



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Particularidades de la Obtención de Recursos TIC a través de la
Contratación Pública en el Ámbito del Ministerio de Defensa*

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Víctor Manuel Grande Corral

DIRECTORES: Fernando Suárez Lorenzo

Francisco Javier Rodríguez Rodríguez

CURSO ACADÉMICO: 2024-2025

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

*Particularidades de la Obtención de Recursos TIC a través de la
Contratación Pública en el Ámbito del Ministerio de Defensa*

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universida_{de}Vigo

RESUMEN

La intención de este trabajo es la de proporcionar una visión de las vicisitudes que determinan y condicionan la obtención de recursos en el ámbito de las tecnologías de la información y las comunicaciones a través de la Contratación Pública en el Ministerio de Defensa.

La propia naturaleza del Ministerio y su singularidad respecto a otras administraciones públicas dificultan o facilitan, según las circunstancias, el proceso de obtención de esos recursos que también tendrán un tratamiento diferente según el tipo de contratación del que se trate.

La singularidad mencionada se vio recogida en un marco legal principal: la Ley 24/2011 del 1 de agosto, de Contratos del Sector Público en los Ámbitos de la Defensa y la Seguridad que dotó de una regulación específica a los contratos que se celebraran en este ámbito.

La norma fundamentó su génesis en dos principios fundamentales que declara la ley en su preámbulo y que en realidad son tres: por una parte, el reconocimiento de la necesidad de salvaguardar la seguridad de la información; por otro lado, se declaraba necesario asegurar la continuidad el suministro de los recursos a lo largo del tiempo, finalmente se concretaba la necesidad de disponer de una regulación específica por la necesidad de disponer de unos procedimientos de contratación más flexibles.

Merecen especial atención, por la especial naturaleza de los recursos que se quiere adquirir, aquellos contratos dirigidos a la obtención de recursos TIC y que son objeto de estudio en este trabajo. La gestión optimizada de los procesos dirigidos a esa obtención, se evidencia capital para atender las necesidades de los organismos dependientes del Ministerio de Defensa.

Se analiza en profundidad un caso de uso de obtención de recursos de ciberdefensa en el ámbito del Ministerio de Defensa por la importancia de este proyecto en relación con las TIC y se analiza también, a este respecto, el uso que se puede hacer de la compra pública de innovación para estimular la innovación y el desarrollo tecnológico en las Fuerzas Armadas.

Se aporta, finalmente, a través del análisis de las empresas participantes en los concursos públicos y de su participación en un cuestionario sobre su visión de la contratación pública de recursos TIC, el punto de vista de la empresa en la cuestión.

PALABRAS CLAVE

1. Contratación Pública
2. TIC (Tecnologías de la Información y Comunicaciones)
3. Ministerio de Defensa (MINISDEF)
4. Ciberseguridad
5. Transformación Digital
6. Modernización Tecnológica
7. Acuerdos Marco
8. Normativa de Contratación Pública
9. Infraestructura Integral de Información para la Defensa (I3D)
10. Plan de Recuperación, Transformación y Resiliencia
11. Eficiencia Energética
12. Sostenibilidad
13. Interoperabilidad
14. Gestión de Contratos
15. Seguridad Nacional
16. Pliegos de Prescripciones Técnicas (PPT)
17. Innovación Tecnológica
18. Evaluación y Seguimiento de Contratos
19. Competencia en el Sector Público
20. Plataformas Electrónicas de Contratación
21. Compra pública de innovación

CONTENIDO

Contenido	1
Índice de Figuras	3
Índice de Tablas.....	4
1 Introducción y objetivos	5
1.1 Contextualización.....	5
1.2 Justificación	6
1.3 Objetivos	6
1.4 Organización del Documento.....	7
2 Estado Del Arte	8
2.1 Marco Normativo en la Contratación Pública del Ministerio de Defensa.	8
2.6 Comparativa Internacional en la Contratación Pública de TIC en Defensa.....	11
2.7 Evolución Histórica Contratación TIC en el Ministerio de Defensa (MINISDEF).....	15
3 Metodologías y Procesos de Contratación	17
3.1 Metodologías en la Contratación Pública de TIC	17
3.1.1 Contratación Centralizada y Acuerdos Marco:.....	17
3.1.2 Procedimiento Abierto Simplificado:	18
3.1.3 Procedimiento Negociado sin Publicidad:.....	19
3.2 Uso de Herramientas Digitales y de Licitación Electrónica:	19
3.3 Procesos Clave en la Contratación de TIC en Defensa.....	21
3.4 Retos y Mejores Prácticas en los Procesos de Contratación de TIC.....	24
3.4.1 Desafíos en la Contratación TIC en Defensa:.....	25
3.4.2 Mejores Prácticas:.....	25
4 Análisis del Presupuesto TIC Minisdef	26
4.1 Clasificación de la licitación según el objeto de los contratos.....	26
4.2 Clasificación por Programas (para qué gastamos)	27
4.3 Clasificación Económica (en qué gastamos)	28
4.4 Evolución del Presupuesto TIC en el Ministerio de Defensa	31
4.4.1 Crecimiento Anual del Presupuesto TIC:	32
4.4.2 Distribución Plurianual del Presupuesto TIC:	32
4.4.3 Distribución del Presupuesto TIC por Áreas de Inversión	33
4.4.4 Principales Programas y Proyectos Financiados con el Presupuesto TIC	35
4.5 Impacto del Presupuesto en la Transformación Digital y la Eficiencia Operativa	37

4.4 Sostenibilidad y Eficiencia Energética en el Presupuesto TIC	37
4.5 Ciberseguridad: Priorización en el Presupuesto y Desafíos.....	38
4.6 Conclusión del Análisis Crítico del Presupuesto TIC.....	39
5 Estudio de Casos y Validación de Procesos	40
5.1 Estudio de Caso: Infraestructura de Ciberseguridad MINISDEF	40
5.1.1 Análisis de las empresas presentadas al concurso.	42
5.1.2 Adjudicación del contrato.....	43
5.1.3 Requisitos principales para la participación	44
5.1.4 Clasificación de Seguridad para el Acuerdo Marco.	46
5.1.5 Objetivos perseguidos y previsiones de cumplimiento.	46
5.1.6 Propuesta de Key Performance Indicators (KPIs)para este acuerdo marco	48
5.3 Mecanismos de Validación y Control en los Procesos de Contratación de TIC.....	49
5.4 Resultados y Recomendaciones	51
6 Implementación de la compra pública de innovación en contratos del minisdef.....	52
6.1 Introducción	52
6.2 Características principales.....	52
6.3 La CPI en el Ministerio de Defensa	53
6.4 Propuesta de explotación de la CPI y visión de futuro	54
7 Análisis de la visión de la empresa.....	57
7.1 Introducción.	57
7.2 Beneficios que les supone participar en contrataciones del ámbito de la defensa.	57
7.3 Desafíos identificados en el proceso de contratación para las empresas	58
7.4 Perspectiva sobre Innovación y Estrategias	59
7.5 Recomendaciones basadas en las respuestas	59
7.6 Análisis de la tipología de empresas que participan en licitaciones del MINISDEF	60
8 Resultados – Análisis Crítico	64
9 Bibliografía.....	68
Anexo I (glosario de términos)	69
Anexo II (Cuestionario empresas)	72
Anexo III (CSA)	77
Anexo IV (COMPUSOF)	82
Anexo V (INETUM).....	87
Anexo VI AM Contrato Ciberseguridad I3D	92

ÍNDICE DE FIGURAS

Ilustración 1.- Adquisición recursos TIC	5
Ilustración 2.- Evolución histórica contratación TIC.-	16
Ilustración 3.- web https://contratacioncentralizada.gob.es/	18
Ilustración 4.- https://contrataciondelestado.es/wps/portal/plataforma	20
Ilustración 5.- Web face https://face.gob.es/es/login	21
Ilustración 6.- Diagrama procesos clave contratación TIC	24
Ilustración 7.- fuente memoria de contratación 2023 del Ministerio de Defensa	26
Ilustración 8.- Distribución presupuesto programas (Estadística A. Económicos 2022)	27
Ilustración 9.- Capítulo 2 Presupuesto gasto MINISDEF 2022	29
Ilustración 10.- Capítulo 6 Presupuesto gastos MINISDEF 2023.....	30
Ilustración 11.- Fuente Memoria Contratación año 2023.....	30
Ilustración 12.- Grafico elaboración propia fuente P.G.E. 2024	31
Ilustración 13.- Fuente Memoria Contratación 2023 Ministerio de Defensa	31
Ilustración 14.- Gráfico elaboración propia. Fuente P.G.E.	32
Ilustración 15.- Gráfico elaboración propia. Datos PGE 2023.....	35
Ilustración 16.- Peligrosidad incidentes CIBER 2021 CCN-CERT	47
Ilustración 17.- Clasificación de los incidentes CCN-CERT en 2021	47
Ilustración 18.- Elaboración propia empleando I.A.	56
Ilustración 19.- Elaboración propia con los datos del acuerdo marco.....	61

ÍNDICE DE TABLAS

Tabla 1.- Comparativa internacional contratación TIC.....14

Tabla 2.- Tabla elaboración propia (Fuente: Presupuestos Generales del Estado)28

Tabla 3.- Definición de lotes A.M. Servicio de Ciberseguridad I3D41

Tabla 4.- .- Elaboración propia (Fuente: Acta órgano de asistencia)42

Tabla 5.- Elaboración propia (Fuente: actas órganos de asistencia)43

Tabla 6.- Elaboración propia (Fuente: PCAP)43

Tabla 7.- Elaboración propia (Fuente: documentación de adjudicación).....44

Tabla 8.- Elaboración Propia (Fuente: cláusula 18 PCAP)45

Tabla 9.- Empresas presentadas al Acuerdo Marco y nacionalidad60

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contextualización

En los últimos años, la integración y desarrollo de las tecnologías de la información y comunicación (TIC) ha transformado de manera significativa el funcionamiento de instituciones públicas, en especial en áreas sensibles como la defensa. Para el Ministerio de Defensa de España (MINISDEF), el uso de las TIC representa una herramienta crítica para modernizar las infraestructuras de seguridad, mejorar la eficiencia y responder de manera rápida a las necesidades operativas y estratégicas en un entorno global cambiante. Sin embargo, la adquisición de recursos TIC en el ámbito de la defensa no solo depende de la capacidad tecnológica, sino que también debe cumplir con estrictas normas de seguridad, confidencialidad y continuidad operativa.

La Ley 9/2017 de Contratos del Sector Público establece el marco normativo general para la contratación pública en España, con el objetivo de asegurar que el gasto público sea eficiente, transparente y esté en sintonía con las políticas de la Unión Europea. En el ámbito de la defensa, la Ley 24/2011 de Contratos del Sector Público en los ámbitos de Defensa y Seguridad añade requisitos específicos para garantizar la protección de información sensible y la seguridad del suministro en contratos relacionados con la defensa.



Ilustración 1.- Adquisición recursos TIC

1.2 Justificación

Este trabajo de investigación trata de analizar las particularidades del proceso de adquisición de TIC mediante contratación pública en el MINISDEF.

La evolución de los entornos digitales en el sector defensa es constante y las estructuras de contratación pública en las TIC deben adaptarse para asegurar tanto la protección de la información crítica como el correcto funcionamiento de la infraestructura tecnológica en defensa. Este trabajo fin de máster (TFM) pretende poner el foco en la importancia de optimizar la contratación de servicios y productos TIC a través de las herramientas disponibles para ello en el sector público, de acuerdo con los principales tipos de contratos: Obras, Suministros y Servicios, y atendiendo a sus particularidades específicas. Se trata de materias tan dispares como la obtención de redes de comunicación, plataformas de software y sistemas de ciberseguridad, contratos de servicios de especializados en TIC o cualquier tipo de infraestructura relacionada, entre otras.

Los desafíos que enfrentan estos procesos son numerosos. Por ejemplo: el MINISDEF debe equilibrar la seguridad nacional con la eficacia y transparencia en el gasto público. Además, la transformación digital en defensa requiere de una alta interoperabilidad y una actualización continua de tecnologías para mantener el nivel de preparación y respuesta. Ante esta necesidad, la investigación en contratación pública y TIC en defensa es una herramienta fundamental para identificar áreas de mejora, racionalizar recursos, y cumplir con los requisitos de seguridad de una manera rentable y sostenible.

1.3 Objetivos

Este TFM tratará de dar una visión de las políticas y prácticas actuales en contratación pública de TIC en el MINISDEF. Se pretende no solo evaluar la normativa vigente, sino también examinar los procesos internos de contratación y su adaptación a las necesidades específicas del sector defensa. A continuación, se detallan los objetivos específicos:

- Evaluar la normativa aplicable en la contratación de TIC en el MINISDEF, incluyendo las leyes y políticas internas, y su alineación con los requisitos de seguridad nacional y eficiencia.
- Examinar los procedimientos de contratación TIC en el MINISDEF, desglosando las fases y prácticas operativas, y analizando su efectividad en el contexto de la defensa.
- Analizar el impacto de las políticas TIC en defensa en términos de seguridad, interoperabilidad y sostenibilidad, determinando cómo contribuyen estas políticas al cumplimiento de los objetivos estratégicos del MINISDEF.

- Proponer recomendaciones para la optimización de los procedimientos de contratación pública en TIC, enfocadas en mejorar la transparencia, reducir los tiempos de adquisición y fomentar la innovación en el sector de defensa.

1.4 Organización del Documento

El trabajo se estructura en diversos capítulos que analizan de la manera más integral posible los aspectos de la contratación pública de TIC en defensa:

- **Capítulo 1 – Introducción y Objetivos.** Se contextualiza y justifica el trabajo, estableciendo los objetivos que se persiguen en él.
- **Capítulo 2 – Estado del arte.** Se analiza la normativa relevante, incluyendo las leyes de contratación y políticas internas del MINISDEF.
- **Capítulo 3 - Metodologías y Procesos de Contratación:** Describe las metodologías utilizadas y los procesos clave en la contratación pública de TIC.
- **Capítulo 4 - Análisis del Presupuesto TIC en el Ministerio de Defensa:** Examina la distribución y evolución del presupuesto destinado a TIC en defensa.
- **Capítulo 5 - Estudio de Caso y Validación de Procesos:** Incluye estudios de casos específicos y mecanismos de validación de los procedimientos.
- **Capítulo 6.- Implementación de la Compra Pública de Innovación en Contratos del Ministerio de Defensa.** Se estudia el uso de esta figura para obtener recursos TIC para que suponga un motor de innovación, colaboración público privada y fomento de la industria.
- **Capítulo 6.- Visión de las empresas Contratación TIC en el Ministerio de Defensa.** En base a un formulario de preguntas propuesto a tres empresas, se analiza su visión sobre la cuestión en virtud a las respuestas dadas.
- **Capítulo 7 - Resultados: Análisis Crítico:** Evalúa los resultados obtenidos y ofrece un análisis crítico de la normativa y procesos en contratación TIC.
- **Capítulo 8 – Oportunidades de Mejora en los Procesos de Contratación:** Resume los hallazgos principales y propone recomendaciones para mejorar la contratación TIC en el MINISDEF.

2 ESTADO DEL ARTE

El marco normativo y las políticas aplicables a la contratación pública en el ámbito del MINISDEF establecen las bases para adquirir y gestionar los recursos de tecnologías de la información y comunicaciones de manera segura y eficiente. La normativa específica de contratación pública en España regula la transparencia, eficiencia y seguridad en la contratación de TIC en defensa.

Este capítulo describe los pilares legales y de políticas internas que guían los procesos de adquisición en TIC, poniendo especial atención a la legislación aplicable y las políticas internas de gestión y transformación digital en el MINISDEF.

Se incluye también una **comparativa internacional** y una **revisión histórica de la evolución de la contratación TIC en el MINISDEF**. Esta ampliación permite contextualizar los procesos de contratación en defensa dentro de una perspectiva más amplia y dinámica, reflejando tanto las prácticas globales como los cambios en las políticas nacionales.

