



PLIEGO DE CLÁUSULAS TÉCNICAS

QUE HAN DE REGIR LA CONTRATACIÓN DE UN
“SERVICIO DE AUTODIAGNÓSTICO E ITINERARIO
DE MEJORA EN CIBERSEGURIDAD PARA EMPRESAS
EN NAVARRA” EN EL MARCO DEL PLAN DE
RECUPERACIÓN, TRANSFORMACIÓN Y
RESILIENCIA FINANCIADO CON FONDOS DE LA
UNIÓN EUROPEA -NEXT GENERATION EU



ABRIL DE 2025

Navarra de Servicios y Tecnologías, S.A.

| C/ Orcoyen, s/n. 31011 Pamplona - Navarra |

| info@nasertic.es

| www.nasertic.es

| Tel: 848 420 500

| Fax: 848 426 751

Índice

1	CONTEXTO.....	2
1.1	Introducción	2
1.2	Iniciativas en el ámbito de la ciberseguridad en Navarra	2
1.3	Objetivos estratégicos en Ciberseguridad para el tejido empresarial navarro....	3
2	OBJETO OBJETIVOS Y ALCANCE DE LA CONTRATACIÓN	5
2.1	Objeto	5
2.2	Objetivos	5
2.3	Alcance	5
3	DESCRIPCIÓN DEL SERVICIO.....	7
3.1	Herramienta de Autodiagnóstico.....	7
3.2	Servicio de formación y soporte	9
3.3	Servicio de supervisión y reporting	10
4	METODOLOGÍA Y PLAN DE TRABAJO	10
5	EQUIPO DE TRABAJO	11
6	DIRECCIÓN Y CONTROL DE LOS TRABAJOS.....	11
7	OBLIGACIONES DE INFORMACIÓN Y DOCUMENTACIÓN.....	12

1 CONTEXTO

1.1 Introducción

Las amenazas a la seguridad de la información han existido siempre, pero ha sido en los últimos años cuando los riesgos asociados a las mismas han sufrido un crecimiento exponencial. La adopción de tecnologías como elementos fundamentales en los procesos de negocio influye de forma relevante en el impacto de los ciberataques. Igualmente, junto con el desarrollo de las nuevas tecnologías ha aumentado la complejidad de los sistemas empleados por los atacantes para poner en jaque la información y ha aumentado la probabilidad de que se produzcan estos ataques. Esto provoca que el riesgo al que se ven expuestas las organizaciones sea especialmente alto, dinámico y difícil de gestionar, tal y como nos demuestra conocer a diario nuevas empresas y entidades que han visto su funcionamiento paralizado por ciberataques.

Es necesario tanto innovar en ciberseguridad como acercar la ciberseguridad a un ámbito cada vez más sensible y expuesto: el tejido empresarial. Por un lado, por la rápida evolución de las tecnologías y la necesidad por parte de las organizaciones de adoptarlas para ser cada vez más competitivas y eficientes. Además, es imprescindible mantener el ritmo de innovación en ciberseguridad para poder adoptar nuevas tecnologías sin superar un nivel de riesgo aceptable. Para ello, se deben generar espacios de colaboración regional público-privada, involucrando administración, empresas y academia, para impulsar la innovación, la adopción de soluciones de ciberseguridad y la generación de talento.

1.2 Iniciativas en el ámbito de la ciberseguridad en Navarra

El Gobierno de Navarra no ha sido ajeno a esta realidad, apostando en este ámbito por dos iniciativas de referencia en Navarra:

- **Polo de Innovación Digital de Navarra (Polo IRIS)**: nace con la misión de *'contribuir a la aceleración de la transformación digital de innovación en Navarra, actuando como catalizador y ventanilla única de la digitalización de la región a través de la prestación eficiente de servicios, la gestión eficaz de sus recursos y la generación de espacios de colaboración con los agentes clave público-privados'*. La visión del Polo es la de *'constituirse como el espacio de referencia en materia de digitalización e innovación de Navarra, favoreciendo la colaboración y generación de alianzas entre todos los agentes económicos y sociales de la región e impulsando su transformación a través de servicios avanzados'*. Se puede caracterizar a través de los siguientes pilares fundamentales:
 1. Como respuesta a los retos de transformación digital de la región.
 2. Como ventanilla única de transformación digital e innovación en Navarra.
 3. Como impulsor de la especialización tecnológica en Navarra.
 4. Como catalizador de servicios digitales al tejido empresarial navarro.
 5. Como promotor de una sociedad digital en Navarra.

