<table>
<tr><th>ÍTEM</th><th>DESCRIPCIÓN</th><th>OFERTA</th><th>NO OFERTA</th></tr>
<tr><td>1.</td><td colspan="3">GENERALIDADES</td></tr>
<tr><td>1.1.</td><td>El contratista deberá contar con la disponibilidad y capacidades técnicas necesarias para realizar las actividades de desarrollo y mantenimiento de software a los sistemas de información de la Dirección de Investigación Criminal e INTERPOL, de la Policía Nacional, mediante la aplicación de metodologías, estándares y buenas prácticas para el análisis, diseño, programación, pruebas e implementación de manera que se garantice la seguridad, confiabilidad, mantenibilidad, compatibilidad y facilidad de prueba en cada uno de los ajustes, correcciones, actualizaciones, configuraciones o nuevas funcionalidades que se desarrollen para satisfacer las necesidades de la entidad.</td><td></td><td></td></tr>
<tr><td>1.2.</td><td>El alcance del proyecto de mantenimiento y desarrollo de software incluye análisis, diseño, desarrollo, pruebas, documentación, acompañamiento en la puesta en producción y garantía de los desarrollos.</td><td></td><td></td></tr>
<tr><td>1.3.</td><td>Stack de desarrollo: para la migración de los servicios y los demás desarrollos requeridos, el contratista deberá contar con personal idóneo, con experiencia comprobable en la implementación de proyectos de software, utilizando el siguiente stack tecnológico:

<table>
<tr><th>Componente</th><th>Tecnología</th></tr>
<tr><td rowspan="4">Backend</td><td>Lenguaje de programación: Java 8 (JDK 1.8)</td></tr>
<tr><td>Framework: Spring Boot 2.6.x, utilizando únicamente dependencias compatibles con Java 8</td></tr>
<tr><td>Gestor de dependencias: Maven 3.8.4 o superior, compatible con Java 8</td></tr>
<tr><td>Propagación de identidad: Implementación basada en JSON Web Tokens (JWT – RFC 7519) compatible con Java 8</td></tr>
<tr><td rowspan="5">Frontend</td><td>Reportes: JasperReports 6 o superior, compatible con Java 8</td></tr>
<tr><td>Framework UI (core): React 18 o superior</td></tr>
<tr><td>Librería UI: Ant Design (última versión estable y compatible)</td></tr>
<tr><td>Gestión de estado: Redux Toolkit Redux Toolkit + RTK Query (última versión estable y compatible)</td></tr>
<tr><td>Enrutamiento: React Router (última versión estable y compatible)</td></tr>
<tr><td>Base de datos</td><td>Lenguaje: TypeScript (última versión estable y compatible)</td></tr>
<tr><td>Servidor de aplicaciones</td><td>Oracle Database 19c o superior</td></tr>
<tr><td>Control de versiones</td><td>Oracle WebLogic Server 12.2.1.4.0 o superior</td></tr>
<tr><td></td><td>Git</td></tr>
</table>

NOTA: El contratista deberá emplear únicamente versiones estables de frameworks, librerías y componentes que mantengan compatibilidad con Java 8, incluyendo los parches de seguridad disponibles dentro de dicha línea de versiones.

No se permitirá el uso de versiones que requieran Java 11, Java 17 o superiores, ni dependencias que introduzcan incompatibilidades con el entorno Java 8 definido para la solución.</td><td></td><td></td></tr>
<tr><td>1.4.</td><td>Las aplicaciones y servicios desarrollados deberán ser empaquetados y entregados en formato WAR, garantizando su compatibilidad con Oracle WebLogic Server 12.2.1.4.0.

No se permitirá el despliegue de aplicaciones en formato JAR ejecutable, ni el uso de servidores embebidos (Tomcat, Jetty u otros) en ambientes productivos.</td><td></td><td></td></tr>
<tr><td>1.5.</td><td>El despliegue deberá realizarse sobre un clúster de Oracle WebLogic Server, compuesto por múltiples Managed Servers, garantizando:

• Alta disponibilidad del servicio.
• Balanceo de carga entre los nodos del clúster.
• Failover automático ante la indisponibilidad de uno o más nodos.

El despliegue deberá efectuarse utilizando un Cluster Target, evitando despliegues manuales por servidor.</td><td></td><td></td></tr>
<tr><td>1.6.</td><td>Las conexiones a base de datos deberán realizarse exclusivamente mediante DataSources configurados en WebLogic, mediante JNDI.

La configuración sensible (credenciales, URLs, claves) deberá externalizarse mediante:</td><td></td><td></td></tr>
</table>

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	• Variables de entorno • Archivos de configuración del servidor • Mecanismos de seguridad propios de WebLogic • No se permitirá la inclusión de credenciales en código fuente.		
1.7.	Las aplicaciones deberán diseñarse bajo el principio de stateless, evitando dependencias de estado en memoria local. En caso de requerirse manejo de sesión, este deberá ser compatible con replicación de sesiones en clúster WebLogic.		
1.8.	Los logs de la aplicación deberán integrarse con el sistema de logs de WebLogic. Los mensajes de error técnicos deberán registrarse únicamente en logs, evitando su exposición al usuario final. Se deberá permitir la trazabilidad de solicitudes entre el API Gateway y los servicios desplegados.		
1.9.	El contratista deberá realizar pruebas que evidencien: • Despliegue exitoso del WAR en el clúster. • Acceso correcto a los servicios desde múltiples nodos. • Comportamiento adecuado ante la caída de uno de los nodos del clúster.		
1.10.	El contratista deberá ejecutar el desarrollo de software empleando metodologías ágiles formalmente establecidas, tales como SCRUM, o un marco de trabajo ágil equivalente, garantizando la adopción de buenas prácticas de ingeniería de software orientadas a la calidad, mantenibilidad y entrega continua de valor.		
1.11.	Todos los desarrollos, integraciones, funcionalidades y demás implementaciones diseñadas específicamente para este proceso, serán propiedad exclusiva de la Policía Nacional. Queda estrictamente prohibida su reproducción, réplica o utilización para fines distintos a los establecidos en este contrato, salvo autorización previa y por escrito de la Policía Nacional.		
1.12.	El contratista deberá realizar todas las pruebas necesarias para garantizar la aprobación técnica y funcional del sistema. Estas pruebas deberán incluir, como mínimo: • Pruebas unitarias: verificar que cada componente o módulo del sistema funcione correctamente de manera aislada. • Pruebas de integración: comprobar la interacción correcta entre los módulos del sistema. • Pruebas funcionales: validar que el sistema cumpla con los requerimientos establecidos y funcione de acuerdo con las especificaciones técnicas. • Pruebas de usuario: asegurar que el sistema cumple con las expectativas de los usuarios finales y los objetivos del proyecto. • Pruebas de rendimiento: evaluar la capacidad del sistema en términos de velocidad, estabilidad y escalabilidad bajo diferentes condiciones. • Pruebas de seguridad: garantizar que el sistema protege adecuadamente los datos y cumple con las normativas de seguridad aplicables. Pruebas de regresión:		
1.13.	El contratista deberá implementar el sistema de información desarrollado en servidores de pruebas, con el propósito de realizar las siguientes evaluaciones: • Pruebas de estrés. • Pruebas de rendimiento. • Pruebas de conectividad. • Evaluaciones de tiempos de respuesta. • Verificación del cumplimiento de los requerimientos del software. Estas pruebas permitirán analizar el comportamiento del sistema y la arquitectura implementada. El periodo de pruebas deberá tener una duración no inferior a 30 días posteriores a su publicación, y los resultados deberán ser validados por la Oficina de Tecnologías de la Información y las Comunicaciones - OFTIC y el usuario líder funcional. Durante este periodo, cualquier inconsistencia o irregularidad identificada deberá ser subsanada. En caso de requerirse un ajuste adicional, este podrá realizarse en un plazo no superior a 30 días, garantizando la resolución de los problemas antes de la entrega final y la aceptación a satisfacción.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
1.14.	El contratista deberá hacer uso de librerías y plugins que tengan una comunidad activa o con soporte del fabricante, los cuales estén realizando verificaciones y cierres de posibles brechas de seguridad en las mismas.		
1.15.	El contratista deberá elaborar un cronograma de trabajo detallado para el proyecto a desarrollar, en el cual se describan las actividades previstas y los plazos de cumplimiento. El cronograma debe incluir, entre otros documentos, el acta de inicio del proyecto y los puntos clave para su seguimiento.		
1.16.	El contratista deberá prever, dentro del plazo contractual establecido, la implementación de funcionalidades adicionales no identificadas durante la fase inicial de levantamiento de requerimientos, siempre que dichas funcionalidades resulten indispensables para garantizar la correcta operación, integridad funcional y cumplimiento de los requisitos del sistema. Estas funcionalidades deberán mantenerse estrictamente alineadas con la arquitectura definida, los modelos de datos, los lineamientos técnicos y el alcance funcional aprobado, sin implicar modificación sustancial del objeto contractual ni alteraciones en los componentes estructurales de la solución; su desarrollo, integración y despliegue deberán ejecutarse conforme al ciclo de vida del software definido en el proyecto, asegurando su incorporación como parte integral de la solución y su validación completa durante las fases de pruebas funcionales, no funcionales y de aceptación.		
1.17.	Se deberá garantizar el cumplimiento de las buenas prácticas de desarrollo seguro. La Oficina de Tecnologías de la Información y de las Comunicaciones, realizará pruebas de vulnerabilidades sobre los desarrollos entregados por el contratista. Cualquier vulnerabilidad identificada deberá ser subsanada en su totalidad por el contratista en un plazo no superior a 30 días, sin perjuicio de que las pruebas sean evaluadas nuevamente una vez realizados los ajustes.		
1.18.	Se deberá considerar las integraciones y conexiones vigentes con otros sistemas de información, así como la compatibilidad con los programas y aplicaciones que están siendo utilizados actualmente por los equipos de la Policía Nacional.		
1.19.	El contratista deberá presentar, dentro de los primeros quince (15) días calendario contados a partir de la fecha del acta de iniciación del contrato, un plan detallado del proyecto. Este plan debe incluir un cronograma de trabajo que contemple las siguientes fases: levantamiento de información, análisis, diseño, construcción, pruebas, aceptación, implementación y capacitación, así como los eventos y productos finales asociados a cada una de ellas. Adicionalmente, el contratista deberá entregar un detalle de la arquitectura propuesta (a alto nivel), junto con el plan de trabajo necesario para todas las integraciones solicitadas. Este plan deberá ser aprobado por la supervisión del contrato antes de su ejecución.		
1.20.	Dada la diversidad de las aplicaciones que se implementarán, en caso de que alguna de ellas requiera la incorporación de software base adicional para su construcción o mantenimiento, las licencias correspondientes deberán ser entregadas a la Policía Nacional, y serán de su propiedad a perpetuidad. Asimismo, el licenciamiento de uso de las aplicaciones será propiedad de la Policía Nacional.		
1.21.	El contratista deberá entregar la totalidad del código fuente correspondiente al software, en formato magnético, junto con los manuales elaborados (editables), también en formato magnético, una vez finalizada la etapa de implementación. Los entregables deben estar debidamente rotulados y respaldados con la documentación que describa su contenido.		
1.22.	El licenciamiento del software debe cubrir todas las implementaciones e integraciones necesarias con los sistemas de la Policía Nacional.		
1.23.	CESIÓN DE DERECHOS PATRIMONIALES El contratista deberá transferir a título gratuito todos los Derechos Patrimoniales del objeto del contrato a través del documento anexo “1DH-FR-0158 CONTRATO DE CESIÓN DE DERECHOS PATRIMONIALES DE AUTOR” y debe estar debidamente registrado ante la Dirección Nacional de Derechos de Autor Unidad Administrativa Especial del Ministerio del Interior y protocolizado ante notaría. El contratista debe registrar el presente contrato en la entidad competente para el Registro de Derecho de Autor y remitir el certificado de inscripción como requisito previo para la suscripción del acta de recibo final a satisfacción y para la realización del último contador de pago correspondiente para cada uno de los desarrollos implementados.		
1.24.	Los trámites de autenticación ante notaría por registro de firma y huella de la cesión de derechos patrimoniales deberán ser asumidos por el contratista sin generar costos adicionales para la Policía Nacional.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
1.25.	El contratista debe anexar como documentos entregables el CONTRATO DE CESIÓN DE DERECHOS PATRIMONIALES DE AUTOR (1DH-FR-0158) y copia del CONTRATO DE CESIÓN que se realizó entre los empleados contratados y la firma contratante, donde transfieren los derechos a la empresa. Los documentos serán entregados al supervisor del contrato con una antelación mínima de cinco (5) días hábiles antes de la finalización del plazo de ejecución del presente proceso contractual.		
1.26.	El contratista deberá entregar mensualmente al supervisor del contrato, con una antelación mínima de cinco (5) días antes de finalizar el mes, un informe detallado de avance y gestión, en el cual se describan de manera clara y estructurada las actividades realizadas sobre cada uno de los sistemas de información objeto del contrato.		
1.27.	El contratista deberá realizar los desarrollos y pruebas unitarias de manera local, posteriormente realizará su despliegue en el ambiente de pruebas (Oracle WebLogic Server 12.2.1.4.0.) en donde deberá realizar las validaciones y tests necesarios, una vez superada la etapa de pruebas funcionales y no funcionales y tras contar con la autorización por parte del supervisor del contrato, se realizará el despliegue en el ambiente de producción previa coordinación con el equipo técnico del Grupo Tecnologías de la Información y las Comunicaciones DIJIN.		
1.28.	Todas las configuraciones requeridas, para adelantar sus actividades, en los ambientes de desarrollo y producción deben ser realizadas por el contratista.		
1.29.	En caso de presentarse alguna falla o error durante un despliegue en producción, la empresa contratista deberá ejecutar la operación de rollback y reestablecer los servicios a su versión estable.		
1.30.	El contratista deberá mantener y asegurar una copia de seguridad diaria y/o control de versiones de todos los códigos fuentes, desarrollos, ajustes y configuraciones con el fin de poder realizar restauraciones o aplicar operaciones de rollback en caso de requerirse. Una vez se realice el paso a producción, el contratista deberá cargar todos los códigos fuentes, desarrollos, ajustes y configuraciones en el servidor de versionamiento de la Dirección de Investigación Criminal e INTERPOL.		
1.31.	Entrega del Proyecto en Repositorio de DevOps El contratista deberá entregar el proyecto completo en el repositorio de DevOps administrado por el Grupo Tecnologías de la Información y de las Comunicaciones DIJIN. Dicha entrega deberá cumplir con las siguientes condiciones: • Rama Master: el código fuente deberá estar actualizado y consolidado en la rama principal (master), asegurando que esta contenga la versión final funcional y aprobada del proyecto. • Historial de cambios: el repositorio deberá incluir el historial completo de cambios realizados durante el desarrollo, garantizando la trazabilidad de las modificaciones. • Estructura estándar: la estructura del repositorio deberá estar organizada de manera que facilite la comprensión, mantenimiento del código, siguiendo las prácticas recomendadas de DevOps. • Accesos y credenciales: el contratista deberá coordinar con el Grupo Tecnologías de la Información y de las Comunicaciones DIJIN para obtener los accesos necesarios al repositorio de DevOps. En ningún caso se permitirá el uso de repositorios externos o plataformas no gestionadas por la institución. Validación final: la entrega del proyecto en el repositorio será validada por el equipo técnico del Grupo Tecnologías de la Información y las Comunicaciones DIJIN, quien verificará que se cumplan todos los lineamientos y requisitos establecidos.		
1.32.	Todos los códigos fuentes de los desarrollos e implementaciones realizadas, así como las librerías y componentes utilizados deberán ser entregados al supervisor del contrato bajo las condiciones establecidas en el ítem anterior (1.31), sin ninguna clase de cifrado que restrinja su uso.		
1.33.	Las herramientas utilizadas para el presente proceso deberán ser licenciadas sin causar costos para la Dirección de Investigación Criminal e INTERPOL.		
2.	**ACTUALIZACIÓN ARQUITECTURA DE SERVICIOS WEB SOAP A API REST**		
2.1.	El contratista deberá realizar la migración de los siguientes servicios web, actualmente implementados bajo arquitectura SOAP y desarrollados en lenguaje de programación Java, hacia una arquitectura de servicios REST, garantizando la continuidad funcional y la compatibilidad con los sistemas integrados existentes.		

