PLIEGO DE PRESCRICIONES TÉCNICAS PARA

"DESARROLLO DE LA ESTRATEGIA DE CIBERSEGURIDAD DE AMVISA Y LA ELABORACIÓN DE UN PLAN DIRECTOR DE CIBERSEGURIDAD EN EL MARCO DEL COMPONENTE DE PROYECTO Nº 14 DEL PROYECTO DE DIGITALIZACIÓN DEL CICLO URBANO DEL AGUA EN VITORIA-GASTEIZ, SMART AMVISA 2025"

Contenido

1. Introducción 3
2. Objetivo 3
3. Arranque, Planificación y Seguimiento del Proyecto 3
3.1. Objetivos de la fase 4
3.2. Resultados de la fase 4
4. Diagnóstico de situación actual de AMVISA 4
4.1. Objetivos de la fase 4
4.2. Resultados de la fase 5
5. Análisis jurídico de la situación 6
5.1. Objetivos de la fase 6
5.2. Resultados de la fase 6
6. Política y Estrategia de Ciberseguridad 7
6.1. Objetivos de la fase 7
6.2. Resultados de la fase 7
7. Análisis de Riesgos y GAP en Ciberseguridad 8
7.1. Objetivos de la fase 8
7.2. Resultados de la fase 9
8. Elaboración Plan Director Ciberseguridad 9
8.1. Objetivos de la fase 9
8.2. Resultados de la fase 10
9. Planificación, dirección y seguimiento del proyecto 11
9.1. Duración y fases del proyecto 11
9.2. Metodología y herramientas. 12
9.3. Equipo de trabajo. 12
9.4. Seguimiento y control 13
10. Plan de facturación 13
11. Formato de los Entregables 14
12. Condiciones 14
13. Gestión de la Propiedad 14
14. Disponibilidad y Confidencialidad de la Información 15
15. Contenido de la propuesta técnica (sobre nº 2) 17**6**

1. Introducción

AMVISA quiere realizar un estudio para desarrollar la Estrategia de Seguridad de sus Sistemas de Información y Comunicaciones adecuada al marco normativo vigente, junto a un Plan Director de Ciberseguridad que la desarrolle.

La idea y objetivo de AMVISA es protegerse contra amenazas que puedan causar pérdidas de información, interrupciones en los servicios y daños a la reputación, considerándose una entidad segura, así como garantizar la confianza de los clientes y continuar del servicio que presta a los ciudadanos.

2. Objetivo

El **objetivo principal** que se persigue con el servicio propuesto es el siguiente:

Asesoramiento organizativo y tecnológico específico para el desarrollo de la estrategia de Seguridad de los Sistemas de Información y Comunicaciones garantizando el cumplimiento legal y normativo que aplique a AMVISA. Asimismo, se deberá elaborar un Plan Director de Ciberseguridad que este alineado con la estrategia el cual concreta los proyectos necesarios a implementar en los próximos años.

Se deberá desarrollar una estrategia de seguridad de los Sistemas de Información y Comunicaciones para proteger la integridad, confidencialidad y disponibilidad de los datos, cumplir con las regulaciones y mantener la confianza en AMVISA.

Se contemplarán los siguientes ámbitos tanto en los entornos de gestión (IT "*Information Technology*") como operativos (OT "*Operational Technology*"):

- Tecnologías y Sistemas
- Procesos y Procedimientos
- Organización y personas

Para ello, el proyecto a presentar se deberá estructurar en, al menos, las siguientes fases:

- ✓ Arranque, Planificación y Seguimiento del Proyecto
- ✓ Diagnóstico situación actual de AMVISA
- ✓ Análisis jurídico respecto a la Ciberseguridad en AMVISA
- ✓ Definición de la Política y la Estrategia de Ciberseguridad
- ✓ Análisis de Riesgos y GAP en materia Ciberseguridad
- ✓ Elaboración Plan Director de Ciberseguridad

3. Arranque, Planificación y Seguimiento del Proyecto

3.1. Objetivos de la fase

En esta fase se deberán establecer los roles y responsabilidades durante el proyecto, asignación de recursos, plazos, etc. para una correcta ejecución del proyecto.

