PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA

ASISTENCIA TÉCNICA PARA APOYO A LA CREACIÓN, MANTENIMIENTO, CONTROL Y EXPLOTACIÓN DE REDES ASOCIADAS A SISTEMAS DE INFORMACIÓN ESPECÍFICOS DEL EJÉRCITO DEL AIRE Y DEL ESPACIO

Elaborado por
Comandante del Grupo de Explotación (CIGES)
Firma: BARRIGAS MUNUERA ALFONSO | 01189542M Firmado digitalmente por BARRIGAS MUNUERA ALFONSO |01189542M Nombre de reconocimiento (DN): c=ES, o=MINISTERIO DE DEFENSA, ou=PERSONAS, ou=CERTIFICADO ELECTRONICO DE EMPLEADO PUBLICO, serialNumber=IDCES-01189542M, sn=BARRIGAS MUNUERA | 01189542M, givenName=ALFONSO, cn=BARRIGAS MUNUERA ALFONSO | 01189542M Fecha: 2024.06.14 10:45:58 +02'00'
Alfonso Barrigas Munuera

1. ORGANISMO DESTINARIO, RESPONSABLE DEL CONTRATO Y DATOS DE CONTACTO

1.1 ORGANISMO DESTINATARIO

Unidad proponente: Centro de Informática de Gestión (CIGES)

Centro directivo: Jefatura de Servicios Técnicos y Ciberespacio (EA)

Departamento/organismo: Ejército del Aire y del Espacio (Ministerio de Defensa)

1.2 RESPONSABLE DEL CONTRATO

Se propone como Responsable del Contrato (REC) a Alfonso Barrigas Munuera, Comandante del Grupo de Explotación (CIGES), quien, con la colaboración de la Jefatura del Grupo de la Calidad, deberá supervisar la prestación del servicio, contando con facultades para aprobar aquellas modificaciones que no tengan repercusiones contractuales.

Para poder realizar los pagos establecidos en el contrato, quien ejerza como REC deberá informar al Órgano de Contratación de la conformidad del servicio prestado o, en caso contrario, de las deficiencias observadas y de las penalizaciones que considere procedentes de acuerdo con este PPT.

1.3 DATOS DE CONTACTO

Dirección Postal: Cuartel General del Ejército Aire. Calle Romero Robledo 8. Madrid 28008

Correo electrónico: abarmun@ea.mde.es

Teléfono: 619 386 381

2. CONTRATO

2.1 TÍTULO DEL CONTRATO

Asistencia técnica para apoyo a la creación, mantenimiento, control y explotación de redes asociadas a sistemas de información específicos del Ejército del Aire y del Espacio.

2.2 OBJETO DEL CONTRATO

Contratación de servicios de asistencia técnica para que, dando apoyo a los medios propios del CIGES, contribuyan al correcto cumplimiento de la misión y funciones encomendadas al Centro y definidas en la Instrucción General IG 10-11, en concreto:

(X) Satisfacer las necesidades CIS en el ámbito específico del Ejército del Aire en materia de sistemas de información y redes asociadas a los mismos, proporcionando servicios y apoyos CIS, conforme a lo dispuesto en la IG 70-13 y la IG 30-8, a todos los Mandos, Unidades, Centros y Organismos del EA, así como a sus destacamentos con ocasión de despliegues en operaciones y ejercicios.

(X) Ejercer las funciones establecidas por la normativa vigente en el EA como Órgano de Apoyo CIS al Emplazamiento (OACISE) del Cuartel General del Ejército del Aire (CGEA), prestando servicios y apoyos CIS, en materia de sistemas de información y redes asociadas, a los Mandos, Unidades, Centros y Organismos ubicados en el CGEA.

( ) Ejercer las funciones de administración y mantenimiento que se le asignen, de conformidad con la IG 01/10 del EMAD relativa al componente CIS del Sistema de Mando y Control Militar (SMCM), como Órgano de Apoyo CIS (OACIS) del Nodo del CGEA, de Primer Nivel, del Sistema de Información Militar del citado SMCM.

Con la asistencia técnica requerida se busca maximizar la operatividad de los servicios ofrecidos por el Centro, dentro de las distintas áreas en que el mismo está estructurado y detalladas para cada lote.

2.3 ASISTENCIA TÉCNICA

Para la prestación de este servicio de asistencia técnica, el Centro de Informática de Gestión (CIGES) requiere de la empresa adjudicataria los perfiles profesionales definidos en el **apartado 4,** para su desempeño según el presente Pliego de Prescripciones Técnicas (PPT).

3. DEFINICIÓN Y ALCANCE DE LOS TRABAJOS

En este apartado se describirán las prestaciones que consistirán en trabajos de consultoría, planificación, estudio de viabilidad, análisis, diseño, construcción, implantación y control para la correcta explotación y operación en producción de sistemas de información, y los mantenimientos evolutivos o adaptativos que permitan la incorporación de nuevas características funcionales con objeto de cubrir la ampliación o el cambio de las necesidades de usuario.