<table>
<tr><th>ÍTEM</th><th>DESCRIPCIÓN</th><th>OFERTA</th><th>NO OFERTA</th></tr>
<tr><td></td><td><table><tr><th>Servicio</th><th>Número de Implementaciones</th></tr><tr><td>Noticias Criminales</td><td>2</td></tr><tr><td>Consulta Antecedentes Judiciales</td><td>4</td></tr><tr><td>Consulta Antecedentes Vehículos</td><td>1</td></tr><tr><td>Combustibles</td><td>1</td></tr></table></td><td></td><td></td></tr>
<tr><td>2.2.</td><td>La migración deberá contemplar la reconstrucción de las interfaces de servicio, la adaptación de los contratos de comunicación, y la exposición de los servicios mediante endpoints REST, utilizando formatos de intercambio de información estándar (JSON y/o XML), de acuerdo con las buenas prácticas de diseño de APIs.</td><td></td><td></td></tr>
<tr><td>2.3.</td><td>El contratista deberá asegurar que:
La lógica de negocio existente sea preservada.
Los servicios migrados mantengan el mismo comportamiento funcional que las implementaciones actuales.
Realizar afinamientos y optimizaciones en las reglas de negocio.
Se garantice la seguridad, trazabilidad, manejo de errores y control de versiones de los servicios.
Se entregue la documentación técnica actualizada de los nuevos servicios expuestos.</td><td></td><td></td></tr>
<tr><td>2.4.</td><td>El contratista deberá realizar la migración de los servicios web existentes basados en arquitectura SOAP hacia una arquitectura moderna de APIs REST, las cuales deberán ser implementadas en Java 8 con Spring Boot y expuestas a través de un API Gateway, asegurando consistencia, calidad y alineación con buenas prácticas de desarrollo de APIs.</td><td></td><td></td></tr>
<tr><td>2.5.</td><td>El API Gateway deberá implementarse como un componente independiente, altamente disponible y sin estado, responsable únicamente del gobierno, seguridad y enrutamiento de las APIs.

La lógica de negocio, el acceso a datos y la orquestación de procesos deberán residir exclusivamente en los servicios backend, los cuales se desplegarán como unidades independientes y serán accesibles únicamente a través del API Gateway.</td><td></td><td></td></tr>
<tr><td>2.6.</td><td>Todos los servicios deberán diseñarse bajo un enfoque API-First, donde el contrato de la API (OpenAPI/Swagger) se defina antes de la implementación, garantizando claridad funcional, desacoplamiento y facilidad de integración.</td><td></td><td></td></tr>
<tr><td>2.7.</td><td>Cada API REST deberá cumplir una responsabilidad claramente definida, evitando la replicación de la lógica monolítica propia de los servicios SOAP existentes.</td><td></td><td></td></tr>
<tr><td>2.8.</td><td>Los endpoints deberán seguir convenciones REST estándar:
Uso correcto de verbos HTTP (GET, POST, PUT, PATCH, DELETE).
Uso de sustantivos en plural para los recursos.
Evitar acciones en la URL (ej. /getData).
Se deberá definir claramente el uso de códigos de respuesta HTTP (200, 201, 400, 401, 403, 404, 409, 500, etc.).</td><td></td><td></td></tr>
<tr><td>2.9.</td><td>Todas las APIs deberán contar con versionamiento explícito, preferiblemente a nivel de URL. Los cambios incompatibles deberán publicarse como una nueva versión, sin romper versiones existentes.</td><td></td><td></td></tr>
<tr><td>2.10.</td><td>Se deberá implementar un mecanismo de manejo de excepciones centralizado (Controller Advice), que capture y procese errores de validación, errores funcionales y excepciones técnicas, retornando respuestas HTTP estandarizadas con mensajes controlados y personalizados para el usuario.

En ningún caso deberán exponerse mensajes internos, trazas de error o detalles técnicos en la respuesta, los cuales deberán registrarse únicamente en los logs del sistema para efectos de auditoría y diagnóstico. El formato de error deberá ser estandarizado (código, mensaje).</td><td></td><td></td></tr>
<tr><td>2.11.</td><td>Cada API deberá quedar configurada y desplegada en modo clúster, de tal manera que se garantice la alta disponibilidad del servicio y la continuidad operativa ante fallos parciales o indisponibilidad de nodos.

Dicha configuración deberá realizarse sobre Oracle WebLogic Server versión 12.2.1.4.0, asegurando el correcto balanceo de carga, la tolerancia a fallos y la correcta operación de los servicios expuestos.</td><td></td><td></td></tr>
<tr><td>2.12.</td><td>Todas las configuraciones de los servicios, incluyendo URLs de servicios externos, credenciales de acceso, parámetros de timeout, configuraciones de pool de conexiones y cualquier otro parámetro</td><td></td><td></td></tr>
</table>

