



## PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES

Nº Expediente: 582024039800
Denominación: ASISTENCIA TÉCNICA PARA EL PROYECTO CYBER-OT
Departamento: TICS
Técnico: JAVIER BERMEJO HIGUERA

<b>1</b>	<b>INTRODUCCIÓN .....</b>	<b>2</b>
<b>2</b>	<b>DESCRIPCIÓN DEL SERVICIO .....</b>	<b>2</b>
<b>3</b>	<b>REQUISITOS LEGALES TÉCNICOS .....</b>	<b>3</b>
<b>4</b>	<b>REQUISITOS DEL SERVICIO .....</b>	<b>3</b>
4.1	Descripción de perfiles profesionales.....	3
4.2	Organización del Servicio .....	6
4.2.1	Recursos materiales y aplicaciones informáticas .....	7
4.3	Trabajos a realizar .....	8
4.4	Seguimiento y control de las prestaciones .....	12
4.5	Criterios para la ejecución del trabajo .....	12
4.5.1	Criterios establecidos por el INTA.....	13
4.5.2	Seguimiento y verificación por parte del proveedor.....	13
<b>5</b>	<b>ACEPTACIÓN DEL SERVICIO POR EL INTA .....</b>	<b>14</b>
<b>6</b>	<b>DOCUMENTACION A ENTREGAR.....</b>	<b>14</b>
6.1	Documentación a entregar con la oferta. ....	14
6.2	Documentación a entregar durante la prestación del servicio. ....	14



## 1 INTRODUCCIÓN

El presente Pliego de Prescripciones Técnicas tiene por objeto fijar las condiciones que se deben exigir en el Procedimiento Abierto del contrato de servicio para la realización de tareas de Asistencia Técnica asociadas al proyecto CYBER OT del Departamento TICS de la Subdirección General de Sistemas Terrestres del INTA.

## 2 DESCRIPCIÓN DEL SERVICIO

El proyecto CYBER OT se basa en el desarrollo de capacidades de ciberseguridad en redes OT (operational technologies)/IT (information technologies) que integran la sensórica y dispositivos IoT (internet of things) utilizados en los ámbitos de logística 4.0, la movilidad autónoma y conectada en entornos estructurados y no estructurados, además de la gestión de la amenaza dron.

El proyecto consta principalmente de los siguientes desarrollos, sobre los que se requerirá la asistencia técnica objeto del contrato:

- Desarrollo de un sistema de reconocimiento de patrones de ataque en redes OT: desarrollo un prototipo que permita integrarlo mediante una interfaz para plugins con arquitecturas existentes de SIEM que permita la detección de patrones de ataque (con respecto al estándar Common Attack Pattern Enumeration and Classification-CAPEC<sup>1</sup>) mediante un enfoque de detección basado en patrones que combina modelos lógico-simbólicos de detección en tiempo real con técnicas de aprendizaje automático (machine learning) en un contexto que aprovecha el paralelismo para poder mantener un volumen masivo de hipótesis paralelas. Por otro lado, diseñar cómo esas técnicas pueden desplegarse sobre arquitecturas de detección en redes OT /IT.
- Desarrollo de una herramienta de reconocimiento, análisis de vulnerabilidades y perfilado de redes OT. Se desarrollará un método de reconocimiento compuesto capaz de combinar los resultados de los distintos métodos de análisis de vulnerabilidades y adaptar el orden y los parámetros con los que se ejecutarán características conocidas de la red OT/IT. Las decisiones se tomarán atendiendo a maximizar la utilidad de la información obtenida y reducir el riesgo de alterar el funcionamiento de la instalación industrial. El método contemplará la presentación de la información obtenida, ampliada, cuando resulte posible, con información sobre vulnerabilidades y métodos de explotación obtenida de bases de datos públicas.
- Desarrollo de un sistema de auditorías de seguridad automático, guiado por inteligencia artificial mediante el uso de un LLM (Large Language Model) al que será necesario realizar *fine-tuning* para adaptar su comportamiento al ámbito de ciberataques a redes IT/OT.
- Estudio de vulnerabilidades criptográficas en protocolos IoT de uso común y compilación de métodos y herramientas de identificación y ataque mediante el

---

<sup>1</sup> CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC™) (mitre.org)



desarrollo y diseño de un entorno de identificación y explotación de vulnerabilidades criptográficas en protocolos de comunicación y mecanismos autenticación/control de acceso, usados habitualmente en redes y dispositivos IoT.

