		
1.9	El contratista garantiza un tiempo de respuesta máximo de una (1) hora siguiente al reporte del caso, en la plataforma de bases de datos, aplicaciones, OUD y Oracle Linux Virtualization Manager, sistema operativo Linux, descrita en el ítem 1.1. Las fallas reportadas deberán ser solucionadas dentro de las seis (06) horas siguientes al conocimiento del caso.		
1.10	El contratista deberá poner a disposición de la Policía Nacional, de manera permanente, los siguientes medios para el reporte de casos: - Mesa de servicio para el reporte de incidentes, seguimiento y control mediante un coordinador quien notificará los avances del mismo. - Número telefónico. - Correo electrónico. - Número móvil celular de un contacto directo.		
1.11	El contratista deberá crear, actualizar y realizar seguimiento a los casos que se generen en los portales de soporte de la firma y reportar permanentemente los avances o estado de los mismos al supervisor del contrato.		
1.12	El contratista llevará control y entregará el reporte de servicio mediante la mesa de servicio, en la cual debe incluir como mínimo la siguiente información: - Nombre del servicio afectado. - Fecha de atención del servicio. - Tiempo de duración del servicio. - Descripción del problema o falla. - Descripción de la solución o de las actividades realizadas en el servicio intervenido. - Nombre y firma del técnico de servicio. - Nombre y firma de recibo a satisfacción del funcionario solicitante.		
1.13	El contratista debe atender los eventos generados en la plataforma tecnológica de objeto del contrato, en horario 7x24 (24 horas X 7 días de la semana).		
2	**SERVICIO DE BASE DE DATOS**		
2.1	El Contratista será responsable de la solución oportuna y efectiva de los errores reportados en las bases de datos de la Oficina de Tecnologías de la Información y las Comunicaciones. Los errores serán reportados por el supervisor del contrato o quien este designe, a través de los canales de comunicación establecidos por el Contratista y detallados en el ítem 1.6 del Anexo Técnico.		
2.2	El contratista garantiza un tiempo de respuesta máximo de una (1) hora siguiente al reporte del caso.		
2.3	Cada solución debe incluir diagnóstico, corrección, validación y un informe detallado que será entregado al supervisor del contrato dentro de las siguientes 48 horas posteriores a la resolución del incidente, cumpliendo con los estándares técnicos y mejores prácticas de la industria.		
2.4	Cuando estén disponibles en el mercado nuevas versiones estables de la base de datos y su actualización sea proyectada por el supervisor del contrato, el contratista debe generar un plan de trabajo detallado que incluya: las etapas del proceso, los recursos requeridos, los plazos		