2.1 Marco Normativo en la Contratación Pública del Ministerio de Defensa.

En el ámbito del MINISDEF, la contratación pública referida a las TIC está regulada por una serie de leyes y normativas específicas que permiten la adaptación de los procedimientos a las necesidades de seguridad y defensa nacional, se destacan a continuación las principales:

- **Ley 9/2017 de Contratos del Sector Público (LCSP):** La **Ley 9/2017** establece los principios de transparencia, competencia, y eficiencia en la contratación pública. Este marco legal general obliga a los órganos de contratación a realizar un uso racional de los recursos y aplicar procedimientos que favorezcan la eficiencia en el gasto público. En el ámbito TIC, la ley permite también **procedimientos de contratación basados en acuerdos marco**, facilitando la centralización de la contratación y la homogeneización de los servicios tecnológicos adquiridos.
- **Ley 24/2011 de Contratos del Sector Público en los ámbitos de Seguridad y Defensa:** Enfocada específicamente en la contratación pública de Defensa y Seguridad, la **Ley 24/2011** adapta la LCSP para responder a las necesidades de confidencialidad, seguridad de suministro y flexibilidad en los contratos de defensa. Esta ley introduce la posibilidad de emplear el **procedimiento negociado** sin publicidad en casos que justifiquen la confidencialidad o los intereses de seguridad, lo que es especialmente relevante en la adquisición de sistemas TIC sensibles.

- **Guía de Contratación Basada en Acuerdos Marco (MINISDEF):** La Guía elaborada por la Subdirección General de Contratación proporciona criterios prácticos para la tramitación de expedientes de contratación en el MINISDEF. Promueve la **racionalización y centralización de la contratación** mediante acuerdos marco, especialmente útil para TIC, dado que permite unificar especificaciones y reducir costes de adquisición. Esta guía es esencial para asegurar que los contratos respeten la normativa, pero también ofrece flexibilidad para adaptarse a las particularidades de cada proyecto.

Se ha hecho mención del principal marco regulatorio, a él se añade normativa de menor rango y de desarrollo como los reglamentos, que resultan fundamentales para concretar los aspectos relativos a la materia. Como se puede observar, la norma general de la contratación pública, Ley 9/2017 de contratos del sector público es muy posterior a la norma particular, Ley 24/2011 específica para los sectores de la defensa y la seguridad. Aspectos fundamentales recogidos en la primera limitan la aplicación de la segunda, que probablemente debería haber sido objeto de actualización para adaptarla a las nuevas circunstancias.

2.2 Marco Estratégico de Sistemas y Tecnologías de la Información y Comunicaciones

Las políticas del MINISDEF en materia de TIC son el resultado de un enfoque estratégico orientado a asegurar que la infraestructura tecnológica y los sistemas de información cumplan con las demandas de interoperabilidad, eficiencia, seguridad y coherencia en la gestión de los sistemas TIC, en este sentido, la normativa fundamental al respecto se detalla a continuación:

- **Orden DEF/2639/2015: Política de Sistemas y Tecnologías de la Información y las Comunicaciones (Política CIS/TIC):** La Orden DEF/2639/2015 establece los principios y directrices que regulan la **gestión de los sistemas TIC en el MINISDEF**. Destaca la creación de una **Infraestructura Integral de Información para la Defensa (I3D)**, orientada a la unificación y centralización de los servicios TIC. Los objetivos de esta política incluyen optimizar los recursos humanos, normalizar los sistemas TIC y garantizar la seguridad en los servicios tecnológicos del MINISDEF
- **Arquitectura Global de Sistemas y Tecnologías de la Información y Comunicaciones (AG CIS/TIC):** La AG CIS/TIC, establecida en la Instrucción 58/2016, es el marco de referencia para la estructuración y gestión de los sistemas TIC en el Ministerio de Defensa. Esta arquitectura proporciona los lineamientos técnicos para la implementación de sistemas interoperables, así

como la orientación en el uso eficiente del presupuesto y recursos en el ámbito TIC. La **AG CIS/TIC facilita el desarrollo de capacidades CIS/TIC** en las Fuerzas Armadas y asegura que los recursos contratados se alineen con las políticas y necesidades operativas.

2.3 Estrategia de Transformación Digital del MINISDEF

La transformación digital es una de las prioridades actuales en el MINISDEF, ya que busca integrar nuevas tecnologías que permitan modernizar y hacer más eficiente la gestión en el ámbito de Defensa.

- **Plan de Transformación Digital del MINISDEF:** Este plan se articula en torno a la mejora de las infraestructuras, la consolidación de servicios TIC, y el desarrollo de **estrategias de ciberseguridad**. El Plan de Transformación Digital destaca la importancia de **convergencia con la Estrategia TIC de la Administración General del Estado (AGE)** y la adecuación a los objetivos del Plan de Recuperación, Transformación y Resiliencia. Además, se enfoca en la digitalización de procesos, la modernización de infraestructuras y el ahorro energético.
- **Impacto del Plan en la Contratación Pública TIC:** La implementación de esta transformación digital implica una serie de desafíos en la contratación de recursos TIC, especialmente en términos de rapidez, adaptabilidad y flexibilidad de los contratos públicos. Para ello, se han desarrollado **programas de sostenimiento y modernización de las infraestructuras TIC**, con un enfoque especial en la seguridad y en la incorporación de tecnologías innovadoras que optimicen los servicios TIC del Ministerio.

2.4 Aspectos Estratégicos de la Contratación TIC en el Ministerio de Defensa

El concepto estratégico de la contratación en el MINISDEF establece un modelo que enfatiza la eficacia en la gestión de recursos, apoyado en políticas de contratación centralizada y técnicas de racionalización.

- **Modelo de Gestión de Compras en Defensa (Modelo DEFENSA):** El Modelo DEFENSA, aprobado mediante la Instrucción 42/2019, reorganiza la función de compras y establece un sistema orientado a la **eficiencia, transparencia y especialización del personal en contratación**. Este modelo impulsa la consolidación de procesos de contratación de TIC bajo un enfoque de mejora continua, asegurando que se cumplan tanto los objetivos operativos como presupuestarios del Ministerio.
- **Racionalización de Recursos y Centralización de Contratos:** La Subdirección General de Contratación del MINISDEF enfatiza la centralización de los contratos TIC a través de acuerdos

marco, facilitando la **gestión eficiente y homogénea de los recursos TIC**. Esta centralización también permite controlar mejor los costos y optimizar la asignación de presupuesto en proyectos de gran impacto en el sector TIC.

2.5 Retos y Oportunidades en la Contratación Pública de TIC en el MINISDEF

La contratación de TIC en Defensa enfrenta retos únicos, tanto por las particularidades de seguridad como por las demandas de interoperabilidad y rápida adaptación a cambios tecnológicos.

1. Desafíos en la Contratación de TIC:

- **Seguridad de la Información:** La contratación de sistemas TIC para la defensa requiere un enfoque riguroso en seguridad, garantizando la protección de datos y la confidencialidad de las operaciones.
- **Adaptación Tecnológica y Presupuesto:** La integración de nuevas tecnologías plantea desafíos financieros, pues es necesario optimizar la asignación de recursos sin afectar la operatividad de los sistemas TIC.

2. Oportunidades para la Mejora de Procesos:

- La implementación de **tecnologías emergentes** como la inteligencia artificial y el blockchain, dentro del marco de transformación digital, podría mejorar los procesos de contratación en el futuro y garantizar una mayor transparencia y seguridad en las adquisiciones.
- El empleo de la compra pública de innovación (CPI), cuyos aspectos principales se tratan más adelante, como medio para obtener soluciones que no existen en el mercado o en desarrollo a través de la colaboración público-privada.

2.6 Comparativa Internacional en la Contratación Pública de TIC en Defensa

La contratación pública de tecnologías de la información y comunicaciones (TIC) en el ámbito de la defensa varía considerablemente entre países, influida por la normativa propia, los recursos tecnológicos disponibles y las alianzas internacionales, como la OTAN. A continuación, se describe cómo algunos países abordan los procesos de contratación de TIC en defensa, lo cual proporciona una perspectiva valiosa para el análisis del modelo español y permite identificar buenas prácticas aplicables al MINISDEF.

- **Estados Unidos: Modelo de Contratación Flexible y Enfoque en la Innovación:**

En Estados Unidos, la contratación de TIC para la defensa está regida principalmente por el **Federal Acquisition Regulation (FAR)** y el **Defense Federal Acquisition Regulation Supplement (DFARS)**, que proporcionan un marco normativo amplio y flexible. Este enfoque permite que el Departamento de Defensa (DoD) adapte sus procesos de contratación para incorporar tecnologías emergentes rápidamente.

Además, el DoD ha implementado iniciativas como la **Other Transaction Authority (OTA)**, un proceso de contratación alternativa que facilita la colaboración con startups y empresas de tecnología innovadora. Este tipo de contratos permite probar y adoptar tecnologías avanzadas (como inteligencia artificial y ciberseguridad) sin las restricciones de los procesos tradicionales de contratación pública. Esta flexibilidad podría servir de ejemplo para el MINISDEF al considerar métodos alternativos de adquisición de tecnologías emergentes.

- **Reino Unido: Enfoque en la sostenibilidad y compromiso con la transparencia:**

En el Reino Unido, la contratación de TIC para el Ministerio de Defensa sigue el marco regulador de la **Public Contracts Regulations 2015**, complementado por directrices específicas para el sector defensa que están alineadas con los principios de transparencia, competencia y sostenibilidad. El **Ministerio de Defensa del Reino Unido (MOD)** emplea modelos de contratación que priorizan la transparencia y el compromiso con la sostenibilidad ambiental en la adquisición de tecnologías.

Un aspecto distintivo del Reino Unido es su enfoque en la sostenibilidad y la reducción de la huella de carbono en los proyectos de TIC. El MOD exige que los contratos incluyan disposiciones de eficiencia energética y sostenibilidad, aspecto que puede inspirar al MINISDEF a integrar objetivos de sostenibilidad en sus procesos de contratación .

- **Alemania: Contratación Rápida y Seguridad en Defensa Cibernética:**

En Alemania, el Ministerio de Defensa utiliza una combinación de procesos de contratación estructurados y procedimientos rápidos para la adquisición de sistemas TIC críticos. En el ámbito de defensa cibernética, Alemania ha desarrollado procesos especializados de contratación que permiten una respuesta rápida a amenazas cibernéticas, garantizando al mismo tiempo la interoperabilidad con sistemas de la Unión Europea y la OTAN.

Además, el **Bundeswehr Cyber and Information Space Command** ha implementado procedimientos específicos para evaluar la ciberseguridad en cada fase del proceso de contratación, incluyendo auditorías de seguridad en la cadena de suministro. Estos protocolos pueden servir de referencia para el MINISDEF al fortalecer las evaluaciones de ciberseguridad en sus propias adquisiciones TIC .

- **Francia: Enfoque centralizado y Colaboración Europea en Contratación de TIC:**

En Francia, la contratación pública de TIC para defensa está centralizada bajo la **Direction Générale de l'Armement (DGA)**, que actúa como el organismo responsable de gestionar las adquisiciones para el Ministerio de Defensa. Francia también participa activamente en iniciativas de contratación conjunta en el marco de la Unión Europea, aprovechando la colaboración para adquirir soluciones tecnológicas avanzadas que cumplan con los estándares de la UE y de la OTAN.

El enfoque centralizado y la colaboración europea facilitan a Francia obtener economías de escala, reduciendo costes y asegurando una interoperabilidad alineada con los estándares europeos. Esta experiencia de centralización y cooperación internacional podría aportar lecciones valiosas para el MINISDEF, especialmente en la contratación de sistemas TIC de uso compartido .

En general, los países han ido abriendo la competencia en aras de buscar la transparencia y abaratar los costes de la contratación sin comprometer la seguridad de la información para lo que se reservan el uso de procedimientos específicos al igual que España.

Por otro lado, es muy frecuente observar como algunos países prefieren establecer mecanismos para favorecer a los proveedores nacionales, especialmente cuando se trata de tecnologías que precisan esa reserva por su criticidad en cuanto a confidencialidad, continuación con la cadena de suministro o incluso fomento de la propia industria o independencia tecnológica.

En cuanto al análisis de los proveedores, relativo a sus evaluaciones de seguridad y capacidad, son análogos a los que se siguen en la contratación del Ministerio de Defensa español.

A continuación se plasma un esquema resumen comparativo de los aspectos más relevantes de los procedimientos de contratación en el ámbito de la defensa de países relevantes, incluyendo España, con expresión de sus características principales relativas a contratación pública TIC en defensa:

País	Agencias Clave	Proceso de Contratación	Elementos Únicos
España	Dirección General de Armamento y Material (DGAM), Ministerio de Defensa	- Regido por la <i>Ley de Contratos del Sector Público</i> y el <i>Real Decreto de Contratación en Defensa y Seguridad</i>. - Competencia en licitaciones, aunque pueden realizarse procedimientos negociados en proyectos estratégicos. - Transparencia y competencia como principios centrales.	- Alto control en seguridad y confidencialidad. - Fomento de la participación de empresas nacionales y de la UE.
EE. UU.	Departamento de Defensa (DoD), Agencia de Logística de Defensa (DLA)	- Basado en el <i>Federal Acquisition Regulation</i> (FAR). - Contratos de precio fijo, costo-reembolso, y otros adaptados. - Licitaciones competitivas con excepciones en seguridad nacional.	- Riguroso cumplimiento de revisiones de seguridad. - Contratos con proveedores nacionales en ciertas áreas.
Reino Unido	Ministerio de Defensa (MoD)	- Utiliza procedimientos abiertos y restringidos según los contratos. - Publicación de oportunidades en el <i>Defence Contracts Online</i> (DCO). - Enfoque en transparencia.	- Priorización del ciclo de vida y sostenibilidad en contratos. - Incentivos para la innovación tecnológica.
Francia	Dirección General de Armamento (DGA)	- Regido por el <i>Code de la Défense</i> y el <i>Code de la Commande Publique</i>. - Contratos abiertos o negociados en proyectos de interés nacional. - Fuerte enfoque en independencia tecnológica.	- Preferencia por producción nacional en sectores estratégicos. - Promoción de tecnología francesa.
Alemania	Oficina Federal de Equipamiento (BAAINBw)	- Basado en la Ley de Contratación Pública. - Procedimientos negociados para proyectos especializados. - Publicación en la <i>Electronic Tendering Platform</i>.	- Requisitos estrictos de cumplimiento de seguridad. - Fomento de proveedores nacionales en sectores críticos.

Tabla 1.- Comparativa internacional contratación TIC.

2.7 Evolución Histórica Contratación TIC en el Ministerio de Defensa (MINISDEF)

La contratación pública de TIC en el Ministerio de Defensa español ha experimentado una evolución significativa en las últimas décadas, impulsada por el avance de las tecnologías de la información y la creciente necesidad de mejorar la seguridad cibernética y la interoperabilidad en el ámbito de defensa. A continuación, se ofrece una breve revisión temporal de esta evolución, destacando los cambios clave en la normativa y las prácticas de contratación.

1990 - Primera Digitalización y Adopción de Sistemas Básicos TIC:

En la década de 1990, el MINISDEF comenzó a digitalizar sus procesos administrativos y operativos, adoptando sistemas de gestión básica de información y comunicaciones. La contratación de TIC se centraba principalmente en la adquisición de hardware y software esencial, sin un enfoque específico en la interoperabilidad o la seguridad avanzada.

Durante esta fase, las contrataciones se realizaban bajo el marco general de contratación pública, sin considerar la especialización en TIC que se demandaría en las siguientes décadas.

2000 - Creación de la Infraestructura Integral y Normativas TIC Iniciales:

Se desarrolló la **Infraestructura Integral de Información para la Defensa (2000I3D)**, un sistema diseñado para unificar y centralizar los servicios de información y comunicaciones en todas las unidades del Ministerio. Esta infraestructura representó el primer esfuerzo significativo para estandarizar y coordinar los recursos TIC.

Este periodo también marcó el inicio de la regulación específica de contratación TIC, con normativas que introdujeron cláusulas de seguridad y calidad en los contratos TIC y exigieron a los proveedores el cumplimiento de estándares mínimos de operatividad.

2010 - Incorporación de la Ciberseguridad y los Procedimientos de Contratación Especializados:

Con el incremento de las amenazas cibernéticas y la necesidad de proteger la información clasificada, el MINISDEF comenzó a implementar medidas específicas de ciberseguridad en sus contrataciones TIC. En 2011 se aprobó la **Ley 24/2011 de Contratos del Sector Público en los ámbitos de la Defensa y de la Seguridad**, que permitió el uso de procedimientos de contratación negociados sin publicidad para adquirir sistemas críticos y altamente confidenciales.

Durante esta década, se desarrollaron los primeros programas de capacitación en ciberseguridad para el personal de TIC del MINISDEF y se establecieron auditorías de seguridad en la cadena de suministro, asegurando que los contratos cumplieran con los requisitos de seguridad y confidencialidad.