- Desarrollo de una plataforma *Cyber Range* para simular entornos de redes OT/IT y realizar pruebas de seguridad y facilitar la formación y entrenamiento del personal técnico.

El cometido del personal solicitado es la realización de los trabajos propios del apoyo al proyecto, **descritos en el apartado 4** de este documento.

La prestación del servicio se efectuará en el siguiente Centro:

INTA Campus de "La Marañosa"  
Carretera San Martin de la vega M301, km 10,50 Madrid.

### 3 REQUISITOS LEGALES TÉCNICOS

Se deberán cumplir todas aquellas normas internas propias del centro especialmente en lo que a seguridad y normas de régimen interior se refiere.

### 4 REQUISITOS DEL SERVICIO

Las actividades a realizar serán aquellas que sirvan de apoyo al proyecto CYBER-OT descrito en el apartado 2, a realizar presencialmente en las instalaciones del campus "La Marañosa" del INTA. El personal se asignará a uno o varios de los paquetes de trabajo definidos para el proyecto, en las condiciones que se establecen en el apartado 4.2. El apoyo consta de **cinco (5) personas con dedicación completa** cumpliendo los requisitos que se muestran a continuación.

#### 4.1 Descripción de perfiles profesionales

La presente contratación requiere los cinco perfiles profesionales que se describen a continuación. El licitador, deberá presentar con la documentación de la oferta el curriculum vitae de cada uno de los componentes del equipo de trabajo que vaya a adscribir a la ejecución del contrato, con el fin de que el INTA pueda comprobar que cumplen las condiciones mínimas exigidas.

**Perfil 1 – Desarrollador C/C++**



Titulación	Título clasificado en el Nivel 2 del MECES o equivalente en: <ul style="list-style-type: none"><li>- Grado en Ingeniería Aeroespacial o Aeronáutica</li><li>- Grado en Ingeniería Industrial</li><li>- Grado en Arquitectura o Ingeniería Naval</li><li>- Grado en Ingeniería de Telecomunicaciones</li><li>- Grado en Ingeniería Informática</li><li>- Grado en Matemáticas</li><li>- Grado en Física</li><li>- Grado en Ciencia de Datos e Inteligencia Artificial</li></ul>
Idiomas	Inglés nivel B2 o equivalente
Cursos, Habilitaciones, Certificaciones y Experiencia	Se requiere una experiencia profesional mínima de 2 años en: <ul style="list-style-type: none"><li>- Experiencia en desarrollo en C/C++</li><li>- Experiencia en diseño de Bases de Datos</li><li>- Experiencia práctica en el diseño y desarrollo de software en entornos colaborativos y multidisciplinares</li></ul>

<b>Perfil 2 – Arquitecto de Sistemas</b>	
Titulación	Título clasificado en el Nivel 2 del MECES o equivalente en: <ul style="list-style-type: none"><li>- Grado en Ingeniería Aeroespacial o Aeronáutica</li><li>- Grado en Ingeniería de Telecomunicaciones</li><li>- Grado en Ingeniería Informática</li><li>- Grado en Matemáticas</li><li>- Grado en Física</li><li>- Grado en Ciencia de Datos e Inteligencia Artificial</li></ul>
Idiomas	Inglés nivel B2 o equivalente
Cursos, Habilitaciones, Certificaciones y Experiencia	Se requiere una experiencia profesional mínima de 2 años como arquitecto de sistemas.