	estimados, las pruebas de compatibilidad, los procedimientos de backup y rollback, replica y la minimización del tiempo de inactividad. Dicho plan debe ser presentado al supervisor del contrato para su revisión y aprobación con al menos 15 días hábiles de antelación, su ejecución deberá garantizar la integridad, seguridad y continuidad operativa de la base de datos, cumpliendo con los estándares técnicos y las mejores prácticas.		
2.5	El Contratista debe verificar e identificar cuellos de botella en las bases de datos de manera mensual, ejecutando acciones correctivas y preventivas para optimizar el rendimiento y garantizar la continuidad operativa. Estas actividades incluirán el análisis de métricas de rendimiento, la resolución de problemas identificados y la implementación de medidas proactivas para evitar futuros inconvenientes.		
2.6	El Contratista debe realizar, de manera mensual, la verificación y en caso de ser necesario, ajuste de los parámetros de configuración de las bases de datos, con el fin de garantizar su óptimo rendimiento y alineación con los requerimientos técnicos y operativos de la Policía Nacional.		
2.7	El Contratista debe verificar, en caso de ser necesario, configurar y optimizar de manera mensual el uso de los siguientes recursos en los servidores y bases de datos: Memoria (RAM), Procesamiento (CPU), Operaciones de Entrada/Salida (I/O), tanto físicas como virtuales.		
2.8	El Contratista debe realizar mensualmente la gestión y verificación del espacio en el sistema de base de datos, lo cual incluye: la revisión de la distribución de datafiles, redologs, filegroups, la identificación y corrección de fragmentaciones, y la optimización del almacenamiento para garantizar un uso eficiente de los recursos. Estas actividades deberán ejecutarse conforme a las mejores prácticas recomendadas por la casa fabricante, asegurando la integridad y el rendimiento óptimo de la base de datos.		
2.9	El contratista debe realizar el mantenimiento mensual de los objetos de la base de datos, incluyendo: vistas, vistas materializadas, índices, tablas, paquetes entre otros; con el fin de garantizar su óptimo funcionamiento y rendimiento. Este mantenimiento incluirá la revisión de la integridad de los datos, bloques corruptos, la optimización de índices, la actualización de estadísticas, la depuración de objetos obsoletos y la verificación del correcto funcionamiento de los procedimientos almacenados y funciones.		
2.10	El contratista debe ejecutar reportes de carga de trabajo (AWR, por sus siglas en inglés) de manera mensual o cuando el supervisor lo requiera, con el fin de analizar el comportamiento y rendimiento de las bases de datos. Con base en los resultados obtenidos, se realizarán las acciones necesarias para optimizar el rendimiento, tales como ajustes en la configuración, reestructuración de índices, redistribución de carga o cualquier otra medida técnica que contribuya a mejorar la eficiencia y estabilidad de las bases de datos.		
2.11	El contratista organiza de manera mensual los objetos existentes en la base de datos, realizando el respectivo dimensionamiento de tablas, índices, vistas, paquetes, funciones y demás elementos, con el fin de garantizar su estructura óptima y eficiente. Esta actividad incluirá la revisión del espacio ocupado, la redistribución de almacenamiento, la identificación de objetos fragmentados o subutilizados, y la aplicación de las correcciones necesarias para mejorar el rendimiento y la gestión de recursos.		
2.12	El contratista debe ejecutar mensualmente procesos de optimización sobre los diferentes objetos que conforman las bases de datos, ya sean de tipo OLAP (procesamiento analítico en línea) u OLTP (procesamiento transaccional en línea), incluyendo entre otros, paquetes, triggers, funciones, procedimientos almacenados, índices, tablas, particiones y demás elementos. Estas actividades tendrán como objetivo mejorar el rendimiento de la base de datos, reducir tiempos de respuesta, optimizar el uso de recursos y detectar de manera oportuna situaciones que puedan comprometer la estabilidad de la plataforma tecnológica.		
2.13	El contratista debe realizar, de manera mensual, la validación de las políticas de auditoría implementadas en las bases de datos, asegurándose de que estas cumplan con los estándares establecidos y los requerimientos del cliente. Durante este proceso, se identificarán y ejecutarán los ajustes necesarios para optimizar la efectividad de las auditorías, garantizando que dichas modificaciones no afecten el rendimiento de las bases de datos. El contratista se compromete a llevar a cabo estas actividades de manera no intrusiva, utilizando metodologías que minimicen el impacto operativo y aseguren la continuidad del servicio.		
2.14	El contratista debe realizar, de manera mensual, la verificación y mantenimiento de la configuración de Oracle Data Guard, asegurándose de que la replicación y sincronización entre la base de datos primaria y la base de datos en espera (standby) funcionen correctamente. Esto incluirá la revisión del estado de los procesos de transporte y aplicación de logs, la validación de la integridad de los datos replicados, la detección y resolución de		