2020 - Transformación Digital y Contratación Sostenible:

En el año 2020, el MINISDEF ha intensificado sus esfuerzos en la transformación digital, asignando un presupuesto creciente para la adquisición de infraestructuras avanzadas y sistemas de ciberseguridad de última generación. Este periodo ha estado influido por la **Ley 9/2017 de Contratos del Sector Público** y el **Plan de Transformación Digital del MINISDEF**, que establece objetivos específicos de digitalización, sostenibilidad y eficiencia energética en las contrataciones TIC.

Las contrataciones actuales buscan no solo satisfacer las necesidades operativas, sino también alinearse con los compromisos de sostenibilidad y reducción de la huella de carbono en defensa. Además, el MINISDEF ha adoptado herramientas de contratación digital que automatizan ciertas fases del proceso, mejorando la transparencia y la eficiencia operativa.



Ilustración 2.- Evolución histórica contratación TIC.-

3 METODOLOGÍAS Y PROCESOS DE CONTRATACIÓN

La normativa sobre contratación pública en general y por ende de la contratación TIC en el MINISDEF exige el uso de metodologías especializadas y procesos estructurados que permitan asegurar la transparencia, eficiencia y eficacia en la obtención de recursos tecnológicos. Como es natural por sus especiales circunstancias hay que adaptar esos principios para que se concilien con otros elementos deseables que ya se han mencionado: seguridad, sostenibilidad, integración, garantía del suministro, etc.

Este capítulo examina las metodologías y los procesos clave empleados en la contratación de TIC en el ámbito de defensa, considerando tanto la normativa aplicable como las particularidades de las adquisiciones en un contexto de alta sensibilidad y seguridad.

3.1 Metodologías en la Contratación Pública de TIC

Como se ha mencionado, las metodologías de contratación aplicadas en el MINISDEF están orientadas a garantizar la optimización de recursos, la seguridad en el suministro y la interoperabilidad entre los sistemas tecnológicos de defensa. A continuación, se describen las metodologías más empleadas en el proceso de contratación pública de TIC.

3.1.1 Contratación Centralizada y Acuerdos Marco:

La contratación centralizada en la contratación pública es un modelo en el que una entidad o departamento central asume la responsabilidad de gestionar y llevar a cabo las compras de bienes y servicios que necesitan distintas áreas u organismos de una administración. Este enfoque busca optimizar los recursos, mejorar la eficiencia y reducir los costos al consolidar las necesidades comunes en un solo proceso de contratación.

En lugar de que cada departamento realice sus propias contrataciones, la entidad centralizada gestiona la contratación a través de procedimientos de contratación como compras centralizadas directas, acuerdos marco o sistemas dinámicos de adquisición que pueden ser utilizados por todas las áreas, lo cual permite obtener economías de escala, simplificar los procedimientos administrativos y mejorar el control y la transparencia del gasto público. La contratación centralizada es especialmente útil en sectores como la tecnología, donde la interoperabilidad y la compatibilidad de sistemas son esenciales, así como en áreas que requieren estándares específicos de calidad y seguridad.

En el MINISDEF, la Subdirección General de Contratación lidera la implementación de acuerdos marco para la contratación de TIC, consolidando los requisitos comunes de varias unidades en un único proceso de adquisición. Esto permite obtener economías de escala y asegurar la interoperabilidad de los sistemas adquiridos, lo cual es esencial en el ámbito de defensa, donde la cohesión y la coordinación tecnológica son críticas para el funcionamiento eficaz de las Fuerzas Armadas.



Ilustración 3.- web <https://contratacioncentralizada.gob.es/>

3.1.2 Procedimiento Abierto Simplificado:

El **procedimiento abierto simplificado** es una modalidad de contratación pública que permite realizar procesos de contratación de menor cuantía o complejidad de manera más ágil. Este procedimiento es ideal para contratos TIC que no requieren de medidas de seguridad avanzadas ni de una planificación estratégica compleja.

Este proceso está regulado por la **Ley 9/2017 de Contratos del Sector Público** y facilita la obtención de productos TIC de uso generalizado que pueden adquirirse con condiciones homogéneas y en plazos más cortos, favoreciendo así la flexibilidad y agilidad en la respuesta a las necesidades tecnológicas inmediatas del MINISDEF.

3.1.3 Procedimiento Negociado sin Publicidad:

Dada la naturaleza sensible de ciertos sistemas TIC en el ámbito de Defensa, el procedimiento negociado sin publicidad permite al MINISDEF contratar de forma directa aquellos bienes y servicios tecnológicos que requieren **confidencialidad y seguridad**. Esta metodología es particularmente relevante cuando los sistemas o servicios contratados implican un alto grado de innovación tecnológica o cuando están destinados a garantizar la seguridad de las operaciones militares y la protección de la información.

El **procedimiento negociado sin publicidad** está recogido tanto en la Ley 9/2017 como en la Ley 24/2011, específica para contratos de defensa y seguridad, y se aplica en aquellos casos donde la publicidad del contrato podría poner en riesgo la seguridad nacional.

3.2 Uso de Herramientas Digitales y de Licitación Electrónica:

En el marco de la **Transformación Digital del Ministerio de Defensa**, se están implementando plataformas electrónicas para gestionar los procesos de contratación. Estas herramientas digitales no solo aseguran una mayor transparencia y trazabilidad en los procesos, sino que también permiten reducir los plazos de ejecución y mejorar la eficiencia en la administración de los contratos de TIC.

La digitalización de la contratación permite automatizar ciertas etapas, como la presentación de ofertas, la evaluación de propuestas y la adjudicación, facilitando un **proceso de contratación más transparente y accesible** para los proveedores, en consonancia con las directrices de la Administración General del Estado.

➤ **Plataforma de Contratación del Sector Público (PLACSP):**

- Esta plataforma es el sistema principal de licitación electrónica en España, donde se publican todas las licitaciones de las administraciones públicas, incluidas las del Ministerio de Defensa. La PLACSP permite la gestión completa del proceso de contratación, desde la publicación de anuncios de licitación hasta la recepción de ofertas electrónicas y la adjudicación del contrato.
- A través de esta plataforma, el Ministerio de Defensa garantiza la transparencia y el acceso público a la información sobre sus contratos, incluyendo pliegos, adjudicaciones y resultados.



Ilustración 4.-<https://contrataciondeestado.es/wps/portal/plataforma>

➤ **Sistema de Licitación Electrónica:**

Integrado en la PLACSP, el sistema de licitación electrónica permite que los proveedores presenten sus ofertas en formato digital, lo cual agiliza el proceso y reduce la burocracia. Este sistema asegura la integridad y confidencialidad de las propuestas y permite la evaluación en línea, simplificando las gestiones administrativas.

➤ **Herramienta de Registro y Supervisión de Contratos:**

El Ministerio de Defensa cuenta con un sistema interno de registro y supervisión para gestionar el ciclo de vida de cada contrato TIC, que incluye desde la planificación inicial hasta el seguimiento y cierre del contrato. Este sistema ayuda a mantener el control y la trazabilidad de cada contrato y asegura el cumplimiento de los plazos y términos establecidos.

➤ **Plataforma de Facturación Electrónica (FACe):**

FACe es el punto general de entrada de facturas electrónicas para la Administración General del Estado. El Ministerio de Defensa usa esta plataforma para gestionar la facturación de los contratos de TIC, lo cual permite reducir el uso de papel, optimizar el procesamiento de pagos y mejorar el control financiero.



Ilustración 5.- Web face <https://face.gob.es/es/login>

➤ **Sistemas de Gestión Documental y Firma Electrónica:**

Para el manejo de documentos y la formalización de contratos, el Ministerio utiliza sistemas de gestión documental integrados con firma electrónica. Esto permite que todos los documentos relevantes (como el Pliego de Prescripciones Técnicas, las ofertas y los contratos firmados) se gestionen y almacenen digitalmente, garantizando su autenticidad y validez legal.

➤ **Sistema de Información de la Gestión Económica (SIGE):**

Es una herramienta utilizada para la gestión presupuestaria y financiera de los contratos. Aunque no es una plataforma de licitación en sí, SIGE permite al Ministerio gestionar el presupuesto y controlar los gastos asociados a cada contrato TIC, asegurando el cumplimiento de los límites financieros y la eficiencia en el uso de los recursos públicos.

3.3 Procesos Clave en la Contratación de TIC en Defensa

La contratación de TIC en el MINISDEF sigue un proceso estructurado que asegura el cumplimiento de los objetivos estratégicos del Ministerio y las normativas vigentes. A continuación, se describen los procesos clave que componen la contratación de TIC en el MINISDEF.

- **Identificación de Necesidades y Planificación de Recursos:**

El proceso de contratación de TIC inicia con la **identificación de necesidades tecnológicas** por parte de las distintas unidades del Ministerio. Esta fase es crítica para definir los requisitos específicos del sistema o servicio que se va a contratar, alineando las adquisiciones con los objetivos operativos del MINISDEF.

La **planificación de recursos** es fundamental en este punto, ya que permite prever el presupuesto necesario y coordinar los tiempos de adquisición con los planes estratégicos del Ministerio. En esta fase, se priorizan los proyectos de mayor impacto en términos de interoperabilidad, seguridad y sostenibilidad.

- **Elaboración del Pliego de Prescripciones Técnicas (PPT):**

El Pliego de Prescripciones Técnicas (PPT) es un documento esencial en el proceso de contratación de TIC, ya que define con precisión las características técnicas, de seguridad y de rendimiento que debe cumplir el bien o servicio contratado. Este pliego se elabora con base en los estándares de calidad y los requisitos de interoperabilidad que rigen en el MINISDEF, así como en las normativas nacionales e internacionales aplicables.

En el caso de sistemas TIC de alta sensibilidad, el PPT también debe incluir requisitos específicos de ciberseguridad y protección de datos que aseguren la confidencialidad y la integridad de la información.

- **Elaboración del Pliego de Cláusulas Administrativas particulares (PCAP):**

Documento fundamental en los procesos de contratación pública. En él se establecen las condiciones administrativas específicas para cada contrato público cuyo objetivo es garantizar la transparencia, igualdad de oportunidades y adhesión a la normativa relativa a la contratación en el sector público.

En los PCAP, se incluyen aspectos tan relevantes para el proceso de contratación y la vigencia de los propios contratos como son: objeto del contrato, requisitos de los licitadores, condiciones de licitación en relación a los aspectos administrativos (procedimiento de adjudicación, criterios de adjudicación, plazos para los hitos contractuales...) u otras

condiciones determinantes del contrato como su duración, aspectos económicos o causas de resolución.

- **Evaluación de Ofertas y Selección de Proveedores:**

La evaluación de las ofertas se realiza en función de su con los aspectos técnicos que marca el PPT (qué queremos contratar) como de los criterios de adjudicación establecidos en el PCAP. Ambos documentos son vinculantes y se complementan para reflejar todos los aspectos tanto técnicos como administrativos del contrato. En los contratos TIC del MINISDEF, los criterios técnicos suelen tener un peso considerable, dado que la calidad y seguridad del servicio son prioritarios en el ámbito de defensa.

La selección de proveedores se basa en un análisis comparativo que pondera el cumplimiento de los requisitos técnicos, el precio, los tiempos de entrega y, en algunos casos, las garantías de seguridad. En los procedimientos abiertos, esta evaluación es transparente y se realiza mediante sistemas de puntuación objetivos, mientras que en los procedimientos negociados sin publicidad se emplean criterios más restrictivos para asegurar la seguridad y confidencialidad del proceso.

- **Formalización y Seguimiento del Contrato:**

Una vez seleccionada la oferta más adecuada, se procede a la formalización del contrato, que incluye las cláusulas y condiciones de ejecución acordadas. En el caso de contratos TIC en defensa, el contrato suele incluir disposiciones de seguridad específicas y acuerdos de confidencialidad.

La fase de seguimiento del contrato es esencial para verificar el cumplimiento de los términos establecidos en el PPT y en el contrato. Este seguimiento incluye auditorías periódicas, control de calidad, y, en el caso de servicios TIC, la verificación de la continuidad y la seguridad del suministro. El Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) es el responsable de gestionar y supervisar el rendimiento de los sistemas TIC del MINISDEF, asegurando que los recursos contratados cumplen con los estándares de operatividad y seguridad requeridos.

- **Evaluación de la Ejecución y Cierre del Contrato:**

Al finalizar el contrato, se realiza una **evaluación de la ejecución** para determinar si el servicio o bien TIC ha cumplido con las especificaciones establecidas y ha satisfecho las necesidades del MINISDEF. Esta evaluación considera aspectos como la calidad, el cumplimiento de los tiempos de entrega y el rendimiento de los sistemas contratados.

En los casos de contratos complejos o de larga duración, el MINISDEF suele realizar un análisis de **lecciones aprendidas**, identificando áreas de mejora para futuras contrataciones. Este proceso de cierre es clave para optimizar los procesos de contratación y asegurar que se mantiene la calidad y seguridad en los sistemas TIC de defensa.

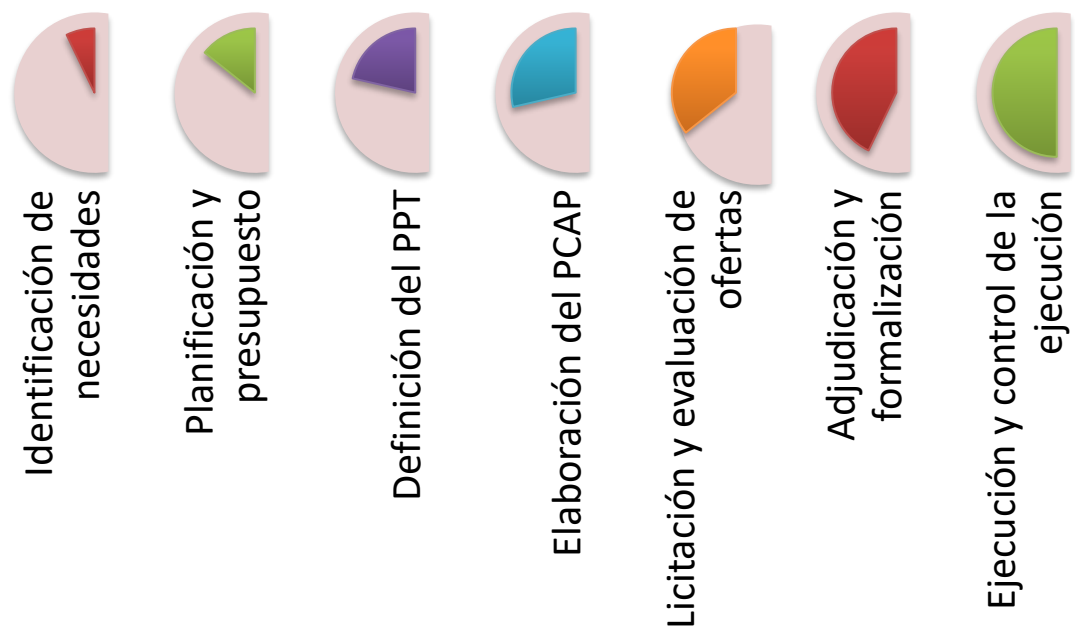


Ilustración 6.- Diagrama procesos clave contratación TIC

3.4 Retos y Mejores Prácticas en los Procesos de Contratación de TIC

El proceso de contratación de TIC en el MINISDEF enfrenta varios desafíos, que incluyen la rápida evolución tecnológica, los estrictos requisitos de seguridad y la necesidad de coordinar los recursos en un entorno de alta sensibilidad operativa.

3.4.1 Desafíos en la Contratación TIC en Defensa:

1. La **adaptación a nuevas tecnologías** supone un reto constante, ya que el MINISDEF debe asegurar que los sistemas contratados sean compatibles con futuras actualizaciones y cumplan con los requisitos de interoperabilidad internacionales.
2. La gestión de la **ciberseguridad en el proceso de contratación** también representa un desafío, ya que es fundamental garantizar la seguridad tanto de los sistemas contratados como de la información manejada durante el proceso de adquisición.

3.4.2 Mejores Prácticas:

La adopción de **acuerdos marco y procedimientos de contratación centralizada** ha demostrado ser una práctica eficiente para racionalizar la adquisición de TIC y asegurar la homogeneidad de los sistemas.

El uso de **herramientas digitales para la contratación** ha mejorado la eficiencia y transparencia del proceso, facilitando el control de los contratos y mejorando la accesibilidad para los proveedores en el ámbito de TIC.

4 ANÁLISIS DEL PRESUPUESTO TIC MINISDEF

El presupuesto destinado a las TIC en el Ministerio de Defensa ha experimentado un aumento de crédito creciente en los últimos años debido al impacto de la transformación digital en el ámbito de la seguridad y la defensa.