Es en el punto tercero, donde el Polo focaliza esfuerzos en el **impulso de áreas de especialización tecnológica** que permitan impulsar la competitividad global de la

Comunidad Foral de Navarra y que, de forma específica, contribuyan al desarrollo de los sectores estratégicos fijados en la Estrategia de Especialización Inteligente de Navarra S4.

Una de estas áreas de especialización es la **Ciberseguridad**. Abarca todas aquellas actividades o procesos mediante los que los sistemas de información y comunicación y el contenido de los mismos son protegidos de o defendidos contra daños y contra su uso, modificación o explotación no autorizados.

- **Navarra Cybersecurity Center (NavCC)**: Su principal objetivo es el **impulso al desarrollo de iniciativas en torno a la ciberseguridad** que deriven en un aumento de la ciber resiliencia en todos los ámbitos de la Comunidad Foral de Navarra, incluyendo el tejido empresarial y con especial foco en pymes y autónomos y establecerse como ventanilla única en materia de seguridad digital.

Las iniciativas se dirigen a la dinamización del sector de la ciberseguridad tanto desde el punto de la oferta de los servicios ofrecidos en la Comunidad Foral, como desde el punto de vista de la demanda y utilización de dichos servicios. Por tanto, tiene como objetivo estratégico contribuir a la transformación socioeconómica sostenible de Navarra en un entorno digital e hiperconectado, seguro y ciberresiliente.

Ambas iniciativas están íntimamente relacionadas, siendo el NavCC el principal instrumento para el desarrollo del área de especialización de ciberseguridad del Polo de Innovación Digital de Navarra IRIS.

1.3 Objetivos estratégicos en Ciberseguridad para el tejido empresarial navarro

En este apartado se definen las bases estratégicas del área de especialización de Ciberseguridad del Polo de Innovación Digital de Navarra para potenciar este ámbito.

La transversalidad y globalidad del ciberespacio supone que la ciberseguridad sea un tema clave en todos los sectores de actividad. Precisamente por ello la cooperación y compartición de avances y conocimiento permiten mayores logros en la protección frente a las ciber amenazas. La ciberseguridad tiene un carácter transversal que afecta a todo el tejido empresarial, pero también a Administraciones Públicas y a la sociedad en su conjunto. Por tanto, el área de especialización de Ciberseguridad del Polo de Innovación Digital de Navarra, entendiendo la ciberseguridad como una oportunidad económica, profesional y empresarial, se centra en potenciar iniciativas tractoras con potencial para escalado en distintos sectores industriales y productivos, incluyendo también acciones relacionadas con la sensibilización respecto a los riesgos inherentes al mundo conectado.

Con todo lo anterior, podemos definir los siguientes **objetivos estratégicos en materia de ciberseguridad, canalizados a través del Navarra Cybersecurity Center (área de especialización del Polo IRIS)**:

1. Contribuir, desde el impulso público, a que el proceso de digitalización y la hiperconectividad en un entorno ciberseguro produzcan una transformación socioeconómica sostenible en términos de **productividad y empleo**.
2. Impulsar proyectos regionales de ciberseguridad, asegurando su eficiencia y maximizando su impacto a través de la **coordinación, la colaboración y la complementariedad** de la colaboración público-privada.
3. Impulsar el **equilibrio territorial** en materia de ciberseguridad, de modo que ningún ámbito se quede rezagado en un objetivo global como el impulso a la cultura de la ciberseguridad para empresas y ciudadanía.
4. Fomentar el crecimiento estratégico de un **sector clave como el TIC**, pero también otros **sectores económicos estratégicos** en las economías regionales a través de la transformación y especialización digital.
5. Establecer las bases para un **entorno de colaboración estable y sostenible** a medio y largo plazo que velen por el avance coordinado en aspectos de ciberseguridad.

Para el desarrollo de los objetivos estratégicos anteriores, se han definido las siguientes **líneas de actuación**:

1. Creación de un centro de ciberseguridad regional.
2. Fomento del ecosistema empresarial en el sector de la ciberseguridad.
3. Creación de centros demostradores.
4. Gestión del talento.
5. Acciones de sensibilización.