	brechas en la sincronización, espacios de almacenamiento y la verificación de los parámetros de configuración para garantizar su alineación con las mejores prácticas.		
2.15	En caso de ser necesario o a solicitud del supervisor del contrato, el contratista debe instalar, configurar y poner en funcionamiento Oracle DataGuard, con el objetivo de garantizar la alta disponibilidad y la replicación de las bases de datos críticas de la Policía Nacional. Esta configuración deberá incluir la sincronización de datos entre la base de datos principal y la secundaria, la implementación de mecanismos de failover automático o manual, y la verificación del correcto funcionamiento de la replicación.		
2.16	El contratista debe revisar mensualmente las políticas de backup implementadas en las bases de datos, evaluando su efectividad mediante pruebas de restauración, consistencia y alineación con las mejores prácticas, con las herramientas dataprotector y veeam backup and replication, según sea el caso. Durante esta revisión, se identificarán oportunidades de mejora y se sugerirán ajustes para optimizar los procesos de respaldo, tales como la frecuencia, el tipo de backup (completo, incremental o diferencial), la retención de copias y la validación de la integridad de los datos. El contratista se compromete a implementar las buenas prácticas recomendadas, garantizando la confiabilidad y disponibilidad de los backups, así como la capacidad de recuperación ante eventuales fallos.		
3	**USUARIO EMPRESARIAL Y AUDITORÍA**		
3.1	El contratista será responsable de brindar soporte técnico, configuración, optimización y en caso de ser necesario la actualización de la plataforma Identity and Access Management (IAM) y Unified Directory (OUD), incluyendo todos sus componentes asociados, tales como bases de datos y sistemas integrados. Estas actividades comprenderán la resolución de incidencias, la implementación de mejoras de rendimiento, la aplicación de parches y actualizaciones de software, así como la gestión y mantenimiento de las bases de datos para garantizar su integridad, disponibilidad y correcto funcionamiento. Todas las acciones deberán ejecutarse previa coordinación y autorización del supervisor del contrato, asegurando el cumplimiento de los estándares de calidad, seguridad y minimizando el impacto en la operación del sistema durante la ejecución de los procedimientos.		
3.2	El Contratista garantizará la conexión y operatividad continua de todos los usuarios activos institucionales mediante soporte técnico especializado y, cuando sea requerido, la actualización de versiones de la plataforma, asegurando su integración con los sistemas Oracle Unified Directory (OUD), Identity and Access Management (IAM) y los conectores licenciados correspondientes (incluyendo expresamente el conector custom Office 365 y el Directorio Activo), comprometiéndose a ejecutar dichas intervenciones previa coordinación y autorización expresa del Supervisor del Contrato, bajo los parámetros de continuidad operativa, estabilidad del sistema y correcto funcionamiento de los servicios, en estricto cumplimiento de los estándares		
3.3	El contratista será responsable de diseñar e implementar la replicación de la plataforma tecnológica de identificación empresarial y gestión de identidades hacia el sitio alterno de la Policía Nacional de Colombia, asegurando la sincronización, disponibilidad y consistencia de los datos entre ambos entornos mediante una prueba de funcionalidad (Disaster Recovery Protocol - DRP). Este procedimiento deberá ejecutarse previa coordinación y autorización del Supervisor del Contrato, garantizando el cumplimiento de los estándares técnicos de seguridad, así como la continuidad operativa de la plataforma.		
3.4	El contratista deberá diseñar, configurar e implementar las estrategias y procesos de respaldo para la plataforma tecnológica de identificación empresarial y gestión de identidades, asegurando la integridad, disponibilidad y recuperabilidad de los datos por medio de pruebas de restauración, documentando el RTO y RPO. Estas actividades se realizarán en coordinación y colaboración con el personal del grupo Administración de Servicios de Infraestructura en la Nube, y previa autorización del supervisor del contrato, garantizando el cumplimiento de los estándares técnicos de seguridad.		
3.5	Todos los procedimientos ejecutados en la plataforma tecnológica de identificación empresarial y gestión de identidades deberán ser debidamente documentados, incluyendo detalles técnicos, configuraciones, procesos, pruebas y buenas prácticas. Adicionalmente, el contratista deberá realizar la transferencia de conocimiento al personal que designe el Supervisor del Contrato, asegurando la comprensión y capacidad operativa necesaria para la gestión y mantenimiento de la plataforma.		
4	**INTELIGENCIA DE NEGOCIOS**		
4.1	El contratista deberá brindar soporte en la administración, optimización, configuración o actualización de la plataforma Business Intelligence Suite Enterprise 12c (BI 12c), incluyendo		