3.1 REQUISITOS FUNCIONALES

Para la correcta prestación del servicio, será necesario que el personal de asistencia técnica esté capacitado para cumplir con los siguientes requisitos, dentro de las atribuciones que correspondan a su perfil profesional:

Requisito	Descripción
Análisis	Toma de requisitos de las necesidades identificadas para una correcta definición de la solución a desarrollar, con la determinación de su viabilidad. Se incluirá en esta fase la información respecto a la integridad, posibles vulnerabilidades y demás riesgos asociados al proyecto.
Diseño	Diseño del proyecto a nivel lógico y/o físico, con un enfoque modular, que incluya la solución, los elementos y subelementos entregables, e identificando cualquier posible adquisición, así como la determinación de los recursos necesarios para impedir efectos que afecten a la operatividad del producto final, tales como cuellos de botella. Estos diseños se plasmarán en documentos usando software Microsoft Visio o equivalente.
Creación / Desarrollo	Ejecución de las acciones técnicas necesarias para llevar a cabo la solución definida en las fases de análisis y diseño, así como el registro y documentación de las mismas, de forma que queden garantizados posteriores mantenimientos
Configuración	Definir adecuadamente los parámetros que garanticen la correcta operación del producto final dentro del entorno tecnológico, así como su intercomunicación con otros sistemas, si así se determinara en las fases de análisis y diseño.
Securización	Implementar medidas de seguridad, siguiendo las Guías STIC publicadas por el CCN y otros estándares de la industria.
Ejecución de pruebas	Definición y realización de todas aquellas pruebas necesarias para garantizar que tanto la configuración como la seguridad implementada permiten hacer uso del producto final de forma eficaz por el usuario final y que la solución se ha implementado de forma adecuada en función de la carga de trabajo esperada.
Instalación	Realizar las acciones necesarias para que el entregable sea dispuesto en la ubicación adecuada, de forma que pueda ser empleada por los usuarios finales.
Control	Mediante la conexión del entregable a distintas soluciones de monitorización, disponer de la capacidad de informar sobre su estado en la red en explotación.
Mantenimiento	Corrección de cualquier deficiencia técnica y/o documental que permita resolver o paliar las incidencias que afecten a los sistemas de información, así como todas las tareas conexas necesarias para poder realizar dicha corrección.
Evolución y mejora	De acuerdo a las mejores prácticas aplicables al sector, proponer el uso de nuevas tecnologías o metodologías que maximicen el uso eficiente de los medios actuales o que permitan su modernización, garantizando así el uso de tendencias vanguardistas.

3.2 REQUISITOS NO FUNCIONALES

3.2.1 Requisitos técnicos

De acuerdo al entorno tecnológico definido en el **ANEXO I**, y considerando exclusivamente los elementos listados de aplicación a las áreas de prestación del servicio identificadas para cada lote, el cumplimiento de los requisitos funcionales deberá hacerse de acuerdo a las características técnicas y metodologías aceptadas en el ámbito particular de la defensa, mediante el uso de las herramientas listadas en el **ANEXO II**.

3.2.2 Metodología

En el desarrollo de las actividades a realizar por la empresa adjudicataria se seguirán las normas, estándares y metodología establecidos en el ámbito del Ministerio de Defensa, así como las instrucciones particulares dictadas por la Jefatura de Servicios Técnicos y Ciberdefensa, a su vez basadas en estándares de la industria y directrices de organismos como el Centro Criptológico Nacional. En el caso de no adaptarse a estas normas, podrían considerarse como no trabajadas las jornadas en que no se estuvieran cumpliendo las indicaciones recogidas por dichos organismos.

3.2.3 Calidad del servicio

El Ejército del Aire en general, así como el CIGES en particular, consideran la calidad y la seguridad factores clave en la implementación de servicios, por lo que se requiere el adecuado cumplimiento de los requisitos identificados, así como el firme compromiso con la mejora continua, para asegurar la eficacia de su Sistema de Gestión de la Calidad, la Seguridad y los Servicios (SGCS).

Para ello, el CIGES tiene establecida la siguiente política: *Asegurar la satisfacción de los Mandos, Unidades, Centros y Organismos (UCOs) del Ejercito del Aire, así como de sus Destacamentos en zona de operaciones, receptores de servicios de tecnologías de la información y la comunicaciones (STIC) proporcionados por el Centro, aplicando los métodos adecuados de actuación para cumplir los requisitos solicitados, los legales y reglamentarios, e implementando las medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información que manejen los Sistemas de Información y Telecomunicaciones*.