2 OBJETO OBJETIVOS Y ALCANCE DE LA CONTRATACIÓN

2.1 Objeto

El objeto del presente pliego es definir las cláusulas técnicas particulares que han de regir la contratación de un **“Servicio de autodiagnóstico e itinerario de mejora en Ciberseguridad para empresas en Navarra”**, detallando objetivos, alcance, así como la descripción de los requisitos técnicos mínimos obligatorios y condiciones técnicas generales que deberán considerarse para la prestación del servicio.

2.2 Objetivos

El principal objetivo de la contratación de un **“Servicio de autodiagnóstico e itinerario de mejora en Ciberseguridad para empresas en Navarra”** es poner a disposición del tejido empresarial navarro una herramienta de autoevaluación y diagnóstico que permita medir, de una manera objetiva y estandarizada, el nivel de madurez en Ciberseguridad de las empresas, proporcionando al mismo tiempo un itinerario de mejora personalizado con una propuesta de acciones que permitan impulsar las capacidades de ciberresiliencia, elevando de esta manera el nivel de madurez en Ciberseguridad de las empresas navarras.

Así mismo, el servicio proporcionará formación, apoyo y supervisión dirigido a integradores locales para que estos puedan hacer uso de la herramienta de autodiagnóstico. De esta manera los integradores locales podrán, fuera del alcance del servicio licitado, utilizar la herramienta para acompañar a las empresas en el proceso de autoevaluación y definición de un plan de mejora personalizado y priorizado.

Adicionalmente, el servicio permitirá al Navarra Cybersecurity Center obtener una visión global y comparativa sectorial del grado de madurez en Ciberseguridad en el tejido empresarial Navarro, a la vez que permitirá cuantificar y medir el nivel de mejora.

Cabe destacar que la herramienta de autoevaluación y diagnóstico se podrá utilizar también en otros ámbitos o contextos, como puede ser el de la Administración Pública, las Entidades Locales o las Sociedades Públicas, siempre dentro de los términos de licenciamiento acordados.

2.3 Alcance

El alcance de la presente contratación comprende los siguientes aspectos, cuyos requisitos técnicos se detallan en el punto 3 DESCRIPCIÓN DEL SERVICIO:

- Herramienta de autodiagnóstico en modalidad SaaS:
 - o Modelo de suscripción con licenciamiento para ejecutar, al menos, **200 autodiagnósticos**
- Servicios de formación y soporte sobre la herramienta:
 - o Servicio de **formación** para **10** integradores locales

- Servicio de soporte sobre la herramienta para resolver dudas e incidencias técnicas
- Servicios de supervisión y reporting sobre el uso de la herramienta:
 - Servicio de **supervisión** sobre un muestreo aleatorio del **25%** de los autodiagnósticos (**50** autodiagnósticos)
 - Creación de un informe global ejecutivo actualizado con periodicidad **trimestral**
 - Creación de informes sectoriales (individuales por cada sector) para **4 sectores** y actualizados con periodicidad **trimestral**

La propuesta presentada deberá cumplir con los siguientes hitos para la ejecución de las diferentes fases del proyecto:

- **FASE 0: Puesta en Marcha de la plataforma SaaS**
Incluye la puesta en marcha de la plataforma de autodiagnóstico en modalidad SaaS y con la personalización de "Look & Feel".
Esta fase deberá quedar entregada y aprobada dentro de los **2 meses** siguientes a la fecha de envío del pedido.
- **FASE 1: Servicios Continuos**
A partir de la fecha de puesta en marcha de la plataforma SaaS, tanto la herramienta de autodiagnóstico como los servicios de formación, soporte, supervisión y reporting estarán activos de manera continua durante la validez del contrato, que finalizará el **31 de Marzo de 2026**.

3 DESCRIPCIÓN DEL SERVICIO

En este apartado se describen las características técnicas que conforman el objeto del contrato y que el adjudicatario deberá prestar, no siendo el listado que aparece a continuación una relación exhaustiva de las características del servicio contratado, sino las actividades generales demandadas por NASERTIC, cubriendo los aspectos de tareas a realizar y resultados esperados.

Los referidos requisitos deben entenderse como mínimos (a excepción de que se indique lo contrario). El licitador puede ofertar prestaciones superiores a las solicitadas, que se tendrán en cuenta durante la valoración técnica de la oferta, en los términos descritos en los criterios de adjudicación detallados en el pliego de cláusulas administrativas.

El adjudicatario deberá aportar y describir en su oferta las funcionalidades de la herramienta de autodiagnóstico, así como el servicio de formación, soporte, supervisión y reporting indicando los conocimientos, metodologías, herramientas y equipo de trabajo.