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	operativo, deberán externalizarse mediante Spring Cloud Config o archivos de propiedades específicos por ambiente (desarrollo, QA, producción). Cada ambiente deberá contar con su archivo de configuración específico siguiendo la nomenclatura estándar: application-{env}.properties o application-{env}.yml, donde {env} representa el identificador del ambiente (dev, qa, prod).		
2.13.	Las credenciales sensibles, tales como contraseñas de base de datos, tokens de integración y claves de cifrado, deberán almacenarse de forma cifrada utilizando herramientas como Spring Vault o Java Simplified Encryption (Jasypt), garantizando que información crítica nunca se exponga en texto plano.		
2.14.	Resiliencia y Tolerancia a Fallos: en todos los desarrollos se deberá implementar el patrón Circuit Breaker, de tal manera que ante un fallo: • La aplicación continúe respondiendo. • Se gestionen las peticiones de forma controlada. • Se evite propagar fallos en cascada. • Se deberá implementar un mecanismo de respuesta alternativa (fallback) con mensajes funcionales y controlados. • Se recomienda el uso de librerías como Resilience4j.		
2.15.	Todas las invocaciones a servicios externos deberán definir: • Timeouts explícitos. • Políticas de reintentos controlados. • No se permitirán reintentos infinitos ni bloqueantes.		
2.16.	El contratista deberá implementar mecanismos de autenticación y autorización, garantizando que únicamente los clientes debidamente autenticados y autorizados puedan realizar solicitudes a las APIs expuestas. Asimismo, deberá incorporar controles de seguridad orientados a la mitigación de vectores de ataque, como ataques de denegación de servicio (DDoS), inyecciones SQL y inyecciones XML, entre otros. • Todas las APIs deberán estar protegidas mediante mecanismos de seguridad centralizados. • Se deberá hacer uso de mecanismos de autenticación reconocidos como (LDAP, OAuth 2.0 / JWT). • No se deberán manejar credenciales directamente en los servicios.		
2.17.	Se deberá implementar caché a nivel de aplicación usando Spring Cache. Las operaciones de lectura intensiva deberán almacenarse en caché con políticas de invalidación apropiadas para mantener la consistencia de datos.		
2.18.	Validación de Entradas: todos los datos de entrada deberán ser validados utilizando Bean Validation (JSR-380). Se deberá evitar el procesamiento de datos incompletos, inválidos o maliciosos.		
2.19.	Separación de Responsabilidades: • La lógica de negocio no deberá residir en los controladores. • Se deberán definir capas claras de servicio y dominio.		
2.20.	Reutilización y Refactorización: • La lógica heredada de los servicios SOAP deberá ser evaluada y refactorizada. • No se permitirá la simple traducción directa de operaciones SOAP a REST sin análisis previo.		
2.21.	Transformación de Datos: • Se deberán definir DTOs específicos para la capa de exposición. • No se permitirá la exposición directa de entidades internas.		
2.22.	Gobierno y Enrutamiento: todas las APIs deberán ser expuestas exclusivamente a través del API Gateway. El Gateway será responsable de: • Enrutamiento. • Seguridad. • Rate limiting. • Control de tráfico.		
2.23.	Rate Limiting y Throttling:		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	• Se deberán definir políticas de limitación de consumo por cliente o aplicación. • Estas políticas deberán proteger los servicios backend de sobrecarga.		
2.24.	Controles de Seguridad: Se deberá implementar CORS (Cross-Origin Resource Sharing) con configuración restrictiva, permitiendo únicamente orígenes autorizados explícitamente definidos en la configuración. No se permitirán configuraciones permisivas con comodines (*) en ambientes de producción.		
2.25.	Todas las APIs que modifiquen estado deberán implementar protección contra ataques CSRF (Cross-Site Request Forgery) mediante tokens anti-CSRF. Las APIs públicas de solo lectura podrán exentarse de este requisito previa justificación.		
2.26.	Se deberá implementar sanitización exhaustiva de todas las entradas del usuario para prevenir inyección SQL, XSS (Cross-Site Scripting), inyección XML y otras vulnerabilidades del OWASP Top 10. La validación deberá realizarse tanto en el lado del cliente como del servidor, siendo esta última la definitiva.		
2.27.	Los tokens JWT utilizados para autenticación deberán tener un tiempo de expiración máximo de 1 hora. Se deberá implementar un mecanismo de refresh tokens con expiración extendida para permitir la renovación de tokens sin requerir autenticación repetida del usuario. Se deberá implementar un mecanismo de blacklisting de tokens que permita la revocación inmediata de tokens comprometidos. El sistema deberá validar contra esta lista en cada solicitud autenticada.		
2.28.	Observabilidad y Monitoreo: Se deberán implementar mecanismos que permitan garantizar la trazabilidad completa de una solicitud, generando identificadores únicos de trazabilidad (trace-id y span-id) para cada solicitud. Estos identificadores deberán propagarse automáticamente en todas las llamadas entre servicios y registrarse en los logs. Los logs deberán seguir un formato estructurado en JSON que incluya campos obligatorios como: timestamp con precisión de milisegundos, nivel de log (ERROR, WARN, INFO, DEBUG), trace-id para correlación de trazas, user-id del usuario que realizó la operación, dirección IP de origen, nombre del servicio, y el mensaje descriptivo del evento. Los logs no deberán contener información sensible.		
2.29.	Todas las APIs deberán exponer endpoints de monitoreo mediante Spring Boot Actuator para fines de observabilidad interna y operación del servicio. Como mínimo, se deberá habilitar /actuator/health, /actuator/metrics, /actuator/info y /actuator/prometheus. Estos endpoints deberán estar protegidos y restringidos a los sistemas de monitoreo y administración, y no deberán ser expuestos públicamente a través del API Gateway. La información proporcionada por Actuator será complementaria a las métricas y controles operativos gestionados por la plataforma de API Management (WSO2).		
2.30.	Métricas y Trazabilidad: Todas las APIs deberán exponer métricas técnicas (latencia, errores, disponibilidad).		
2.31.	El contratista deberá implementar un plan de pruebas para todas las APIs desarrolladas o migradas, incluyendo como mínimo: • Pruebas unitarias: validación aislada de la lógica de negocio, servicios y componentes internos, utilizando frameworks compatibles con Java 8. • Pruebas de integración: validación del correcto funcionamiento de los endpoints REST, incluyendo interacción con base de datos, componentes JNDI, servicios externos y configuración de seguridad. • Pruebas de contrato (Contract Testing): verificación de que las APIs cumplen con las especificaciones publicadas (OpenAPI/Swagger), garantizando compatibilidad entre consumidor y proveedor. Se deberá validar estructura de request/response, códigos HTTP, encabezados y esquemas JSON definidos.		
2.32.	Se deberá implementar el patrón Repository para encapsular toda la lógica de acceso a datos. Esto facilitará las pruebas unitarias mediante mocks y permitirá cambiar la tecnología de persistencia sin impactar la lógica de negocio.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	Las consultas complejas deberán optimizarse mediante la creación de índices apropiados en las columnas frecuentemente utilizadas en cláusulas WHERE, JOIN y ORDER BY. Se deberá realizar análisis de planes de ejecución (EXPLAIN PLAN) para identificar y corregir consultas ineficientes.		
2.33.	Auditoría y trazabilidad de operaciones: Todas las peticiones realizadas sobre las APIs expuestas deberán contar con un mecanismo de auditoría integral, que permita garantizar la trazabilidad completa de las operaciones ejecutadas por los usuarios, tanto a nivel funcional como de datos. La auditoría deberá implementarse mediante mecanismos persistentes en la base de datos, tales como tablas de auditoría bajo un modelo maestro–detalle, así como el uso de funciones, procedimientos almacenados, disparadores (triggers), paquetes u otros componentes equivalentes, según corresponda, que permitan registrar los cambios efectuados campo a campo sobre la información administrada. El sistema deberá almacenar, como mínimo, la siguiente información para cada operación auditada: • Tipo de operación realizada (CRUD). • Valor anterior y valor actual del dato modificado, cuando aplique. • Dirección IP del equipo desde el cual se realizó la operación. • Nombre del equipo (host) desde el cual se realizó la operación. • Identificador del usuario que ejecutó la operación. • Fecha y hora exacta de la operación. • Unidad a la que pertenece el usuario. • Identificador de la API, servicio u operación invocada. • Cualquier otro campo que se defina durante la etapa de levantamiento y definición de requerimientos. La información de auditoría deberá ser íntegra, consistente, no modificable y consultable, y deberá cumplir con los lineamientos de seguridad, confidencialidad y retención de información establecidos por la entidad.		
2.34.	Todas las APIs REST desarrolladas deberán ser desplegadas en el servidor Oracle WebLogic del ambiente productivo y deberán ser registradas y publicadas en la herramienta de API Manager (ítem 3) para su exposición controlada a consumidores internos o externos. Cada API deberá contar con una especificación formal en estándar OpenAPI 3.0, describiendo de manera completa sus endpoints, parámetros, estructuras de datos, códigos de respuesta y versionamiento. El contratista deberá importar dicha especificación en la plataforma de API Management y configurar los endpoints correspondientes, apuntando a las URLs reales de los servicios desplegados en WebLogic. Asimismo, se deberán aplicar las políticas de seguridad, control de acceso, limitación de tráfico, versionamiento y gobierno de APIs, garantizando que la exposición pública de los servicios se realice exclusivamente a través del API Gateway y bajo un esquema de direccionamiento estandarizado.		
2.35.	Documentación: • Todas las APIs deberán contar con documentación OpenAPI actualizada. • La documentación deberá reflejar ejemplos reales de uso.		
2.36.	Diagramas de arquitectura requeridos El contratista deberá entregar actualizados los siguientes diagramas de arquitectura, los cuales permitirán comprender la solución propuesta, su despliegue, seguridad e integración. • Diagrama de Arquitectura Lógica (Vista de alto nivel): debe mostrar la estructura general de la solución y la interacción entre los principales componentes. • Diagrama de Arquitectura Física / Despliegue • Diagrama de Despliegue de Aplicaciones (WAR en WebLogic) • Diagrama de Flujo de Seguridad (Autenticación y Autorización) • Diagrama de Migración SOAP → REST		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	• Diagrama de Flujo de Manejo de Errores Los diagramas deberán: • Estar en formato estándar (UML, C4 Model o equivalente). • Mantener nomenclatura clara y consistente. • Deberán entregarse como parte de la documentación técnica final.		
3.	**INSTALACIÓN Y CONFIGURACIÓN WSO2 API MANAGER EN CLÚSTER**		
3.1.	Las APIs REST resultantes de la migración desde arquitectura SOAP deberán ser publicadas y accesibles exclusivamente a través de WSO2 API Manager, operando con autenticación y controles de acceso y políticas correspondientes. Asimismo, la plataforma deberá operar en modalidad de alta disponibilidad en clúster activo-activo, con balanceo efectivo de carga y mecanismos que garanticen continuidad del servicio ante la caída controlada de uno de los nodos, sin impacto perceptible para los consumidores y permitiendo su reincorporación automática una vez restablecido. El contratista deberá garantizar que las APIs mantengan íntegramente la lógica de negocio original y la compatibilidad funcional con los sistemas actualmente integrados, sin generar afectaciones en los procesos existentes. Cualquier ajuste u optimización deberá ser documentada y aprobada por la entidad.		
3.2.	El contratista deberá instalar la herramienta WSO2 API Manager versión 4.3.0 o una versión superior compatible.		
3.3.	Especificaciones de Infraestructura: El contratista deberá instalar y configurar dos máquinas virtuales con sistema operativo Linux para alojar los nodos del clúster de WSO2 API Manager. Cada máquina virtual deberá contar con las siguientes especificaciones mínimas de hardware: • 8 núcleos virtuales de CPU (vCPU) • 16 GB de memoria RAM • 100 GB de almacenamiento en disco SSD • Interfaz de red con conectividad a la red corporativa y capacidad de comunicación entre nodos Las máquinas virtuales deberán nombrarse según los parámetros indicados por el personal técnico del Grupo Tecnologías de la Información y las Comunicaciones DIJIN y contar con direcciones IP estáticas para garantizar la estabilidad de la configuración del clúster. NOTA: Los recursos de hardware para la creación de las máquinas virtuales serán proveídos por el Grupo Tecnologías de la Información y las Comunicaciones DIJIN.		
3.4.	En cada máquina virtual, el contratista deberá realizar la instalación y configuración de los siguientes componentes previos a la instalación de WSO2 API Manager: • Java Development Kit (JDK) versión 11 o JDK 17 según los requisitos oficiales de WSO2 API Manager. • Las variables de entorno JAVA_HOME y PATH deberán configurarse correctamente apuntando a la instalación de Java. Estas variables deberán agregarse al perfil del sistema (/etc/environment o /etc/profile.d/) para garantizar su persistencia tras reinicios. • Se deberán ajustar los límites del sistema operativo (ulimit) para permitir el número adecuado de archivos abiertos y procesos. Estos límites deberán configurarse en /etc/security/limits.conf. • Se deberá configurar sincronización de tiempo mediante NTP (Network Time Protocol) o chrony para garantizar consistencia temporal entre ambos nodos del clúster. • Se deberá configurar la resolución de nombres (DNS) o archivo /etc/hosts para que cada nodo pueda resolver el nombre del otro nodo.		
3.5.	Para la implementación del clúster de WSO2 API Manager, el contratista deberá configurar una base de datos centralizada y compartida entre todos los nodos, utilizando un motor oficialmente soportado por el fabricante y compatible con JDBC. Se deberán crear y configurar los esquemas requeridos por la plataforma para el almacenamiento de metadatos, configuraciones, usuarios, roles, políticas y		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	componentes compartidos, ejecutando los scripts oficiales de inicialización según la documentación del producto. Asimismo, se deberá configurar adecuadamente el pool de conexiones y los parámetros de rendimiento recomendados, garantizando alta disponibilidad, consistencia transaccional y seguridad. El usuario de base de datos asignado deberá contar con los privilegios necesarios para la correcta operación, mantenimiento y actualización de la plataforma. NOTA: Los recursos de base de datos serán proveídos por el Grupo Tecnologías de la Información y las Comunicaciones DIJIN.		
3.6.	El contratista deberá configurar el clúster de WSO2 API Manager en modo activo-activo, garantizando alta disponibilidad y escalabilidad horizontal, de acuerdo con las mejores prácticas y la documentación oficial del fabricante. La configuración deberá incluir la habilitación del mecanismo de clustering mediante Hazelcast para la sincronización de sesiones, caché y estado entre nodos, estableciendo un método de descubrimiento confiable (preferiblemente TCP-IP con definición explícita de nodos) y asegurando la correcta parametrización de puertos y nombres de host únicos por instancia. Se deberán configurar adecuadamente los nodos como Gateway Workers, validar la correcta comunicación interna entre instancias y garantizar la apertura y disponibilidad de los puertos requeridos, evitando conflictos de red o restricciones de firewall. La configuración final deberá asegurar consistencia operativa, tolerancia a fallos y correcto balanceo de carga entre los nodos del clúster.		
3.7.	El contratista deberá configurar la seguridad de la plataforma WSO2 API Manager conforme a las mejores prácticas del fabricante y a las políticas de seguridad de la Policía Nacional, garantizando la protección integral de la infraestructura y de las APIs expuestas. Esta configuración deberá incluir el aseguramiento de credenciales administrativas mediante la eliminación de contraseñas predeterminadas y aplicación de políticas de complejidad robustas; la sustitución de los certificados, keystores y truststores por certificados oficiales de la entidad conforme a su política PKI; la habilitación exclusiva de comunicaciones seguras mediante HTTPS con TLS 1.2 o superior, deshabilitando HTTP en ambientes productivos; la implementación de mecanismos de control de tráfico mediante políticas de Rate Limiting y Throttling en los diferentes niveles soportados por la plataforma; la configuración de LDAP como mecanismo estándar de autenticación y autorización, incluyendo el uso de scopes y roles para garantizar el principio de mínimo privilegio; y la activación de mecanismos de auditoría que registren las operaciones administrativas y de consumo de APIs, permitiendo trazabilidad, monitoreo y cumplimiento normativo.		
3.8.	El contratista deberá implementar y configurar los mecanismos de monitoreo y analítica de la plataforma WSO2 API Manager, habilitando la recolección, procesamiento y visualización de métricas de uso y desempeño de las APIs. Se deberán configurar paneles de control que permitan visualizar indicadores clave tales como volumen de invocaciones, tiempos de respuesta y latencia, tasas de error, consumo por aplicación o suscriptor y tendencias de crecimiento. De igual manera, se deberán definir y habilitar alertas automáticas ante eventos críticos relacionados con disponibilidad, degradación de desempeño, incremento de errores o saturación de límites de consumo, garantizando una gestión proactiva de la operación y continuidad del servicio.		
3.9.	El contratista deberá implementar una política de respaldo y recuperación ante desastres para las máquinas virtuales donde se instalará la plataforma WSO2 API Manager, garantizando la continuidad operativa y la protección de la información. Los respaldos deberán ejecutarse con una periodicidad definida y conservarse conforme a las políticas de retención establecidas por la entidad. Asimismo, el contratista deberá documentar y validar mediante pruebas controladas el procedimiento completo de recuperación (Disaster Recovery), estableciendo tiempos objetivos de recuperación (RTO) y puntos objetivos de recuperación (RPO) acordes con los niveles de servicio definidos, para lo cual se deberá realizar una prueba de restauración de las máquinas virtuales a fin de comprobar su integridad.		
3.10.	El contratista deberá entregar documentación técnica de la implementación de WSO2 API Manager, con el nivel de detalle necesario para que el equipo técnico de la entidad pueda administrar, operar, mantener y solucionar incidentes de la plataforma. La documentación deberá incluir como mínimo: la guía completa de instalación y configuración del entorno, la descripción de parámetros y personalizaciones aplicadas, los diagramas de arquitectura que representen la topología y componentes involucrados, los procedimientos operativos estándar para tareas recurrentes de administración y mantenimiento, y una guía de resolución de problemas con los escenarios más frecuentes y sus respectivas acciones correctivas. Toda la documentación deberá entregarse en formato digital editable y actualizada conforme a la configuración final implementada en producción.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
3.11.	El contratista deberá crear y probar los scripts automatizados de respaldo, monitoreo y mantenimiento en lenguajes como Bash o Python, que faciliten la operación rutinaria del sistema.		
3.12.	El contratista deberá garantizar que el flujo de invocación de las APIs migradas siga una arquitectura controlada y segura desde el cliente hasta el backend desplegado en Oracle WebLogic Server. Todas las solicitudes externas deberán ingresar a través del balanceador de carga hacia la URL pública del API Gateway, utilizando comunicación HTTPS y mecanismos de autenticación. El API Gateway deberá validar la identidad del consumidor, verificar permisos y políticas de acceso, aplicar los controles y políticas establecidas antes de redirigir la petición al endpoint productivo configurado en WebLogic. El servicio backend procesará la lógica de negocio y retornará la respuesta al Gateway, donde se aplicarán las políticas de salida, métricas y registros de auditoría correspondientes, completando así el ciclo de invocación bajo un esquema de alta disponibilidad, trazabilidad y control centralizado.		
3.13.	El contratista deberá garantizar la correcta configuración de la conectividad de red entre la plataforma WSO2 API Manager y el servidor Oracle WebLogic donde se encuentran desplegados los servicios backend, asegurando comunicación estable, segura y de alto desempeño. Para tal efecto, se deberán realizar las configuraciones que permitan el tráfico entre los nodos del clúster y los puertos expuestos por WebLogic. Asimismo, se deberán configurar parámetros adecuados de timeout de conexión y lectura en las invocaciones realizadas desde el API Gateway hacia los servicios backend, con el fin de prevenir bloqueos o degradación del servicio ante fallas de red. En caso de ser necesario, se deberá implementar autenticación mutua mediante certificados digitales (mTLS) para asegurar la validación bidireccional entre WSO2 y WebLogic, garantizando la confidencialidad e integridad de las comunicaciones internas.		
3.14.	El contratista deberá configurar mecanismos de gestión de errores y resiliencia en la plataforma WSO2 API Manager para proteger los servicios backend desplegados en Oracle WebLogic y garantizar estabilidad operativa. Se deberán habilitar políticas de manejo de fallos que incluyan patrones de tolerancia a errores, como circuit breaker y reintentos controlados para fallos transitorios, evitando la propagación masiva de solicitudes hacia servicios degradados. En caso de indisponibilidad o error del backend, el API Gateway deberá retornar respuestas estandarizadas que no expongan información técnica sensible, preservando la seguridad y la experiencia del consumidor. Asimismo, todas las invocaciones fallidas deberán registrarse con el nivel de detalle necesario para análisis y trazabilidad, incluyendo identificación de la API, consumidor, tipo de error y tiempos de respuesta, permitiendo la correlación y el diagnóstico oportuno de incidentes.		