Asimismo, como compromiso con el producto desarrollado, este Centro acentuará los procesos necesarios para llevar a cabo la mejora en la disponibilidad, fiabilidad, funcionalidad, mantenibilidad, seguridad y usabilidad de las soluciones desarrolladas en el Centro.

Para hacer realidad esta política, se requiere la participación activa de todos y cada uno de los implicados en los trabajos a realizar. Por ello se requiere formación continua, tanto del propio personal como del personal facilitado por el contratista, así como unos medios técnicos adecuados, pues de otra forma esta política no puede ser entendida, implantada o mantenida a todos los niveles de la organización.

Como consecuencia, a nivel organizativo, el Sistema de Gestión hace uso de las mejores prácticas y de la normativa aplicable, para llegar a ofrecer el nivel de servicio demandado por los usuarios. En este sentido, el SGCS implantado por el CIGES, se ha orientado a los servicios TIC requeridos por las UCOs y contempla la totalidad de los procesos relacionados con el ciclo de vida de sus desarrollos, todo ello usando como referencia, entre otros, los siguientes estándares:

ISO 9001	Sistemas de Gestión de la Calidad (SGC)
ISO 20000	Gestión de servicios de Tecnologías de la Información (TI)
ISO 15504	Determinación de la capacidad de mejora del proceso de software.
ISO 27001	Certificación de los Sistemas de Gestión de Seguridad de la Información (SGSI)

Además, son de aplicación en el Centro los siguientes requisitos adicionales del ámbito OTAN incluidos en las Publicaciones Aliadas de Aseguramiento de la Calidad (AQAP), adaptadas al ámbito nacional por las Publicaciones Españolas de Calidad (PECAL) del Ministerio de Defensa:

PECAL/AQAP 2110	Requisitos OTAN de aseguramiento de la calidad para el diseño, desarrollo y la producción
PECAL/AQAP 2210	Requisitos OTAN de aseguramiento de la calidad del software, suplementarios a la PECAL 2110

Como resultado de la adecuada aplicación de esta normativa, el SGCS del CIGES ha sido auditado y certificado por la Dirección General de Armamento y Material del Ministerio de Defensa (DGAM), para el análisis, diseño, desarrollo, producción, distribución, operación y mantenimiento de software de gestión.

Por tanto, el adjudicatario del contrato debe saber que a los perfiles profesionales que presten la asistencia técnica objeto de este expediente se le exigirá:

(X) Haber sido formado previamente en el aseguramiento de la calidad, seguridad de la información y buenas prácticas para la mejora de los servicios TIC.

(X) Conocer plenamente la normativa mencionada en este apartado del PPT.

(X) Compartir y aceptar la política del CIGES.

(X) Haber sido formado previamente en el aseguramiento de la calidad, seguridad de la información y buenas prácticas para la mejora de los servicios TIC.

(X) Disponer de la experiencia y conocimientos técnicos para realizar su trabajo eficientemente, cumpliendo los objetivos del CIGES y los niveles de servicio que puedan acordarse (SLA).

Además, el Ejército del Aire y del Espacio está certificado en su totalidad en el ámbito de la gestión ambiental, conforme a los requisitos de la norma UNE-EN ISO 14001.

Por ello, se exigirá como garantía de adecuación a los estándares y buenas prácticas mencionados que la **empresa adjudicataria aporte**, por considerarse de aplicación al objeto del contrato:

(X) Documentación que acredite que el SGC de la empresa está certificado según norma ISO 9001 e ISO 20000 con un alcance apropiado para la prestación de los servicios requeridos en el presente documento.

(_) Documentación que acredite que el SGSI de la empresa está certificado según norma ISO 15504 con un alcance apropiado para la prestación de los servicios requeridos en el presente documento.

(X) Documentación que acredite que el SGSI de la empresa está certificado según norma ISO 27001 con un alcance apropiado para la prestación de los servicios requeridos en el presente documento.

(X) Declaración expresa de la disposición del SGC de la empresa a colaborar con el SGCS del CIGES y de la aceptación de todas las especificaciones relativas a calidad contempladas en el presente documento.

(X) Declaración de aceptación de los términos recogidos en la PECAL 2110 acerca de los elementos a proporcionar para poder realizar las evaluaciones contempladas en dicha normativa.

(_) Declaración de aceptación de los términos recogidos en la PECAL 2210 acerca de los elementos a proporcionar para poder realizar las evaluaciones contempladas en dicha normativa.

(X) Documentación que acredite que el Sistema de Gestión Ambiental de la empresa está certificado según norma ISO 14001 con un alcance apropiado para la prestación de los servicios requeridos en el presente documento.