El adjudicatario se obliga a guardar secreto y a hacerlo guardar al personal que emplee para la prestación del servicio, respecto a toda la información que con motivo del desarrollo de los trabajos llegue a su conocimiento, no pudiendo utilizarla para sí o para otra persona o entidad.

Para la prestación del servicio, el **adjudicatario** deberá ejecutar las siguientes actividades y cumplir con los siguientes requerimientos:

3.1 Herramienta de Autodiagnóstico

El servicio incluirá la **provisión de una herramienta de autodiagnóstico**, basada en una plataforma SaaS, que permita a las empresas navarras realizar de manera autónoma (o con el apoyo de integradores locales debidamente formados), y en base a cuestionarios, la medición de su **nivel de madurez en Ciberseguridad** y la generación de **planes de mejora personalizados**.

El objetivo de la herramienta de autodiagnóstico es proporcionar transparencia sobre el estado actual de madurez en Ciberseguridad de las PYMEs navarras, en base a una mejor información sobre su posicionamiento y la disponibilidad de un lenguaje común entre todas las partes involucradas.

Para ello, la herramienta de autodiagnóstico debe de implementar un **modelo de calificación de ciberseguridad**, estableciendo diferentes niveles de madurez, basado en un marco común, estandarizado y contrastable de controles que cubran los diferentes dominios de la Ciberseguridad de acuerdo con los principales **estándares de referencia** (NIST, ISO, ENS...).

La **herramienta de autodiagnóstico** deberá cumplir con los siguientes requisitos mínimos:

- La medición del **nivel de madurez** se realizará en base a cuestionarios estandarizados que cubran los diferentes dominios de la Ciberseguridad.
- La herramienta dispondrá de dos niveles de cuestionarios, un **cuestionario básico** para un diagnóstico rápido inicial orientado a establecer la línea base y los objetivos de madurez, y un **cuestionario avanzado** para obtener las calificaciones de madurez, así como una serie de recomendaciones concretas de mejora que permitan alcanzar los objetivos previamente establecidos.
- Las capacidades de Ciberseguridad evaluadas en los cuestionarios deben estar basadas en un **marco de controles común** para todas las empresas, para lograr la mayor objetividad posible, clasificadas en dominios y secciones alineados con los principales **estándares de referencia** (NIST, ISO, ENS...)
- El sistema de medición utilizado deberá definir **niveles estandarizados de madurez** (por ejemplo: A-B-C-D...) que apliquen tanto a nivel global de la empresa como a nivel de cada uno de los dominios de Ciberseguridad evaluados.
- La herramienta permitirá **delimitar el alcance** de los servicios que cada empresa desee evaluar, así como definir los **objetivos de nivel de madurez** que se consideren adecuados. Los cuestionarios se deberán adaptar en base a esta información, de manera que sean más precisos y no incluyan preguntas que no sean de aplicabilidad para la empresa en cuestión.
- La herramienta debe ser capaz de considerar la **existencia de auditorías o acreditaciones** con las que cuente la entidad (NIST, ISO, ENS...) para no requerir dar respuesta a cuestiones que dichas evaluaciones ya presuponen.
- La herramienta deberá ser capaz de proporcionar una serie de **recomendaciones de mejora personalizadas**, a partir de los objetivos fijados y los resultados del cuestionario avanzado, proponiendo una serie de medidas concretas que permitan alcanzar esos objetivos.
- La herramienta debe ser capaz de realizar un **análisis GAP** frente a los principales estándares de referencia (NIST, ISO, ENS...)
- La herramienta deberá ser capaz de generar **informes** que permitan obtener una visión completa sobre las capacidades de cada entidad, junto con los elementos limitantes que impiden alcanzar el nivel requerido y el plan de acción propuesto.
- La herramienta deberá contar con un **manual o guía de ayuda** que facilite el uso y comprensión de la misma.
- El acceso a la herramienta se hará a través de una plataforma SaaS centralizada, públicamente accesible y convenientemente securizada. Se proporcionará un proceso seguro para el registro de los usuarios/entidades.
- La plataforma deberá permitir la definición de diferentes roles de acceso en función de la tipología de los grupos de usuarios (empresas finales, integradores y NavCC) y deberá poder adaptar, en la medida de lo posible, el **"look and feel"** de la

herramienta o los informes de acuerdo a los colores corporativos y logos del Navarra Cybersecurity Center.