	la gestión de reportes y la bodega de datos. Estas actividades se realizarán a solicitud del supervisor del contrato, garantizando el correcto funcionamiento, rendimiento y actualización de los componentes, así como la generación y mantenimiento de reportes conforme a los requerimientos técnicos y operativos de la institución.		
4.2	En caso de ser necesario, a solicitud del Supervisor del Contrato, el contratista deberá instalar, configurar y poner en funcionamiento Oracle Business Intelligence 12c (BI 12c) o una solución equivalente, con el objetivo de garantizar la implementación y operación de herramientas de inteligencia de negocios que permitan el análisis y la generación de reportes para la Policía Nacional. Esta configuración deberá incluir la integración con las fuentes de datos existentes, la definición de métricas, la creación de dashboards y reportes personalizados, así como la optimización del rendimiento de la plataforma.		
5	**SERVICIO DE APLICACIÓN Y MONITOREO**		
5.1	Se requiere soporte, optimización, configuración o actualización en servidor de aplicaciones weblogic versión 12c y 14c (servidor middleware), Red Hat JBoss Enterprise Application Platform, WebLogic Suite (Forms Services, Reports Service, WebLogic Server) y Application Server Suite (Forms Services, Reports Service, Containers for Java), herramienta Cloud Control versión 13c, Oracle Linux virtualization Manager Oracle Linux KVM Host versión 4x. Estas actividades se realizarán a solicitud del supervisor del contrato, garantizando el correcto funcionamiento, rendimiento y actualización de los componentes, así como la generación y mantenimiento de reportes conforme a los requerimientos técnicos y operativos de la institución.		
5.2	El contratista se compromete a proporcionar soporte técnico, configuración, optimización y actualización de la herramienta Enterprise Manager Cloud Control, incluyendo los agentes (targets) asociados, conforme a los requerimientos del supervisor del contrato o de la persona que este designe. Como parte integral del servicio, el Contratista realizará una transferencia de conocimiento técnico especializado al personal designado por el supervisor del contrato o quien haga sus veces, abarcando aspectos avanzados de administración de la herramienta, tales como: mejores prácticas para la gestión de targets, optimización de rendimiento, configuración de políticas de monitoreo, uso de métricas personalizadas, y técnicas avanzadas para la explotación de las funcionalidades de la consola, incluyendo métodos eficientes y procedimientos optimizados para maximizar su eficacia. Este requerimiento se ejecutará únicamente cuando el supervisor del contrato o quien este designe lo solicite, garantizando la correcta implementación, operación y aprovechamiento de las capacidades de la herramienta.		
5.3	En caso de ser necesario, el contratista, a solicitud y en coordinación con la supervisión del contrato o quien esta designe, deberá instalar, configurar e implementar en cluster el software de aplicaciones weblogic. Esto incluirá la revisión de requerimientos para la instalación y configuración, la definición del modo y tipo de instalación, la instalación del producto (binario), la configuración de weblogic (incluyendo la creación de dominios) y el despliegue de aplicaciones desarrolladas en tecnologías como Java, PL/SQL web, forms, entre otras. Todas las actividades se realizarán conforme a los estándares técnicos y de seguridad, asegurando la operatividad y estabilidad del entorNro.		
5.4	Cundo el Supervisor del Contrato lo solicite, el contratista deberá realizar el afinamiento a las plataformas WebLogic desplegadas en la infraestructura de la Policía Nacional, optimizando el rendimiento de las aplicaciones desplegadas en el ambiente de contingencia y sitio principal, analizando los datos de rendimiento y de parámetros de la máquina virtual Java (JVM) ajustando los parámetros de WebLogic Server así: Monitoreo y Tuning al JRockit JVM: - Tuning al JRockit JVM - Configuración de parámetros de JVM - Monitoreo y Tuning al Hotspot JVM Configuración de otros recursos de servidor WebLogic: - Modo de inicio de dominio - Rendimiento de E/S nativo - Hilos atascados - Accesos de conexión Tuning JDBC:		