<b>Perfil 3 – Pentester</b>
-----------------------------



Titulación	Título clasificado en el Nivel 2 del MECES o equivalente en: <ul style="list-style-type: none"><li>- Grado en Ingeniería de Telecomunicaciones</li><li>- Grado en Ingeniería Informática</li></ul>
Idiomas	Inglés nivel B2 o equivalente
Cursos, Habilitaciones, Certificaciones y Experiencia	Se requiere una experiencia profesional mínima de 2 años como pentester.

#### **Perfil 4 – Experto en Inteligencia Artificial y Machine Learning**

Titulación	Título clasificado en el Nivel 2 del MECES o equivalente en: <ul style="list-style-type: none"><li>- Grado en Ingeniería de Telecomunicaciones</li><li>- Grado en Ingeniería Informática</li><li>- Grado en Ciencia de Datos e Inteligencia Artificial</li><li>- Grado en Inteligencia Artificial</li></ul>
Idiomas	Inglés nivel B2 o equivalente
Cursos, Habilitaciones, Certificaciones y Experiencia	Se requiere una experiencia profesional mínima de 2 años en Inteligencia Artificial y Machine Learning y contando al menos con las siguientes competencias: <ul style="list-style-type: none"><li>- Conocimiento en Lenguajes de Programación como Python, Java o Go</li><li>- Competencia en el uso de bibliotecas y frameworks populares de IA y machine learning, como <i>TensorFlow</i>, <i>PyTorch</i>, <i>scikit-learn</i>, <i>Keras</i>, o equivalentes</li><li>- Conocimientos de Large Language Models (LLM) para su entrenamiento y despliegue</li><li>- Experiencia en tecnologías de contenedores: implementación, gestión y optimización de tecnologías de contenedores (Kubernetes y Docker) en entornos de producción y particularmente experiencia en proyectos de aprendizaje automático</li></ul>



<b>Perfil 5 – Experto en Big Data</b>	
Titulación	Título clasificado en el Nivel 2 del MECES o equivalente en: <ul style="list-style-type: none"><li>- Grado en Ingeniería de Telecomunicaciones</li><li>- Grado en Ingeniería Informática</li><li>- Grado en Ciencia de Datos e Inteligencia Artificial</li><li>- Grado en Inteligencia Artificial</li><li>- Grado en Estadística</li><li>- Grado en Matemáticas</li></ul>
Idiomas	Inglés nivel B2 o equivalente
Cursos, Habilitaciones, Certificaciones y Experiencia	Se requiere una experiencia profesional mínima de 2 años en Big Data y contando al menos con las siguientes competencias: <ul style="list-style-type: none"><li>- Conocimiento de la plataforma de análisis de datos Splunk</li><li>- Experiencia en tecnologías de Big Data, como Hadoop, Spark, etc., así como en análisis de datos a gran escala</li><li>- Conocimientos de bases de datos orientadas a grafos</li></ul>

Los perfiles profesionales presentados en la oferta, con sus cualificaciones, serán vinculantes para el ofertante en caso de resultar adjudicatario de la oferta.

La falsedad en el nivel de conocimientos técnicos del equipo ofertado y los conocimientos reales demostrados en la ejecución de los trabajos, o una ejecución de los trabajos manifiestamente ineficiente o negligente, implicará asumir penalidades, y en último término, podrá provocar **la resolución del contrato**.

El INTA de ninguna forma ostentará la condición de empleador respecto de los trabajadores contratados por el adjudicatario, que presten directa o indirectamente servicios para la ejecución del contrato.

No se podrán incluir en la oferta personas con contrato comprometido con otra entidad, pública o privada, para el mismo periodo de ejecución de esta contratación. La comprobación fehaciente de esta anomalía podrá significar la exclusión de la oferta.

#### 4.2 Organización del Servicio

El servicio requerido lo formarán los **cinco (5) perfiles técnicos** descritos en el apartado 4.1 actuando uno de ellos como responsable y coordinador del equipo.



La empresa adjudicataria deberá disponer de una estructura de mando entre su personal, de modo que exista un responsable que coordine la prestación del servicio con el responsable técnico del contrato del INTA del campus "La Marañosa". Esta figura será denominada como **coordinador técnico**.