4.	**MANTENIMIENTO Y DESARROLLO DE NUEVAS FUNCIONALIDADES EN EL SISTEMA DE INFORMACIÓN INTEGRADA DE AUTOMOTORES (I2AUT)**		
4.1.	El contratista deberá realizar la revisión integral de los reportes asociados al sistema de información, con el fin de verificar su correcta operación, consistencia y alineación con los requerimientos funcionales definidos. Como parte de esta actividad, se deberán analizar, ajustar y optimizar los reportes y las vistas de base de datos utilizadas para la generación de los mismos, garantizando que la información consultada sea verídica, íntegra y consistente, y que refleje de manera adecuada el estado real de los datos en el sistema. Los ajustes deberán contemplar la validación de la estructura de las vistas, las consultas subyacentes, el rendimiento de ejecución y la correcta presentación de la información a los usuarios finales, dejando evidencia de los cambios realizados y de las validaciones efectuadas.		
4.2.	El sistema deberá permitir que el Reporte de Citas sea parametrizable por el usuario, de tal manera que este pueda seleccionar dinámicamente las columnas que desea visualizar, de acuerdo con su perfil. Adicionalmente, el sistema deberá habilitar la exportación del reporte en los formatos Excel y PDF, garantizando que dicha funcionalidad esté disponible únicamente para los usuarios que cuenten con el rol o permisos correspondientes. La parametrización y los archivos exportados deberán respetar la integridad y consistencia de la información, así como los formatos y estándares visuales establecidos por la entidad.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
4.3.	El contratista deberá realizar el desacoplamiento del reporte de citas actualmente asociado al módulo de administración de turnos, trasladando su funcionalidad al módulo de reportes, de conformidad con la arquitectura definida del sistema de información. El reporte de citas deberá continuar ofreciendo las capacidades funcionales definidas, incluyendo la parametrización por columnas, filtros, control de acceso por roles y exportación a los formatos autorizados, asegurando su correcta integración dentro del módulo de reportes.		
4.4.	El contratista deberá realizar los ajustes necesarios en el sistema para permitir la agrupación de perfiles de usuario en roles, de manera que los permisos y funcionalidades puedan ser asignados, seleccionados o deseleccionados tanto de forma individual como en grupo, mediante una estructura jerárquica tipo árbol. La funcionalidad deberá permitir: • Visualización jerárquica de roles, perfiles y permisos. • Selección y deselección masiva de permisos por nodo o subárbol. • Selección y deselección individual de permisos específicos. La gestión de roles y perfiles deberá cumplir con los lineamientos de seguridad establecidos, garantizando la trazabilidad de los cambios realizados y la correcta aplicación de los permisos asignados.		
4.5.	Se deberá crear el perfil “Administración de Turnos Seccional”, el cual permitirá a los usuarios asignados gestionar exclusivamente la información del módulo de Administración de Turnos correspondiente a su unidad o seccional, sin posibilidad de acceso o visualización de información perteneciente a otras unidades. Este perfil deberá contemplar, como mínimo: • Acceso restringido únicamente a las funcionalidades del módulo Administración de Turnos. • Limitación de la gestión, consulta y modificación de datos a la unidad/seccional asociada al usuario autenticado. • Aplicación de controles de seguridad a nivel de aplicación y, cuando aplique, a nivel de base de datos. • Integración con el esquema de roles y permisos del sistema, garantizando la segregación de funciones. • Registro en los mecanismos de auditoría de todas las operaciones realizadas por los usuarios con este perfil. La implementación deberá ser validada en los ambientes de prueba antes de su habilitación en producción.		
4.6.	Se deberá implementar un esquema de perfilamiento individual y granular para cada una de las opciones funcionales de todos los módulos que componen el sistema de información I2AUT, permitiendo la asignación y revocación de permisos de manera independiente y controlada. Este esquema deberá contemplar, como mínimo: • Definición de permisos a nivel de módulo, submódulo y opción funcional (pantallas, acciones, servicios o funcionalidades específicas). • Asignación de permisos tanto individualmente como mediante roles agrupados, conforme a la estructura de perfiles definida por la entidad. • Capacidad de habilitar o deshabilitar opciones de manera dinámica sin requerir cambios en el código fuente. • Aplicación de controles de autorización a nivel de interfaz gráfica, servicios backend (API/servicios REST) y, cuando aplique, acceso a datos. • Restricción de acceso basada en el perfil del usuario autenticado, garantizando el principio de mínimo privilegio. • Integración con los mecanismos de auditoría y trazabilidad, registrando las operaciones realizadas según el perfil asignado.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	• Soporte para estructuras jerárquicas o tipo árbol en la administración de permisos, facilitando la gestión masiva o individual de opciones. La implementación deberá ser validada en los ambientes de prueba, asegurando que las restricciones de acceso se apliquen de forma consistente en todos los módulos del sistema.		
4.7.	El contratista deberá realizar la actualización de las plantillas correspondientes a los formatos de certificación y devolución, con especial énfasis en la validación y ajuste de los datos asociados a códigos, catálogos y demás información estática contenida en dichos formatos. Así mismo, se deberá agregar la información correspondiente al pago de la cita en el reverso de la plantilla. Una vez realizadas las actualizaciones, el contratista deberá validar los formatos y dejar evidencia de las pruebas efectuadas, asegurando su correcto funcionamiento.		
4.8.	El contratista deberá realizar los ajustes funcionales y desarrollos tecnológicos necesarios para la digitalización integral del formato de Certificación de Revisión Técnica, actualmente emitido en formato físico, con el propósito de incorporarlo y gestionarlo electrónicamente dentro del sistema de información I2AUT. La solución deberá permitir el registro estructurado de toda la información requerida, incluyendo la incorporación de las firmas de los peritos responsables del procedimiento (mediante mecanismos de firma electrónica o firma digital conforme a la normativa vigente), el cargue y almacenamiento de fotografías de improntas y demás soportes documentales que garanticen la trazabilidad del proceso. Cada certificación generada deberá garantizar su integridad, autenticidad y no repudio mediante la implementación de funciones hash criptográficas o mecanismos equivalentes que permitan validar que el documento no ha sido alterado desde su emisión. Adicionalmente, se deberá implementar un mecanismo de sellado de tiempo (timestamp) que registre de manera verificable la fecha y hora exacta de generación y firma del documento, permitiendo demostrar su existencia en un momento determinado. Asimismo, el sistema deberá generar automáticamente un código QR de verificación incluido en el documento digital, el cual permita validar en línea la autenticidad de la certificación mediante un servicio de consulta que confirme su estado, integridad y vigencia. El código QR deberá llevar a una interfaz de aterrizaje en la aplicación web de agendamiento de turnos para la revisión técnica en identificación de automotores en donde se le mostrará al usuario la información que confirme o no su validez.		
4.9.	El contratista deberá desarrollar la funcionalidad de generación automática de codificación consecutiva para las devoluciones de automotores, garantizando que dicha identificación sea única, secuencial, inmutable y controlada por el sistema, sin intervención manual por parte de los usuarios. Para lo cual se deberá contemplar como mínimo: • Definición de la estructura del código (prefijos, sufijos, longitud y formato), de acuerdo con los lineamientos establecidos por la entidad. • Control de concurrencia para evitar duplicidades en escenarios de alta transaccionalidad. • Persistencia y trazabilidad del consecutivo generado. • Mecanismos de validación que impidan la modificación manual del código una vez asignado. • Compatibilidad con los procesos de consulta, reporte y auditoría del sistema. La funcionalidad deberá ser implementada y validada en los ambientes correspondientes antes de su despliegue en producción.		
4.10.	Se deberán implementar las reglas de negocio a nivel de frontend y backend que permitan la inserción, consulta y actualización de información asociada a autorizaciones de uso provisional de automotores emitidas por diferentes entidades. Para tal efecto, el contratista deberá: • Ajustar el modelo de datos, incorporando los campos necesarios en las tablas correspondientes, garantizando la integridad referencial y la correcta normalización de la información.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	• Implementar y/o ajustar la lógica en la capa de presentación (frontend) que permita el registro, actualización y consulta de los datos, mediante el uso de componentes de interfaz gráfica, controles, validaciones y funciones de UI, garantizando una interacción consistente y segura para el usuario final. • Modificar la lógica de negocio del sistema para permitir el registro, actualización y consulta controlada de dicha información. • Actualizar las vistas y consultas de antecedentes de vehículos, de tal manera que los registros asociados a resoluciones de uso provisional sean excluidos de los resultados de dichas consultas. • Garantizar que la exclusión de la información se aplique de forma consistente tanto a nivel de base de datos como en los servicios de aplicación que consuman dichas vistas. • Implementar los mecanismos de auditoría y trazabilidad para los nuevos campos, registrando como mínimo las operaciones de creación, modificación y eliminación, así como los valores anteriores y actuales, conforme a los lineamientos de auditoría definidos para el sistema. • Validar los ajustes en los ambientes de desarrollo y pruebas, asegurando que las modificaciones no afecten el comportamiento funcional ni el rendimiento de las consultas existentes.		
4.11.	Se deberá implementar el enlace e integración de la información de los pagos realizados desde la aplicación de Agendamiento de Turnos Automotores, a través del canal PSE, con el objetivo de garantizar la trazabilidad completa del proceso de pago. El contratista deberá: • Asociar cada transacción de pago con el turno, usuario, servicio y referencia correspondiente, garantizando la unicidad y consistencia de los registros. • Almacenar los identificadores de transacción provistos por la pasarela de pagos (PSE) y los estados intermedios y finales del pago. • Implementar mecanismos de control de errores, reintentos y conciliación, que permitan identificar pagos pendientes, fallidos o inconsistentes. • Garantizar la trazabilidad y auditoría de las operaciones relacionadas con los pagos, incluyendo fechas, estados, usuario, canal, dirección IP y demás datos relevantes. • Asegurar que la información de pagos pueda ser consultada y reportada por los perfiles autorizados, sin afectar la seguridad ni la confidencialidad de los datos. • Validar la integración en los ambientes de prueba y preproducción, verificando la correcta correlación entre los eventos del proceso y los registros almacenados.		
4.12.	En el Módulo Revisiones Técnicas, sección Revisiones Encontradas, se deberá habilitar la opción para el cargue y almacenamiento del certificado físico en formato PDF, asociado de manera individual a cada revisión técnica realizada a un automotor. El contratista deberá: • Implementar en la interfaz de usuario la funcionalidad de cargue de archivos PDF, garantizando una experiencia de uso clara y controlada. • Asociar el archivo cargado a la revisión técnica específica y al vehículo correspondiente, asegurando la correcta trazabilidad del documento. • Validar el formato, tamaño máximo y contenido permitido del archivo, conforme a las políticas de seguridad definidas. • Almacenar el certificado de forma segura, en un repositorio documental, según la arquitectura definida por la entidad. • Controlar el acceso, consulta y descarga del certificado únicamente a los usuarios con los perfiles autorizados. • Registrar la auditoría y trazabilidad de las operaciones de cargue o consulta del documento. • Validar la correcta operación de la funcionalidad en los ambientes de desarrollo, pruebas y producción.		
4.13.	Se deberá implementar una regla de negocio de bloqueo automático para la expedición de certificaciones, cuando el vehículo se encuentre sujeto a medidas cautelares, requerimientos administrativos o requerimientos judiciales, conforme a la información registrada y vigente en el sistema.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	Para tal efecto, el contratista deberá: • Validar de manera obligatoria, previo a la expedición de cualquier certificación, la existencia de restricciones activas asociadas al vehículo. • Impedir la generación, visualización y/o descarga de la certificación cuando se detecte alguna condición de bloqueo. • Informar al usuario, mediante mensajes claros y personalizados, la causa específica del bloqueo, sin exponer información sensible. • Registrar la trazabilidad y auditoría de los intentos de expedición bloqueados, incluyendo el vehículo, usuario, fecha, motivo del bloqueo y módulo involucrado. • Garantizar que la validación se aplique de forma consistente en la interfaz de usuario, servicios de aplicación y, cuando aplique, a nivel de base de datos. • Permitir la habilitación automática de la expedición de certificaciones una vez las restricciones hayan sido levantadas o marcadas como inactivas, conforme a los procedimientos definidos. • Validar la correcta implementación de esta regla en los ambientes de prueba y producción, asegurando que no se afecten otros procesos del sistema.		
4.14.	En el Módulo Administración de Turnos se deberá desarrollar la funcionalidad para el envío de notificaciones por correo electrónico a los usuarios que hayan agendado citas a través de la aplicación de Agendamiento de Turnos Automotores, con el fin de informar eventos relevantes del proceso. Adicionalmente, el sistema deberá permitir la publicación de notificaciones, avisos o comunicados visibles en el frontend de la página de agendamiento, utilizando contenido en formato de texto y/o imágenes, conforme a los lineamientos definidos por la entidad. Igualmente se deberá realizar el diseño de la plantilla de correo, incluyendo asunto, contenido, variables dinámicas y elementos gráficos. La funcionalidad deberá contemplar, como mínimo: • Envío de notificaciones por correo electrónico asociadas al agendamiento, modificación, confirmación, cancelación o recordatorio de citas. • Gestión de mensajes informativos en la interfaz de la página de agendamiento, con control de vigencia, orden de visualización y estado (activo/inactivo). • Control de acceso para la creación, edición y publicación de notificaciones, limitado a los perfiles autorizados. • Registro de la trazabilidad y auditoría de las notificaciones enviadas y publicadas, incluyendo fecha, usuario y tipo de evento. • Manejo de errores y reintentos en el envío de correos electrónicos, garantizando la confiabilidad del proceso. • Validación funcional de la correcta visualización y envío de las notificaciones en los ambientes de prueba y producción.		
4.15.	Se deberá ajustar la funcionalidad de reasignación de turnos para permitir la reprogramación de citas de manera controlada y autorizada, garantizando que ninguna cita pueda ser reasignada sin contar previamente con la aprobación del Jefe de la Sala Técnica de la unidad correspondiente. La implementación deberá contemplar, como mínimo: • Definición de un flujo de aprobación previo a la reasignación o reprogramación de una cita. • Restricción de la funcionalidad únicamente a los usuarios y perfiles autorizados para solicitar o aprobar la reprogramación. • Registro de la solicitud, aprobación o rechazo de la reasignación, incluyendo usuario solicitante, usuario aprobador, fecha, hora y motivo. • Aplicación de validaciones que impidan la modificación del turno en ausencia de la aprobación correspondiente. • Notificación a los usuarios involucrados sobre el estado de la solicitud de reprogramación. • Integración del proceso con los mecanismos de auditoría y trazabilidad, dejando evidencia de todos los cambios realizados.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	• Validación del correcto funcionamiento del flujo en los ambientes de desarrollo y pruebas, asegurando que se cumplan las reglas de negocio definidas.		
4.16.	En el Módulo de Gestión Administrativa se deberá ajustar la lógica de creación y administración de roles, de tal manera que esta funcionalidad quede restringida exclusivamente al perfil de Administrador Funcional, conforme a las políticas de seguridad y control definidas por la entidad. Adicionalmente, se deberán incorporar los campos “Caso SIGMA” y “Número GEPOL”, este último deberá validarse con el Sistema Gestor Documental, con el fin de verificar la autenticidad y veracidad del número de la comunicación asociada al registro. La implementación deberá contemplar, como mínimo: • Restricción de acceso a la creación, modificación y eliminación de roles únicamente al Administrador Funcional. • Validaciones que impidan la ejecución de estas acciones por usuarios no autorizados. • Incorporación de los campos Caso SIGMA y GEPOL en los formularios y modelos de datos correspondientes. • Integración con el Sistema Gestor Documental para la verificación del número de comunicación, garantizando la consistencia de la información. • Manejo de errores y mensajes informativos cuando la validación con el sistema externo no sea exitosa. • Registro de la auditoría y trazabilidad de las operaciones relacionadas con la gestión de roles y la validación documental. • Validación funcional y técnica en los ambientes de desarrollo y pruebas.		
4.17.	Actualización capa de Backend y Frontend El contratista deberá identificar, evaluar y actualizar las bibliotecas, librerías, dependencias y demás componentes utilizados tanto en la capa backend como en la capa frontend que se encuentren obsoletos, descontinuados o con vulnerabilidades conocidas, sustituyéndolos por versiones más recientes y estables, garantizando en todo momento su compatibilidad estricta con Java 8. La actividad deberá contemplar, como mínimo: • Análisis del inventario de dependencias y componentes actualmente utilizados en el proyecto. • Actualización controlada de las dependencias, asegurando la compatibilidad funcional y técnica con el stack tecnológico definido. • Corrección de vulnerabilidades de seguridad identificadas, conforme a reportes de fabricantes, CVE u otras fuentes reconocidas. • Ejecución de pruebas funcionales, de regresión y de seguridad posteriores a las actualizaciones, para verificar que no se afecte el comportamiento del sistema. • Documentación de los cambios realizados, incluyendo versiones anteriores, versiones actualizadas y justificación del cambio. • Validación y aprobación de las actualizaciones por parte del supervisor del contrato, previo a su despliegue en los ambientes correspondientes. • Garantía de que las actualizaciones no introduzcan dependencias incompatibles con la arquitectura existente ni con las políticas de la entidad.		
4.18.	El contratista deberá realizar la actualización de la capa frontend del sistema de información I2AUT utilizando tecnologías modernas y ampliamente soportadas, garantizando criterios de calidad, seguridad, mantenibilidad y escalabilidad. El desarrollo del frontend deberá basarse en React JS versión 18 o superior como librería base para la construcción de interfaces de usuario, garantizando un renderizado eficiente, reutilización de componentes y una adecuada separación de responsabilidades.		
4.19.	Se empleará Ant Design (AntD) como framework de componentes visuales, con el fin de asegurar una interfaz gráfica consistente, accesible, responsiva y alineada con estándares empresariales, facilitando la construcción de formularios, tablas, modales, notificaciones y demás elementos transaccionales.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
4.20.	Se deberá realizar la migración y estandarización completa de la capa frontend de la aplicación, eliminando el uso actual de Material-UI, Bootstrap y demás librerías de UI que se identifiquien, con el fin de unificar la interfaz gráfica bajo el framework Ant Design (AntD) para React JS. Para tal efecto, el contratista deberá: • Identificar y retirar todas las dependencias asociadas a Material-UI y Bootstrap, así como cualquier otro componente de UI no estandarizado. • Migrar los componentes existentes (formularios, tablas, modales, validaciones, notificaciones, layouts, etc.) a componentes nativos de Ant Design, manteniendo la funcionalidad actual. • Garantizar la consistencia visual, de usabilidad y experiencia de usuario (UX/UI) en toda la aplicación. • Ajustar estilos personalizados, temas y hojas de estilo para que sean compatibles con Ant Design, utilizando la paleta de colores institucional. • Verificar la compatibilidad de la versión de Ant Design seleccionada con la versión de React definida en el proyecto. • Corregir posibles conflictos de estilos, dependencias o comportamientos derivados de la migración. • Ejecutar pruebas funcionales y de regresión para validar que la migración no afecte el comportamiento de la aplicación. • Documentar los cambios realizados y actualizar la guía de estilos o lineamientos de frontend, cuando aplique. • La migración deberá realizarse de forma controlada y validada en los ambientes de capa de aplicación (local, pruebas y producción) como se establece en los ítems 1.27 y 1.28 del presente anexo técnico, garantizando la estabilidad, mantenibilidad y evolución futura de la capa frontend.		
4.21.	La solución deberá contemplar un mecanismo de gestión de navegación que permita definir flujos funcionales, control de acceso y rutas protegidas, haciendo uso de la herramienta React Router. El desarrollo deberá realizarse empleando TypeScript, con el fin de garantizar tipado fuerte, claridad en los contratos de datos y reducción de errores en tiempo de desarrollo.		