Este capítulo examina la distribución del presupuesto TIC, su evolución temporal y las áreas prioritarias de inversión. El análisis se basa en los datos presupuestarios más recientes y en los objetivos estratégicos de digitalización y sostenibilidad del MINISDEF.

En los presupuestos, como principal política económica de un país, se refleja la creciente importancia de las tecnologías de la información y comunicaciones en las operaciones de defensa. La evolución del presupuesto responde, fundamentalmente, a la necesidad de modernizar las infraestructuras tecnológicas y fortalecer la ciberseguridad en un entorno cada vez más complejo y digitalizado.

4.1 Clasificación de la licitación según el objeto de los contratos

En esta clasificación se atiende a la taxonomía (clasificación) del objeto del contrato, en la siguiente table se reflejan los expedientes por cada uno de los sectores; como se puede anticipar, interesa especialmente a este trabajo el gasto correspondiente a TIC (CIS):

Sectores según el objeto de los contratos	Número de expedientes	Importe licitado
Armamento y material	5.028	1.558.215.086,52 €
Infraestructura	4.371	370.895.007,01 €
Funcionamiento	12.759	337.394.187,11 €
CIS	411	323.289.967,40 €
Sanidad	927	44.854.827,38 €
Formación	545	24.461.412,80 €
I+D	18	4.817.088,81 €
Personal	65	826.361,84 €
Total	24.124	2.664.753.938,87 €

Ilustración 7.- fuente memoria de contratación 2023 del Ministerio de Defensa

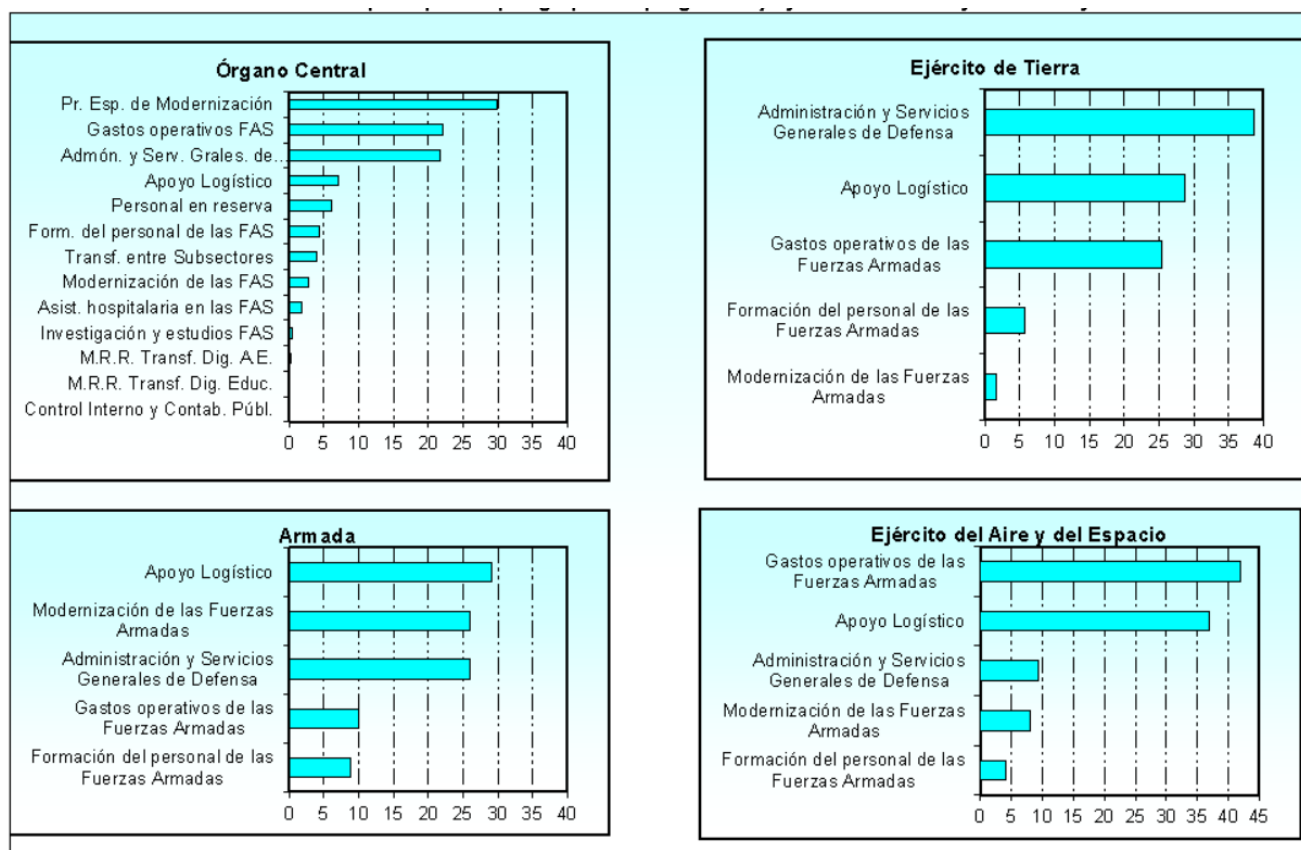


Ilustración 8.- Distribución presupuesto programas (Estadística A. Económicos 2022)

4.2 Clasificación por Programas (para qué gastamos)

En esta clasificación los créditos se ordenan por su finalidad (para qué se gasta), indicando los objetivos que el programa persigue y clasificados por áreas de gasto, políticas de gasto, grupos de programas y programas, éstos últimos, a su vez se pueden desarrollar en subprogramas.¹

De acuerdo con la memoria de contratación del año 2023, un volumen muy significativo del importe adjudicado por el órgano central se emplea en los Programas Especiales de Modernización, que dotan a las FAS de sistemas de tecnología avanzada que precisan de unas características muy especiales como son la **fabricación plurinacional**, un **proceso de obtención largo** y unos **métodos de contratación particularmente complejos**.²

Estudiando el presupuesto de gastos por programas, se identifican los programas y subprogramas con los que se acometen los gastos e inversiones en materia TIC, aunque no exclusivamente porque por su globalidad y transversalidad, no extraña que también permeen a otras partidas presupuestarias.

¹ Ley 47/2003, de 26 de noviembre, General Presupuestaria.

² Memoria de Contratación 2023 Ministerio de Defensa.

Considerado lo anterior, estos son los principales programas de gasto con el desglose cuando tiene lugar:

PROGRAMA	121M (Administración y servicios Generales
SUBPROGRAMA	121M.3 (Administración CIS)
CONCEPTOS	Arrendamiento de equipos de procesos de información y otro inmovilizado material
	Material informático no inventariable
	Suministro de material electrónico, eléctrico y de comunicaciones
	Estudios y trabajos técnicos realizados por otras empresas, relacionados con el subprograma
PROGRAMA	122N (Apoyo Logístico)
SUBPROGRAMA	122N.3 (Mantenimiento CIS)
CONCEPTOS	Gastos derivados del mantenimiento de los sistemas de información y las comunicaciones, realizados por medios propios o ajenos

Tabla 2.- Tabla elaboración propia (Fuente: Presupuestos Generales del Estado)

4.3 Clasificación Económica (en qué gastamos)

La pregunta a la respuesta de la clasificación económica de la estructura del presupuesto. Los gastos en TIC se acometen fundamentalmente con los capítulos 2³ y 6⁴ del presupuesto de gastos.

Ejecutado el presupuesto, se evidencia en las memorias de contratación del Ministerio de Defensa lo efectivamente contratado y si la previsión inicial reflejada en el presupuesto se ha trasladado a la contratación real a través de los distintos procedimientos de contratación, si una y otra se concilian, se podría decir que se ha seguido la política presupuestaria.

En esos capítulos 2 y 6 los grandes proyectos son los protagonistas de la ejecución del gasto, y dentro de estos grandes proyectos las TIC tienen un papel preponderante porque permean a muchos de los aspectos y ámbitos de esos grandes proyectos. A veces no es fácil discernir qué parte del gasto de los grandes proyectos se consume en aspectos TIC.

En los detalles presupuestarios de las ilustraciones siguientes se muestra extractos de los capítulos 2 y 6 del presupuesto. Se observa claramente como parte del presupuesto del capítulo 2 se consume en trabajos realizados por otras empresas y profesionales, este concepto relativo a las TIC incluye la externalización de servicios en este ámbito que no se pueden acometer “in house” por falta de recursos o de capacitación técnica

³ Gastos corrientes en bienes y servicios.

⁴ Inversiones Reales.

Artículo / Concepto	PRESUPUESTO INICIAL 2022 (01)	EJERCICIO PRESUPUESTARIO 2023 (02)	DIFERENCIAS	
			(02-01)	%
Art. 20 Arrendamientos y cánones	30.163,28	24.633,38	-5.529,90	-18,33
200 Arrendamientos terrenos y bienes naturales	3.505,00	3.535,90	30,90	0,88
202 Arrendamientos edificios y otras construcciones	1.269,90	1.158,00	-111,90	-8,81
203 Arrendamientos maquinaria, instalaciones y utillaje	18,00	29,00	11,00	61,11
204 Arrendamientos medios de transporte	2.125,45	2.230,88	105,43	4,96
205 Arrendamientos mobiliario y enseres	716,39	1.046,97	330,58	46,15
206 Arrendamientos equipos para procesos de información	260,73	266,40	5,67	2,17
208 Arrendamientos de otro inmovilizado material	3,34	21,50	18,16	543,71
209 Cánones	22.264,47	16.344,73	-5.919,74	-26,59
Art. 21 Reparaciones, mantenimiento y conservación	94.171,28	114.720,66	20.549,38	21,82
210 Infraestructura y bienes naturales	1,00	2,00	1,00	100,00
212 Edificios y otras construcciones	69.580,49	87.186,82	17.606,33	25,30
213 Maquinaria, instalaciones y utillaje	16.171,07	13.966,63	-2.204,44	-13,63
214 Elementos de transporte	861,51	987,63	126,12	14,64
215 Mobiliario y enseres	2.399,97	3.033,27	633,30	26,39
216 Equipos para procesos de la información	5.016,24	9.404,31	4.388,07	87,48
218 Bienes situados en el exterior	140,00	140,00	0,00	0,00
219 Otro inmovilizado material	1,00	0,00	-1,00	-100,00
Art. 22 Material, suministros y otros	693.259,32	795.739,59	102.480,27	14,78
220 Material de oficina	13.054,56	9.810,67	-3.243,89	-24,85
221 Suministros	277.029,06	349.898,87	72.869,81	26,30
222 Comunicaciones	32.848,69	37.562,73	4.714,04	14,35
223 Transportes	33.725,18	41.373,50	7.648,32	22,68
224 Primas de seguros	7.285,00	6.385,00	-900,00	-12,35
225 Tributos	2.606,56	2.991,37	384,81	14,76
226 Gastos diversos	38.927,00	50.199,34	11.272,34	28,96
227 Trabajos realizados por otras empresas y profesionales	187.783,27	197.518,11	9.734,84	5,18
228 Gastos originados por participación de las FAS en operaciones de mantenimiento de la paz	100.000,00	100.000,00	0,00	0,00
Art. 23 Indemnizaciones por razón del servicio	90.554,91	90.554,91	0,00	0,00
230 Dietas	67.917,96	67.917,96	0,00	0,00
231 Locomoción	14.161,42	14.161,42	0,00	0,00
232 Traslado	6.811,02	6.811,02	0,00	0,00
233 Otras indemnizaciones	1.664,51	1.664,51	0,00	0,00
Art. 24 Gastos de publicaciones	333,00	350,00	17,00	5,11
240 Gastos de edición y distribución	333,00	350,00	17,00	5,11
Art. 25 Conciertos de asistencia sanitaria	50,00	0,00	-50,00	-100,00
259 Otros conciertos de asistencia sanitaria	50,00	0,00	-50,00	-100,00
Art. 29 Gastos corrientes en bienes y servicios. Mecanismo de Recuperación y Resiliencia	500,00	500,00	0,00	0,00
290 Gastos corrientes en bienes y servicios. Mecanismo de Recuperación y Resiliencia	500,00	500,00	0,00	0,00
TOTAL CAPÍTULO 2	909.031,79	1.026.498,54	117.466,75	12,92

Ilustración 9.- Capítulo 2 Presupuesto gasto MINISDEF 2022

Para analizar más en profundidad el capítulo 6 del presupuesto, habría que ir al desglose de los gastos para definir cuánto se asigna a aspectos relacionados con las TIC, aunque, como ya se ha dicho, estos gastos tienen a menudo una naturaleza tan transversal que es difícil disociarlos dentro de los grandes programas para ofrecer una visión certera de cuánto se gasta realmente en TIC sin hacer un análisis financiero detallado de cada proyecto.

Artículo / Concepto	PRESUPUESTO INICIAL 2022 (01)	EJERCICIO PRESUPUESTARIO 2023 (02)	DIFERENCIAS	
			(02-01)	%
Art. 63 Inversión de reposición asociada al funcionamiento de los servicios	587,99	587,99	0,00	0,00
630 Inversión de reposición asociada al funcionamiento de los servicios	587,99	587,99	0,00	0,00
Art. 65 Inversiones militares en infraestructura y otros bienes	3.180.801,14	5.246.648,10	2.065.846,96	64,95
650 Inversiones militares en infraestructura y otros bienes	332.793,56	344.931,80	12.138,24	3,65
655 Programas Especiales de Modernización del Ejército de Tierra	563.440,96	934.495,92	371.054,96	65,86
656 Programas Especiales de Modernización de la Armada	665.214,84	1.082.842,99	417.628,15	62,78
657 Programas Especiales de Modernización del Ejército del Aire	1.368.942,56	2.136.988,07	768.045,51	56,11
658 Programas Especiales de Modernización de interés conjunto	250.409,22	747.389,32	496.980,10	198,47
Art. 66 Inversiones militares asociadas al funcionamiento de los servicios	425.311,26	437.534,11	12.222,85	2,87
660 Inversiones militares asociadas al funcionamiento operativo de los servicios	214.951,16	227.174,01	12.222,85	5,69
668 Gastos originados por participación de las FAS en operaciones de mantenimiento de la paz	210.360,10	210.360,10	0,00	
Art. 67 Gastos militares de inversiones de carácter inmaterial	25.115,60	27.013,24	1.897,64	7,56
670 Gastos militares en inversiones de carácter inmaterial	25.115,60	27.013,24	1.897,64	7,56
Art. 69 Inversiones reales: Mecanismo de Recuperación y Resiliencia	15.500,00	157.145,33	141.645,33	913,84
690 Inversión nueva en infraestructuras y bienes destinados al uso general. Mecanismo de Recuperación y Resiliencia.	0,00	112.891,67	112.891,67	
691 Inversión de reposición en infraestructuras y bienes destinados al uso general. Mecanismo de Recuperación y Resiliencia	0,00	43.753,66	43.753,66	
692 Inversión nueva asociada al funcionamiento operativo de los servicios. Mecanismo de Recuperación y Resiliencia	15.500,00	500,00	-15.000,00	-96,77
TOTAL CAPÍTULO 6	3.647.315,99	5.868.928,77	2.221.612,78	60,91

Ilustración 10.- Capítulo 6 Presupuesto gastos MINISDEF 2023

En la gráfica siguiente se muestran los operadores económicos que han recibido mayor presupuesto adjudicado, éstos, como se aprecia, concentran el 70% del importe total del presupuesto:

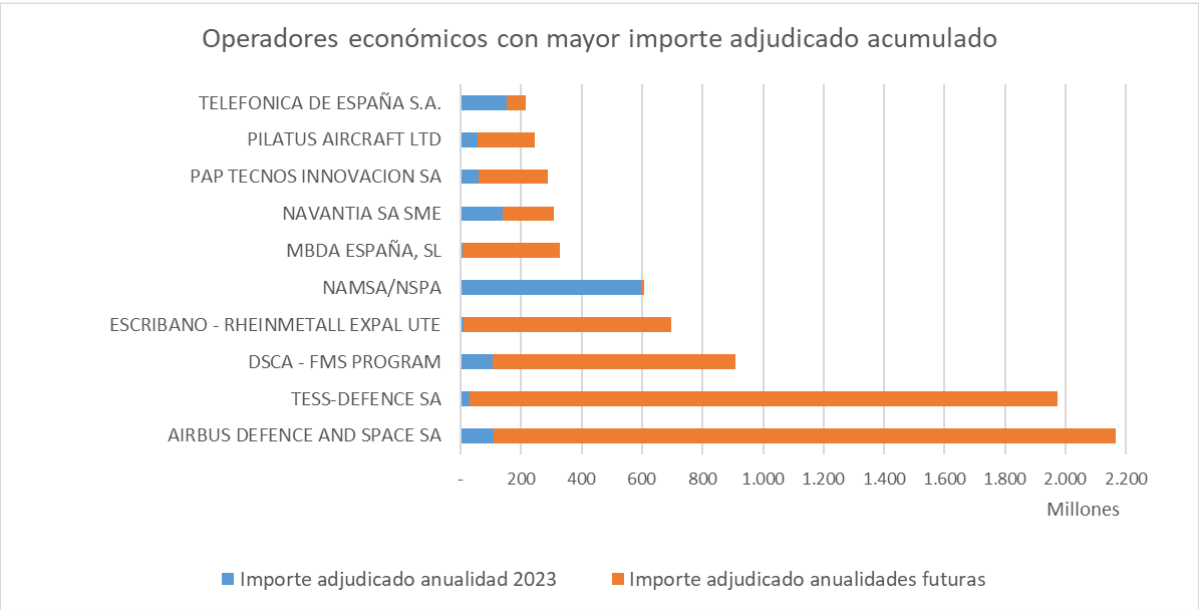


Ilustración 11.- Fuente Memoria Contratación año 2023

4.4 Evolución del Presupuesto TIC en el Ministerio de Defensa

Como la inversión en general, la correspondiente a las TIC en el MINISDEF ha aumentado de manera significativa en los últimos años, impulsada por los objetivos de modernización de la infraestructura tecnológica y de ciberseguridad en el contexto de una defensa más conectada y eficiente. Esta evolución refleja tanto la importancia de las TIC en el ámbito de defensa como el compromiso del MINISDEF con la transformación digital y la interoperabilidad en sus sistemas y plataformas.