Corresponderá al INTA la supervisión de la correcta realización de los trabajos. A tal efecto hará las indicaciones oportunas al adjudicatario para el mejor cumplimiento de los objetivos perseguidos conforme a lo establecido en el presente Pliego de Prescripciones Técnicas, a través del coordinador técnico designado por el adjudicatario. El adjudicatario, a través del coordinador técnico, es el encargado de distribuir el trabajo entre el personal encargado de la ejecución del contrato, así como de impartir a dichos trabajadores las órdenes e instrucciones que sean necesarias.

El horario del servicio estará comprendido con carácter general entre las 07:00 horas a 15:00 horas de forma ininterrumpida, de lunes a viernes, en las instalaciones del INTA en La Marañosa, de acuerdo con las necesidades del INTA. El número total máximo de horas del servicio (los cinco perfiles incluidos) será de 1.764 horas anuales por persona.

De forma excepcional y por requerimiento del INTA, para atender eventos clave de la organización, puede requerirse la asistencia de un técnico fuera de las instalaciones del INTA. Se considera que en ningún caso en más de 10 ocasiones al año y siempre dentro del territorio nacional.

Las vacaciones se cubrirán atendiendo a la siguiente distribución: en los meses de julio y agosto deberá permanecer, al menos un técnico

La empresa adjudicataria deberá ajustar su plan de trabajo al calendario laboral del INTA, con el fin de no mantener personal los días que no está abierto el Centro.

La cobertura de bajas laborales será por cuenta de la empresa adjudicataria. Las bajas o ausencias deberán cubrirse en un plazo máximo de 48 horas, a petición del responsable del expediente.

Diariamente, el coordinador técnico contactará con el responsable de INTA para la supervisión de los trabajos a realizar e informar de las incidencias, si las hubiera. Mensualmente, el coordinador técnico entregará al responsable de INTA un informe, detallando las tareas realizadas e incidencias acaecidas durante el mes vencido. Al coordinador técnico se le comunicará con 15 días de antelación la planificación horaria de las semanas posteriores.

#### 4.2.1 Recursos materiales y aplicaciones informáticas

La empresa adjudicataria será la responsable de proporcionar, al menos, un **ordenador portátil** a cada miembro del equipo. Este equipo podrá ser plataformado con las políticas requeridas para el acceso a las redes internas del Departamento del INTA correspondiente, una vez que el personal llegue a las instalaciones del INTA. Las características mínimas de este equipo serán:



PC portátil con pantalla de al menos 15 pulgadas  
Sistema operativo Windows 10/11, con licencia profesional  
Suite de Office 365 con licencia en vigor para toda la duración del contrato  
16 Gb de memoria RAM  
512 Gb de disco duro SSD

*1 Equipo portátil*

Además, el coordinador técnico dispondrá de un **teléfono móvil** de contacto para comunicación con el responsable del INTA asignado, durante la jornada laboral.

Asimismo, será de su cargo el mantenimiento y renovación de dicho material.

#### 4.3 Trabajos a realizar

Las tareas y labores a ejecutar como objeto el contrato se llevarán a cabo principalmente en las instalaciones del campus La Marañosa del INTA a efectos cumplir con los requerimientos de estudios, formación, investigación, tareas de ingeniería y asistencia técnica relativas al proyecto CYBER-OT del Departamento TICS de la Subdirección General de Sistemas Terrestres del INTA.

Para el **Perfil 1 – Desarrollador C/C++**:

- Desarrollo de aplicaciones para sistemas de comunicaciones tácticas.
- Desarrollo de test unitarios y de integración.
- Gestión del ciclo de vida del software, utilización de herramientas de control de versiones.
- Asesoramiento en la mejora de los procesos y procedimientos existentes.
- Elaboración de informes.
- Formación y asesoramiento al personal del INTA en el ámbito del desarrollo de software, cuando se requiera.
- Análisis y redacción de documentación técnica relativa a los puntos anteriores.
- Participación en proyectos y otros apoyos técnicos para el INTA en “La Marañosa”.
- Así como todos aquellos trabajos que se estimen por parte del responsable del contrato para cumplir el objeto del presente expediente.