Se determinarán los interlocutores y se realizará una planificación temporal detallada y consensuada por las partes.

- Establecer un marco de coordinación general del proyecto.
- Definir roles y responsabilidades que participarán.
- Establecer plazos concretos para la realización de tareas.
- Evaluación continua del proyecto.
- Mecanismos y protocolos de calidad aplicables.

3.2. Resultados de la fase

Como resultado de esta fase, se deberá obtener:

- Presentación de los equipos de proyecto, interno y externo.
- Asignación de fases a roles internos.
- Planificación del proyecto con detalle de fechas para los hitos de entrega.
- Establecer mecánicos de Seguimiento periódico y de control del proyecto.

Entregable 1. Informe de la/s reunión/es de Arranque (*Kick-off*).

- ✓ Debe incluir al menos el resultado de todas reuniones de Arranque (*Kick-off*) así como los puntos indicados anteriormente: equipos de proyecto (interno y externo), asignación de fases a roles internos, planificación del proyecto con detalle de fechas para los hitos de entrega, mecánicos de Seguimiento periódico y de control del proyecto, etc.

4. Diagnóstico de situación actual de AMVISA

4.1. Objetivos de la fase

Se realizará un estudio de la situación de AMVISA en materia de Ciberseguridad analizando todos aspectos no sólo técnicos, sino también incluyendo los procesos de negocio, organizativos y normativos en las diferentes áreas de la empresa, tanto en su entorno de gestión como operativo, para ello:

- Se deberá realizar la recogida de información de los distintos ámbitos de control que se establecen en las normas de referencia:

  - Realización de entrevistas con el personal de las distintas áreas de la empresa: Gerencia + 7 áreas (Abastecimiento, Saneamiento,

Proyectos y Obras, Tratamiento y Calidad, RRHH, Administración y Finanzas, I&T)

- Inspección in situ de sistemas e instalaciones. (1 EDAR, 1 ETAP, 2 oficinas centrales)
- Solicitud de información a los responsables de cada proceso para soportar un análisis adecuado, por ejemplo verificando los modelos de petición de consentimiento, la revisión de cláusulas y contratos ya existentes con terceros y cualquier otro elemento que pueda ser considerado de interés.
- Conocimiento de AMVISA: los proyectos, tanto operacionales como organizativos, presentes y futuros, así como las revisiones de crecimiento a corto y medio plazo.
- Aplicación de técnicas y herramientas de evaluación técnica ampliamente reconocidas a nivel internacional y respaldadas por la normativa vigente. Al menos se deberá realizar un *PenTesting* ("*Penetration Testing*"), así como otras metodologías y herramientas complementarias que el licitante consideren sean de utilidad para identificar vulnerabilidades en sistemas Informáticos y redes de Comunicación.
- Revisión de las iniciativas definidas en el Plan Estratégico AMVISA.

- Se recogerá un inventario detallado de los distintos Sistemas de Información y Comunicaciones.
- Se hará una definición de los responsables sobre los Sistemas de Información y Comunicaciones en AMVISA (equipos, personas, software, instalaciones…) tanto en los entornos de gestión IT como como operativos OT (especialmente en la ETAP y la EDAR).
- Será necesario Identificar el nivel de adecuación de las medidas de Ciberseguridad establecidas por las normas de referencia: analizando los controles de las normas de referencia aplicados en AMVISA así como el estado de madurez en el que se encuentran.
- Se deberá elaborar el informe detallado que muestre el estado de AMVISA, identificando DAFO especialmente los Riesgos en cada ámbito con respecto a las normas de referencia, así como otras entidades gestoras de ciclo integral del agua y servicios públicos de referencia.

4.2. Resultados de la fase

Como resultado de esta fase, se deberá elaborar:

· Informe de análisis detallado, incluyendo un resumen ejecutivo dirigido a miembros de AMVISA, para facilitar su comprensión e integración en el proyecto , que aporte una visión clara del estado actual y los aspectos

clave que requieren atención prioritaria para la adecuación normativa y la mejora continua en materia de Ciberseguridad en la organización.