La **herramienta de autodiagnóstico** deberá contar con un modelo de **licenciamiento** basado exclusivamente en el número de autoevaluaciones y el periodo de validez de las licencias:

- Cada licencia de autoevaluación deberá permitir la realización del cuestionario básico y el avanzado
- Al tratarse de una modalidad SaaS, el licenciamiento incluirá todas las actividades de mantenimiento y actualización de la plataforma

La **herramienta de autodiagnóstico** se entiende como herramienta en modalidad **SaaS**, viva y en constante evolución, por lo que será labor exclusiva del adjudicatario el mantenimiento de la misma y las actualizaciones a las nuevas versiones que se liberen como parte de la evolución estratégica de la herramienta durante el plazo de vigencia del contrato, sin que ello suponga ningún coste adicional al ya establecido.

3.2 Servicio de formación y soporte

El servicio incluirá acciones de **formación y soporte** dirigidas a las **empresas integradoras locales**, que les habilite para realizar el **acompañamiento** que las empresas finales necesiten para realizar el autodiagnóstico.

El objetivo del **servicio de formación y soporte** es poder involucrar en el proceso de diagnóstico y mejora a integradores locales, que acompañen a las empresas finales y se conviertan en socios de confianza para la definición e implantación (a posteriori y fuera del alcance de este servicio) de los planes de mejora, garantizando que estos integradores trabajen de una manera estandarizada en base a un modelo común.

El servicio de **formación y soporte** deberá cumplir con los siguientes requisitos mínimos:

- Se realizarán **formaciones** en el uso de la herramienta para los **integradores locales**, que les permita poder **validar** que los cuestionarios se cumplimentan correctamente, así como interpretar y contextualizar las recomendaciones concretas que permitan generar un plan de mejora personalizado.
- Se proporcionará un **servicio de soporte** para resolver las consultas o incidencias técnicas reportadas por los usuarios de la plataforma. A tal efecto se dispondrá de una herramienta de **Help Desk** que permita realizar el seguimiento de las consultas/incidencias en base a una serie de **SLAs** acordados.
- Se proporcionará una plataforma de **compartición de ficheros** segura para el intercambio de información de manera controlada

3.3 Servicio de supervisión y reporting

El servicio incluirá acciones de **supervisión y reporting** cuyo objetivo es controlar los procesos de autoevaluación para garantizar que se realizan de manera correcta, mientras que se ofrece una visión agregada y comparativa sobre los niveles de madurez de las empresas.

El servicio de **supervisión** deberá cumplir con los siguientes requisitos mínimos:

- Se llevará a cabo, por parte del prestatario del servicio, una **supervisión y validación** continua de los autodiagnósticos y planes de mejora mediante un proceso de muestreo aleatorio.
- El objetivo es garantizar que los integradores están realizando un uso adecuado de la herramienta y que están guiando correctamente a las empresas en la cumplimentación de los cuestionarios y en la interpretación de las recomendaciones de mejora.
- El proceso de supervisión estará basado en una serie de reuniones con el integrador y la empresa correspondiente para revisar y validar todo el proceso.

El servicio de **reporting** deberá cumplir con los siguientes requisitos mínimos:

- Se generarán **informes globales ejecutivos** a medida que permitan obtener una visión global sobre los niveles de madurez de las empresas navarras, así como una visión comparativa por los diferentes sectores de actividad.
- Se generarán **informes individuales por sector** a medida que deberán proporcionar un resumen ejecutivo de las fortalezas y debilidades de las empresas de un determinado sector, identificando los quick-wins y listando de acciones más prioritarias y que contribuirían de manera más significativa al incremento del nivel de madurez del sector.

4 METODOLOGÍA Y PLAN DE TRABAJO

La empresa licitadora deberá proponer de manera clara la metodología a seguir durante el desarrollo del proyecto, cumpliendo los objetivos y características fijados en el presente pliego (3 DESCRIPCIÓN DEL SERVICIO). En la metodología la empresa licitadora deberá detallar la forma en la que abordará cada uno de los servicios definidos para el proyecto. El nivel de detalle aportado será el necesario para expresar que el método propuesto permitirá alcanzar los objetivos fijados.

La empresa licitadora deberá presentar un plan de trabajo que incluya, al menos, las tareas, hitos y entregables asociados a los trabajos. Dichas propuestas deberán estar basadas en su experiencia y se incluirá una descripción que detalle cada tarea definiéndola con un grado de profundidad que permita comprender su alcance.