### Para el Perfil 2 – Arquitecto de Sistemas:

- Propuesta y creación de las infraestructuras basadas en contenedores, entornos *cloud*, o virtualización, necesarias para los diferentes paquetes de trabajo del proyecto.
- Diseño y desarrollo de infraestructuras como servicio (IaaS).
- Desarrollo de paneles de control y visualizaciones: Crear paneles de control interactivos y visualizaciones de datos que permitan a los analistas de seguridad monitorear y analizar los datos de forma eficiente.
- Asesoramiento sobre las necesidades de hardware y software para el proyecto.
- Crear entornos de pruebas aislados y replicables dentro de la infraestructura de contenedores, con diferentes configuraciones de red, sistemas operativos y aplicaciones para simular escenarios realistas de ciberataques y defensa.
- Diseñar y crear laboratorios de formación interactivos, con ejercicios prácticos y simulaciones de ataques que permitan aprender y practicar habilidades de ciberseguridad y hacking ético.
- Desarrollar *scripts* y *pipelines* de CI/CD (Integración Continua / Entrega Continua) para automatizar el despliegue de entornos de pruebas y la ejecución de pruebas de seguridad en la infraestructura de contenedores.
- Configurar sistemas de monitorización y gestión para supervisar el rendimiento, la disponibilidad y la seguridad de la infraestructura de contenedores, con alertas automáticas para detectar y responder a posibles incidentes.
- Mantenerse al tanto de las últimas tendencias y avances en tecnologías de contenedores y ciberseguridad, y realizar actualizaciones y mejoras continuas en las infraestructuras creadas para el proyecto.
- Elaboración de informes.
- Formación y asesoramiento al personal del INTA, cuando se requiera.
- Análisis y redacción de documentación técnica relativa a los puntos anteriores.
- Participación en proyectos y otros apoyos técnicos para el INTA en “*La Marañososa*”.
- Así como todos aquellos trabajos que se estimen por parte del responsable del contrato para cumplir el objeto del presente expediente.

### Para el Perfil 3 – Pentester:

- Ejecución de pruebas de penetración y creación de patrones de ataque. En general operaciones asociadas a *Red Team* contra la plataforma asignada.



- Crear reglas y firmas de detección de intrusiones basadas en patrones conocidos de ataques y exploits.
- Crear un plan detallado de los tipos de ataques que se llevarán a cabo, incluyendo pruebas de penetración de red, pruebas de aplicaciones web, ingeniería social, explotación de vulnerabilidades, etc.
- Recopilar datos detallados sobre los ataques realizados, incluyendo registros de actividad, capturas de pantalla, evidencia de explotación exitosa, credenciales comprometidas, etc.
- Desarrollo de herramientas de ciberseguridad.
- Elaboración de informes.
- Formación y asesoramiento al personal del INTA, cuando se requiera.
- Análisis y redacción de documentación técnica relativa a los puntos anteriores.
- Participación en proyectos y otros apoyos técnicos para el INTA en “La Marañososa”.
- Así como todos aquellos trabajos que se estimen por parte del responsable del contrato para cumplir el objeto del presente expediente.

Para el **Perfil 4 – Experto en Inteligencia Artificial y Machine Learning**:

- Supervisar y gestionar la infraestructura que soporta una plataforma de Machine Learning (ML), incluyendo servidores (físicos o virtuales), almacenamiento de datos y recursos de red.
- Llevar a cabo el mantenimiento tanto a nivel de hardware como de software de los servidores del Laboratorio de Inteligencia Artificial (IA), para asegurar su correcto funcionamiento ininterrumpido.
- Apoyar en la dirección, control y seguimiento del despliegue de servicios en la plataforma de Machine Learning (ML) del Laboratorio de IA.
- Implementar políticas y herramientas para proteger los datos contra accesos no autorizados y posibles brechas de seguridad. Esto incluye la gestión de cifrado de datos, autenticación, autorización, y auditorías de seguridad.
- Implementar y utilizar herramientas de monitoreo para supervisar el rendimiento de la plataforma, como Zabbix, Prometheus, Grafana o similares.
- Ayudar a resolver problemas técnicos, asegurando que la plataforma esté siempre operativa. Esta actividad incluye la actualización y mantenimiento de la documentación técnica correspondiente.
- Estudiar y analizar las tendencias, avances técnicos y normativos en materia de aprendizaje automático, infraestructura de TI y prácticas de seguridad.



- Colaborar en el diseño y en la elección de tecnologías de IA.
- Diseñar y ejecutar los estudios, proyectos y pilotos para incorporar nuevas funcionalidades en la plataforma, y colaborar en su posterior implantación.
- Elaboración de informes.
- Formación y asesoramiento al personal del INTA, cuando se requiera.
- Análisis y redacción de documentación técnica relativa a los puntos anteriores.
- Participación en proyectos y otros apoyos técnicos para el INTA en “La Marañososa”.
- Así como todos aquellos trabajos que se estimen por parte del responsable del contrato para cumplir el objeto del presente expediente.

#### Para el Perfil 5 – Experto en Big Data:

- Análisis de datos de registros de eventos de seguridad de diferentes fuentes, como firewalls, sistemas de detección de intrusiones (IDS), registros de servidores, etc.
- Limpiar y normalizar los datos para eliminar ruido, errores y datos redundantes. Esto incluye la estandarización de formatos de registro, la detección y corrección de valores atípicos, y la conversión de datos no estructurados a formatos estructurados.
- Análisis de datos para identificar tendencias, patrones y anomalías. Esto puede implicar la aplicación de técnicas de visualización de datos para comprender mejor la distribución y la correlación entre las variables.
- Desarrollar modelos de datos que capturen los diferentes tipos de ataques y comportamientos maliciosos. Esto puede incluir el diseño de esquemas de datos y la creación de modelos de datos dimensionales o de grafo para representar las relaciones entre entidades.
- Desarrollo de algoritmos de detección de anomalías: Implementar algoritmos de aprendizaje automático y técnicas de minería de datos para detectar patrones de ataque inusuales y comportamientos maliciosos en los datos.
- Crear paneles de control interactivos y visualizaciones de datos que permitan a los analistas de seguridad monitorear y analizar los datos de forma eficiente.
- Optimizar el rendimiento de los sistemas de análisis de datos para garantizar tiempos de respuesta rápidos y eficiencia en el procesamiento de grandes volúmenes de datos.
- Investigar y evaluar constantemente nuevas herramientas, tecnologías y técnicas en el campo de la seguridad de la información y el análisis de big data.



- Documentar los procesos, metodologías y hallazgos del análisis de datos de seguridad, y proporcionar capacitación a otros miembros del equipo de seguridad según sea necesario.
- Elaboración de informes.
- Formación y asesoramiento al personal del INTA, cuando se requiera.
- Análisis y redacción de documentación técnica relativa a los puntos anteriores.
- Participación en proyectos y otros apoyos técnicos para el INTA en “*La Marañososa*”.
- Así como todos aquellos trabajos que se estimen por parte del responsable del contrato para cumplir el objeto del presente expediente.

#### 4.4 Seguimiento y control de las prestaciones

Corresponde al INTA, destinatario de los trabajos, la supervisión de las tareas para lograr los objetivos, en base a las especificaciones del presente pliego, proponer las modificaciones que convenga introducir o, en su caso, proponer la suspensión de los trabajos si existiese causa suficientemente motivada.

El equipo de trabajo que el adjudicatario aporte se integrará en un grupo de trabajo mixto en el que también participará personal propio del INTA.

El seguimiento y control del desarrollo de las prestaciones, se realizará a través de informes mensuales enviados por email en formato digital, en los que la empresa adjudicataria aportará un informe de situación en el que se reflejarán los datos estadísticos de actividad y las incidencias de funcionamiento. Además se podrán establecer reuniones de seguimiento con el coordinador técnico en cualquier momento.