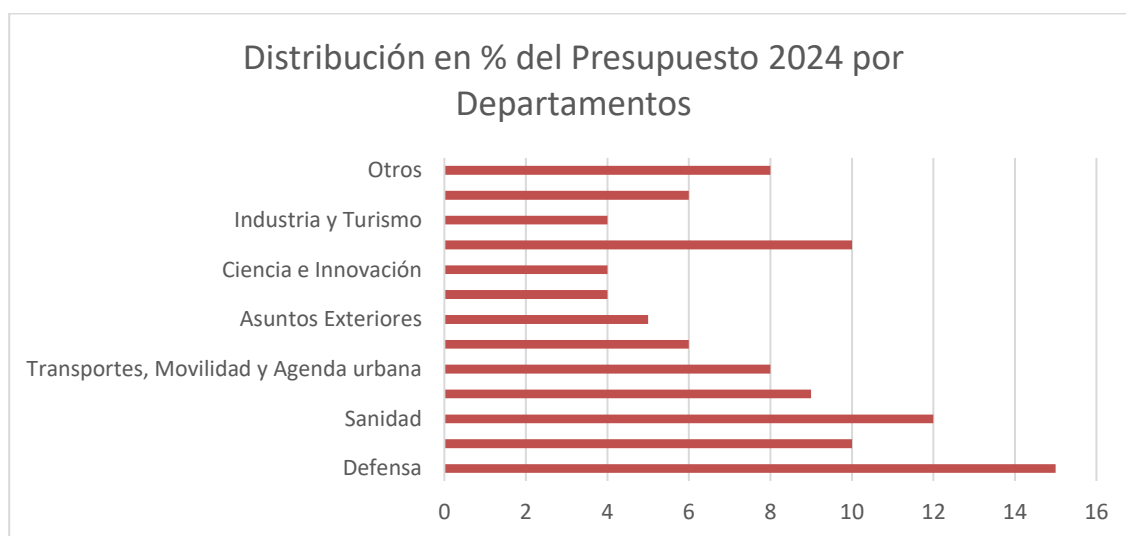


Ilustración 12.- Grafico elaboración propia fuente P.G.E. 2024

En el año 2023, el gasto se distribuía de la siguiente manera en función de quién hacía el gasto (clasificación orgánica)



Ilustración 13.- Fuente Memoria Contratación 2023 Ministerio de Defensa

En la siguiente gráfica se muestra el incremento de gasto en función del ejercicio presupuestario en los últimos años (12.827,18 millones de euros para 2023 – incremento de un 26,31% sobre el 2022)

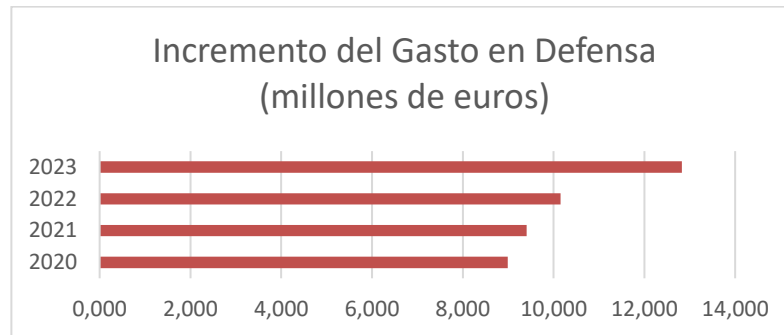


Ilustración 14.- Gráfico elaboración propia. Fuente P.G.E.

4.4.1 Crecimiento Anual del Presupuesto TIC:

En el presupuesto general de 2023, el MINISDEF dice haber asignado una partida creciente para TIC, alcanzando un incremento en el presupuesto consolidado en relación con el año 2022, aunque no se ofrecen datos concretos.⁵ Se declara que este aumento se alinea con los objetivos del Plan de Recuperación, Transformación y Resiliencia y con el Plan de Acción para la Transformación Digital del MINISDEF, orientado a modernizar las capacidades tecnológicas y operativas de Defensa.⁶

También se subraya que la tendencia de crecimiento ha sido constante en los últimos cinco años, con un enfoque en aumentar las capacidades de ciberseguridad, optimizar la infraestructura y facilitar la interoperabilidad en el ámbito nacional e internacional, especialmente con los países de la OTAN. En realidad es bastante difícil determinar cuánto ha sido el aumento observando los presupuestos. Muchas de las partidas presupuestarias no aparecen específicamente asignadas o proceden de incluso de otros departamentos ministeriales, vía modificaciones de créditos.

A pesar de lo anterior, se puede decir que se observa un incremento en estas partidas, aunque en ocasiones es difícil especificarlo y se sustancia en declaraciones contenidas en los presupuestos.

4.4.2 Distribución Plurianual del Presupuesto TIC:

La asignación de presupuesto TIC sigue un plan plurianual, que persigue una mejor gestión y sostenibilidad de las inversiones en infraestructuras de largo plazo. Este modelo se presenta como clave para asegurar la continuidad en proyectos de gran envergadura, como la modernización de

⁵ Presupuesto MINISDEF año 2023.

⁶ Plan de acción del Ministerio de Defensa para la Transformación Digital.

los centros de datos, la renovación de equipos y el desarrollo de infraestructuras de telecomunicaciones seguras.

A través de los proyectos plurianuales se pretende optimizar el gasto y reducir el riesgo de desactualización tecnológica en los sistemas TIC de defensa, permitiendo que las inversiones se realicen de forma progresiva, acorde a las necesidades operativas y los avances tecnológicos⁷.

4.4.3 Distribución del Presupuesto TIC por Áreas de Inversión

El presupuesto TIC en el MINISDEF se distribuye entre diferentes áreas clave, priorizando aquellas que tienen un impacto directo en la seguridad, eficiencia y modernización de las Fuerzas Armadas. A continuación, se detallan las principales áreas de inversión.

- **Infraestructura y Modernización de Centros de Datos:**

Una de las principales partidas del presupuesto TIC se destina a la modernización de infraestructuras críticas, incluyendo **centros de datos y redes de comunicación**. La consolidación de la infraestructura de datos bajo una Infraestructura Integral de Información para la Defensa (I3D) es una de las prioridades del MINISDEF, pues permite centralizar y mejorar la interoperabilidad de los sistemas TIC en las Fuerzas Armadas.⁸

Estas inversiones permiten reducir costos operativos a largo plazo mediante la eficiencia energética y la consolidación de recursos, además de mejorar la seguridad y la resiliencia de los sistemas TIC en entornos críticos.

- **Ciberseguridad:**

Dada la naturaleza sensible de las operaciones de Defensa, la **ciberseguridad** es uno de los pilares de la inversión en TIC. El MINISDEF ha incrementado la asignación de recursos a este ámbito en respuesta a las crecientes amenazas cibernéticas y a la necesidad de proteger tanto la infraestructura como la información clasificada y las comunicaciones militares.⁹

Las inversiones en ciberseguridad incluyen la adquisición de herramientas de monitoreo, detección y respuesta ante incidentes, así como la capacitación en seguridad para el

⁷ Presupuesto del Ministerio de Defensa 2023

⁸ Plan de acción del Ministerio de Defensa para la Transformación Digital.

⁹ Plan de acción del Ministerio de Defensa para la Transformación Digital.

personal y la implementación de tecnologías avanzadas para la protección de datos y sistemas.

- **Transformación Digital y Automatización de Procesos:**

La transformación digital es otro de los focos estratégicos de la inversión TIC, con una asignación presupuestaria orientada a **digitalizar y automatizar procesos** administrativos y operativos. Estas inversiones están en línea con la Estrategia TIC de la Administración General del Estado, que busca agilizar la gestión pública mediante tecnologías digitales, reduciendo la carga administrativa y mejorando la transparencia y eficiencia.

En el MINISDEF, estas partidas permiten mejorar los sistemas de gestión de contratos, el seguimiento de proyectos y la interoperabilidad de los sistemas administrativos y operativos, alineando la infraestructura TIC con los objetivos de eficiencia y sostenibilidad del Ministerio.

- **Interoperabilidad y Adquisición de Sistemas de Comunicación Segura:**

La interoperabilidad es fundamental en el ámbito de defensa, especialmente en el contexto de las alianzas internacionales como la OTAN. Una parte del presupuesto TIC se destina a asegurar que los sistemas de comunicación y los datos puedan ser compartidos y utilizados en tiempo real con los aliados, cumpliendo con estándares de seguridad internacionales.¹⁰

La adquisición de sistemas de comunicación seguros y de infraestructura que cumpla con los estándares internacionales permite una respuesta coordinada y eficaz en operaciones conjuntas, garantizando la compatibilidad y la seguridad de las comunicaciones militares.

- **Sostenibilidad y Eficiencia Energética en TIC:**

En línea con los compromisos de sostenibilidad del gobierno, el MINISDEF ha destinado una porción de su presupuesto TIC a iniciativas de **eficiencia energética y sostenibilidad** en sus infraestructuras tecnológicas. Estos proyectos incluyen la implementación de fuentes de energía renovable en centros de datos y la optimización del consumo energético en equipos y redes.¹¹

¹⁰ Marco Estratégico de Sistemas y Tecnologías de la Información y Comunicaciones del MINISDEF. (2022).

¹¹ Declaración de los Presupuestos Generales del Estado 2023

Esta partida también se relaciona con la reducción de la huella de carbono en el sector de Defensa, contribuyendo a los objetivos de sostenibilidad establecidos en la Agenda 2030 y reforzando el papel del MINISDEF en la protección del medio ambiente.

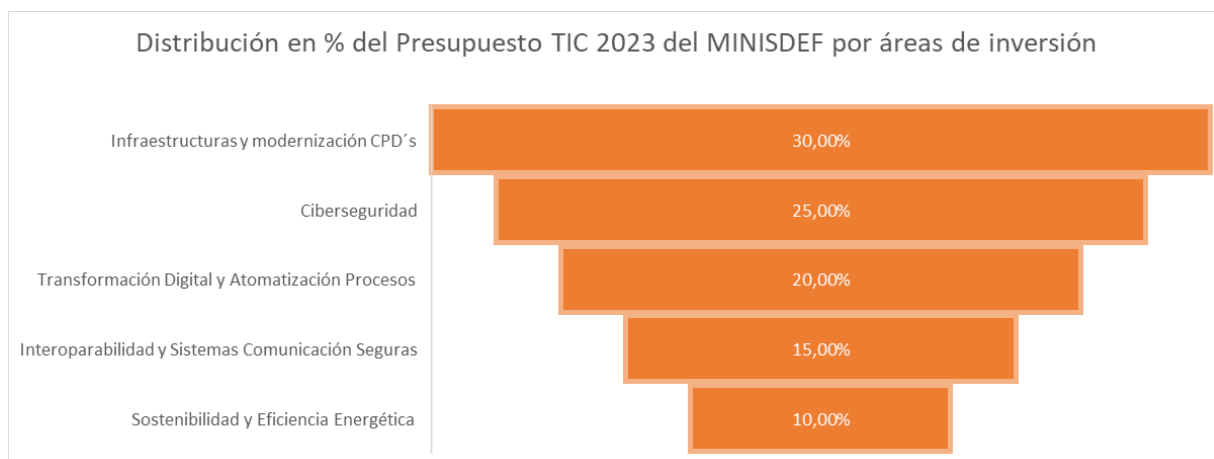


Ilustración 15.- Gráfico elaboración propia. Datos PGE 2023

4.4.4 Principales Programas y Proyectos Financiados con el Presupuesto TIC

El presupuesto TIC en el MINISDEF financia una serie de programas y proyectos clave, que reflejan la estrategia de modernización y defensa digital del Ministerio. A continuación, se destacan algunos de los programas y proyectos de mayor relevancia.

- **Programa de Ciberdefensa Nacional:**

Este programa se centra en la protección de la infraestructura de defensa ante posibles amenazas cibernéticas y en la implementación de medidas proactivas de ciberdefensa. Las inversiones en este ámbito buscan fortalecer la capacidad de respuesta del MINISDEF ante ataques cibernéticos y asegurar la continuidad operativa de los sistemas críticos de defensa¹².

El programa de ciberdefensa incluye el desarrollo de **centros de operaciones de ciberseguridad (SOC)**, herramientas de detección y mitigación de amenazas, y alianzas internacionales para compartir conocimientos y estrategias de defensa cibernética.

¹² Plan de acción del Ministerio de Defensa para la Transformación Digital.

- **Plan Integral de Transformación Digital (PITD):**

El PITD es uno de los proyectos más ambiciosos del MINISDEF en términos de modernización tecnológica, con objetivos de digitalización, automatización de procesos y mejora de la interoperabilidad. Este plan integra iniciativas de innovación en inteligencia artificial, big data y blockchain, con el fin de optimizar la gestión de recursos y mejorar la toma de decisiones en operaciones militares.

El plan también contempla la integración de los sistemas TIC del Ministerio con la Estrategia TIC de la AGE, asegurando así la coherencia y compatibilidad con otras agencias gubernamentales¹³.

- **Programa de Modernización de Centros de Datos y Redes de Comunicación:**

Este programa, que se ejecuta de manera plurianual, busca modernizar los **centros de datos y las redes de comunicación** del MINISDEF, garantizando su seguridad y eficiencia. La actualización de esta infraestructura es crítica para soportar el creciente volumen de datos y las demandas operativas del Ministerio.

Las inversiones en este programa permiten al MINISDEF consolidar sus recursos de TIC, optimizar el uso de espacio y reducir costos energéticos, contribuyendo al mismo tiempo a la sostenibilidad ambiental de las operaciones de defensa¹⁴.

- **Iniciativas de Sostenibilidad y Eficiencia Energética:**

Las iniciativas de sostenibilidad buscan reducir el impacto ambiental de las operaciones TIC, con proyectos que incluyen la implementación de energías renovables en centros de datos y la mejora de la eficiencia energética en redes y equipos. Estas medidas contribuyen tanto a la reducción de la huella de carbono del MINISDEF como a la optimización de costos operativos a largo plazo.¹⁵

Las inversiones en sostenibilidad también están alineadas con el compromiso del MINISDEF con los objetivos de la Agenda 2030, permitiendo una operación más respetuosa con el medioambiente y eficiente.

¹³ Plan de acción del Ministerio de Defensa para la Transformación Digital.

¹⁴ Política de Sistemas TIC MINISDEF (Orden Def. 2639/2015)

¹⁵ Concepto estratégico y política general de compras del MINISDEF 2022

4.5 Impacto del Presupuesto en la Transformación Digital y la Eficiencia Operativa

(se incluye un análisis crítico en cada apartado)

1. Digitalización de Procesos y Eficiencia en la Administración:

La asignación de presupuesto a la digitalización de procesos administrativos ha permitido automatizar tareas y mejorar la transparencia en la gestión de contratos y presupuestos. Estas iniciativas han reducido la carga administrativa y optimizado el uso de los recursos humanos, permitiendo que el personal se enfoque en tareas estratégicas de mayor valor.

