TÉRMINOS DE REFERENCIA

Unidad Orgánica:	Oficina General de Tecnología de la Información
Meta Presupuestaria:	Sec. Fun. 0228 - Desarrollo y Mantenimiento de los Sistemas Informáticos
Actividad del POI	AOI00107200151 Gestión de la Infraestructura Tecnológica y Seguridad Informática.

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de Auditoría de Sistemas Informáticos.

2. OBJETIVO DE LA CONTRATACIÓN.

Contratar un servicio especializado de auditoría integral de seguridad de la información sobre las aplicaciones y sistemas críticos de la entidad, que permita evaluar de manera sistemática los controles técnicos y de gestión implementados, identificar vulnerabilidades, brechas de cumplimiento normativo, deficiencias de control y riesgos asociados, así como emitir recomendaciones técnicas orientadas a fortalecer la disponibilidad, integridad y confidencialidad de la información.

3. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

Fortalecer la protección de la información pública y la resiliencia digital de la entidad, mediante la identificación y mitigación de riesgos de seguridad de la información en los sistemas críticos, contribuyendo a la prevención, detección y respuesta oportuna ante incidentes, así como a la operación continua, confiable y segura de los servicios digitales, en alineamiento con estándares internacionales.

4. ALCANCE

Ítem	Cantidad	Und. Medida	Descripción del Servicio
01	01	Servicio	Servicio de Auditoría de Sistemas Informáticos.

4.1. Sistemas a auditar:

- Sistema Nacional de Conductores – SNC
- Registro Nacional de Sanciones – RNS
- Sistema de Información Integrado de Aeronáutica - DTA, DGAC.
- Sistema de Trámite Documentario – STD.

5. ANTECEDENTES

No aplica.

6. DESCRIPCIÓN DE LAS ACTIVIDADES A REALIZAR

El servicio comprenderá las siguientes actividades/consideraciones que deben ser cumplidos por el Contratista:

- La ejecución del servicio no deberá causar daño alguno en la información del Ministerio de Transportes y Comunicaciones.
- La ejecución de las pruebas no pondrá en riesgo, en ningún momento, la continuidad operativa de los sistemas y servicios informáticos del Ministerio de Transportes y Comunicaciones.

- El contratista será responsable de formular al Ministerio de Transportes y Comunicaciones el requerimiento de la información necesaria para la auditoría, conducir las reuniones requeridas y ejecutar las pruebas que correspondan en el marco de la auditoría.
- El contratista deberá firmar un acta de acuerdo de confidencialidad, la cual será entregada por la OGTI hasta los dos (02) días calendario a partir del día siguiente de notificada la orden de servicio.
- Deberá realizarse **por lo menos una reunión semanal** para reportar el avance de la auditoría.
- El contratista deberá coordinar con el personal designado por la Oficina General de Tecnología de la Información el acceso a sistemas, ambientes y documentación.
- El contratista deberá mantener disponible el personal especializado requerido durante toda la ejecución.
- El contratista deberá registrar y documentar todas las actividades realizadas durante el servicio.
- El contratista deberá reportar de inmediato cualquier hallazgo crítico o indicio de incidente de seguridad.
- El contratista deberá elaborar y presentar un **Plan de Trabajo**, en el cual se incluya el cronograma, responsables, matriz de alcance y canal de notificación de las observaciones y/o aprobación del referido plan. El Plan de Trabajo deberá ser aprobado por la OITSI y comunicado al proveedor, dentro del mismo día, a través del correo electrónico.
- Los informes entregados al Ministerio de Transportes y Comunicaciones como parte del servicio deben ser completamente en español, a excepción de los papeles de trabajo de la evaluación o los reportes técnicos utilizados los cuales podrían estar en idioma inglés y deben acompañar el informe
- Todos los entregables serán presentados en formato digital y cifrados con una contraseña para asegurar la confidencialidad de la información.
- El contratista deberá realizar la revisión, discusión y validación de los hallazgos identificados con la Entidad, atendiendo y levantando las observaciones formuladas, e incorporando los ajustes necesarios en el informe final integrado.
- El contratista deberá elaborar y presentar un **Informe Final Integrado**, con consolidado de hallazgos, priorización, plan de remediación y recomendaciones críticas.
- El contratista deberá presentar las evidencias técnicas y documentales que respalden cada hallazgo o análisis.
- El contratista deberá realizar una presentación ejecutiva y la socialización de los resultados finales ante la Oficina General de Tecnología de la Información de la Entidad, asegurando la exposición clara de los hallazgos, conclusiones y recomendaciones priorizadas.