Entregable 2. Informe diagnostico de la situación de AMVISA respecto al ámbito de la Ciberseguridad.

- ✓ Se facilitará un informe detallado de situación en el que se reflejará el cumplimiento de los requerimientos de la normativa en AMVISA para las categorías identificadas. Dicho informe deberá contener al menos un análisis DAFO (Debilidades, Amenazas, Fortalezas y Oportunidades en materia Ciberseguridad AMVISA) que puede visualizarse en un Gráfico: radial o de araña o similar, que permita tener una visión resumida de la situación actual. Se considerara de interés la posible elaboración de un *Benchmarking* con otras entidades gestoras de ciclo integral del agua y servicios públicos de referencia.

5. Análisis jurídico de la situación

5.1. Objetivos de la fase

Se deberá realizar un **análisis jurídico** previo para determinar la normativa/s a aplicar y el nivel de cumplimiento de esta/s, conforme a las obligaciones regulatorias que se exigen para garantizar la protección de la información que se maneja en AMVISA.

Son muchas las normativas existentes y se necesita definir cuáles son las que aplican como punto inicial del proyecto y en función de las cuales se desarrollarán los controles, medidas, evaluaciones de riesgos, etc.

5.2. Resultados de la fase

Como resultado de esta fase, se deberá obtener:

- Informe jurídico en el que se recoja la normativa/s de obligado cumplimiento en AMVISA. En base a esta normativa a cumplir, se desarrollará el proyecto.

Entregable 3. Informe a nivel jurídico sobre la normativa de aplicación en AMVISA.

- ✓ Se deberá elaborar un informe que al menos sintetice de manera clara y concisa los requisitos legales y técnicos que son de obligado cumplimiento para AMVISA respecto a la normativa vigente en materia de Ciberseguridad y la protección de datos, con sus correspondientes justificaciones jurídicas.

Este informe jurídico deberá como mínimo presentar las principales conclusiones de dichos requerimientos normativos y legales, que son de obligado cumplimiento y sus oportunas recomendaciones legales, en base a las normativas de referencia en la materia, por ejemplo, a la nueva Directiva Europea NIS2, al Esquema Nacional de Seguridad (ENS) y al Reglamento General de Protección de Datos (RGPD).

6. Política y Estrategia de Ciberseguridad

6.1. Objetivos de la fase

Se elaborará una Política y una Estrategia de Ciberseguridad, que determinará el conjunto de directrices que rigen la forma de gestionar y proteger la información en AMVISA garantizando en todo momento su confidencialidad, integridad y disponibilidad, y además, que sirva para prevenir y mitigar los riesgos que pueden afectarla. Se deberán recoger como mínimo los siguientes contenidos:

- La misión de AMVISA.
- El marco legal y regulatorio de sus actividades: especificar las normas de obligado cumplimiento en AMVISA.
- Objetivo de la política alineado con los objetivos estratégicos.
- Alcance de la política: áreas, procesos, actividades, activos y personas a las que les aplica.
- Los roles y funciones en materia de Ciberseguridad, definiendo las responsabilidades y el procedimiento para su designación y renovación garantizando la segregación de los mismos.
- El compromiso de AMVISA con los principios básicos de la norma.
- Periodicidad de revisión del documento.
- Riesgos IA

6.2. Resultados de la fase

Como resultado de esta fase, se deberá obtener:

· Política y Estrategia de Ciberseguridad de AMVISA.

Entregable 4. Política y Estrategia de Ciberseguridad de AMVISA.

✓ Dicho documento debe definir al menos los objetivos y el alcance de la política, especificando las áreas, activos y personas a las que aplica. Asimismo, debe establecer los principios de Ciberseguridad, roles y responsabilidades claras para garantizar el cumplimiento, incluyendo la

asignación de funciones específicas en la gestión de riesgos y la respuesta ante incidentes.

El documento debe contemplar el compromiso de AMVISA para implantar y mantener las normas y controles que sean necesarios para proteger sus sistemas y datos, alineándose con la normativa vigente y los estándares sectoriales, y fomentando una cultura interna de Ciberseguridad y concienciación en toda la organización.