- **Análisis Crítico:** Aunque se han logrado avances en la digitalización, la velocidad de transformación es aún limitada por las restricciones presupuestarias y la priorización de otros gastos. Sería beneficioso realizar una **revisión de los resultados de digitalización** para asegurar que cada proyecto de automatización justifique su inversión. La implementación de tecnologías como la inteligencia artificial para el análisis de datos o el blockchain para la trazabilidad de contratos podrían mejorar aún más la eficiencia si reciben una asignación adecuada.

2. Mejora de la Transparencia y Control del Gasto:

La digitalización y automatización han mejorado la transparencia en el control presupuestario, permitiendo un seguimiento más riguroso de los recursos asignados y una mejor evaluación de los resultados de los proyectos TIC.

- **Análisis Crítico:** Aunque la transparencia ha mejorado, la falta de métricas de rendimiento específicas dificulta una evaluación completa del impacto de los proyectos. La ausencia de indicadores de retorno de inversión (ROI) y de eficiencia dificulta el análisis de la rentabilidad del presupuesto TIC. Sería recomendable que el MINISDEF implemente **indicadores clave de rendimiento (KPIs)** para medir la efectividad de cada inversión, evaluando el beneficio real de cada partida presupuestaria.

4.4 Sostenibilidad y Eficiencia Energética en el Presupuesto TIC

1. Iniciativas de Sostenibilidad y Eficiencia Energética:

En los últimos años, el MINISDEF ha asignado una parte de su presupuesto TIC a proyectos de sostenibilidad, como la optimización del consumo energético en centros de

datos y el uso de energías renovables. Estos esfuerzos reflejan un compromiso con la reducción de la huella de carbono en el ámbito de defensa.

- **Análisis Crítico:** Aunque estas iniciativas son un paso positivo, la asignación presupuestaria para sostenibilidad es limitada en comparación con otras áreas. La inversión en tecnologías de eficiencia energética debería incrementarse para cumplir con los compromisos medioambientales de la Agenda 2030. Asimismo, la adopción de tecnologías en la nube y centros de datos eficientes podría ayudar a reducir los costes energéticos, optimizando el presupuesto a largo plazo.

2. Evaluación del Impacto Ambiental y Rendimiento de los Proyectos TIC:

Las inversiones en sostenibilidad también buscan mejorar la imagen institucional del MINISDEF y alinearse con las políticas de sostenibilidad del gobierno. Sin embargo, pocos proyectos TIC actuales incorporan métricas de impacto ambiental, lo cual dificulta evaluar su contribución a los objetivos de sostenibilidad.

- **Análisis Crítico:** La ausencia de **indicadores de sostenibilidad** limita la capacidad de medir el éxito de estas inversiones. Sería recomendable que el MINISDEF incorpore métricas de impacto ambiental en sus proyectos TIC, evaluando factores como la reducción de emisiones de CO₂ y el ahorro energético. Este enfoque permitiría identificar oportunidades de mejora y justificar futuras inversiones en sostenibilidad.

4.5 Ciberseguridad: Priorización en el Presupuesto y Desafíos

1. Priorización de la Ciberseguridad en el Presupuesto TIC:

Dado el aumento de las amenazas cibernéticas, el MINISDEF ha asignado un presupuesto significativo a la ciberseguridad, invirtiendo en infraestructura de monitoreo, sistemas de detección y respuesta, y en la capacitación del personal en prácticas de ciberseguridad. Esto refuerza la capacidad del Ministerio para enfrentar amenazas y proteger información sensible.

- **Análisis Crítico:** Si bien la inversión en ciberseguridad es esencial, el enfoque está orientado principalmente a la adquisición de tecnologías de defensa. Es necesario destinar más recursos a la **gestión de la ciberseguridad en la cadena de suministro** y a la colaboración con otros países aliados para mejorar la defensa cibernética. La inversión

en análisis predictivo y herramientas de inteligencia artificial también podría optimizar la capacidad de respuesta del MINISDEF frente a incidentes cibernéticos.

2. Capacitación y Conciencia en Ciberseguridad:

Una parte del presupuesto en ciberseguridad se ha destinado a la formación del personal, con el objetivo de sensibilizar y capacitar a los empleados en la identificación y gestión de riesgos cibernéticos. La capacitación continúa siendo esencial en un entorno donde las amenazas evolucionan rápidamente.

- **Análisis Crítico:** La capacitación del personal es efectiva, pero aún insuficiente en comparación con la magnitud de las amenazas actuales. La ciberseguridad debería estar integrada en la cultura organizacional del MINISDEF, fomentando una **formación continua** que incluya simulaciones de ataques y evaluaciones de habilidades periódicas. La inversión en programas de formación avanzada y certificación en ciberseguridad fortalecería la respuesta y la resiliencia del Ministerio ante ataques cibernéticos.

4.6 Conclusión del Análisis Crítico del Presupuesto TIC

El presupuesto TIC en el MINISDEF ha permitido avances importantes en la modernización, ciberseguridad y sostenibilidad de sus infraestructuras tecnológicas. Sin embargo, el análisis crítico sugiere que existen áreas de mejora en la asignación y gestión de los recursos. En particular, se recomienda una mayor flexibilidad en la estructura presupuestaria, un enfoque más fuerte en la evaluación de resultados y el rendimiento de las inversiones, y una priorización de la sostenibilidad y la ciberseguridad en la cadena de suministro.

Este análisis crítico del presupuesto proporciona una base para optimizar la gestión de recursos TIC en el MINISDEF, asegurando que las inversiones tecnológicas no solo mejoren la operatividad, sino que también se adapten a las necesidades y desafíos actuales del ámbito de defensa.

5 ESTUDIO DE CASOS Y VALIDACIÓN DE PROCESOS

Este capítulo analiza la implementación práctica de los procesos de contratación pública de las TIC en el Ministerio de Defensa mediante el estudio de un caso suficientemente relevante referenciado a las TIC. El estudio de caso se complementa con una evaluación de los mecanismos de validación utilizados para asegurar que los procedimientos cumplan con los estándares de eficiencia, transparencia y seguridad establecidos por la normativa aplicable.

Este desarrollo permite entender cómo se aplican los procesos de contratación de TIC en casos prácticos dentro del Ministerio de Defensa y resalta los mecanismos de validación que aseguran que los recursos TIC adquiridos cumplan con los estándares requeridos en el ámbito de defensa.

Se analiza con detalle el estudio de caso relativo a la Infraestructura de Ciberseguridad para el MINISDEF, en tanto en cuanto se considera el más relevante desde el punto de vista de relación con la materia de este TFM, su importancia en este ámbito para el Ministerio y su potencial como contrato paradigmático para extraer información relevante para el análisis.

5.1 Estudio de Caso: Infraestructura de Ciberseguridad MINISDEF

Uno de los proyectos de contratación pública más relevantes en el MINISDEF en los últimos años ha sido la adquisición de infraestructuras de ciberseguridad destinadas a proteger los sistemas y la información clasificada del Ministerio frente a amenazas cibernéticas.

Para un mejor seguimiento y análisis se ha incluido como anexo III el acuerdo marco del contrato, se relacionan a continuación sus características principales:

Expediente de contratación: 2022/SP03032003/00000330

https://contrataciondelestado.es/wps/poc?uri=deeplink%3Adetalle_licitacion&idEvl=8AFaVaNaXwd7h85%2Fpmmsfw%3D%3D

Valor estimado del Contrato: 61.011.031,77 €.

Tipo de Tramitación: Urgente.

Tipo de Contrato: Suministros (por tener mayor relevancia económica que la parte correspondiente a los servicios)

Órgano de Contratación: Dirección Económico Financiera de la Dirección General de Infraestructura MDE

Procedimiento de adjudicación: Negociado con publicidad.

Iniciativa del contrato: Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC) del MINISDEF.

Plazo de duración del AM: 3 años desde la formalización (mayo 2023) terminará en mayo de 2026.

- **Descripción del Proyecto:**

El proyecto consistió en la adquisición de un conjunto de herramientas avanzadas para la monitorización, detección y respuesta ante incidentes de ciberseguridad. Los objetivos incluían no solo el fortalecimiento de la seguridad perimetral y la defensa contra ataques externos, sino también la protección de datos sensibles y la optimización de los tiempos de respuesta en caso de un ciberataque.

La contratación incluyó tecnologías como sistemas de detección de intrusiones (IDS), firewalls de última generación y sistemas de monitoreo continuo que permitieran al equipo de ciberdefensa anticiparse y responder rápidamente a posibles amenazas.

- **Metodología empleada:** El proyecto se realizó mediante un **acuerdo marco**, de herramientas y servicios de ciberseguridad para la Infraestructura Integral de Información para la Defensa (I3D) permitiendo una contratación centralizada de servicios de ciberseguridad a nivel nacional. Se pretendía facilitar la obtención de herramientas compatibles con la infraestructura TIC existente y aseguró una mejor integración de los nuevos sistemas en la red del MINISDEF. Se identificaron los lotes siguientes:

Lote	Descripción
1	Suministros y servicios profesionales para el nodo de interconexión III de la I3D
2	Suministros y servicios profesionales para la gestión de eventos de seguridad de la I3D
3	Suministros y servicios profesionales para la interoperabilidad y coordinación en la prevención, detección y respuesta de amenazas en la I3D.
4	Suministros y servicios profesionales para el Centro de Operaciones de Seguridad de la I3D
5	Suministros y servicios de ciberseguridad transversales de la I3D
6	Suministros y servicios profesionales para la gestión y adecuación al Esquema Nacional de Seguridad en la I3D

Tabla 3.- Definición de lotes A.M. Servicio de Ciberseguridad I3D

- **Procedimiento negociado con publicidad:**

Dado que se declaró que la seguridad de los sistemas y la protección de la información eran prioritarias, con esta premisa se justificó el procedimiento negociado que, supuestamente, permitiría una adquisición rápida y segura de la infraestructura, garantizando así la confidencialidad en todas las etapas del proceso (el PPT se clasifica como “Difusión Limitada”, así como parte de los anexos, a algunos de ellos se les da una clasificación de seguridad de “Confidencial”

- **Previsión de resultados e Impacto del Proyecto:**

Se pretende con el contrato que la implementación de esta infraestructura de ciberseguridad mejore significativamente la capacidad del MINISDEF para detectar y responder a amenazas cibernéticas, reforzando la seguridad de sus sistemas y la protección de sus comunicaciones militares.

Se manifestó como capital que la interoperabilidad con los sistemas de ciberseguridad de otros países de la OTAN permitiera al MINISDEF compartir información sobre amenazas y mejorar la coordinación de la ciberdefensa en operaciones conjuntas.

5.1.1 Análisis de las empresas presentadas al concurso.

Se presentaron un total de trece empresas que se admitieron definitiva o provisionalmente al concurso y a las que posteriormente se les invitaría a presentar sus ofertas. Son las que se relacionan. Como se puede apreciar, son empresas importantes del sector de las tecnologías de la información y las comunicaciones, y por la entidad del contrato, se presentan por sí mismas o constituyendo unión temporal de empresas (UTE)

EMPRESAS PRESENTADAS
ACUNTIA S.A.U.
ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L.
Babel Sistemas de Información, S.L.
CENTRO REGIONAL DE SERVICIOS AVANZADOS S.A.
Deloitte Advisory, S.L.
EVOLUTIO CLOUD ENABLER S.A.
PricewaterhouseCoopers Asesores de Negocios, S.L.
SISTEMAS INFORMATICOS ABIERTOS, S.A.U.
THALES ESPAÑA SISTEMAS, S.A.U.
TRC INFORMATICA, S.L.
Telefónica Soluciones de Informática y Comunicaciones de España S.A.U.
UTE OESIA-ACCENTURE
UTE INETUM-INNOTECH

Tabla 4.- - Elaboración propia (Fuente: Acta órgano de asistencia)

De las trece empresas presentadas que se admitieron, finalmente solo se presentan 7 al concurso y a los lotes que consta para cada una de ellas, se puede comprender, independientemente de cuáles son los motivos para no presentar ofertas, que esto merma la competitividad:

EMPRESAS QUE REALIZARON OFERTA	LOTES
UTE INETUM-INNOTECH	2 y 4
EVOLUTIO CLOUD ENABLER S.A.U. LOTES	2 y 5
CENTRO REGIONAL DE SERVICIOS AVANZADOS S.A.	6
SISTEMAS INFORMÁTICOS ABIERTOS S.A.	2
TRC INFORMÁTICA S.L. LOTES	2,3 y 5
OESIA NETWORKS S.L.	2 y 5
TELEFÓNICA SOLUCIONES DE INFORMÁTICA Y COMUNICACIONES S.A.U. LOTES	1, 2, 3, 4, 5

Tabla 5.- Elaboración propia (Fuente: actas órganos de asistencia)

5.1.2 Adjudicación del contrato

Se valoran los criterios de los pliegos de acuerdo con los que se indican y sus porcentajes:

Lote	Criterio	Ponderación
1	Precio	65%
1	Otros (automático)	15%
1	Otros (juicio de valor)	20%
2	Precio	74%
2	Otros (automático)	6%
2	Otros (juicio de valor)	20%
3	Precio	69%
3	Otros (automático)	11%
3	Otros (juicio de valor)	20%
4	Precio	65%
4	Otros (automático)	15%
4	Otros (juicio de valor)	20%
5	Precio	70%
5	Otros (automático)	10%
5	Otros (juicio de valor)	20%
6	Precio	60%
6	Otros (automático)	20%
6	Otros (juicio de valor)	20%

Tabla 6.- Elaboración propia (Fuente: PCAP)

Como se puede apreciar, se da una importancia determinante a los criterios relacionados con la oferta económica que junto con los criterios valorables automáticamente (aspectos como el plazo

de entrega, la garantía ofrecida, etc.) son determinantes para la adjudicación. Los criterios dependientes de un juicio de valor (20% en todos los lotes) y que tienen más subjetividad por su naturaleza, figuraban en los pliegos de prescripciones técnicas y no se hacen constar aquí por su clasificación de seguridad (difusión limitada) pero que tienen que ver con aspectos como la experiencia del licitador en proyectos similares, la calidad del equipo técnico, la propuesta metodológica que se ofrezca... Éstos últimos determinan en mucho menor medida que los aspectos económicos la adjudicación. Cabría preguntarse si un contrato de naturaleza tan técnica no precisaría que los criterios técnicos de valoración tuvieran más peso en relación a los aspectos económicos.

En cualquier caso, resultaron adjudicatarias las empresas que se relacionan:

Lote	Empresa Adjudicataria	Importe de Adjudicación (Sin impuestos)
1	Telefónica Soluciones de Informática y Comunicaciones de España S.A.U.	11.244.352,04 €
2	TRC INFORMÁTICA, S.L.	2.075.723,92 €
3	TRC INFORMÁTICA, S.L.	6.615.000,00 €
4	Telefónica Soluciones de Informática y Comunicaciones de España S.A.U.	7.229.406,62 €
5	EVOLUTIO CLOUD ENABLER S.A.	11.276.917,84 €
6	CENTRO REGIONAL DE SERVICIOS AVANZADOS S.A.	600.300,00 €
	IMPORTE TOTAL DE LAS OFERTAS	39.041.700,42 €

Tabla 7.- Elaboración propia (Fuente: documentación de adjudicación)

El total de la adjudicación, excluyendo los impuestos se elevó a 39.041.700,42 €, que supone una rebaja mínima sobre el importe estimado para los tres primeros años, excluidas la posible prórroga de un año. Esa estimación se hizo constar el PCAP y era de 40.104.817,36 €, lo que evidencia lo preciso de la citada estimación.

Seguramente ese ajuste en el precio de salida del acuerdo marco no estimuló la participación de pequeñas empresas sin el músculo económico de las grandes que generan economías de escala y pueden hacer ofertas más competitivas.

5.1.3 Requisitos principales para la participación

En este punto se analizarán los requisitos que deben tener las empresas para poder participar en contratos de esta magnitud, se intentara vincular su exigencia con el efecto estimulante o disuasorio que pudieran tener, yendo en detrimento su presencia de la mayor o menor participación.

En primer lugar hay que comentar que las empresas deben estar convenientemente clasificadas, en España o el país de origen donde se reconozca esa clasificación poder participar. Además de lo

anterior, destaca la de demanda de solvencia económico-financiera y técnica o profesional a través de justificaciones de diversa índole sobre su actividad que se explicitan en el PCAP.