Durante la ejecución de los trabajos objeto del contrato el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por el INTA a tales efectos, toda la información y documentación que estas soliciten para disponer de un pleno conocimiento técnico 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.

#### 4.5 Criterios para la ejecución del trabajo



#### 4.5.1 Criterios establecidos por el INTA

Cuando se produzca una variación en el personal que compone el servicio, la empresa adjudicataria deberá comunicarlo a su interlocutor en INTA con la máxima antelación posible, con al menos cinco días de anticipo al comienzo de los trabajos.

La valoración final de la productividad y calidad de los trabajos de las personas que realizan la asistencia corresponde al INTA, siendo potestad suya el solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de quince días, por otra persona de igual perfil, si existen razones justificadas que lo aconsejen como los siguientes criterios/incumplimientos:

- Por falta de corrección en su comportamiento.
- No observancia de las normas de seguridad y vigilancia del recinto.
- Retraso en la elaboración y ejecución de los trabajos a realizar.
- Incumplimiento de los objetivos del expediente.
- Incumplimiento de las normas relativas a Seguridad de la Información y PRL.

Además del personal mínimo requerido, se podrá solicitar al contratista adicionalmente personal para un período mínimo de un mes, cursando la petición con cuarenta y ocho horas de antelación, en las condiciones establecidas para el personal mínimo.

Sin perjuicio de la formación que sea necesaria de manera previa al inicio del servicio, el responsable del contrato podrá solicitar formación específica para el personal de la empresa adjudicataria, en base a una necesidad que pudiera surgir a lo largo de la duración del expediente. Esta formación deberá iniciarse en un plazo no superior a tres meses, siendo esta formación a cargo de la empresa adjudicataria. Esta formación tendrá un coste máximo anual de 5.000 € + IVA por perfil.

#### 4.5.2 Seguimiento y verificación por parte del proveedor

El proveedor deberá elaborar un plan de seguimiento con las actividades de verificación que irá realizando durante la vigencia del contrato, con independencia de las actividades de seguimiento que el INTA considere oportunas realizar, para las cuales, el proveedor deberá facilitar la información y datos que INTA le requiera.

Dicho plan deberá contener al menos:

- Calendario de actividades de seguimiento.
- Verificaciones a realizar.
- Responsables de las verificaciones.



## 5 ACEPTACIÓN DEL SERVICIO POR EL INTA

El servicio deberá cumplir los requisitos contenidos en el presente pliego.

Para comprobar la idoneidad y aceptación final de los trabajos realizados, el INTA se reserva el derecho de realizar las comprobaciones pertinentes para la aceptación del servicio.

## 6 DOCUMENTACION A ENTREGAR

La documentación a entregar se puede considerar en dos fases diferentes:

### 6.1 Documentación a entregar con la oferta.

- Curriculum vitae firmado por cada una de las personas propuestas en cada perfil de trabajo. Se incluirá al menos las titulaciones, experiencia profesional, nivel de idiomas, certificaciones y formación complementaria específica. En particular, en cuanto a la experiencia se solicita detallar los servicios o proyectos realizados relacionados con las competencias requeridas y trabajos a realizar recogidos en PPT incluyendo una breve descripción del objeto, duración y funciones desempeñadas.

Extensión máxima 2 DIN-A4 por Curriculum vitae

### 6.2 Documentación a entregar durante la prestación del servicio.

- Al inicio de la ejecución: programa de trabajo y plan de seguimiento.
- Mensualmente: parte mensual de trabajo reflejando las horas realmente realizadas, las actividades realizadas y las incidencias del servicio.
- Informes, estudios, investigaciones realizadas por el personal aportado para el expediente.
- A la finalización: resumen e informe final del servicio, con los registros emitidos durante su ejecución.

EL TÉCNICO RESPONSABLE

JAVIER BERMEJO HIGUERA