3.2.4 Coordinación del servicio

El adjudicatario, de común acuerdo con el responsable del contrato, designará a una persona del equipo de asistencia técnica como coordinador del servicio que deberá:

- Actuar como interlocutor entre el adjudicatario y el CIGES.
- Realizar el control y seguimiento de las actividades realizadas por el equipo de asistencia técnica y del cumplimiento de los requisitos de este PPT, aportando toda la documentación que se le pueda requerir.
- Coordinar y controlar los horarios de entrada y salida, las jornadas laborales realizadas y pendientes, las incorporaciones del personal, las sustituciones, las penalizaciones, las jornadas de vacaciones, los permisos, bajas por enfermedad, etc.
- Elaborar un informe mensual de seguimiento del contrato que incluya como mínimo la información de las tareas y tiempos invertidos que personal de asistencia técnica ha desempeñado.
- Resolver las incidencias y peticiones de cambios que puedan producirse relacionadas con el servicio con la aprobación previa del director técnico del contrato.

El coste de estas tareas de coordinación será **por cuenta del adjudicatario**, sin ningún cargo para el Ministerio de Defensa.

3.2.5 Datos de carácter personal

Las tareas de asistencia técnica objeto de este contrato no conllevan, necesariamente en sí mismas, el tratamiento posterior ni simultáneo de datos de carácter personal. Pero, por la naturaleza de los servicios de asistencia técnica a contratar, es posible que se acceda a datos de carácter personal.

Aunque estos servicios no se encuadren exactamente en la figura de "encargado del tratamiento" establecido en el artículo 33 de la Ley Orgánica 3/2018, el adjudicatario declara conocer la legislación vigente en materia de protección de datos, y que el personal que preste la asistencia técnica ha sido instruido en esta materia.

Por lo tanto, en caso de tener lugar este acceso, como consecuencia de los servicios a prestar, se compromete a observar los requisitos establecidos en esta legislación conforme a las instrucciones del responsable de los datos de carácter personal (responsable de fichero) a los que pudiera acceder, y que no aplicará o utilizará dichos datos con fin distinto al que figure en este acuerdo y contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

De igual forma, el CIGES se compromete a no difundir ni utilizar para otros fines que los de la ejecución de este contrato, cualquier dato de carácter personal del adjudicatario y del personal de la asistencia técnica.

3.2.6 Prevención de riesgos laborales

La empresa adjudicataria asumirá sus responsabilidades legales en materia de información, formación, medios, medidas y otras acciones preventivas en materia de prevención de riesgos laborales, respecto al personal de asistencia técnica contratado que realice sus cometidos en las instalaciones del CIGES.

- El CIGES, por su parte, tramitará a través de los responsables designados por la empresa adjudicataria la información en materia de PRL relativa a:
  - Los riesgos existentes en el centro de trabajo que afecten al personal contratado.
  - Información sobre las medidas de protección y prevención correspondientes que se aplican en las instalaciones del Centro.
  - Las actividades de formación ante emergencias que se aplican al personal externo que presta sus servicios habitualmente en las instalaciones del Centro.

- La información en materia de PRL que la empresa adjudicataria debe remitir al CIGES será la relativa a:
  - Los riesgos que por la actividad de sus trabajadores contratados para prestar asistencia técnica en instalaciones del CIGES puedan afectar a los trabajadores del CIGES o de otras empresas.
  - Los riesgos que pueden sufrir sus trabajadores por su labor desarrollada en las instalaciones del CIGES.
  - La formación en materia PRL por parte de la empresa respecto a sus trabajadores contratados para prestar asistencia técnica en instalaciones del CIGES.
  - Las medidas adoptadas y los medios empleados por la empresa para prevenir riesgos laborales durante el desarrollo de las labores de sus trabajadores en instalaciones del CIGES.

4. REQUISITOS DE LOS PERFILES PROFESIONALES

Los requisitos expuestos a continuación responden a los siguientes criterios:

- Establecen una relación entre las habilidades requeridas y la formación necesaria para adquirirlas.
- Son adecuados al nivel de complejidad que se exigirá en las tareas a desarrollar.
- Son coherentes con la definición del Grupo/Clase correspondiente en el convenio colectivo en uso.

4.1 REQUISITOS PROFESIONALES PERFIL PPR1

Perfil			
Técnico de redes			
ID. Req	**Requisito**	**Descripción**	**Carácter**
RP101	Titulación	Título de Técnico superior [i] (nivel MECES 1) [ii] de aplicación al objeto del contrato.	Obligatorio
RP102	Certificado [vii]	CISCO CCNA [iii].	Obligatorio
RP103	Experiencia	3 años de experiencia acreditada en configuraciones en electrónica de redes [iv].	Obligatorio
RP104	Acreditación	Habilitación Personal de Seguridad (HPS) “RESERVADO NACIONAL” + “NATO SECRET” + “EU SECRET” [v].	Obligatorio
RP105	Características	(Ver apartado Mejoras/Variantes para el perfil) [vi].	Deseables

[i)] Se consideran en esta categoría, por la naturaleza del contrato, las siguientes titulaciones u otras equivalentes, oficiales u homologadas por el Ministerio de Educación, Formación Profesional y Deportes:
- Técnico Superior en Sistemas de Telecomunicaciones e Informáticos.
- Técnico Superior en Administración de Sistemas Informáticos en Red.