6.1. Auditoría de Seguridad Técnica

a) El contratista deberá realizar el análisis de vulnerabilidades en aplicaciones web, aplicaciones cliente/servidor, API, servicios web, microservicios, bases de datos e interfaces de integración.
b) El contratista deberá ejecutar evaluaciones de hardening sobre los componentes revisados.
c) El contratista deberá realizar pruebas de explotación controlada, previa autorización formal de la entidad.

d) El contratista deberá realizar pruebas de seguridad bajo el enfoque de caja gris, combinando información parcial de la arquitectura interna con técnicas de evaluación externa, con el fin de obtener una visión realista del nivel de exposición de los sistemas críticos.
e) Las pruebas de seguridad se ejecutarán exclusivamente en los entornos de producción de los sistemas evaluados, dentro de una ventana de intervención previamente autorizada por la Entidad. El contratista deberá coordinar y cumplir estrictamente los horarios aprobados, garantizando la continuidad operativa, la integridad de la información y la no afectación de los servicios críticos durante la ejecución de las actividades.
f) El contratista deberá analizar los registros (logs) de seguridad y eventos históricos de los sistemas indicados en el numeral 4.1. con un periodo de tiempo de revisión no mayor a seis (06) meses.
g) El contratista deberá identificar intentos de intrusión, evidencias de malware o comportamientos anómalos.
h) El contratista deberá revisar los mecanismos de autenticación, autorización y control de accesos.
i) El contratista deberá validar la aplicación del principio de mínimo privilegio.
j) El contratista deberá elaborar y presentar un **Informe de Evaluación Técnica de Vulnerabilidades**, detallado por sistema y con vulnerabilidades, evidencias, nivel de riesgo (CVSS) e impacto.
k) El contratista deberá realizar una valoración contextual de cada hallazgo identificado, considerando el impacto operacional, la afectación potencial a la disponibilidad del servicio y la relevancia institucional del sistema evaluado.
l) El contratista deberá asegurar que cada hallazgo identificado cuente con evidencia replicable y trazabilidad completa.
m) El contratista deberá analizar y evaluar los mecanismos de gestión de incidentes de seguridad de la información implementados por la Entidad, verificando su alineamiento con la Norma ISO/IEC 27035, e identificando brechas, debilidades y oportunidades de mejora.

6.2. Auditoría de Gestión y Procesos

a) El contratista deberá revisar políticas, procedimientos, roles, responsabilidades y documentación vigente.
b) El contratista deberá evaluar el cumplimiento de los controles del Anexo A de ISO/IEC 27001:2022.
c) El contratista deberá validar el cumplimiento de cláusulas relevantes de ISO/IEC 27001 (gestión de riesgos, operaciones, desempeño y mejora).
d) El contratista deberá elaborar y actualizar las matrices y evidencias necesarias para soportar cada hallazgo.
e) El contratista deberá elaborar y presentar un **Informe de Evaluación de Controles ISO 27001**, con análisis del cumplimiento del Anexo A de la norma, hallazgos, madurez y recomendaciones.
f) El contratista deberá elaborar y presentar un **Informe de Análisis de Riesgos,** con matriz probabilidad-impacto, nivel de riesgo inherente y residual, y controles existentes/faltantes.

6.3. Análisis de Impacto al Negocio BIA

a) El contratista deberá realizar un BIA por cada sistema crítico con brechas significativas o falta de documentación.

b) El contratista deberá Identificar procesos dependientes y evaluar el impacto por interrupción.
c) El contratista deberá determinar MTPD, RTO y RPO por sistema.
d) Contratista deberá Identificar recursos necesarios para garantizar la continuidad operativa.
e) El contratista deberá elaborar y presentar un **Informe de análisis de impacto al negocio BIA**, incluyendo procesos impactados, MTPD, RTO, RPO e impacto cualitativo y cuantitativo.

6.4. Revisión de Incidentes o Penetraciones Previas

a) El contratista deberá revisar logs históricos de los sistemas evaluados, con un periodo de tiempo de revisión no mayor a seis (06) meses.
b) El contratista deberá verificar la integridad de archivos, bases de datos y repositorios.
c) El contratista deberá analizar eventos y alertas registradas en sistemas SIEM o equivalentes.
d) El contratista deberá Identificar indicadores de compromiso (IoC) y posibles brechas no detectadas.
e) El contratista deberá elaborar y presentar un **Informe de Incidentes o Intentos de Penetración**, con evidencias, origen probable, IoC y recomendaciones.