7. Análisis de Riesgos y GAP en Ciberseguridad

7.1. Objetivos de la fase

Disponer de un análisis global de los riesgos desde el punto de vista de la Ciberseguridad

Tras la validación de los anteriores Informes (Entregables 1, 2, 3 y 4) por parte de AMVISA, se desarrollará un Análisis de Riesgos y GAP conforme a los requisitos definidos en el Análisis Jurídico y la Política realizadas, con el fin de diseñar una Hoja de Ruta personalizada que guíe a AMVISA hacia el pleno cumplimiento normativo.

Se debe contemplar un análisis específico de los riesgos relacionados con la Inteligencia Artificial (IA) y otras tecnologías emergentes, a fin permitir identificar brechas adicionales y definir iniciativas y proyectos de mitigación acordes con la normativa vigente y las mejores prácticas para la gestión de tecnologías IA en entornos públicos, asegurando así una protección integral y actualizada de los activos críticos de AMVISA.

Detalle de objetivos:

1. Realizar la Valoración y Categorización del Sistema.

En base al análisis previo realizado, para la definición del alcance definitivo, se realizará la valoración y categorización de los servicios.

2. Análisis de riesgos

- Realizar un análisis de riesgos a los que estén expuestos los sistemas, considerando además los riesgos de las tecnologías emergentes como la IA.
- Evaluación de los riesgos: Se deberá tener en cuenta el impacto y la probabilidad de los mismos.

- Priorizar los riesgos para permitir identificar aquellos que representan una mayor amenaza para responder ante ellos en primer lugar, con los recursos de los que se dispone AMVISA.

3. Declaración de Aplicabilidad – Perfil de cumplimiento específico

- Tras el análisis de riesgos se elaborará la Declaración de Aplicabilidad (SoA) – documento donde se registran los controles de Ciberseguridad que son **necesarios** y si éstos se encuentran implementados o no.

7.2. Resultados de la fase

Se dispondrá de una Hoja de Ruta que facilitará la planificación de actividades para la adecuación en un tiempo razonable a los requerimientos de la norma.

Entregable 5. Análisis de Riesgos y GAP en materia Ciberseguridad para AMVISA.

- ✓ Este documento debe contener, al menos, la identificación de los sistemas y activos críticos, la evaluación y descripción de las amenazas y vulnerabilidades relevantes, así como el análisis detallado del impacto y la probabilidad de ocurrencia de cada riesgo identificado e incluyendo un análisis específico de los riesgos relacionados con la Inteligencia Artificial (IA). Además, debe priorizar los riesgos en función de su gravedad, proponiendo las medidas de mitigación más adecuadas para cada caso y facilitando así la toma de decisiones y la asignación eficiente de los recursos disponibles en AMVISA. Incluyendo un “Mapa de riesgos” donde se identifique para cada ámbito: los escenarios de amenazas, las acciones correctivas identificadas y la clasificación del nivel de riesgo identificado.
- ✓ Asimismo, el documento deberá incluir una evaluación GAP que compare la situación actual de los controles y prácticas de ciberseguridad con los requisitos marcados por la normativa de referencia, identificando claramente las brechas existentes y estableciendo recomendaciones concretas para cerrar dichas brechas y alcanzar el nivel de cumplimiento requerido.

8. Elaboración Plan Director Ciberseguridad

8.1. Objetivos de la fase

Elaboración de un Plan Director de Ciberseguridad.

En el presente punto se trabajará en la definición y entrega de un Plan Director de Ciberseguridad que ayude a alcanzar los siguientes objetivos de AMVISA.

- Alineamiento de la Ciberseguridad, las tecnologías de la información, las tecnologías de operación y los procesos con los objetivos de la empresa.
- Optimización de las inversiones en Ciberseguridad, mediante el establecimiento de un método de retorno de la inversión que permita a medio plazo mantener e incluso reducir su coste aumentando por el contrario su nivel de seguridad.
- Acompañar las decisiones en materia de Ciberseguridad teniendo en cuenta la gestión del riesgo corporativo.
- Establecimiento de un Plan de Formación en materia Ciberseguridad adaptado a sus necesidades, capacidades y objetivos estratégicos, con el detalle suficiente como para que se pueda asignar recursos y avanzar con su realización.