[ii)] En caso de no presentarse una titulación de dicho nivel, pero sí disponer de una de las titulaciones indicadas en el apartado de Mejoras/Variantes para el perfil, se tendrá por satisfecho este requisito, además de considerarse como elemento evaluable.

[iii)] Credencial específica del sector, obtenida a través del fabricante (CISCO) a quienes superan la evaluación sobre el contenido de todos los módulos del curso denominado “CISCO CCNA”. De esta forma se acredita que se ha adquirido la capacitación esperada sobre distintos aspectos de redes informáticas, tales como arquitectura, diseño, modelo, protocolos, elementos, seguridad, switching y routing.

[iv)] Se requiere esta experiencia mínima para garantizar la adaptación del perfil a las condiciones particulares del centro, de forma que pueda desarrollar sus actividades con la autonomía que se define en el grupo y área o categoría correspondiente al presupuesto asignado para gastos de personal. Además, responde al entorno tecnológico donde conviven dispositivos de vanguardia con elementos en su ciclo de vida extendido que es necesario dominar para poder mantener o sustituir.

[v)] De acuerdo a las características establecido en el **apartado 5.8**. **Este requisito debe considerarse obligación esencial del contrato a los efectos previstos en el artículo 211.1f) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.**

[vi)] Otros requisitos deseables en el perfil se han definido como elementos evaluables mediante fórmulas- Estos requisitos incluyen un nivel superior de experiencia y formación. Con ello se busca incrementar el valor añadido del perfil propuesto, por permitirle realizar las tareas de forma más autónoma y eficiente, de acuerdo a las tecnologías en uso y la entidad de los proyectos.

[vii)] El certificado/certificación no tiene equivalente, pues debe garantizar conocimientos en tecnologías concretas pertenecientes al catálogo de productos autorizados para su uso en este Centro.

5. ASPECTOS ADICIONALES PARA LA PRESTACIÓN DEL SERVICIO

5.1 LUGAR DE PRESTACIÓN DE LOS SERVICIOS

Por norma general, la prestación de los servicios se efectuará en la sede de la Administración. No obstante, para llevar a cabo tareas relacionadas con la recogida de requisitos, implantación y puesta en marcha u otras similares, donde resulte más conveniente para la correcta ejecución de los trabajos, se podrán requerir puntualmente desplazamientos dentro de territorio nacional, con el alcance definido en el **apartado 5.2**. Adicionalmente, se valorará la capacidad para realizar estas mismas actividades a nivel internacional, conforme a los criterios de valoración definidos en el PCAP y cuyos costes asociados no superarán el 10% del presupuesto de licitación de cada lote, debiendo en estos casos aportar los documentos necesarios que lo acrediten.

En consideración del entorno técnico definido en el **ANEXO I**, cabe destacar que la prestación del servicio podrá desarrollarse en régimen de teletrabajo sólo con carácter excepcional siempre y cuando el marco tecnológico, las condiciones de seguridad y otras circunstancias oportunas así lo aconsejen y lo permitan.

5.2 OTROS LUGARES HABITUALES DE PRESTACIÓN DEL SERVICIO

De acuerdo a los servicios prestado por el CIGES, a los proyectos actualmente en desarrollo y a los sistemas en producción que requieren de análisis, mantenimiento o instalación, en ocasiones es necesario llevar a cabo determinadas actividades en otros emplazamientos del Ejército del Aire, normalmente dentro de la Comunidad de Madrid, siendo el más habitual, aunque no el único, la Base Aérea de Torrejón. Cualquier oferta presentada deberá tener en cuenta esta circunstancia. La variación eventual del lugar de prestación de servicio no conllevará la variación del cómputo total de las jornadas laborales imputables al contrato, en tanto el servicio se ajustará, en la medida de lo posible, al horario habitual del servicio.

5.3 MEDIOS MATERIALES

Todos los medios materiales necesarios para la correcta prestación del servicio, correrán **a cargo del adjudicatario,** sin coste alguno para el Ministerio de Defensa, y se ajustarán al listado de “Herramientas de uso general” incluido en el **ANEXO II**.

Justificación reforzada:

Las previsiones de medios informáticos y licencias en el Ministerio de Defensa se hacen en base a la plantilla existente. La incorporación de personal de asistencia técnica aumenta dichas necesidades, y en tanto la adquisición de medios y licencias no es inmediata, para garantizar la adecuada incorporación de nuevo personal es necesario que los recursos anteriormente listados se pongan a disposición del personal desde el inicio del contrato.