6.5. Metodología del Proveedor

El contratista deberá **aplicar metodologías, marcos de referencia, herramientas y buenas prácticas reconocidas internacionalmente**, garantizando la calidad, confiabilidad y trazabilidad de los resultados de la auditoría.

6.5.1. Enfoque Técnico

El contratista deberá basar las actividades técnicas, como pruebas de seguridad, análisis de vulnerabilidades y revisiones de configuración, en los siguientes estándares y guías mínimas:

- **OWASP Testing Guide v4 o superior**
- **OWASP Top 10 (versión vigente)**
- **OSSTMM (Open Source Security Testing Methodology Manual)**
- **NIST SP 800-53** y **NIST SP 800-115**
- **SANS Top 25**
- Buenas prácticas de **hardening** basadas en **CIS Benchmarks** o equivalentes.

6.5.2. Enfoque de Gestión

El contratista deberá asegurar que la auditoría sea realizada bajo lineamientos de gestión de seguridad y continuidad de negocio, considerando como referencia:

- **ISO/IEC 27001:2022**
- **ISO/IEC 27002:2022**
- **ISO/IEC 27005** (gestión de riesgos)
- **ISO/IEC 22301** (continuidad del negocio y análisis de impacto – BIA)

6.5.3. Herramientas Mínimas

El contratista deberá emplear herramientas especializadas para garantizar rigor técnico y trazabilidad de hallazgos, incluyendo al menos:

- **Escáner de vulnerabilidades** (Nessus, OpenVAS, Qualys o equivalente).
- **Herramientas de análisis de código** (cuando aplique).
- **Herramientas de explotación controlada**, tales como Metasploit u otras similares.
- **Herramientas de monitoreo de logs y/o SIEM**, cuando estas existan en la infraestructura de la entidad.

7. ENTREGABLES

El (la) contratista deberá presentar un (01) informe por cada entregable según lo descrito en el numeral 6, de acuerdo al siguiente detalle:

Entregables	Contenido del entregable	Plazo
Primer entregable	• Un (01) Plan de Trabajo de acuerdo a lo establecido en el numeral 6 y Acta de acuerdo de confidencialidad firmada por el contratista.	Hasta 05 días calendario, contados a partir del día siguiente de suscrito el contrato o notificada la orden de servicio.
Segundo entregable	• Un (01) Informe de Evaluación Técnica de Vulnerabilidades de acuerdo a lo establecido en el numeral 6.1	Hasta 15 días calendario, contados a partir del día siguiente de suscrito el contrato o notificada la orden de servicio.
Tercer entregable	• Un (01) Informe de Evaluación de Controles de la ISO 27001 de acuerdo a lo establecido en el numeral 6.2	Hasta 25 días calendario, contados a partir del día siguiente de suscrito el contrato o notificada la orden de servicio.
Cuarto entregable	• Un (01) Informe de Análisis de Riesgos de acuerdo a lo establecido en el numeral 6.2	Hasta 35 días calendario, contados a partir del día siguiente de suscrito el contrato o notificada la orden de servicio.
Quinto entregable	• Un (01) Informe de Análisis de Impacto al negocio BIA de acuerdo a lo establecido en el numeral 6.3	Hasta 45 días calendario, contados a partir del día siguiente de suscrito el contrato o notificada la orden de servicio.
Sexto entregable	• Un (01) Informe de Incidentes o Intentos de Penetración de acuerdo a lo establecido en el numeral 6.4	Hasta 55 días calendario contados a partir del día siguiente de suscrito el contrato o notificada la orden de servicio.
Séptimo entregable	• Un (01) Informe final integrado con consolidado de hallazgos, priorización, plan de remediación y recomendaciones críticas.	Hasta 65 días calendario contados a partir del día siguiente de suscrito el contrato o notificada la orden de servicio.

Todo entregable deberá ser ingresado por mesa de partes o mesa de partes virtual de la entidad, dirigido al área usuaria responsable de dar la conformidad.

8. PRESTACIONES ACCESORIAS

No aplica.

9. MEDIDAS DE SEGURIDAD EN LA PRESTACIÓN DEL SERVICIO

No aplica.

10. PLAZO Y LUGAR DE LA PRESTACIÓN

10.1. Plazo de ejecución del servicio

El plazo de ejecución del servicio de auditoría de sistemas para el Ministerio de Transportes y Comunicaciones, será por un periodo de sesenta y cinco (65) días calendario, contados a partir del día siguiente de suscrito el contrato o notificada la orden de servicio.