Deberá quedar recogido en dicho Plan, las acciones a realizar de acuerdo con toda la información recogida en las fases anteriores del proyecto, con la estimación de costes, recursos, esfuerzo y duración. Además, debe al menos incorporar:

- Propuesta de indicadores de seguimiento y mecanismos de revisión periódica del Plan Director de Ciberseguridad.
- Definición de un sistema de mejora continua y actualización frente a nuevas amenazas y cambios regulatorios.

8.2. Resultados de la fase

Como resultado de esta fase, AMVISA dispondrá de un Plan Director de Ciberseguridad adaptado a sus necesidades, capacidades y objetivos estratégicos, con el detalle suficiente como para que se pueda asignar recursos y avanzar con la planificación de los proyectos.

Entregable 6. Plan Director de Ciberseguridad AMVISA.

✓ Este documento debe al menos recoger y detallar todas las acciones, proyectos, costes, recursos y plazos identificados en las fases previas, ajustándose a las necesidades y capacidades específicas de AMVISA. Así como, ofrecer un marco estructurado para planificar, asignar recursos y avanzar de manera coordinada en la mejora continua de la ciberseguridad, asegurando el cumplimiento normativo y la resiliencia frente a amenazas actuales y/o emergentes.

- ✓ El documento además debe recopilar y organizar todos los puntos fundamentales identificados en dichas fases a fin guiar en un proceso de adecuación normativa para AMVISA. Contendrá el listado detallado de proyectos necesarios para cumplir con los requerimientos legales y estándares del sector, definiendo para cada proyecto al menos su prioridad, alcance y descripción, coste estimado y plazo de ejecución.
- ✓ Por otro lado, debe estar justificado documentalmente el requisito legal o normativo que da origen a cada proyecto, estableciendo claramente la relación entre las iniciativas propuestas y las obligaciones en materia de ciberseguridad aplicables a AMVISA.
- ✓ Por último, este documento debe contener un Plan de Formación que al menos estructure e indique un programa formativo adaptado a los distintos perfiles y responsabilidades dentro de la organización. Incluyendo un análisis previo de los perfiles de los trabajadores por departamentos y responsabilidades, un calendario de sesiones, y la metodología específica para cada grupo, garantizando un mínimo de dos horas de formación por perfil y al menos una sesión remota. Además, debe contener la periodicidad, los métodos de evaluación y el material formativo requerido. Este plan debe garantizar que el personal responsable del manejo de la información y la Ciberseguridad esté debidamente capacitado, contribuyendo a la concienciación y al cumplimiento de las normativas aplicables en materia de Ciberseguridad.

9. Planificación, dirección y seguimiento del proyecto

En la ejecución y gestión del proyecto se contemplarán los siguientes puntos.

9.1. Duración y fases del proyecto

El proyecto se dividirá como mínimo en las siguientes fases que se deberán desarrollar en un periodo máximo de 6 meses desde la fecha de firma del contrato:

1. Arranque, Planificación y Seguimiento del Proyecto
   - ➢ **Entregable 1. Informe de la/s reunión/es de Arranque (*Kick-off*).**
2. Diagnóstico de situación actual de AMVISA
   - ➢ **Entregable 2. Informe diagnóstico de la situación de AMVISA respecto al ámbito de la Ciberseguridad.**
3. Análisis jurídico de la situación
   - ➢ **Entregable 3. Informe a nivel jurídico sobre la normativa de aplicación en AMVISA.**

4. Política y Estrategia de Ciberseguridad
   - **Entregable 4. Política y Estrategia de Ciberseguridad de AMVISA.**
5. Análisis de Riesgos y GAP en Ciberseguridad
   - **Entregable 5. Análisis de Riesgos y GAP en materia Ciberseguridad para AMVISA.**
6. Elaboración Plan Director Ciberseguridad
   - **Entregable 6. Plan Director de Ciberseguridad AMVISA.**

Cada una de los entregables indicados al final de cada fase deberá ser verificado por AMVISA. De no contar alguna entrega con su visto bueno, se consideraría que el contratista ha incumplido la obligación principal del contrato, siendo este hecho causa de resolución del contrato conforme a lo establecido en el artículo 211 de la Ley de Contratos del Sector Público. El licitador sólo tendría derecho al cobro de la parte proporcional a la duración del último visto bueno recibido.