El coste y naturaleza asociados a los medios solicitados se considera razonable y proporcional, por ser herramientas relacionadas con el habitual cometido de las empresas que puedan competir por la presente licitación y no ser específicas para este contrato.

Excepciones:

No obstante, cuando a criterio del CIGES la prestación del servicio lo requiera, el personal que preste la asistencia técnica deberá utilizar los medios materiales facilitados por el Ministerio de Defensa y cumplir estrictamente todas las normas de uso establecidas por este Ministerio.

5.4 HORARIO DE TRABAJO

Como norma general, la prestación del servicio se realizará en el horario de trabajo del CGEA (Madrid), y excepcionalmente en el horario de trabajo que en cada caso rija en el lugar del desplazamiento.

El personal del contratista se regirá por el calendario laboral de Madrid (Comunidad y Municipio), que es por el que se rige el emplazamiento establecido como lugar de trabajo. A efectos del contrato, los tiempos de desplazamiento de ida y vuelta al lugar de trabajo correrán a cargo del contratista y no se computarán a ningún efecto como concepto facturable. Tampoco podrán cargarse como servicios extraordinarios cuando, por razones operativas justificadas, se trabaje fuera del horario habitual.

5.5 COMPENSACIÓN POR PERÍODOS DE AUSENCIA DEL PERSONAL

Las horas generadas como consecuencia de los períodos de ausencia del personal que presta asistencia técnica generarán una bolsa de horas de las cuáles se podrá hacer uso cuando las circunstancias lo requieran a petición del responsable del contrato y en coordinación con la empresa adjudicataria.

La horas mencionadas serán destinadas a la ejecución de los trabajos definidos en el **apartado 3**, que podrán realizarse por personal adicional con la capacitación adecuada, según los perfiles establecidos en este documento y dependiendo de las necesidades del CIGES.

5.6 SUSTITUCIÓN DEL PERSONAL

La sustitución del personal que presta la asistencia técnica se realizará a petición del CIGES o del adjudicatario, solamente por razones justificadas o de fuerza mayor, debiendo comunicarse la petición entre las partes con al menos **15 días** naturales de antelación.

En casos de fuerza mayor (fallecimiento, incapacitación, rescisión del contrato laboral, etc.) la comunicación se realizará **inmediatamente**.

En todos los casos la sustitución requerirá:

- Propuesta del adjudicatario con los detalles que justifican la sustitución y la entrega de la documentación necesaria para verificar el cumplimiento de los requisitos mínimos exigidos en el PPT.
- La dedicación de un mínimo de **15 jornadas** laborales de adaptación por persona sustituta.

En todos los casos las jornadas de adaptación serán **por cuenta del adjudicatario**, sin coste alguno para el Ministerio de Defensa.

5.7 CUMPLIMIENTO DEL ESQUEMA NACIONAL DE SEGURIDAD

El presente contrato específico tiene por objeto la prestación de un servicio, que incluye entre sus funciones implementar la seguridad en sistemas y la supervisión de la operación diaria de los mismos.

En cumplimiento del artículo 13.5 del ENS, es obligación del adjudicatario designar una Persona de Contacto (POC) que canalice y supervise el cumplimiento de los anteriores requisitos y las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes de seguridad en el ámbito de dicho servicio de desarrollo. Dicha Persona de Contacto será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en el organismo destinatario de la prestación.

El organismo destinatario informará de sus deberes, obligaciones y responsabilidades en materia de seguridad en lo relativo al sistema de información al personal puesto a disposición del servicio por el adjudicatario, en cumplimiento del artículo 15 del ENS. Esta información se realizará una vez iniciada la ejecución del contrato. Es obligación del adjudicatario supervisar la actuación de dicho personal, para verificar que se siguen los procedimientos establecidos por el organismo, se aplican las normas indicadas y los procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

En aplicación del artículo 16 del ENS, se han determinado los requisitos de formación y experiencia del personal implicado en la ejecución del contrato que se han indicado en el **apartado 4**.

Medidas del Anexo II del RD 311/2022 que son de aplicación al presente contrato específico:

1. Sistemas de categoría BÁSICA:
   a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo. El organismo destinatario dispone de estos entornos y proporcionará las normas de uso, junto con el resto de información que proporcionará al inicio de la ejecución del contrato específico.

2. Sistemas de categoría MEDIA:
   a) Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

b) Se aplicará una metodología de desarrollo seguro reconocida que:
   i) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
   ii) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (overflow).
   iii) Tratará específicamente los datos usados en pruebas.
   iv) Permitirá la inspección del código fuente.

c) Se aplicará el principio de seguridad integral desde el diseño del sistema, especialmente:
   i) Los mecanismos de identificación y autenticación.
   ii) Los mecanismos de protección de la información tratada.
   iii) La generación y tratamiento de pistas de auditoría.

d) Las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales, el organismo destinatario impartirá las oportunas instrucciones para garantizar el nivel de seguridad correspondiente. Es obligación del adjudicatario asegurarse de que el personal asignado al servicio cumple dichas instrucciones.