10.2. Lugar de prestación

El presente servicio se realizará en forma remota o híbrida y/o en la sede del Ministerio de Transportes y Comunicaciones, sito Jr. Zorritos N° 1203 - Cercado de Lima.

11. REQUISITOS DEL PROVEEDOR

11.1. Condiciones Generales

- Tener Registro Único de Contribuyente habilitado.
- Tener Código de Cuenta Interbancario registrado.
- Tener Registro Nacional de Proveedores en el Capítulo que corresponda (se excluye en el caso que el valor de bien sea menor o igual a 1 UIT).

11.2. Condiciones Particulares

a) Perfil del Proveedor:

✓ **Experiencia:**

El proveedor deberá presentar un mínimo de **cuatro (4) servicios prestados similares** al objeto de la contratación y/o actividad dentro de un periodo no menor a cuatro (4) años de ejecución del servicio. Se considera servicios prestados similares los siguientes:

- Análisis de vulnerabilidades de seguridad.
- Pruebas de seguridad o Pentesting
- Auditoría de ti o de sistemas.
- Servicios de auditoría forense informática.
- Evaluaciones de seguridad de la información y/o ciberseguridad respecto al marco regulatorio y estándares internacionales.
- Evaluación de implementaciones de sistemas informáticos.
- Servicios de Ethical Hacking.
- Servicios de Ciberseguridad.

b) Perfil del personal propuesto:

❖ **Un (01) Gerente de Proyecto**

Actividades

- Planificar y gestionar el servicio.
- Supervisar, realizar control metodológico y gobernanza.
- Gestionar entregables, validación y cierre.

Formación académica: Deberá acreditar una copia simple de su título profesional (Ingeniero Electrónico y/o Eléctrico y/o Telecomunicaciones y/o Sistemas y/o Redes y Comunicaciones y/o Informática y/o Industrial).

Certificaciones: Lead Auditor ISO 27001, CISA, CISM y/o CRISC.

Experiencia: Experiencia mínima de **cuatro (4) años** en la gestión y/o conducción de servicios de auditoría de TI y/o auditoría forense informática, o en la implementación del sistema de gestión de seguridad de la información y/o gestión de ciberseguridad y/o Ethical Hacking.

- **Dos (02) Auditores**

  Actividades
  - Ejecutar la auditoría de seguridad técnica
  - Ejecutar la auditoría de gestión, riesgos e incidentes
  - Documentar hallazgos, elaborar informes técnicos, brindar soporte técnico durante la validación de hallazgos

  Formación académica: Deberá acreditar una copia simple de su bachiller (Ingeniero Electrónico y/o Eléctrico y/o Telecomunicaciones y/o Sistemas y/o Redes y Comunicaciones y/o Informática y/o Industrial)

  Certificaciones:
  - **Auditor de Seguridad y Cumplimiento**
    Certificaciones **Lead Auditor ISO 27001, CISA, CISM y/o CRISC y/o ISO 27001 Senior Lead Auditor.**

  - **Auditor de Ethical Hacking**
    Certificaciones de hacking ofensivo como **OSCP (Offensive Security Certified Professional) y/o OSWE (Offensive Security Web Expert) y/o GPEN (GIAC Penetration Tester) y/o CEH Master y/o EWPT.**

  Experiencia: Experiencia mínima de **dos (2) años** participando en la ejecución de servicios de auditoría de TI y/o auditoría forense informática y/o Ethical Hacking.

12. RESPONSABILIDAD DEL PROVEEDOR

Es preciso mencionar que el proveedor es el responsable directo y absoluto de las prestaciones que realizará, debiendo responder por la ejecución de la prestación del servicio.

13. RESPONSABILIDAD DEL AREA USUARIA

El área usuaria entregará y facilitará accesos al proveedor del servicio, de lo siguiente:

- Acceso a la información contenida en los sistemas, plataformas o aplicativos informáticos necesarios para la ejecución del contrato cuando corresponda, otorgando las instrucciones necesarias para su adecuada utilización y protección de datos que resulten aplicables.

14. FORMA Y CONDICIONES DE PAGO

El pago se realizará en soles, en **dos (02) armadas**, previa presentación del entregable solicitado y conformidad respectiva a cargo de la Oficina de Infraestructura Tecnológica y Seguridad Informática – OITSI.