5 EQUIPO DE TRABAJO

El equipo estará formado por el número de profesionales, perfiles y dedicaciones que la empresa adjudicataria considere necesario para satisfacer, con garantías, todos y cada uno de los servicios antes descritos. En particular, se considera que el equipo de trabajo debería estar, al menos, compuesto por los siguientes perfiles:

- **Gestor del Servicio:** punto único de contacto para el control de la operativa del servicio
- **Equipo de Consultoría:** encargado de proporcionar los servicios de formación, supervisión y reporting personalizado
- **Equipo de Soporte:** con un modelo separado en niveles según las capacidades y actividades que realicen (por ejemplo: operador, analista, ingeniero)

Los profesionales que sean responsables de la ejecución del trabajo deberán disponer de la cualificación y experiencia necesarias para que se lleven a cabo de forma satisfactoria los trabajos indicados y se alcancen los objetivos deseados.

El personal asignado al contrato dependerá exclusivamente de la empresa adjudicataria. En ningún supuesto podrá considerarse con relación laboral, contractual, funcional o de naturaleza alguna respecto del Gobierno de Navarra, NASERTIC, y/o sociedades participadas por los mismos, tanto durante la vigencia del contrato como al término de este.

6 DIRECCIÓN Y CONTROL DE LOS TRABAJOS

Corresponde a la Dirección Técnica del proyecto en NASERTIC, la completa supervisión y dirección de los trabajos, proponer las modificaciones convenientes o, en su caso, proponer la suspensión de los mismos si existiese causa suficientemente motivada.

Para la supervisión de la marcha de los trabajos, NASERTIC indicará al comienzo del proyecto, la persona que ostentará la Dirección de Proyecto en NASERTIC y la composición de miembros del Equipo Director. Las funciones de este equipo en relación con el presente pliego serán:

- Velar por el adecuado cumplimiento de los servicios contratados.
- Independientemente de las reuniones ya establecidas en el Plan de Proyecto, la Dirección de Proyecto podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento del calendario del proyecto, así como la correcta consecución de los objetivos propuestos. El adjudicatario será responsable de la redacción y distribución de los informes de seguimiento y las correspondientes actas de reunión.
- Con el fin de garantizar que se satisfacen las necesidades y prioridades establecidas por el Equipo Director de Proyecto, se marcarán desde el lanzamiento las directrices

- de los trabajos a realizar, siendo estas directrices de obligado cumplimiento por parte del adjudicatario.
- Durante el desarrollo del proyecto se podrán solicitar, como parte de las tareas de seguimiento y control, entregas intermedias que permitan tanto la verificación del trabajo realizado, como evitar y reducir riesgos de desviación (en plazo y/o alcance) a lo largo del proyecto.

En las reuniones periódicas se evaluarán todas aquellas incidencias habidas que se hubieran originado en el cumplimiento de los objetivos planificados. Cuando a juicio de la Dirección del Proyecto, tales incidencias fueran imputables al adjudicatario, por falta de responsabilidad, incompetencia, desidia u otras causas de índole similar, podría la facturación resultante quedar minorada por el importe que corresponda de acuerdo a las penalizaciones establecidas en el Pliego de Cláusulas Administrativas Particulares.

7 OBLIGACIONES DE INFORMACIÓN Y DOCUMENTACIÓN

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por la Dirección de Proyecto, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

Así mismo, el adjudicatario estará obligado a asistir y colaborar, a través del personal que designe a este propósito, en las reuniones de seguimiento del proyecto definidas por la Dirección de Proyecto, quién se compromete a citar con la debida antelación al personal de la adjudicataria.

Como parte de las tareas objeto del contrato, el adjudicatario se compromete a generar la documentación de los trabajos realizados, de acuerdo con los criterios que establezca en cada caso la Dirección de Proyecto. Toda la documentación específica generada por el adjudicatario durante la ejecución del contrato será propiedad exclusiva de NASERTIC sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización por escrito de NASERTIC, que la concederá, en su caso y con expresión del fin, previa petición formal del adjudicatario.

En este sentido, el adjudicatario deberá informar a la Dirección de Proyecto sobre distintos aspectos relacionados con el funcionamiento y la calidad de los servicios prestados. Entre ellos será necesario presentar un informe en el formato y con la periodicidad que defina la Dirección de Proyecto, de cumplimiento de los servicios.

El adjudicatario proporcionará, sin coste adicional para la Sociedad, una copia en soporte digital con toda la documentación generada durante la prestación de los servicios objeto del contrato.