Es obligación del adjudicatario elaborar y mantener actualizada una relación formal de los componentes software de terceros empleados en el sistema de información. El adjudicatario mantendrá un histórico de los componentes utilizados en las diferentes versiones del sistema durante todo el periodo de ejecución del contrato específico. El contenido mínimo de la lista de componentes contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, y en su caso, se adecuará a lo descrito en la correspondiente Guía CCN-STIC en su versión más actualizada.

5.8 HABILITACIONES DE SEGURIDAD

El lugar de prestación de los servicios se encuentra catalogado como Zona de Acceso Restringido (ZAR) Clase II y, además, para el correcto cumplimiento de los requisitos funcionales definidos, será imprescindible manejar información clasificada, de grado “RESERVADO NACIONAL” + “NATO SECRET” + “EU SECRET”. Por ello, las empresas contratistas necesitan disponer de una Habilitación de Seguridad de Empresa (HSEM) del grado adecuado o superior a la clasificación de dicha información, que las faculta para generar y acceder a información clasificada, sin que pueda manejarla o almacenarla en sus propias instalaciones.

Igualmente, los perfiles propuestos deben estar en posesión de una Habilitación Personal de Seguridad (HPS) igual o superior a los grados de la información anteriormente mencionada. No obstante, se aceptará que la HPS del perfil se encuentre en estado “En Trámite” en el momento del inicio del contrato, en tanto su obtención inicial requiere de un periodo que de otra forma limitaría la competencia y la disponibilidad de perfiles. Este punto no eximirá a la empresa de tener la HSEM en vigor en el momento de presentar la oferta. La denegación, revocación o no consecución de la HPS durante el periodo de ejecución del contrato conllevará la sustitución del perfil que preste el servicio.

Se significa que el nivel de clasificación de los sistemas, y de la información que en ellos hay contenida, se considera de un nivel superior a cualquiera de los definidos en el ENS, por lo que, aunque los sistemas no se encuentran categorizados dentro de dicho Esquema, se contemplan las medidas más restrictivas en él recogidas, además de las medidas adicionales adecuadas para el nivel de clasificación específico del sistema donde se realicen las actividades. Estas medidas incluyen, entre otras, el uso de cifrado de datos y transmisiones, controles avanzados de acceso lógico y físico o manipulación de elementos del sistema para reducir su superficie expuesta a amenazas.

La pérdida de la habilitación personal de seguridad por parte del personal prestatario de los servicios de asistencia técnica durante la ejecución del presente contrato, bien sea por revocación o denegación de la renovación de la misma, requerirá la sustitución del mismo, en los términos y condiciones indicados en el **apartado 5.6**.

ANEXO I DESCRIPCIÓN DEL ENTORNO TÉCNICO Y FUNCIONAL EXISTENTE

I.1. DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN EXISTENTES

Los sistemas de información existentes son, en líneas generales, sistemas empleados para el manejo de información de uso oficial, o con un nivel de clasificación superior, a los que se accede tanto desde territorio nacional como desde destacamentos en el extranjero, y que pueden ser de carácter fijo o desplegable.

I.1.1. Área de redes. Descripción de los sistemas existentes

La composición de los sistemas del área de redes incluirá, por lo general, uno o varios de los siguientes elementos:

- Líneas de Comunicaciones: Circuitos de datos que permiten el intercambio de información.
- Electrónica de Red: Infraestructura que permite la interconexión de equipos y periféricos.
- Tecnologías WLAN: LAN inalámbricas empleadas en la conexión de cualquier tipo de dispositivo y/o clientes de red.
- Telefonía IP: Equipamiento para permitir el uso de telefonía por datos.
- Sistemas de Videoconferencia IP: Servicio multimedia de interacción entre distintos grupos de trabajo.
- Dispositivos de protección de perímetro.: Permiten el control del tráfico de la red, aceptación/denegación del tráfico en base a unas políticas o reglas de acceso.
- Plataforma SIEM: Para la administración de eventos y obtención de información de seguridad.
- Otros dispositivos de comunicaciones: Configuración e instalación de routers.

Además, se requiere el empleo de herramientas que permiten las siguientes tareas:

- Gestión y monitorización de redes LAN: Administración de redes sobre rutas de recursos.
- Implementación de protocolos de Securización: Conjunto de reglas y protocolos de comunicación para configuraciones seguras a través de la red.
- Control de acceso en redes LAN: Contemplará los equipos y el conjunto de protocolos para definir como asegurar los nodos de la red antes del acceso a ella.
- Análisis de integridad, vulnerabilidades y riesgos: Modelo de relación entre la amenaza y la vulnerabilidad de los elementos expuestos.
- Aplicación de plantillas de seguridad: Uso de guías STIC del CCN para securización de redes.