	- Enunciados de la instrucción de sincronización. - Ajuste Transacciones - Parámetros específicos de la base de datos de optimización. Tuning de clústeres de servidores WebLogic: - Optimización de la arquitectura a implementar para weblogic. - Equilibradores de carga - Persistencia de sesión.		
5.5	En caso de ser necesario, el contratista en coordinación con el Supervisor del Contrato, realizará para los servidores de los dominios del Fusion Middleware para el plan de contingencia requerida por la Oficina de Tecnologías de la Información y las Comunicaciones, las actividades que se relacionan a continuación: - Dimensionamiento de recursos del sistema. - Implementación de particiones para disco. - Seguimiento de los logs del sistema. - Limpieza de logs y ficheros. - Control de accesos en el entorNro. - Instalación y configuración del dominio Weblogic para aplicaciones J2EE y PL-SQL WEB. - Pruebas de reinicio del entorno de los servicios desplegados en los servidores de Weblogic. - Tuning de memoria requerido para cada nodo de weblogic. - Optimización y configuración de los pools de conexiones a base de datos. - Optimización y configuración del acceso vía Web a la consola de administración. - Limpieza de logs por cada Instancia. - Instalación del JDK. - Despliegue de herramientas adicionales.		
5.6	En caso de ser necesario, el contratista en coordinación con el Supervisor del Contrato, realizará para el Oracle HTTP Server – OHS las siguientes actividades: - Revisión de los logs de acceso y errores. - Limpieza de logs. - Revisión de políticas de acceso a las diferentes aplicaciones. - Revisión de políticas de Single Sign-ON configuradas. - Instalación y configuración para certificados SSL.		
5.7	En caso de ser necesario, el contratista en coordinación con el Supervisor del Contrato deberá aplicar las correcciones (parches) necesarias para garantizar el correcto funcionamiento de la plataforma a las últimas versiones liberadas en el mercado.		
5.8	En caso de ser necesario, el contratista en coordinación con el Supervisor del Contrato deberá dimensionar adecuadamente, la memoria para mantener un buen desempeño de los servidores de aplicación y monitoreo.		
6	**SISTEMA OPERATIVO**		
6.1	El Contratista deberá aplicar las actualizaciones estables y oficialmente liberadas por el fabricante de los sistemas operativos Linux, previa validación de las matrices de compatibilidad con los entornos afectados, garantizando en todo momento la integridad de los archivos de configuración del sistema operativo y de las aplicaciones en operación. Dicho procedimiento se ejecutará bajo solicitud del Supervisor del Contrato.		
6.2	El Contratista deberá verificar la configuración y, en caso de ser necesario, realizar la reinstalación del sistema operativo en máquinas físicas o virtuales, incluyendo todos los paquetes, dependencias y librerías requeridas según las especificaciones técnicas de la herramienta o producto a implementar. Dicho procedimiento se ejecutará bajo solicitud del Supervisor del Contrato.		
6.3	El Contratista deberá realizar la instalación, configuración y validación de los sistemas operativos y herramientas en los servidores físicos de la Policía Nacional que funcionan como hosts de virtualización bajo Oracle Linux Virtualization Manager (OLVM), asegurando el cumplimiento de los estándares técnicos establecidos; asimismo, en caso de ser requerido, realizará los ajustes, afinamientos y actualizaciones necesarias para garantizar el óptimo funcionamiento, rendimiento y estabilidad de la plataforma de virtualización, a solicitud del Supervisor del Contrato.		
6.4	El contratista deberá realizar las configuraciones necesarias y estrategias para diseñar, implementar el proceso de respaldo y restauración de la plataforma de virtualización Oracle Linux Virtualization Manager (OLVM) de los servidores físicos y virtuales. Este se deberá		

	configurar y aplicar en compañía del personal integrante del Grupo Administración Servicios de Infraestructura en la Nube y previa coordinación con el supervisor del contrato.		
7	**INFORMES Y/O PRODUCTOS**		
7.1	El contratista debe entregar un informe mensual detallado de las actividades realizadas en las plataformas tecnológicos definidas en el ítem 1.1.		
7.2	Durante la ejecución de las actividades objeto del contrato, el contratista deberá, en todo momento, facilitar a las personas designadas por la Oficina Tecnologías de Información y las Comunicaciones de la Policía Nacional, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizadas para resolverlos. Esta documentación técnica deberá ser suministrada en formato digital al supervisor del contrato a través de la cuenta de correo electrónico oftic.gusin@policia.gov.co.		
8	**TRANSFERENCIA DE CONOCIMIENTO Y DOCUMENTACIÓN**		
8.1	El contratista deberá realizar transferencia de conocimientos de los procedimientos que se ejecuten sobre la plataforma Oracle descrita en el ítem 1.1. del presente anexo técnico, al personal integrante del grupo Administración Servicios de Infraestructura en la Nube. Después de cada visita se deberá entregar la documentación técnica en formato digital editable que contenga de manera detallada las actividades ejecutadas en los servidores durante la visita de mantenimiento.		
9	**GARANTÍA DEL SERVICIO**		
9.1	El contratista deberá garantizar por un periodo de un (1) mes, los servicios realizados en la plataforma descrita en el ítem 1.1. del presente anexo técnico, contados a partir de la prestación a satisfacción del servicio. Si se presentase algún inconveniente, deberá inmediatamente realizar las actualizaciones, parches o actividades necesarias, con el fin de mantener la disponibilidad de los servicios.		
10	**PRESENTACIÓN DE LA PROPUESTA**		
10.1	En la oferta presentada se debe marcar las casillas de cumple o no cumple sin cambiar o modificar el formato y ningún numeral del anexo técnico, igualmente escribir el número de folio donde se encuentra la especificación a ofertar.		
10.2	La oferta presentada, deberá ser firmada y avalada por un ingeniero electrónico o de sistemas o electricista o de telecomunicaciones anexando copia de la tarjeta profesional, como lo indica el artículo 20 de la Ley 842 de 2003 "PROPUESTAS Y CONTRATOS". Las propuestas que se formulen en las licitaciones y concursos abiertos por entidades públicas del orden nacional, seccional o local, para la adjudicación de contratos cuyo objeto implique el desarrollo de las actividades catalogadas como ejercicio de la ingeniería, deberán estar avalados, en todo caso, cuando menos, por un ingeniero inscrito y con tarjeta de matrícula profesional en la respectiva rama de la ingeniería."		
11	**EXPERIENCIA DE LOS PROFESIONALES**		
11.1	Con el fin de garantizar la idoneidad del personal involucrado en el proceso de mantenimiento, el contratista deberá contar con personal calificado, respaldado y certificado por el fabricante, que asegure una solución oportuna a cualquier inconveniente que se presente durante la ejecución de los trabajos establecidos en las especificaciones técnicas, sin que ello genere costos adicionales para la Policía Nacional. La Policía Nacional requiere que los profesionales asignados al equipo de trabajo posean la idoneidad, experiencia general y específica necesarias para asegurar la calidad de las actividades realizadas en la plataforma descrita en el ítem 1.1. Por ello, el contratista deberá proveer servicios con ingenieros de sistemas o telecomunicaciones o carreras afines, garantizando así un cumplimiento técnico adecuado. El profesional o el equipo de profesionales propuestos deberán cumplir con los documentos que se relacionan a continuación, así: • El oferente en la propuesta deberá adjuntar para cada profesional, fotocopia o certificado digital de su matrícula o tarjeta profesional; en el caso de profesionales nacionales o extranjeros cuyo título haya sido obtenido fuera del país, deberá incluirse igualmente el enlace de la página web de la entidad emisora que permita verificar en línea la autenticidad del respectivo documento, teniendo en cuenta que los títulos obtenidos en el extranjero deben encontrarse debidamente convalidados en Colombia.		