4.22.	El consumo de los servicios expuestos por la capa backend deberá realizarse mediante librerías estándar para comunicación HTTP o herramientas especializadas para la gestión de estado remoto de acuerdo con la complejidad de los flujos de información requeridos.		
4.23.	En los casos en que se requiera la gestión de estado global compartido entre distintos módulos de la aplicación, el contratista deberá emplear mecanismos adecuados, como Redux Toolkit o tecnologías equivalentes, limitando su uso a escenarios donde sea estrictamente necesario y evitando su aplicación en estados locales o formularios.		
4.24.	Se deberá implementar un conjunto de mejoras orientadas a optimizar el flujo de navegación y la interacción de los usuarios con la aplicación, con el objetivo de simplificar su uso, reducir la complejidad operativa y hacer la plataforma más intuitiva y fácil de utilizar. Para la implementación el contratista deberá contemplar, como mínimo: • Revisión y optimización de los flujos de navegación entre módulos, pantallas y funcionalidades. • Simplificación de procesos y formularios, reduciendo pasos innecesarios y mejorando la claridad de las acciones disponibles. • Estandarización de componentes visuales, mensajes, íconos y comportamientos de la interfaz. • Mejora de la jerarquía visual y organización de la información, facilitando la comprensión por parte del usuario. • Implementación de mensajes de ayuda, validaciones claras y retroalimentación inmediata ante las acciones del usuario. • Garantía de consistencia en la experiencia de usuario en todos los módulos del sistema. • Validación de los ajustes mediante pruebas de usabilidad con usuarios autorizados o representativos. • Documentación de los cambios realizados y actualización de los manuales de usuario, cuando aplique.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	Estas mejoras deberán realizarse sin afectar la seguridad, el desempeño ni la funcionalidad existente de la aplicación y harán parte del proceso de aceptación de los desarrollos.		
4.25.	Se deberá habilitar y configurar de manera adecuada la protección contra ataques CSRF (Cross-Site Request Forgery) en la aplicación, con el fin de prevenir la ejecución de solicitudes no autorizadas en nombre de usuarios autenticados. Para la implementación el contratista deberá contemplar, como mínimo: • Habilitación del mecanismo de protección CSRF a nivel de la aplicación, conforme a las capacidades del framework de seguridad utilizado. • Implementación y validación de tokens CSRF en todos los formularios y solicitudes que modifiquen estado (creación, actualización, eliminación). • Inclusión automática del token CSRF en las peticiones realizadas desde el frontend hacia el backend. • Configuración controlada de excepciones únicamente para los endpoints públicos o no autenticados, debidamente identificados y justificados. • Evitar peticiones a las APIs desde cualquier origen (CORS Permisivos). • Garantía de que los endpoints excluidos de la protección CSRF no expongan operaciones sensibles ni de modificación de datos. • Manejo adecuado de errores y mensajes informativos cuando se detecten solicitudes sin token o con token inválido. • Validación del correcto funcionamiento de la protección CSRF mediante pruebas de seguridad en los ambientes definidos. • Documentación de la configuración realizada y de los endpoints exceptuados, para efectos de auditoría y mantenimiento. La implementación deberá alinearse con las buenas prácticas de seguridad OWASP y no deberá afectar la experiencia de usuario ni el desempeño de la aplicación.		
4.26.	Ajuste modelo de auditoría El contratista deberá revisar y ajustar el modelo de auditoría del sistema de información I2AUT de manera que se garantice la trazabilidad completa de las operaciones ejecutadas por los usuarios, tanto a nivel funcional como de datos. La auditoría deberá implementarse mediante mecanismos persistentes en la base de datos, tales como tablas de auditoría bajo un modelo maestro–detalle, así como el uso de funciones, procedimientos almacenados, disparadores (triggers), paquetes u otros componentes equivalentes, según corresponda, que permitan registrar los cambios efectuados campo a campo sobre la información administrada. El sistema deberá almacenar, como mínimo, la siguiente información para cada operación auditada: • Tipo de operación realizada (CRUD). • Valor anterior y valor actual del dato modificado, cuando aplique. • Dirección IP del equipo desde el cual se realizó la operación. • Nombre del equipo (host) desde el cual se realizó la operación. • Identificador del usuario que ejecutó la operación. • Fecha y hora exacta de la operación. • Unidad a la que pertenece el usuario. • Identificador de la API, servicio u operación invocada. • Cualquier otro campo que se defina durante la etapa de levantamiento y definición de requerimientos. La información de auditoría deberá ser íntegra, consistente, no modificable y consultable, y deberá cumplir con los lineamientos de seguridad, confidencialidad y retención de información establecidos por la entidad.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
4.27.	Para consultas que retornen grandes volúmenes de datos, se deberá implementar paginación mediante limit/offset o cursor-based pagination. La paginación deberá ser configurable por el cliente con límites máximos definidos para prevenir sobrecarga del servidor.		
4.28.	El contratista deberá garantizar que las tecnologías empleadas sean compatibles entre sí, cuenten con soporte vigente, y se encuentren alineadas con las buenas prácticas recomendadas por los fabricantes, asegurando la correcta integración con la capa de servicios backend y el cumplimiento de los requerimientos funcionales y no funcionales del sistema. Adicionalmente, el contratista deberá: • Realizar la revisión de las funcionalidades existentes relacionadas con los desarrollos efectuados. • Identificar posibles ajustes, correcciones o mejoras necesarias para garantizar la coherencia funcional y técnica del sistema. • Implementar las modificaciones requeridas, previa validación y aprobación por parte del supervisor del contrato.		
5.	**DOCUMENTACIÓN**		
5.1.	El contratista deberá elaborar y entregar la documentación completa correspondiente al desarrollo del proyecto, tanto en medio físico como en medio digital, con una antelación mínima de cinco (5) días hábiles antes de la finalización del plazo de ejecución del presente proceso contractual.		
5.2.	El contratista deberá entregar la siguiente documentación en idioma castellano, asegurando que cumpla con los estándares requeridos para la implementación y operación de la solución: • Manual de usuario final: Instrucciones detalladas para que los usuarios puedan operar la solución de manera efectiva, incluyendo ejemplos prácticos y resolución de problemas comunes. • Manual técnico de la solución implementada: Documentación técnica que describa la arquitectura, configuraciones, dependencias y cualquier otro aspecto necesario para el mantenimiento y actualización de la solución. • Modelos de arquitectura: Representación gráfica y descriptiva de la arquitectura de la solución, incluyendo los componentes, interacciones y flujos principales del sistema. • Modelos de casos de uso: Diagramas y descripciones que detallen los diferentes escenarios de interacción entre los usuarios y el sistema, especificando las funcionalidades principales y secundarias. • Modelos entidad / relacional: Diagramas que representen la estructura de la base de datos, detallando las entidades, relaciones y atributos utilizados en la solución. La entrega deberá realizarse con una antelación mínima de cinco (5) días hábiles antes de la finalización del plazo de ejecución del presente proceso contractual conforme a los formatos y lineamientos establecidos por la entidad, quedando como insumo para la operación, mantenimiento y evolución futura del sistema.		
5.3.	Para cada uno de los desarrollos, ajustes o mantenimientos realizados, el contratista deberá actualizar el Manual de Usuario y el Manual Técnico o Catálogo de Servicios, incorporando de manera clara y estructurada las nuevas funcionalidades, cambios implementados y ajustes derivados del mantenimiento evolutivo o correctivo.		
5.4.	Con el fin de garantizar que los desarrollos satisfagan las necesidades de la Dirección de Investigación Criminal e INTERPOL, el contratista deberá realizar el levantamiento, análisis y documentación de los requisitos funcionales y no funcionales del sistema, de manera previa y/o paralela a las actividades de desarrollo, realizando la identificación clara de los requisitos, reglas de negocio y flujos de información. Para ello deberá utilizar los formatos definidos por la Policía Nacional.		
6.	**TRANSFERENCIA DE CONOCIMIENTO**		
6.1.	El contratista deberá realizar una transferencia de conocimiento de al menos 40 horas en las instalaciones que la Policía Nacional - Dirección de Investigación Criminal e INTERPOL indique, dirigida a un mínimo de 4 personas, en temas de desarrollo de software, así como en temas de administración, monitoreo, troubleshooting y configuración de la plataforma de API Management (WSO2). La actividad deberá realizarse una vez se encuentren implementados los desarrollos en el ambiente de producción y antes de la finalización del plazo de ejecución del presente proceso contractual.		
7.	**SOPORTE**		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
7.1.	El contratista debe brindar soporte y funcional sobre los desarrollos, ajustes, configuraciones y componentes entregados, bajo un esquema de atención 5*8 (cinco días a la semana, ocho horas al día), durante un (1) año contado a partir de la suscripción del acta de recibido a satisfacción por parte de la entidad. El soporte deberá incluir como mínimo la atención, análisis, diagnóstico y corrección de incidentes, errores funcionales, fallas de software, problemas de rendimiento y vulnerabilidades asociadas a los desarrollos implementados, así como el acompañamiento técnico requerido para garantizar la estabilidad y continuidad operativa de la solución. Todas las actividades de soporte deberán quedar debidamente documentadas y.		
7.2.	El contratista deberá disponer del personal idóneo para brindar soporte técnico y funcional, a través de servicio telefónico, presencial y por correo electrónico.		
7.3.	La emergencia deberá ser atendida en un tiempo máximo de dos (2) horas, contadas a partir del reporte de la falla, en las instalaciones de la Policía Nacional – Dirección de Investigación Criminal e INTERPOL, cuando el problema no haya podido ser solucionado mediante soporte telefónico y el supervisor del contrato o el funcionario encargado de la solución implementada solicite expresamente asistencia presencial. Si el problema persiste, se deberá enviar a los ingenieros al sitio, quienes deberán resolver la falla en un tiempo no mayor a 48 horas.		
7.4.	El contratista se compromete a subsanar los fallos y defectos que se presenten en el software implementado, así como cualquier inconveniente en sus funcionalidades, durante el período de garantía solicitado, contado a partir de la fecha de entrega a satisfacción. En caso de que los fallos o defectos no puedan ser subsanados, el contratista deberá proporcionar una solución alternativa que permita la continuidad de la operación de la plataforma. Además, el contratista asumirá los costos de los recursos humanos o tecnológicos necesarios para implementar dicha solución alternativa.		
8.	**GARANTÍA**		
8.1.	El sistema deberá contar con una garantía de un (1) año, contada a partir del recibido a satisfacción. Esta garantía cubrirá los modelos, integraciones, desarrollos a medida, software, hardware y servicios entregados con el sistema. Se deberá contemplar la detección y corrección de las fallas de la solución implementada, así como el suministro y/o reemplazo de los módulos de aplicación que presenten daños o deficiencias en su funcionamiento.		
8.2.	Las actualizaciones de versiones o mejoras como por ejemplo en el GUI (interfaz gráfica) que se requieren para su normal funcionamiento deben ser asumidas por el contratista, durante el periodo de garantía.		
8.3.	El contratista se comprometerá a entregar toda la documentación necesaria, incluyendo manuales, diseños y esquemas, para las labores de mantenimiento correctivo. La información entregada incluirá manuales con los procedimientos de solución para los sistemas y subsistemas, tanto en hardware como en software.		
9.	**ESPECIFICACIONES DE IDONEIDAD Y EXPERIENCIA DEL PERSONAL PROFESIONAL**		
9.1.	El oferente deberá presentar las hojas de vida y toda la documentación necesaria para acreditar la experiencia y conocimiento académico de los profesionales teniendo en cuenta su importancia y criticidad de participación en el presente proceso, las actividades objeto del contrato no podrán ser ejecutadas por un solo profesional o ingeniero.		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
9.2.	**PROFESIONAL EN GERENCIA DE PROYECTOS** El oferente deberá presentar en su propuesta un (1) profesional en Ingeniería de Sistemas o Ingeniería de Software o carreras afines. El profesional ofertado debe cumplir con los siguientes requisitos: Para medir la experiencia del profesional se deberá aportar certificaciones expedidas por empresas privadas o estatales donde haya laborado y demuestre tener experiencia en mínimo tres proyectos en donde haya participado como gerente de proyectos. Para la demostración del perfil profesional como gerente de proyectos, deberá aportarse: • Tarjeta Profesional respectiva de acuerdo a su profesión con mínimo cinco (5) años de expedición. • Certificación vigente de la matrícula expedida por el respectivo consejo profesional. • Maestría o especialización en Gerencia de proyectos o Sistemas Gerenciales de Ingeniería; para lo cual deberá adjuntar una fotocopia del acta de grado o documento equivalente que acredite la especialización.		
9.3.	**PROFESIONAL EN ARQUITECTURA DE SOFTWARE** El oferente deberá presentar en su propuesta un (1) profesional en Ingeniería de Sistemas o Ingeniería de Software o carreras afines. El profesional ofertado debe cumplir con los siguientes requisitos: Para medir la experiencia del profesional se deberá aportar certificaciones expedidas por empresas privadas o estatales donde haya laborado y demuestre tener experiencia en implementación de proyectos como arquitecto de software o en diseño y construcción de software empresarial o en arquitecturas Java empresariales y APIs REST, arquitecturas orientadas a servicios (SOA). Para la demostración del perfil profesional deberá aportarse los siguientes documentos: • Tarjeta Profesional respectiva de acuerdo a su profesión con mínimo tres (3) años de expedición. • Certificación vigente de la matrícula expedida por el respectivo consejo profesional. • Posgrado en Arquitectura de Software o Ingeniería de Software.		
9.4.	**PROFESIONALES EN DESARROLLO FRONT END** El oferente deberá presentar en su propuesta mínimo un (1) profesional en Ingeniería de Sistemas o Ingeniería de Software o carreras afines. El profesional ofertado debe cumplir con los siguientes requisitos: Para medir la experiencia del profesional deberá aportar certificaciones expedidas por empresas privadas o estatales donde haya laborado y demuestre tener participación en proyectos de desarrollo de software empresarial con tecnologías como React JS, Redux, TypeScript. Para la demostración del perfil profesional deberá aportarse los siguientes documentos: • Tarjeta Profesional respectiva de acuerdo a su profesión con mínimo tres (3) años de expedición. • Certificación vigente de la matrícula expedida por el respectivo consejo profesional. • Mínimo dos (2) certificaciones en desarrollo de frontend avanzado con tecnologías como React JS, TypeScript, Redux, Axios. NOTA: Todas las certificaciones deben ser expedidas por entidades o academias reconocidas en la industria del software. No serán tenidas en cuenta certificaciones de asistencia.		
9.5.	**PROFESIONALES EN DESARROLLO BACK END (JAVA)**		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	El oferente deberá presentar en su propuesta mínimo tres (3) profesionales en Ingeniería de Sistemas o Ingeniería de Software o carreras afines. El profesional ofertado debe cumplir con los siguientes requisitos: Para medir la experiencia del profesional deberá aportar certificaciones expedidas por empresas privadas o estatales donde haya laborado y demuestre tener participación en proyectos de desarrollo de software empresarial con el lenguaje de programación Java y Spring Boot, desarrollo e implementación de servicios REST y/o SOAP. • Tarjeta Profesional respectiva de acuerdo a su profesión con mínimo tres (3) años de expedición. • Certificación vigente de la matrícula expedida por el respectivo consejo profesional. • Certificación en desarrollo de software con Java avanzado. • Certificación en desarrollo avanzado de aplicaciones web con Java y Spring Boot, desarrollo de APIs REST con Java y Spring Boot. NOTA: Todas las certificaciones deben ser expedidas por entidades o academias reconocidas en la industria del software. No serán tenidas en cuenta certificaciones de asistencia.		
9.6.	**PROFESIONAL EN DESARROLLO BACK END (PL/SQL)** El oferente deberá presentar en su propuesta mínimo un (1) profesionales en Ingeniería de Sistemas o Ingeniería de Software o carreras afines. El profesional ofertado debe cumplir con los siguientes requisitos: Para medir la experiencia del profesional deberá aportar certificaciones expedidas por empresas privadas o estatales donde haya laborado y demuestre tener experiencia en desarrollo de software empresarial con el lenguaje de programación de base de datos Oracle PL/SQL. El profesional ofertado debe cumplir con los siguientes requisitos: • Tarjeta Profesional respectiva de acuerdo a su profesión con mínimo dos (2) años de expedición. • Certificación vigente de la matrícula expedida por el respectivo consejo profesional vigente. • Certificación en programación en Oracle PL/SQL avanzado para versión 19c o superior. NOTA: Todas las certificaciones deben ser expedidas por entidades o academias reconocidas en la industria del software. No serán tenidas en cuenta certificaciones de asistencia.		
9.7.	**PROFESIONAL DE SISTEMA OPERATIVO** El oferente deberá presentar en su propuesta mínimo un (1) profesional en Ingeniería de Sistemas o Ingeniería de Software o carreras afines. El profesional ofertado debe cumplir con los siguientes requisitos: Para medir la experiencia del profesional deberá aportar certificaciones expedidas por empresas privadas o estatales donde haya laborado y demuestre tener experiencia en mínimo tres proyectos en donde haya participado en la instalación o configuración o implementación de sistemas operativos Linux. Para la demostración del perfil profesional deberá aportarse los siguientes documentos: • Tarjeta profesional con mínimo cinco (5) años de expedición. • Certificación vigente de la matrícula expedida por el respectivo consejo profesional. • Certificación en Oracle Linux 8 System Administrator. NOTA: Todas las certificaciones de Oracle deben debe ser expedidas por el fabricante. No serán tenidas en cuenta certificaciones de asistencia.		
9.8.	**PROFESIONAL EN BASES DE DATOS**		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	El oferente deberá presentar en su propuesta mínimo un (1) profesional en Ingeniería de Sistemas o Ingeniería de Software o carreras afines. El profesional ofertado debe cumplir con los siguientes requisitos: Para medir la experiencia del profesional deberá aportar certificaciones expedidas por empresas privadas o estatales donde haya laborado y demuestre tener experiencia en mínimo tres proyectos en donde haya participado en la instalación o configuración o implementación de productos Oracle Database. Para la demostración del perfil profesional deberá aportarse los siguientes documentos: • Tarjeta profesional con mínimo cinco (5) años de expedición. • Certificación vigente de la matrícula expedida por el respectivo consejo profesional. • Certificación Oracle Database Administration 2019 Certified Professional o superior • Certificación Oracle Database 19c: RAC, ASM, and Grid Infrastructure Administrator Oracle Certified o superior. NOTA: Todas las certificaciones de Oracle deben debe ser expedidas por el fabricante. No serán tenidas en cuenta certificaciones de asistencia.		
9.9.	**PROFESIONAL CAPA DE APLICACIÓN** El oferente deberá presentar en su propuesta mínimo un (1) profesional en Ingeniería de Sistemas o Ingeniería de Software o carreras afines. El profesional ofertado debe cumplir con los siguientes requisitos: Para medir la experiencia del profesional deberá aportar certificaciones expedidas por empresas privadas o estatales donde haya laborado y demuestre tener experiencia en mínimo tres proyectos en donde haya participado en la instalación o configuración o implementación de API Gateways y Oracle WebLogic Server 12.2.1.4.0 o superior. Para la demostración del perfil profesional deberá aportarse los siguientes documentos: • Tarjeta profesional con mínimo cinco (5) años de expedición. • Certificación vigente de la matrícula expedida por el respectivo consejo profesional. • Certificación Oracle WebLogic Server 12c Certified Implementation Specialist Oracle o superior. NOTA: Todas las certificaciones de Oracle deben debe ser expedidas por el fabricante. No serán tenidas en cuenta certificaciones de asistencia.		
9.10.	**PROFESIONAL DOCUMENTADOR Y TESTER DE SOFTWARE** El oferente deberá presentar en su propuesta mínimo un (1) profesional en Ingeniería de Sistemas o Ingeniería de Software o Tecnólogo en Análisis y Desarrollo de Sistemas de Información o carreras afines. El profesional ofertado debe cumplir con los siguientes requisitos: El oferente deberá presentar las hojas de vida y toda la documentación necesaria para acreditar la experiencia y conocimiento académico del profesional, debido a su importancia y criticidad de participación en el presente proceso. El profesional ofertado debe cumplir con los siguientes requisitos: • Para medir la experiencia del profesional deberá aportar certificaciones expedidas por empresas privadas o estatales donde haya laborado y demuestre tener experiencia como documentador y tester de software.		
9.11.	La oferta presentada, deberá ser firmada y avalada por un ingeniero electrónico y/o sistemas y/o 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		