NRO. DE PAGOS	PORCENTAJE DE PAGO
Primer Pago	50% del monto total del contrato u orden de servicio, previa presentación de los **entregables primero, segundo, tercero y cuarto**, de acuerdo al numeral 7 y del otorgamiento de conformidad de servicio correspondiente.
Segundo Pago	50% del monto total del contrato u orden de servicio, previa presentación de los **entregables quinto, sexto y séptimo** de acuerdo al numeral 7 y del otorgamiento de conformidad de servicio correspondiente.

15. CONFORMIDAD

La conformidad del servicio será otorgada por la **Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información**, previa verificación del entregable respectivo.

De existir observaciones, LA ENTIDAD CONTRATANTE las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar NO MAYOR AL 30% DEL PLAZO DEL ENTREGABLE CORRESPONDIENTE, DEPENDIENDO DE LA COMPLEJIDAD O SOFISTICACIÓN DE LAS SUBSANACIONES A REALIZAR. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD CONTRATANTE puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD CONTRATANTE no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

16. CONFIFENCIALIDAD

El proveedor se obliga a mantener y guardar estricta reserva y absoluta confidencialidad todos los documentos e informaciones de la entidad a los que tenga acceso en ejecución del presente contrato. Se entiende que la obligación asumida por contratista está referida no solo a los documentos e informaciones señalados como "confidenciales" sino a todos los documentos e informaciones que en razón del presente contrato o vinculado con la ejecución del mismo, pueda ser conocida por cualquier medio por el contratista.

17. PENALIDAD POR MORA

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD CONTRATANTE le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo con la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo}}$$

Donde: **F = 0.40**

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD CONTRATANTE no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme al numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

18. PENALIDAD POR OTROS TIPOS DE PENALIDAD

No aplica.

19. RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.
Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

a) Por acumulación del monto máximo de la penalidad por mora o por el monto máximo para otras penalidades, en la ejecución de la prestación a su cargo.
b) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
c) Incumplimiento de obligaciones contractuales, por causa atribuible al contratista.
d) Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
e) Por incumplimiento de la cláusula anticorrupción y antisoborno.
f) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
g) Por la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público.
h) También puede resolverse de forma total o parcial del contrato menor por mutuo acuerdo entre las partes, previa opinión del área usuaria. Esta disposición sólo podrá aplicarse para las contrataciones de servicios técnicos, profesionales y/o especializados realizados por personas naturales (locadores de servicios).
i) Asimismo, la entidad podrá resolver (total o parcialmente) la orden o contrato, en caso desaparezca la necesidad por parte del área usuaria, debiendo remitirse a la Oficina de Abastecimiento un informe debidamente sustentado y precisando los entregables que no serán ejecutados por el contratista.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo a lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

20. ANTICORRUPCIÓN Y SOBORNO

A la suscripción de este contrato, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación[1] y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato[2]. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco[3]. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar[4].

21. RESPONSABILIDADES DE VICIOS OCULTOS

Indicar el plazo máximo de responsabilidad que tendrá el contratista por los vicios ocultos del servicio ofertado, cuyo plazo no podrá ser menor a un (01) año contado a partir de emitida la conformidad.

---

[1] Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas.

[2] Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.

[3] Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

[4] Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

22. PROPIEDAD INTELECTUAL

El Ministerio de Transportes y Comunicaciones tendrá todos los derechos de propiedad intelectual (sin limitación, patentes, derechos de autor, nombres comerciales y marcas registradas respecto a los productos u otros materiales relacionados a la contratación).

23. DECLARACIÓN JURADA DE INTERESES

No aplica.

24. GESTIÓN DE RIESGOS

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

25. SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes sobre la validez, nulidad, interpretación, ejecución, terminación o eficacia de los contratos menores se resuelven mediante conciliación, conforme lo dispuesto en el numeral 81.3 del artículo 81 de la Ley.

26. GARANTÍAS

No aplica.

27. APLICACIÓN SUPLEATORIA

En todo lo no previsto en la presente contratación se aplicará de manera supletoria la Ley General de Contrataciones Públicas su Reglamento; demás normas generales y específicas que resulten aplicables y el Código Civil, siempre que no se contradiga con las disposiciones establecidas en los Términos de Referencia.

28. REGLAMENTOS TÉCNICOS, NORMAS Y/O SANITARIAS

No aplica.

29. SANCIONES

La presente contratación se sujeta a lo establecido en el Título VI de la Ley General de Contrataciones Públicas Ley ° 32069 referido al régimen de infracciones y sanciones.

RAFAEL VÍCTOR PORTA DE LA CRUZ
Director
Oficina de Infraestructura Tecnológica y Seguridad Informática