	Además, el oferente deberá garantizar que el profesional propuesto, o el equipo de profesionales propuesto, cumpla en conjunto con la totalidad de las certificaciones exigidas para el correcto desarrollo de los servicios solicitados, pudiendo optar por presentar un único profesional que acredite por sí solo todas las certificaciones requeridas, o bien un equipo cuyos integrantes, de manera colectiva, cubran la totalidad de dichas certificaciones • Certificación de aprobación en Oracle Database 12c RAC and Grid Infraestructure Administrator de versión 12c o superior, para lo cual deben anexar las certificaciones correspondientes expedidas por el fabricante. • Certificaciones Oracle Certified Professional, Oracle WebLogic Server 12c Administrator. • Certificación Oracle Identity Governance Suite 11g Certified Implementation Specialist o Oracle Identity Governance Suite 11 g PS3 Implementation Essentials o Oracle Access Management Suite Plus 11g Implementation Specialist. • Oracle Certified Professional - Oracle Linux System Administrator o Red Hat Certified Systems Engineer (RHCE) version Linux 7 o superior. El oferente deberá adjuntar dos (2) certificaciones expedidas por entidad pública o privada, mediante las cuales el personal propuesto acredite su participación en actividades de instalación, configuración o mantenimiento de los productos respecto de los cuales se encuentra certificado.		
12	**CONFIDENCIALIDAD DE LA INFORMACIÓN**		
12.1	Si la Policía Nacional, considera pertinente someter a estudio de seguridad al personal que prestará los servicios, el contratista permitirá y facilitará todos los medios que la Entidad le solicite para este fin.		
12.2	El CONTRATISTA se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del contrato que se encuentre clasificada como confidencial; así como los lugares a los cuales tenga acceso con ocasión de su servicio. Para lo cual el oferente deberá diligenciar el formulario "ACUERDO DE CONFIDENCIALIDAD" y entregarlo junto con la oferta.		
13	**COMPROMISO DE ANTICORRUPCIÓN**		
13.1	El contratista deberá cumplir con el compromiso de anticorrupción durante la ejecución del contrato manifestando que se encuentra dispuesto a suministrar la información propia que resulte necesaria para aportar transparencia al mismo y si se comprueba el incumplimiento del contrato, sus empleados, representantes, asesores o de cualquier otra persona que actúe en su nombre, es causal suficiente para la terminación anticipada del contrato. Para lo cual el oferente deberá diligenciar el formulario "COMPROMISO ANTICORRUPCIÓN" y entregarlo junto con la oferta.		
14	**SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO**		
14.1	En el tiempo de ejecución del contrato y durante la garantía el contratista deberá cumplir con el protocolo de seguridad de instalaciones y normas internas de seguridad física en cada una de las unidades policiales en todo el territorio colombiano, para lo cual el oferente deberá diligenciar el FORMULARIO "SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO" y entregarlo junto con la oferta.		
14.2	El oferente deberá acreditar el cumplimiento de los Estándares Mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG.SST), en los términos establecidos por el Decreto 1072 de 2015 y por la Resolución 0312 de 2019 del Ministerio del Trabajo, mediante la presentación de la calificación oficial radicada ante la Administradora de Riesgos Laborales ARL y/o ante el Ministerio del Trabajo de conformidad con la circular 027 de 2026, correspondiente al año inmediatamente anterior a la fecha de cierre del presente proceso de selección. En caso de presentarse en unión temporal o consorcio deberá anexarse el documento de cada uno de los integrantes.		
15	**CONDICIONES AMBIENTALES**		
15.1	El oferente deberá presentar el certificado de consulta del Registro Único de Infractores Ambientales (RUIA), expedido a través del enlace oficial del Ministerio de Ambiente: https://vital.minambiente.gov.co/SILPA_UT_PRE/RUIA/ConsultarSancion.aspx?Ubic=ext. En caso de presentarse como unión temporal o consorcio, deberá aportarse el certificado RUIA		