I.1.2. Área de sistemas. Descripción de los sistemas existentes

La composición de los sistemas del área de sistemas incluirá, por lo general, uno o varios de los siguientes elementos:

- Servidores: Sistemas diseñado para proveer servicios y recursos a otras computadoras o dispositivos en una red.
- Estaciones o clientes de trabajo: Dispositivos que permiten a los usuarios el uso de las herramientas instaladas e interactuar con sistemas informáticos centralizados o remotos.
- Elementos de seguridad: Aquellos dispositivos o herramientas que permitan disminuir la vulnerabilidad de los equipos. Pueden ser elementos lógicos (herramientas software) o elementos físicos.
- Equipos virtualizados: Aquellos servidores o estaciones de trabajo que existen de forma lógica sobre unos mismos recursos físicos (memoria, capacidad de procesado, almacenamiento, etc.), permitiendo así su máximo aprovechamiento y facilitando su escalabilidad

Además, se requiere el empleo de herramientas que permiten las siguientes tareas:

- Gestión y monitorización de sistemas: Administración de los sistemas en producción y control sobre el estado de los mismos.
- Implementación de protocolos de Securización: Conjunto de reglas que, aplicadas a los sistemas, aumentan su protección frente a amenazas.
- Control de acceso: Contemplará las medidas a implementar para controlar los usuarios que pueden acceder a los sistemas, así como el registro de las actividades que se realicen por dichos usuarios.
- Análisis de integridad, vulnerabilidades y riesgos: Modelo de relación entre la amenaza y la vulnerabilidad de los elementos expuestos.
- Aplicación de plantillas de seguridad: Uso de guías STIC del CCN para securización de sistemas.

I.2. DESCRIPCIÓN DEL ENTORNO TECNOLÓGICO

El entorno tecnológico en el que se desarrollarán las actividades se encuentra, por norma general, aislado, de forma que ofrece servicio a usuarios internos, no siendo posible, en la mayoría de los casos, su conexión a redes externas o a internet.

El equipamiento en uso puede ser tanto de uso comercial como de uso exclusivo en el ámbito de la defensa.

Por ambos motivos se considera importante que el perfil propuesto disponga de amplios conocimientos técnicos previos y alta capacidad de aprendizaje y adaptación.

ANEXO II HERRAMIENTAS EN USO

Para llevar a cabo las tareas dentro de cada área de prestación del servicio existente en el Centro, existe en la actualidad una serie de herramientas autorizadas, no estando garantizado el uso de alternativas distintas a las expuestas, de acuerdo a requisitos de seguridad o limitaciones de licenciamiento o adquisición.

II.1. HERRAMIENTAS DE USO GENERAL

- Equipo con Sistema Operativo Windows.
- Clientes con navegador Firefox o Microsoft Edge.
- Clientes con Microsoft Office, LibreOffice y Adobe Reader.

II.2. ÁREA DE SOPORTE A USUARIOS. HERRAMIENTAS ESPECÍFICAS

- Herramienta de ticketing SCANS.
- Herramienta de gestión de proyectos Jira.

II.3. ÁREA DE REDES. HERRAMIENTAS ESPECÍFICAS

- Líneas de comunicaciones: HDLC, PPP y E1. Empleo de QoS, protocolos de routing y enlace satélite.
- Electrónica de Red: Extreme Networks en un 90 %, Cisco y Huawei.
- Dispositivos de comunicaciones: Routers Cisco y Huawei.
- IPSEC: VPNs.
- Tecnologías WLAN: HP y Ubiquiti.
- Gestión y monitorización de redes LAN (SNMPv3). Extreme Networks Management Center.
- Telefonía IP: CISCO y Asterisk.
- Sistemas de Videoconferencia IP (Polycom).
- Dispositivos de protección de perímetro: Palo Alto, Cisco ASA/Firepower, Checkpoint y Fortinet.
- Análisis de integridad, vulnerabilidades y riesgos.
- Plataforma SIEM: AlienVault OSSIM.
- Controles de acceso en redes LAN. Extreme Networks NAC.

II.4. ÁREA DE SISTEMAS. HERRAMIENTAS ESPECÍFICAS

- Servidores: Windows Server y Linux
- Bases de datos: Oracle y SQL Server
- Servicios de virtualización: VMWare
- Herramientas de ciberseguridad: CLARA, CLAUDIA, Tenable NESSUS
- Herramientas de gestión TI (ITSM): ProactivaNET
- Base de datos relacionales: Oracle
- Servidores web Apache
- Servidores de aplicaciones Oracle Weblogic y Apache Tomcat