Particular importancia tiene el requisito de la garantía para este tipo de contratos que disuade en muchas ocasiones de la participación, en este caso no se exigía garantía provisional, exigiendo solamente el acuerdo marco el establecimiento de una garantía definitiva por los importes que se señalan a continuación por parte de los que resultasen adjudicatarios.

Lote	Garantía Definitiva
1	562.216,60 €
2	155.989,57 €
3	331.698,62 €
4	361.470,33 €
5	563.845,89 €
6	30.018,85 €

Tabla 8.- Elaboración Propia (Fuente: cláusula 18 PCAP)

En cuanto al Régimen de Pagos¹⁶ se estableció lo siguiente:

- Para las prestaciones de tipo suministro: Pago del precio de los suministros, previa entrega y recepción de conformidad con la totalidad del suministro.
- Para las prestaciones de tipo servicio: pagos trimestrales, previo certificado de conformidad del responsable del Contrato Basado.

Como es natural y frecuente, el pago de la cosa entregada o el servicio se supedita a la conformidad por parte de los responsables que tengan la función de acreditarlo. En este contrato, se observa un régimen de pagos que no genera demasiado quebranto a las empresas adjudicatarias pues, sobre todo en el caso de los servicios, se realizan trimestralmente después de cumplido y de los suministros, una vez entregados de conformidad.

Es muy frecuente que un régimen de pagos más largo, que obliga a las empresas a anticipar crédito por largos períodos (pagos a un año o incluso a la finalización del servicio) disuada en muchos casos a la presentación de oferta, pues solo las empresas importantes cuentan generalmente con la financiación necesaria para anticipar gastos durante largos períodos sin recibir entregas a cuenta o pagos relativamente rápidos una vez finalizado.

¹⁶ Cláusula 43 de PCAP.

Merece también la pena comentar que tampoco se establecen cláusulas de revisiones de precios, con lo que los posibles adjudicatarios comprometen el gasto sin saber cuánto les van a costar exactamente los suministros o servicios al final de la ejecución.

5.1.4 Clasificación de Seguridad para el Acuerdo Marco.

El contrato se clasificó como reservado de acuerdo con la instrucción 52/2013, de 17 de junio del Subsecretario de Defensa, por la que se aprueban las Normas para la Seguridad de la Información del Ministerio de Defensa en poder de las empresas.¹⁷

De acuerdo con lo anterior, se exigía de todas las empresas se atuvieran al marco normativo establecido en las normas de la Autoridad Nacional para la Protección de la Información Clasificada. Siendo así, deberían disponer de Habilitación de Seguridad de Empresa (HSEM) y Habilitación de Seguridad de Establecimiento (HSES), ésta última para todos los lotes exceptuando el número 6. Caso de presentar las de otros estados, éstas deberían estar reconocidas por la Autoridad Delegada para la Seguridad de la Información Clasificada.

También deberían contar con Habilitación Personal de Seguridad (HPS) de grado reservado, todas aquellas personas vinculadas al acuerdo marco por parte de la empresa o que manejaran información relativa al mismo.¹⁸

En este punto hay que decir que es frecuente que las empresas refieran la dificultad que les supone obtener y mantener las clasificaciones de seguridad, siendo también éste un elemento disuasorio para su presencia en las licitaciones públicas.

5.1.5 Objetivos perseguidos y previsiones de cumplimiento.

En el punto 2 (justificación de la necesidad) del informe razonado de la necesidad del acuerdo marco, se declara pormenorizadamente el porqué de esa necesidad, relacionando la ciberprotección del MINISDEF con la normativa vigente y las atribuciones y obligaciones que cada autoridad relacionada con el acuerdo marco tiene conferidas.

Se constata que el nivel de amenazas de ciberataques se ha incrementado notablemente con los conflictos actuales y la situación geopolítica, que se manifiesta en escenarios reales de guerras híbridas (ciberguerra), donde las soluciones comerciales de ciberseguridad, incluida la inteligencia civil tienen una importancia capital.

¹⁷ Cláusula 6 del PCAP.

¹⁸ Cláusula 6 del PCAP

En ese mismo documento, se hacen explícitos los incidentes de ciberseguridad en el año 2021 que se plasma en el siguiente gráfico:

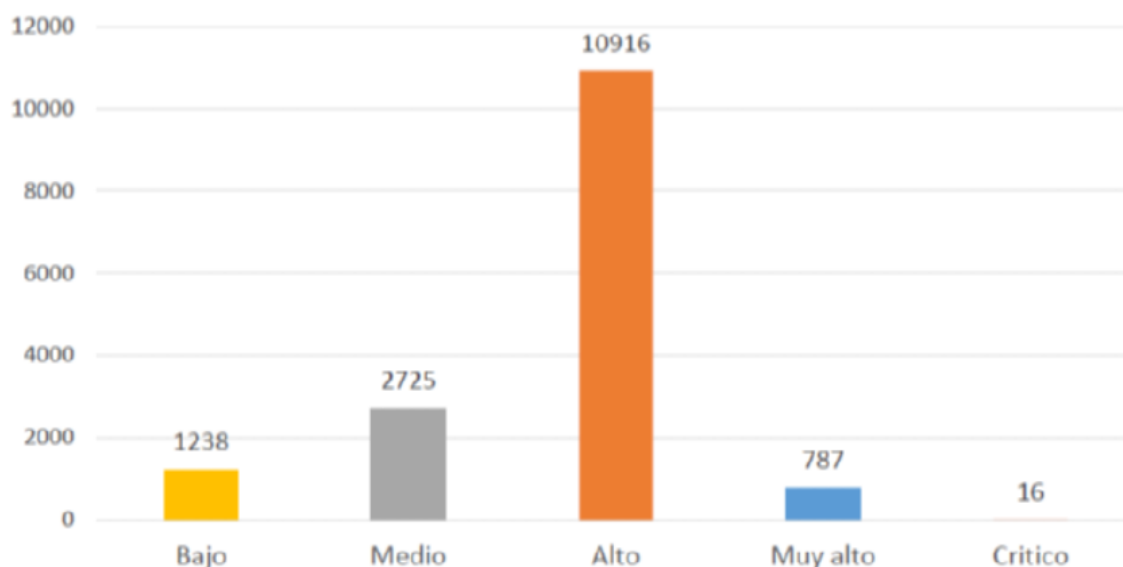


Ilustración 16.- Peligrosidad incidentes CIBER 2021 CCN-CERT

También se ofrece información gráfica de los incidentes, segregada por su tipo, de acuerdo con los datos del Centro Nacional de Inteligencia y sus órganos especializados en este ámbito.

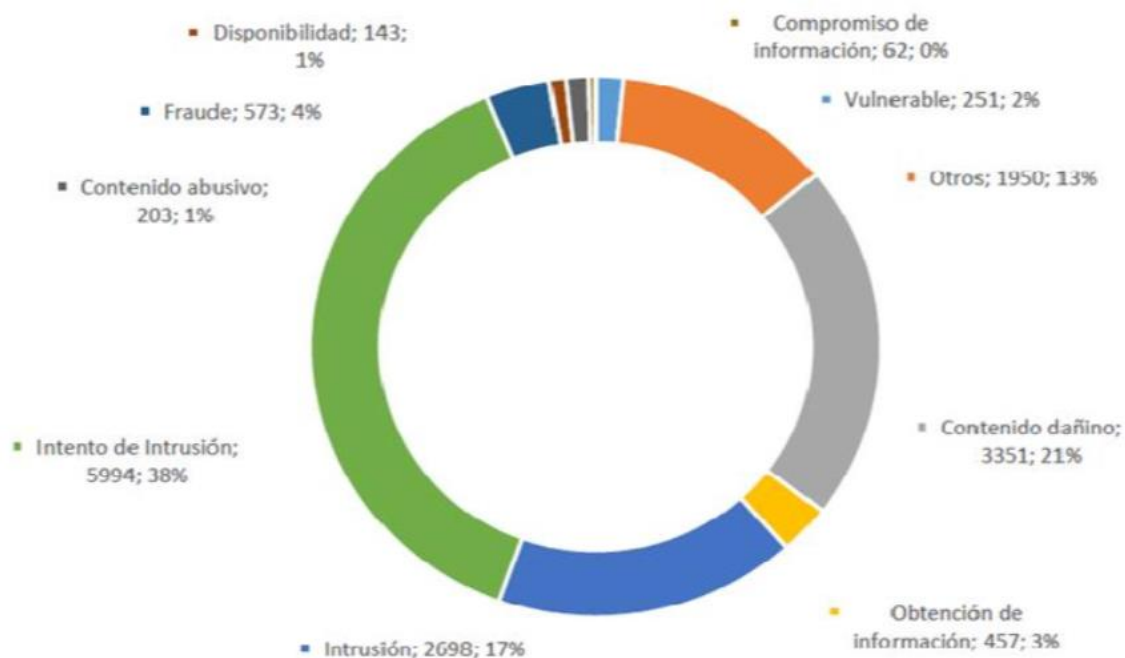


Ilustración 17.- Clasificación de los incidentes CCN-CERT en 2021

Se declara literalmente que la necesidad a satisfacer “De conformidad con lo dispuesto en el artículo 67.2. b) del RGLCAP, las necesidades administrativas a satisfacer mediante el presente AM son las de establecer las condiciones generales para la prestación de un servicio de

Ciberseguridad adecuado a las nuevas amenazas, cada vez más sofisticadas por lo que se hace necesario fortalecer las capacidades de prevención proactiva y cibervigilancia del Ministerio de Defensa.

*De conformidad con lo dispuesto en el artículo 28 de la LCSP y tal como se justifica en la documentación obrante en el expediente, el AM **resulta necesario** para el cumplimiento del fin perseguido, y el objeto y contenido del mismo **es idóneo** para la satisfacción de las necesidades identificadas”*

5.1.6 Propuesta de Key Performance Indicators (KPIs) para este acuerdo marco

Como se ha visto en el punto anterior y aunque se declaran los objetivos del acuerdo marco que tiene vigencia hasta 2026, con posible prórroga de un año, no parecen implementarse herramientas específicas en términos de eficiencia operativa o mejora de la seguridad que permitan conocer el grado de cumplimiento del acuerdo marco, por ende el grado de satisfacción con lo obtenido en la inversión.

En este punto, se proponen a continuación algunos KPIs que podría haber valorado incluir en este contrato en relación a los procesos de contratación y las herramientas implantadas.

En relación con los procesos de contratación:

- **Eficiencia del proceso:**
 - Tiempo total del proceso de contratación (desde la publicación del anuncio hasta la adjudicación).
 - Coste administrativo del proceso de contratación.
 - Número de licitadores por lote.
- **Cumplimiento de la normativa:**
 - Número de recursos presentados.
 - Resultados de las auditorías de contratación.
- **Transparencia:**
 - Accesibilidad de la información del proceso de contratación.
 - Claridad de los criterios de adjudicación.

En relación con las herramientas implantadas:

- **Efectividad de las herramientas:**

- Número de incidentes de ciberseguridad detectados y prevenidos.
- Tiempo de respuesta a incidentes de ciberseguridad.
- Nivel de cumplimiento del Esquema Nacional de Seguridad (ENS).
- **Eficiencia de las herramientas:**
 - Coste de mantenimiento de las herramientas.
 - Rendimiento de las herramientas (tiempo de procesamiento, consumo de recursos).
 - Integración de las herramientas con los sistemas existentes.
- **Satisfacción del usuario:**
 - Encuestas de satisfacción a los usuarios de las herramientas.
 - Número de solicitudes de soporte técnico.

KPIs adicionales:

- **Impacto en la organización:**
 - Mejora en la seguridad de la información.
 - Reducción de riesgos de ciberseguridad.
 - Mejora en la eficiencia operativa.
- **Retorno de la inversión (ROI):**
 - Beneficios económicos derivados de la implantación de las herramientas.
 - Reducción de costes por incidentes de ciberseguridad.

Recomendaciones:

- Los KPIs deberían ser específicos, medibles, alcanzables, relevantes y con plazos definidos (SMART).
- Se deben establecer mecanismos de seguimiento y evaluación de los KPIs.
- Los KPIs deben ser revisados y actualizados periódicamente.

5.3 Mecanismos de Validación y Control en los Procesos de Contratación de TIC

La validación y el control de los procesos de contratación son esenciales para asegurar que los recursos TIC adquiridos cumplan con los estándares de calidad, seguridad y eficiencia exigidos en el ámbito de

defensa. A continuación, se describen algunos de los principales mecanismos de validación implementados en el MINISDEF.

- **Auditorías de Cumplimiento y Control de Calidad:**

Para garantizar el cumplimiento de los términos del contrato, el MINISDEF realiza auditorías periódicas durante el proceso de contratación y en las etapas de ejecución del contrato. Estas auditorías permiten verificar que el proveedor esté cumpliendo con las especificaciones técnicas, los tiempos de entrega y los estándares de seguridad pactados.

Las auditorías también aseguran que los recursos TIC entregados cumplen con los requisitos de interoperabilidad y compatibilidad con la infraestructura tecnológica existente, un aspecto crucial en el ámbito de defensa.

- **Pruebas de Seguridad y Validación Técnica:**

Antes de implementar cualquier nuevo sistema TIC, el MINISDEF realiza pruebas de seguridad y de rendimiento que validan la solidez del sistema frente a posibles amenazas cibernéticas y su capacidad para integrarse sin comprometer la red de comunicaciones y los sistemas existentes.

En el caso de los sistemas de ciberseguridad, estas pruebas incluyen **simulaciones de ciberataques** y evaluaciones de vulnerabilidades, lo que permite identificar y corregir posibles debilidades antes de la implementación definitiva.

- **Monitoreo Continuo y Evaluación del Rendimiento:**

Una vez que el sistema TIC se encuentra en funcionamiento, el MINISDEF implementa un sistema de **monitoreo continuo** para evaluar su rendimiento y detectar posibles incidencias en tiempo real. El Centro de Sistemas y Tecnologías de la Información y Comunicaciones (CESTIC) supervisa el funcionamiento de los sistemas TIC y mantiene un registro de eventos que permite anticipar problemas y realizar ajustes si es necesario.

Este monitoreo continuo asegura que los sistemas contratados operen de manera óptima y cumplan con los requisitos de seguridad y operatividad en entornos críticos.

- **Evaluación de Proveedores y Lecciones Aprendidas:**

Al finalizar cada contrato, se lleva a cabo una evaluación integral del proveedor, en la que se analizan el rendimiento, la capacidad de respuesta y el cumplimiento de los estándares acordados. Esta evaluación permite al MINISDEF mantener un registro actualizado de proveedores confiables y mejorar los procesos de selección en futuras contrataciones.

Además, el MINISDEF implementa un proceso de análisis de lecciones aprendidas, donde se documentan los puntos fuertes y áreas de mejora en cada proyecto de contratación TIC. Este análisis retrospectivo permite optimizar continuamente los procesos de contratación y adaptar los procedimientos a las nuevas necesidades y desafíos del Ministerio.

5.4 Resultados y Recomendaciones

A partir del estudio de caso y de los mecanismos de validación descritos, se pueden extraer las siguientes conclusiones y recomendaciones:

- **Eficiencia en el Uso de Acuerdos Marco:**

Los acuerdos marco han demostrado ser una metodología eficaz para la contratación centralizada en el ámbito de defensa, ya que permiten la adquisición de soluciones tecnológicas homogéneas y aseguran la compatibilidad y escalabilidad de los sistemas TIC en el MINISDEF.

- **Mejora Continua en Ciberseguridad:**

Los estudios de caso confirman que el refuerzo de la ciberseguridad mediante la implementación de tecnologías avanzadas y la constante validación de los sistemas es fundamental para la protección de la información clasificada y la infraestructura digital del Ministerio. Es recomendable que el MINISDEF continúe invirtiendo en capacitación en ciberseguridad para el personal y en herramientas de detección y mitigación de amenazas.

- **Revisión de Procesos de Validación y Control de Calidad:**

Los mecanismos de validación descritos, como el monitoreo continuo y las pruebas de seguridad, han mostrado ser efectivos para asegurar la calidad y operatividad de los sistemas TIC contratados. No obstante, se recomienda revisar periódicamente estos procesos para adaptarlos a las nuevas amenazas y a la evolución de las tecnologías, estableciendo KPI's al efecto.