	de cada uno de sus integrantes. Así mismo, este certificado deberá ser presentado durante la ejecución del contrato cuando el supervisor lo requiera, con el fin de verificar la existencia o no de sanciones ambientales vigentes.		
15.2	El oferente deberá verificar la necesidad de permisos, licencias, concesiones o autorizaciones ambientales de acuerdo a su actividad comercial y, de ser legalmente exigibles, obtenerlos y presentar el documento emitido por la autoridad ambiental competente. En caso de que no aplique deberá declararlo el representante legal bajo la gravedad de juramento mediante certificación, asumiendo plenamente las consecuencias legales, ambientales y contractuales que se deriven del incumplimiento. Se deberán mantener vigentes durante toda la ejecución del contrato.		
16	**EXPERIENCIA DEL PROPONENTE**		
16.1	**EXPERIENCIA GENERAL PROPONENTE NACIONAL O EXTRANJERO CON SUCURSAL O DOMICILIO EN COLOMBIA -RUP** El Registro Único de Proponentes es el instrumento a través del cual se verificará el requisito de experiencia del proponente, para tal efecto las personas naturales, las personas jurídicas, las uniones temporales, los consorcios u otra forma de asociación que participen en este proceso, deberán acreditar la experiencia con mínimo uno (01) máximo tres (03) contratos celebrados y ejecutados con entidades públicas y/o privadas, identificados con el siguiente código UNSPSC y que su valor sumado sea igual o superior a 115,71 SMMLV, así:		

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	VALOR EXPRESADO EN SMMLV
81112200	Servicios basados en Ingeniería, Investigación y Tecnología	Servicios informáticos	Mantenimiento y soporte de software	115,71

JUSTIFICACIÓN: la exigencia de acreditar el cien por ciento (100 %) del valor estimado del presente proceso en SMMLV se justifica en la alta criticidad de las plataformas tecnológicas objeto de mantenimiento y soporte, las cuales respaldan servicios esenciales de bases de datos, sistemas operativos, aplicaciones, autenticación, monitoreo, respaldo y continuidad tecnológica de la Policía Nacional. Sù indisponibilidad o falla puede afectar directamente la operación institucional, comprometiendo la prestación de servicios misionales, administrativos y operativos.

NOTA 1: si los contratos acreditados fueron realizados bajo la modalidad de Consorcio, de Unión Temporal u otras formas de asociación, se tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del Consorcio, de la Unión Temporal u otras formas de asociación, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del Consorcio, la Unión Temporal u otras formas de asociación, donde deberá constar el porcentaje de participación de cada uno de los integrantes para la ejecución del contrato. Sin embargo, la misma puede ser certificada por uno solo de los integrantes.

NOTA 2: en el caso de proponentes plurales, todos sus integrantes deben registrar experiencia en el RUP con el código UNSPSC antes señalado.

NOTA 3: en la presentación de la oferta, el oferente deberá diligenciar y entregar el formulario "EXPERIENCIA GENERAL DEL PROPONENTE", donde relacionará los contratos para la evaluación.