9.2. Metodología y herramientas.

Dentro de las ofertas presentadas, cada empresa licitante deberá detallar la metodología de desarrollo y las herramientas con la que se abordará la ejecución del presente proyecto. Además, en el proceso de licitación se valorará especialmente la utilización e implantación de herramientas estándar y reconocidas bajo las normativas de aplicación vigentes. Esta exigencia garantizará que las soluciones aportadas estén alineadas con las mejores prácticas y requerimientos regulatorios actuales, aportando mayor fiabilidad, interoperabilidad y calidad a los resultados del proyecto.

9.3. Equipo de trabajo.

AMVISA designará el equipo de trabajo responsable conforme a su criterio y en función de los requerimientos y perfiles propuestos en las ofertas presentadas por las empresas licitantes. Esta designación tendrá en cuenta la experiencia, competencias y capacidad demostrada en las candidaturas para garantizar una adecuada ejecución y cumplimiento de los objetivos del proyecto.

Por parte de la empresa adjudicataria, se asignarán **como mínimo** para este proyecto:

- **Responsable de proyecto y consultor:**
  - Titulación técnica universitaria en Ingeniería de Informática o Telecomunicaciones.
  - Máster Universitario Ciberseguridad y/o formación y capacitación acreditable en seguridad de la información.
  - Experiencia mínima de 10 años en tareas similares a este proyecto.

- **Consultor sénior:**
  - Titulación técnica universitaria en Ingeniería de Informática o Telecomunicaciones.
  - Máster Universitario Ciberseguridad y/o formación y capacitación acreditable en seguridad de la información.
  - Experiencia mínima de 5 años en tareas similares a este proyecto.

En la oferta se deberá incluir los siguientes aspectos relativos al equipo de trabajo:

- Historial profesional de cada miembro del equipo.
- Responsabilidades y roles dentro del proyecto.

9.4. Seguimiento y control

El seguimiento y control del proyecto quedará definido en la fase inicial de Definición, Planificación inicial y seguimiento, acordado entre AMVISA y la empresa adjudicataria.

10. Plan de facturación

En la oferta, el licitador debe incluir la programación justificada de las actuaciones, donde se incluirá con detalle la programación de trabajos y tareas que se desarrollarán en el proyecto. En dicha programación, para su definición, se tendrán en cuenta el conjunto de instalaciones y medios auxiliares precisos, así como las situaciones provisionales que deban establecerse. Además, se indicarán las interrelaciones entre las diversas tareas y actividades, el plazo parcial de cada una de ellas y sus trabajadores asociados.

La Contratación se realizará por un pedido único por la totalidad del importe del servicio y con compromiso mínimo de una duración de 3 meses para el análisis o auditorías internas y 3 meses más (6 meses en total) para el resto de las tareas. Se planteará la siguiente facturación del servicio:

- **20%** del proyecto al inicio del servicio
- **10%** del proyecto en cada uno de los 6 Entregables definidos para el proyecto y que están condicionadas a la recepción, tras el visto bueno por parte de AMVISA.
- **20%** del proyecto a la finalización del servicio y visto bueno de AMVISA

El importe de los cargos es debido a la recepción de la factura y deberá ser satisfecho mediante transferencia dentro de los 30 días naturales posteriores a la fecha de emisión de la misma.

El contratista entregará factura en el registro de entrada de la AMVISA para su tramitación y en ella deberán identificarse los órganos administrativos a los que vaya dirigida la misma referenciando el número de Expediente PRTR **26/2025**.