<table>
<tr><th>ÍTEM</th><th>DESCRIPCIÓN</th><th>OFERTA</th><th>NO OFERTA</th></tr>
<tr><td></td><td>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.</td><td></td><td></td></tr>
<tr><td>9.12.</td><td>El oferente deberá presentar las hojas de vida y toda la documentación necesaria para acreditar la experiencia y conocimiento académico del profesional, debido a su importancia y criticidad de participación en el presente proceso. Así mismo el oferente deberá adjuntar una carta de exclusividad para este proyecto que debe contener mínimo el número telefónico y correo electrónico de la persona, a fin de validar la aprobación, aceptación y autorización por parte de los profesionales para ser presentados y utilizada su hoja de vida en el presente proceso.</td><td></td><td></td></tr>
<tr><td>9.13.</td><td>Durante la ejecución del proyecto no se deben cambiar los ingenieros asignados sin una justificación certificada y avalada por el supervisor del contrato.</td><td></td><td></td></tr>
<tr><td>10.</td><td colspan="3">EXPERIENCIA DEL PROPONENTE</td></tr>
<tr><td>10.1.</td><td>El contratista, ya sea persona natural o jurídica, nacional o extranjera, domiciliada o con sucursal en Colombia, así como los fabricantes, comercializadores y/o distribuidores autorizados en Colombia, ya sea de forma individual o conjunta (consorcio o unión temporal), deberán registrar su experiencia en el Registro Único de Proponentes del Registro Único Empresarial de la Cámara de Comercio correspondiente a su domicilio principal, de acuerdo con lo establecido en el Artículo 2.2.1.1.1.5.3 del Decreto 1082 de 2015.</td><td></td><td></td></tr>
<tr><td>10.2.</td><td>La oferta presentada, deberá ser firmada y avalada por un ingeniero electrónico o sistema o 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."</td><td></td><td></td></tr>
<tr><td>10.3.</td><td>Clasificación de experiencia UNSPSC – RUP