	EXPERIENCIA ESPECÍFICA PROPONENTE NACIONAL O EXTRANJERO CON SUCURSAL O DOMICILIO EN COLOMBIA El proponente que vaya a proveer los servicios objeto del presente proceso de contratación, trátese de personal natural o jurídica, deberá anexar mínimo una (01) máximo tres (03) constancias (certificaciones o actas de liquidación) de contratos celebrados y ejecutados con entidades públicas y/o privadas, cuyo objeto sea igual o similar al objeto de la presente contratación "MANTENIMIENTO DE PLATAFORMAS DE BASES DE DATOS, SISTEMAS OPERATIVOS Y SERVICIOS DE APLICACIÓN DE LA POLICÍA NACIONAL", documentos que como mínimo deberán tener la siguiente información: 1. Nombre del contratista 2. Nombre del contratante 3. Objeto del contrato 4. Valor del contrato 5. Fecha de suscripción y fecha de inicio del contrato 6. Fecha de terminación del contrato 7. Personal de contacto para verificar la información: teléfono fijo o celular, correo electrónico institucional, logo (en caso de certificación). 8. Estado del contrato: ejecutado o liquidado. 9. Si es certificación, deberá estar suscrita por el funcionario competente para tal fin. 10. Manifestación clara y explícita donde se evidencie que el contratista cumplió a cabalidad con el objeto del contrato. 11. Porcentaje del valor del contrato que ejecutó como miembro de un consorcio, unión temporal u otra forma de asociación. La experiencia debe comprobarse en los siguientes ítems: •Database EE 12c, 18c, 19c o 21c. •Backup and Recovery, RMAN y ASM. •Dataguard. •Weblogic 12c •Oracle Unified Directory 12c. •Oracle Linux versiones 7.x o 8.x o Red Hat versiones 7.x o 8x. **NOTA 1**: en cumplimiento del artículo 2.2.1.2.4.2.18 del Decreto 1082 de 2015, el Decreto 1860 de 2021 el cual reglamentó parcialmente la Ley 2069 de 2020 "Por medio de la cual se impulsa el emprendimiento en Colombia" y el artículo 1° del Decreto 0287 de 2026 "Por el cual se modifican los artículos 2.2.1.2.4.2.6., 2.2.1.2.4.2.7. y 2.2.1.2.4.2.8. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación", se toma como criterio diferencial para las MiPymes y los emprendimientos y empresas de personas con discapacidad, el número de contratos para la acreditación de la experiencia. Por tanto, deberán anexar mínimo una (01) máximo cuatro (04) constancias (certificaciones o actas de liquidación) que cumplan con lo antes relacionado **NOTA 2**: la experiencia especifica presentada deberá estar registrada en el Registro Único de Proponentes, no serán tenidas en cuenta aquellas constancias de contratos que no se encuentren registrados. **NOTA 3**: si la información relacionada en el (RUP) para acreditar la experiencia no se puede verificar, la entidad se reserva la facultad de solicitar información adicional. **NOTA 4**: no se aceptarán auto certificaciones. **NOTA 5**: no se tendrán en cuenta las certificaciones de contratos en ejecución. **NOTA 6**: no se aceptan certificaciones con enmendaduras o que presenten inconsistencias no subsanadas. **NOTA 7**: cuando los documentos no indiquen su valor en SMMLV o si estos son de años anteriores a 2026, se hará la respectiva conversión de acuerdo al año en que terminó el contrato. La verificación será realizada por el comité evaluador técnico.		

	NOTA 8: si los contratos acreditados fueron realizados bajo la modalidad de consorcio, unión temporal u otras formas de asociación, se tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del consorcio, unión temporal u otras formas de asociación, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del consorcio, unión temporal u otra forma de asociación, donde deberá constar el porcentaje de participación de cada uno de los integrantes en la ejecución del contrato. **NOTA 9**: en el caso de proponentes plurales, todos sus integrantes deben registrar experiencia en el RUP según el código UNSPSC requerido en el presente proceso de selección. **NOTA 10**: en el caso que el proponente haya participado en procesos de fusión o escisión empresarial, debe tomar para estos efectos, exclusivamente los contratos que le hayan asignado en el respectivo proceso de fusión o escisión, para ello debe aportar el certificado del contador público o del revisor fiscal (si la persona jurídica tiene revisor fiscal) que así lo acredite. La Policía Nacional se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma.		

Intendente **JHEYNS FABIAN RIAÑO MATEUS**
Estructurador Estudio Previo

Intendente **CARLOS ALBERTO JIMENEZ ÁVILA**
Estructurador Estudio Previo

Intendente Jefe **LEYDER PINEDO MURAYARI**
Estructurador Estudio Previo