Las facturas deberán ser conformadas por el Responsable del Contrato y deberá emitirse de conformidad con las disposiciones vigentes y, específicamente constará: numeración seriada, fecha de expedición, descripción de los trabajos realizados, NIF del expedidor y destinatario y el IVA repercutido.

Si se observase que la factura presentada adolece de algún requisito exigible, se solicitará su subsanación sin que empiece a computarse el plazo para el pago hasta su corrección.

11. Formato de los Entregables

El soporte de todos los Entregables deberán ser presentados en formato editable e incluir únicamente los logotipos requeridos por la financiación en el marco del Plan de Recuperación, Transformación y Resiliencia (PERTE Digitalización del Ciclo del Agua) y el propio logo de AMVISA. No se admitirán documentos en formato cerrado o con logotipos no autorizados por las directrices de dicha financiación.

12. Condiciones

Las empresas que opten a la prestación del servicio objeto de la presente licitación deben comprometerse a cumplir como mínimo con las condiciones indicadas en los pliegos (administrativo y técnico).
El trabajo de desarrollo interno se podrá realizar en las instalaciones de la empresa adjudicataria, pero al menos las reuniones de seguimiento, entrevistas y la revisión de las instalaciones se debe realizar en las distintas instalaciones de AMVISA. Los medios, equipos y desplazamientos necesarios del personal de la empresa adjudicataria serán a cargo de la misma.

13. Gestión de la Propiedad

Cualquier resultado del trabajo que se derive de esta contratación, parametrización, desarrollos, adaptaciones y documentación específica, informes, será propiedad de AMVISA y no podrá ser utilizado por la entidad adjudicataria para otros fines que no sean los descritos en el pliego.

Si se desea utilizar la prestación del presente servicio en el marketing de la empresa adjudicataria, se deberá informar y solicitar el consentimiento previo de AMVISA.

14. Disponibilidad y Confidencialidad de la Información

El adjudicatario estará obligado a facilitar a AMVISA la totalidad de la información relativa al proyecto en el momento que AMVISA se la solicite y en el formato establecido.

En lo referente a la Confidencialidad, el adjudicatario se compromete a mantener la más estricta confidencialidad y secreto sobre la información confidencial, comprometiéndose a no revelarla a terceros, salvo en los casos específicamente previstos en este Pliego, debiendo implementar las medidas técnicas, jurídicas, formativas y organizativas que garanticen dichas obligaciones de confidencialidad y secreto.

El adjudicatario se compromete a limitar el acceso a la información confidencial a las personas de su organización que estrictamente precisen tener acceso para el cumplimiento del contrato, debiendo por otro lado, con carácter previo a que se produzca dicho acceso a la información confidencial, suscribir un contrato de confidencialidad que garantice el cumplimiento de lo dispuesto en el presente pliego. De igual modo, el adjudicatario se compromete a suscribir acuerdos de confidencialidad en iguales términos a los reflejados en el presente pliego con cualesquiera empresas, asociaciones, fundaciones, profesionales, etc., a los que se les pueda subcontratar, cuando esto sea posible según las previsiones del contrato, parte de las acciones a acometer en el proyecto.

La información confidencial única y exclusivamente podrá ser utilizada por el adjudicatario en el marco del presente compromiso y con el único objetivo del cumplimiento y desarrollo del mismo, no pudiendo emplearse ni aplicarse para otro tipo de propósito o finalidad diferente a la contenida en el contrato.

Al momento de la finalización del contrato, por cualesquiera causas que fueran, el adjudicatario, con carácter general y salvo que haya otra previsión en el contrato, deberán proceder a la devolución de la información y en su caso, a la eliminación de manera efectiva y segura de sus sistemas informáticos en el caso de que la hubiera incorporado a los mismos.

El deber de confidencialidad estará vigente durante la vigencia del contrato y se mantendrá en vigor los cinco (5) años siguientes a su finalización con independencia de la causa que motive la resolución. Por su parte, el ámbito territorial del compromiso de confidencialidad será mundial.