El proponente o cada uno de los miembros del consorcio o unión temporal que vayan a proveer los bienes y/o servicios objeto del presente proceso de selección, trátese de personas naturales y/o jurídicas, deben registrar experiencia en los segmentos, familias y clases, del Registro Único de Proponentes de acuerdo a lo establecido en el Numeral 1.1. DESCRIPCIÓN GENERAL DEL OBJETO del presente estudio previo.</td><td></td><td></td></tr>
<tr><td>10.4.</td><td>EXPERIENCIA GENERAL PROPONENTE NACIONAL O EXTRANJERO CON SUCURSAL O REPRESENTACIÓN 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 o privadas, identificados con el código UNSPSC descrito en el numeral 1.1 de la DESCRIPCIÓN DEL OBJETO del estudio previo y que su valor sumado sea igual o superior a 336.96 SMMLV, así:

<table>
<tr><th>CLASIFICACIÓN UNSPSC</th><th>SEGMENTO</th><th>FAMILIA</th><th>CLASE</th><th>VALOR EXPRESADO EN SMMLV</th></tr>
<tr><td>81111500</td><td>SERVICIOS BASADOS EN INGENIERÍA, INVESTIGACIÓN Y TECNOLOGÍA
81000000</td><td>SERVICIOS INFORMÁTICOS
81110000</td><td>INGENIERIA DE SOFTWARE O HARDWARE
81111500</td><td>336.96</td></tr>
</table>