Se entenderá como información confidencial, cualesquiera datos, procedimientos, técnicas, know-how, informaciones o explicaciones que sobre los anteriores elementos se realice, con independencia de la naturaleza que tengan ya sea técnica, comercial o económica, que AMVISA revele, comunique o ponga a disposición del adjudicatario, con independencia del medio o procedimiento empleado para ello, incluido la comunicación oral, durante la vigencia del contrato.

No obstante, no tendrá la consideración de información confidencial y por tanto no estará sometida a las obligaciones estipuladas en la presente cláusula toda aquella información que el adjudicatario estuviera en condiciones de probar que:

- ✓ Hubiera sido conocida por el adjudicatario por un medio legítimo con anterioridad a haber sido recibida de AMVISA.
- ✓ Sea en el momento de recibirla de AMVISA, o se convierta más tarde, de carácter público o de dominio público.
- ✓ Se reciba a través de terceros que no tengan ninguna obligación de confidencialidad con el adjudicatario.
- ✓ Sea desarrollada por el adjudicatario independientemente de la información confidencial que ha recibido de AMVISA siempre y cuando se pueda acreditar documentalmente.
- ✓ El adjudicatario se vea obligado a poner en conocimiento de un tercero por exigencia legal. No obstante, en dicho caso el adjudicatario notificará con la mayor brevedad posible a AMVISA dicha circunstancia para que pueda tomar las medidas que estime oportunas con el fin de preservar la confidencialidad de dicha Información. En cualquier caso, el adjudicatario se compromete a facilitar únicamente aquella información que estén obligadas a divulgar, y a llevar a cabo cuantos actos sean necesarios para preservar la confidencialidad de la información.
- ✓ AMVISA le autorice a divulgar.

Una vez concluida la prestación del contrato, la entidad adjudicataria estará obligada a entregar a AMVISA todos los soportes que contengan datos de carácter personal y/o confidencial o proceder a su destrucción según se acuerde entre las partes. En este último caso la empresa deberá presentar un certificado que acredite su destrucción. Para la destrucción de ficheros en soporte papel se deberán utilizar necesariamente destructoras de papel.

15. Contenido de la propuesta técnica (sobre nº 2)

El contenido de la propuesta debe contener al menos, como mínimo, una **Memoria Técnica** que incluya una estimación detallada de las horas de recursos internos de AMVISA requeridas para la ejecución de la propuesta. Asimismo, debe también incluir la información adicional relevante relativa a los recursos planteados para la realización de este proyecto.

El documento debe también especificar los mecanismos de coordinación y comunicación previstos entre el equipo adjudicatario y AMVISA, así como detallar los criterios de control de calidad y los indicadores de seguimiento de la ejecución.

Finalmente, se incluirá la justificación técnica de las soluciones propuestas, haciendo referencia a estándares, normativas aplicables y mejores prácticas del sector para garantizar el alineamiento con los objetivos estratégicos y regulatorios de AMVISA.

A modo resumen, la propuesta técnica (sobre nº 2) presentada debe estar compuesta por una **Memoria Técnica** que contenga al menos:

1. **Metodología de ejecución** planteada que debe adecuarse a requisitos técnicos y normativos, así como a la problemática y necesidades de AMVISA.
2. **Medios humanos y técnicos**, con el organigrama del equipo de trabajo, sus perfiles profesionales (incluyendo específicamente sus *Curriculum Vitae* y su historial profesional en tareas similares) y su dedicación estimada para este proyecto. Se considerará la utilización de herramientas estándares reconocidas que puedan ser mantenidas y utilizadas por AMVISA tras la finalización del proyecto.
3. **Programación y planificación** de los trabajos, con una estimación detallada de las horas de recursos internos requeridos por parte de AMVISA y la indicación explicita de las metodologías o herramientas de gestión que están previstas se apliquen a este proyecto.
4. **Mecanismos de coordinación, comunicación, criterios de control de calidad e indicadores de seguimiento** previstos para el proyecto, incluyendo un análisis de riesgos para su correcta implementación y su plan de mitigación correspondiente.

Firmado digitalmente por IGNACIO BASTERRA LASA - 16271730N
Fecha: 2025.11.10 10:15:25 +01'00'