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.</td><td></td><td></td></tr>
</table>

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	NOTA 2: en el caso de proponentes plurales, todos sus integrantes deben registrar experiencia en el RUP con el código UNSPSC antes señalado. Si se requiere experiencia ESPECÍFICA se recomienda el siguiente texto: **EXPERIENCIA ESPECÍFICA PROPONENTE NACIONAL O EXTRANJERO CON SUCURSAL EN COLOMBIA** El proponente que vaya a proveer los bienes o 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, documentos que como mínimo deberán tener la siguiente información: • Nombre del contratista • Nombre del contratante • Objeto del contrato • Valor del contrato • Fecha de suscripción y fecha de inicio del contrato • Fecha de terminación del contrato • Personal de contacto pai a verificar la información: teléfono fijo o celular, correo electrónico institucional, logo (en caso de certificación). • Estado del contrato: ejecutado o liquidado. • Si es certificación, deberá estar suscrita por el funcionario competente para tal fin. • Manifestación clara y explícita donde se evidencie que el contratista cumplió a cabalidad con el objeto del contrato. • Porcentaje del valor del contrato que ejecutó como miembro de un consorcio, unión temporal u otra forma de asociación. NOTA 1: de conformidad con lo establecido en los artículos 2.2.1.2.4.2.15 y 2.2.1,2.4.2.18 del Decreto 1082 de 2015, adicionados por el artículo 3 del Decreto 1860 de 2021, se toma como criterio diferencial para las MiPymes y para los emprendimientos y empresas conformadas por mujeres, 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 específica 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 2025, 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		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	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. NOTA 11: en la presentación de la oferta, el oferente deberá diligenciar y entregar el formulario "EXPERIENCIA DEL PROPONENTE", donde relacionará los contratos para la evaluación. La Dirección de Investigación Criminal e INTERPOL se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma. Si pueden participar extranjeros SIN DOMICILIO o SIN SUCURSAL EN COLOMBIA se recomienda el siguiente texto: **PROPONENTE EXTRANJERO SIN DOMICILIO O SIN SUCURSAL EN COLOMBIA** El proponente extranjero, personas naturales o jurídicas, deberá anexar mínimo una (01) y máximo tres (03) constancias (certificación o acta 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, la sumatoria de la cuantía de dichos contratos deberá ser igual o superior a 342.67 SMMLV. Las constancias deberán contener como mínimo la siguiente información: • Nombre del contratista. • Nombre del contratante. • Objeto del contrato. • Valor del contrato. • Fecha de suscripción y fecha de inicio del contrato. • Fecha de terminación del contrato. • Personal de contacto para verificar la información: teléfono fijo o celular, correo electrónico institucional, logo (en caso de certificación). • Estado del contrato: ejecutado o liquidado. • Si es certificación, deberá estar suscrita por el funcionario competente para tal fin. • Manifestación clara y explícita donde se evidencie que el contratista cumplió a cabalidad con el objeto del contrato. • Porcentaje del valor del contrato que ejecutó como miembro de un consorcio, unión temporal u otras formas de asociación. NOTA 1: No se aceptarán auto certificaciones. NOTA 2: No se tendrán en cuenta las certificaciones de contratos en ejecución. NOTA 3: No se aceptan certificaciones con enmendaduras o que presenten inconsistencias no subsanadas. NOTA 4: cuando los documentos no indiquen su valor en SMMLV o si estos son de años anteriores a 2025, se hará la respectiva conversión de acuerdo al año en que terminó el contrato. La verificación será realizada por el comité evaluador técnico. NOTA 5: 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		

ÍTEM	DESCRIPCIÓN	OFERTA	NO OFERTA
	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. NOTA 6: en el caso de proponentes plurales, todos sus integrantes deben acreditar experiencia en contratos ejecutados con objeto igual o similar al del presente proceso de contratación. NOTA 7: 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. NOTA 8: los proponentes extranjeros deben diligenciar el formulario “CERTIFICACIÓN DE CONTRATOS PARA ACREDITACIÓN DE EXPERIENCIA PROPONENTE EXTRANJERO SIN SUCURSAL o DOMICILIO EN COLOMBIA". La Dirección de Investigación Criminal e INTERPOL se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma.		
10.5.	**ASPECTOS GENERALES DE CONFIDENCIALIDAD**		
10.6.	Las personas encargadas del desarrollo, instalación y configuración del producto entregado deberán someterse a un estudio de seguridad llevado a cabo por la Dirección de Inteligencia de la Policía Nacional durante la vigencia del contrato. En caso de que alguno de los colaboradores involucrados no apruebe dicho estudio, el contratista estará obligado a reemplazar a la persona en cuestión por otra que cumpla con las mismas condiciones de experiencia exigidas, quien también deberá someterse al estudio de seguridad.		
10.7.	En virtud del presente contrato, el contratista se compromete a no divulgar ninguna información que obtenga o conozca durante la ejecución del mismo que esté marcada como confidencial. Esto incluye, pero no se limita, a la información relacionada con los lugares a los cuales tenga acceso con motivo de su desarrollo, así como cualquier otra información considerada confidencial. El contratista deberá firmar el formulario de acuerdo de confidencialidad correspondiente.		

ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN	OFERTA	NO OFERTA
El oferente se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente proceso y que se encuentra marcada como confidencial, así como sobre los lugares a los cuales tenga acceso y sea revelada información marcada como confidencial. Por tal razón, deberá diligenciar un acuerdo de confidencialidad y no revelación de la información, el cual se encuentra en el formulario "***ACUERDO DE CONFIDENCIALIDAD".***		

COMPROMISO ANTICORRUPCIÓN	OFERTA	NO OFERTA
El oferente se obliga a cumplir con el compromiso de anticorrupción dentro del proceso 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 proponente, sus empleados. representantes, asesores o de cualquier otra persona que en el proceso de contratación actué en su nombre, es causal suficiente para el rechazo de la oferta o para la terminación anticipada del contrato. si el incumplimiento ocurre con posterioridad a la adjudicación del mismo, para lo cual deberá diligenciar el formulario "***COMPROMISO ANTICORRUPCIÓN".***		

SISTEMAS DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO	OFERTA	NO OFERTA
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 el Ministerio del Trabajo, mediante la presentación de la calificación oficial radicada ante la Administradora de Riesgos Laborales ARL y ante el Ministerio del Trabajo correspondiente al año inmediatamente anterior a la fecha de cierre del presente proceso de selección. El oferente debe acreditar, mediante los soportes documentales pertinentes, el cumplimiento de las obligaciones legales relacionadas con el pago de los aportes al Sistema de Seguridad Social Integral, prestaciones sociales y afiliación y pago a la Administradora de Riesgos Laborales ARL de sus trabajadores, cualquiera sea la modalidad de vinculación contractual.		

REQUISITOS AMBIENTALES	OFERTA	NO OFERTA
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 que puedan afectar la ejecución del objeto contractual. 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 por la naturaleza de su actividad comercial deberá declararlo de forma escrita el representante legal bajo la gravedad de juramento, asumiendo plenamente las consecuencias legales, ambientales y contractuales que se deriven del incumplimiento. Se deberán mantener vigentes durante toda la ejecución del contrato. Este requisito se debe entregar junto con la oferta.		