6 IMPLEMENTACIÓN DE LA COMPRA PÚBLICA DE INNOVACIÓN EN CONTRATOS DEL MINISDEF

6.1 Introducción

Si bien en el estudio de caso del punto 5.1 "Acuerdo Marco de herramientas y servicios de ciberseguridad para la Infraestructura Integral de Información para la Defensa (13D)" que ha sido objeto de un mayor estudio en este trabajo por su importancia económica y técnica, no se menciona explícitamente la compra pública de innovación (CPI), es cierto que se declara, explícitamente, que se persigue encontrar soluciones innovadoras en ciberseguridad. Esto sugiere que el Ministerio de Defensa podría haber empleado el modelo de la CPI en ese contrato como lo ha hecho en otros proyectos de importancia por su gran potencial.

Esta estrategia empleada por las administraciones públicas para fomentar la innovación mediante la contratación de bienes, servicios u obras que no existen en el mercado o que precisan de una mejora o relanzamiento con una visión diferente, busca, en lugar de adquirir soluciones ya existentes, animar a que las empresas desarrollen nuevas tecnologías, productos o servicios para satisfacer las necesidades específicas de la Administración.

Convenio CDTI y Entidad Publica



Consulta preliminar del Mercado

Licitación

6.2 Características principales

Estas son las notas principales de la CPI:

- **Demanda como motor de innovación:** La administración pública actúa como cliente que estimula la creación de soluciones innovadoras al plantear retos que no tienen una respuesta estándar en el mercado.
- **Colaboración público-privada:** Impulsa la cooperación entre el sector público y las empresas, universidades o centros de investigación.
- **Reducción de riesgos para empresas:** Ofrece apoyo financiero y un mercado inicial para innovaciones, ayudando a las empresas a superar barreras de entrada.

- **Mejora de servicios públicos:** Promueve soluciones más eficientes, sostenibles y adaptadas a las necesidades de los ciudadanos.

Estos son algunos ejemplos de uso en la sociedad civil para los que se ha empleado la CPI en el ámbito de las TIC:

- Desarrollo de tecnologías para ciudades inteligentes.
- Soluciones sostenibles en energía renovable.
- Sistemas avanzados para la salud y el cuidado de personas mayores.

6.3 La CPI en el Ministerio de Defensa

La CPI en el sector de defensa en España ha sido empleada para impulsar el desarrollo de tecnologías avanzadas que fortalecen las capacidades de las Fuerzas Armadas.

A continuación, se citan algunos ejemplos destacados del uso de la CPI en el MINISDEF:

1. Submarino S-83 con Sistema de Propulsión AIP

Descripción: Navantia desarrolló e instaló un innovador sistema de propulsión independiente del aire (AIP) en el submarino S-83. Este sistema, basado en tecnología de hidrógeno y bioetanol renovable, permite que los submarinos permanezcan sumergidos por períodos más prolongados, mejorando su capacidad operativa y seguridad.

Resultado: Este avance tecnológico posiciona a los submarinos españoles a la vanguardia, ofreciendo una ventaja competitiva en el ámbito internacional y reforzando la autonomía estratégica de la Armada Española.

2. Adquisición de 25 Aviones Eurofighter

Descripción: El Gobierno de España firmó un contrato para adquirir 25 aviones Eurofighter, que fueron ensamblados en las instalaciones de Airbus en Getafe, Madrid. Este encargo formó parte del programa Halcón II y buscaba reemplazar parte de la flota de F-18 del Ejército del Aire y del Espacio.

Resultado: Las entregas, que comenzarán en 2030, pretenden fortalecer las capacidades del ejército español y su rol en la OTAN, además de generar más de 16.000 empleos, que redundan en el compromiso de la nación gobierno con la inversión en defensa y la industria nacional.

3. Puente Ferry Anfibio para Tanques Leopard

Descripción: El Ejército de Tierra español aprobó la adquisición de un nuevo puente anfibio modular de pontones autopropulsados, diseñado para transportar vehículos pesados como los tanques Leopard 2E. Este equipo reemplazará al obsoleto Puente Tablero Flotante (PTF).

- **Resultado:** Con un presupuesto máximo de 82,5 millones de euros, este equipo mejora significativamente la capacidad operativa del Ejército, facilitando operaciones conjuntas con países aliados de la OTAN y la UE.

Estos ejemplos ilustran cómo la CPI en el sector de defensa permite a España desarrollar y adquirir tecnologías innovadoras que mejoran la eficacia y seguridad de sus Fuerzas Armadas, al tiempo que impulsan la industria nacional y la creación de empleo.

6.4 Propuesta de explotación de la CPI y visión de futuro

En la obtención de recursos del Ministerio de Defensa, muy especialmente en la adquisición de recursos TIC, se puede seguir explotando la CPI como herramienta muy valiosa para el desarrollo de tecnologías que satisfagan las nuevas demandas y la evolución en este campo. Siendo así, a continuación se detallan algunos de los aspectos en los que la CPI pudiera tener un carácter muy relevante en el futuro:

- **Modernizar las Fuerzas Armadas:** Fomentando el desarrollo de tecnologías innovadoras en áreas como la ciberseguridad, la inteligencia artificial, la robótica o los sistemas de comunicación.
- **Mejorar la eficiencia:** Ayudando a desarrollar soluciones que mejoren la eficiencia de los procesos del Ministerio de Defensa, como la gestión de recursos, la logística o la formación.
- **Impulsar la industria de la defensa:** Fomentando la participación de empresas españolas en el desarrollo de nuevas tecnologías, contribuyendo al crecimiento económico y la creación de empleo.

Concretándolo en aspectos específicos, empleando la CPI se podrían abordar retos específicos como los siguientes:

- **Ciberseguridad avanzada:** Sistemas de detección y mitigación de amenazas cibernéticas basados en inteligencia artificial y aprendizaje automático.

- **Comunicación segura y resiliente:** Desarrollo de redes de comunicación cuántica o sistemas de encriptación inquebrantable.
- **Gestión de datos masivos:** Soluciones para el análisis en tiempo real de grandes volúmenes de datos estratégicos provenientes de satélites, drones y sensores.
- **Automatización y logística inteligente:** Uso de algoritmos avanzados para optimizar el despliegue de recursos y la logística militar.
- **Redes de comando y control basadas en 5G/6G:** Desarrollo de redes móviles de alta velocidad y baja latencia para uso militar.
- **Sistemas autónomos de defensa cibernética:** Plataformas de inteligencia artificial capaces de identificar y responder automáticamente a ciberamenazas en tiempo real.
- **Software de simulación avanzada:** Herramientas para entrenamientos militares mediante realidad virtual y aumentada.
- **Plataformas descentralizadas de toma de decisiones:** Utilizar blockchain para garantizar transparencia y seguridad en las operaciones logísticas y administrativas.

Para implementar la CPI con éxito, el Ministerio de Defensa podría intentar optimizar algunos procesos que tienen que ver con:

- **Identificar necesidades específicas:** Es fundamental definir con precisión qué necesidades no pueden ser satisfechas con las soluciones existentes y requieren el desarrollo de nuevas tecnologías.
- **Fomentar la participación de empresas:** Se deben establecer mecanismos para que las empresas puedan presentar propuestas innovadoras y recibir apoyo en el desarrollo de las mismas.
- **Simplificar los procesos de contratación:** Los procesos de CPI suelen ser más complejos que los de compra pública tradicional, por lo que es importante simplificarlos para facilitar la participación de las empresas.
- **Evaluar el impacto:** Es importante realizar un seguimiento y evaluación de los proyectos de CPI para asegurar que cumplen con los objetivos y que la inversión realizada se traduce en beneficios para el Ministerio de Defensa.

En resumen, la CPI podría ser una herramienta estratégica para el Ministerio de Defensa, permitiéndole acceder a tecnologías innovadoras, mejorar su eficiencia e impulsar la industria de la defensa española.



Ilustración 18.- Elaboración propia empleando I.A.

7 ANÁLISIS DE LA VISIÓN DE LA EMPRESA

7.1 Introducción.

Se ha propuesto a las tres empresas de sector TIC que se relacionan participar en la confección del cuestionario (anexo II), con el fin de analizar sus respuestas y reflejar en este TFM su visión y experiencia acerca de la contratación de recursos TIC en el Ministerio de Defensa:

- CSA
- COMPUSOF S.A.
- INETUM ESPAÑA.

La participación de empresas privadas en la contratación pública es un elemento clave para el desarrollo y modernización de los sistemas de tecnologías de la información y comunicaciones (TIC) en el ámbito de la defensa. Este capítulo trata de analizar sondear la percepción de las empresas que han participado en concursos públicos del Ministerio de Defensa. Así, a través de sus opiniones, se intentará identificar beneficios, desafíos y áreas de mejora en los procesos de contratación TIC.

7.2 Beneficios que les supone participar en contrataciones del ámbito de la defensa.

Entre los aspectos positivos, las empresas participantes destacaron los aspectos asociados a la contratación TIC en el Ministerio de Defensa siguientes:

- **Ampliación del mercado:** La participación en concursos públicos permite a las empresas acceder a contratos de gran volumen y establecer relaciones estratégicas con el sector público generando dinámicas de perspectiva de negocio estable y con la seguridad que ofrece contratar con el sector público.
- **Innovación tecnológica:** Los contratos en defensa TIC ofrecen una oportunidad para implementar soluciones tecnológicas avanzadas que fortalecen las capacidades de seguridad y operativas, y además les permiten contrastar su grado de competitividad en cuanto a innovación.
- **Estabilidad financiera:** La adjudicación de contratos en defensa, caracterizados por su alta especialización, representa una fuente de ingresos confiable y de largo plazo.
- **Fortalecimiento de la reputación corporativa:** Trabajar con el Ministerio de Defensa refuerza la credibilidad de las empresas en el mercado público y privado.

7.3 Desafíos identificados en el proceso de contratación para las empresas

A pesar de que destacan beneficios sobre los inconvenientes, las empresas enfrentan desafíos significativos en los concursos públicos de TIC en defensa, entre ellos destacan los siguientes:

- **Competencia con Grandes Empresas del Sector:** La elevada competitividad es uno de los principales obstáculos para empresas medianas y pequeñas. Los requisitos técnicos y financieros, diseñados para proyectos de gran escala, favorecen a corporaciones establecidas, limitando la participación de nuevos actores.
- **Complejidad en los Pliegos Técnicos:** Aunque los pliegos técnicos son generalmente claros, algunas empresas refieren ambigüedades y falta de especificidad en ciertos contratos. Esto dificulta la preparación de propuestas adecuadas y genera interpretaciones diversas entre los participantes.
- **Burocracia y Procesos Largos:** El tiempo requerido para completar los procesos administrativos es percibido como un reto. Los procedimientos extensos no solo aumentan los costos indirectos, sino que también pueden desalentar la participación de empresas con recursos limitados.
- **Problemas Técnicos en Plataformas Electrónicas:** Las plataformas digitales de contratación presentan desafíos, especialmente en la gestión de ofertas complejas. Algunas empresas señalaron dificultades técnicas en los portales electrónicos, lo que afecta la transparencia y eficiencia del proceso.
- **Forma de pago en los contratos de larga duración:** Aunque no se haga mención expresa en el formulario, un comentario generalizado entre las empresas, especialmente en los contratos de larga duración, es que resulta determinante para presentarse a una licitación la forma de pago que determine la administración. Si no se establecen pagos parciales o avances en el mismo sobre la ejecución parcial, las empresas son reticentes a presentarse a los concursos que requieren una gran inversión pues tienen que asumir una financiación de los proyectos que, sobre todo para las pequeñas y medianas empresas, es inasumible.

7.4 Perspectiva sobre Innovación y Estrategias

Las empresas participantes valoraron positivamente el enfoque del Ministerio en la modernización tecnológica, aunque identificaron áreas de mejora:

- **Facilitación de Innovaciones Tecnológicas:** En general, las empresas consideran que los procedimientos actuales permiten la incorporación de tecnologías innovadoras en algunos casos, pero podrían optimizarse para fomentar soluciones disruptivas.
- **Alineación Estratégica:** Aunque las estrategias del Ministerio se perciben como alineadas con las necesidades tecnológicas, algunas empresas sugieren ajustes para reflejar mejor los avances del mercado TIC.

7.5 Recomendaciones basadas en las respuestas

A la vista de la información obtenida del formulario se proponen las siguientes recomendaciones para optimizar los procesos de contratación pública TIC, facilitando la gestión que aquéllas tienen que realizar cuando se presentan a un concurso público en nuestro ámbito:

- **Claridad en los Pliegos Técnicos**
 - Redacción más precisa de los requisitos y especificaciones técnicas.
 - Inclusión de ejemplos y casos de uso para evitar ambigüedades.
- **Simplificación de Procesos Administrativos**
 - Reducción de trámites burocráticos mediante la automatización de procesos en plataformas electrónicas.
 - Introducción de plazos más cortos para la adjudicación de contratos.
- **Mejora en las Plataformas de Contratación**
 - Optimización técnica de los portales de licitación para gestionar mejor las ofertas complejas.
 - Capacitación y soporte técnico para los usuarios de las plataformas.

○ **Fomento de la Participación de Empresas Medianas y Pequeñas**

- Diseño de contratos que favorezcan la participación de empresas de menor tamaño, a través de lotes más accesibles y requisitos menos restrictivos.
- Programas de colaboración para facilitar el acceso al mercado público.
- Flexibilidad en los medios de pago de los contratos, sobre todo en aquéllos de alto importe o larga duración para que se establezcan pagos parciales en función de lo ejecutado para que la empresa no tenga que anticipar la financiación durante largo tiempo.

En definitiva, si bien parece que la percepción de las empresas sobre la contratación pública TIC en el Ministerio de Defensa es valorada por los beneficios estratégicos y financieros que ofrecen, los desafíos asociados a la competencia, la burocracia y los requisitos técnicos requieren atención. Implementar las recomendaciones presentadas podría contribuir a optimizar los procesos de contratación, promoviendo una colaboración más eficiente entre el sector público y privado y fortaleciendo las capacidades TIC en el ámbito de la defensa.

7.6 Análisis de la tipología de empresas que participan en licitaciones del MINISDEF

Con las empresas del estudio del caso del punto 5.1 (Infraestructura de Ciberseguridad MINISDEF), se tratará de conocer la tipología de las empresas que se presentan a los concursos públicos, al menos a aquéllos de cierta entidad económica y dificultad técnica, en este ámbito TIC. Se replica a continuación el cuadro de las empresas participantes en aquel contrato con expresión de su país de origen:

EMPRESAS PRESENTADAS	ORIGEN
ACUNTIA S.A.U.	ESPAÑA
ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L.	ESPAÑA
Babel Sistemas de Información, S.L.	ESPAÑA
CENTRO REGIONAL DE SERVICIOS AVANZADOS S.A.	ESPAÑA
Deloitte Advisory, S.L.	REINO UNIDO
EVOLUTIO CLOUD ENABLER S.A.	ESPAÑA
PricewaterhouseCoopers Asesores de Negocios, S.L.	REINO UNIDO
SISTEMAS INFORMATICOS ABIERTOS, S.A.U.	ESPAÑA
THALES ESPAÑA SISTEMAS, S.A.U.	FRANCIA
TRC INFORMATICA, S.L.	ESPAÑA
Telefónica Soluciones de Informática y Comunicaciones de España S.A.U.	ESPAÑA
UTE OESIA-ACCENTURE	ESPAÑA
ACCENTURE	ESTADOS UNIDOS
INETUM	FRANCIA
INNOTECH	ESPAÑA

Tabla 9.- Empresas presentadas al Acuerdo Marco y nacionalidad

Ya se mencionó en el estudio del caso que de las trece empresas que mostraron interés en participar en el acuerdo marco (las últimas dos parejas presentadas en UTE) solamente siete de ellas presentaron finalmente oferta económica y no a todos los lotes objeto del acuerdo marco.

Considerado lo anterior, sería difícil concretar los motivos por los que algunas de esas empresas, todas de una cierta relevancia en el mercado y la gran mayoría multinacionales de prestigio y fuerza en el sector, no presentaron ofertas.

A continuación, se presenta un análisis de la tipología de empresas que participan en las licitaciones del documento "Licitadores Presentados y Admitidos", clasificándolas según los criterios indicados:

Por país de origen:

- **España:** La mayoría de las empresas que participaron en este acuerdo marco son de origen español.

Algunos ejemplos son: Telefónica Soluciones de Informática y Comunicaciones de España S.A.U., TRC INFORMÁTICA, S.L., EVOLUTIO CLOUD ENABLER S.A. y CENTRO REGIONAL DE SERVICIOS AVANZADOS S.A., entre otras.

- **Internacional:** Hay empresas con presencia internacional que también participan en las licitaciones.

Como por ejemplo ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L. e INETUM (de origen francés) y PricewaterhouseCoopers Asesores de Negocios, S.L. (de origen británico), INETUM.

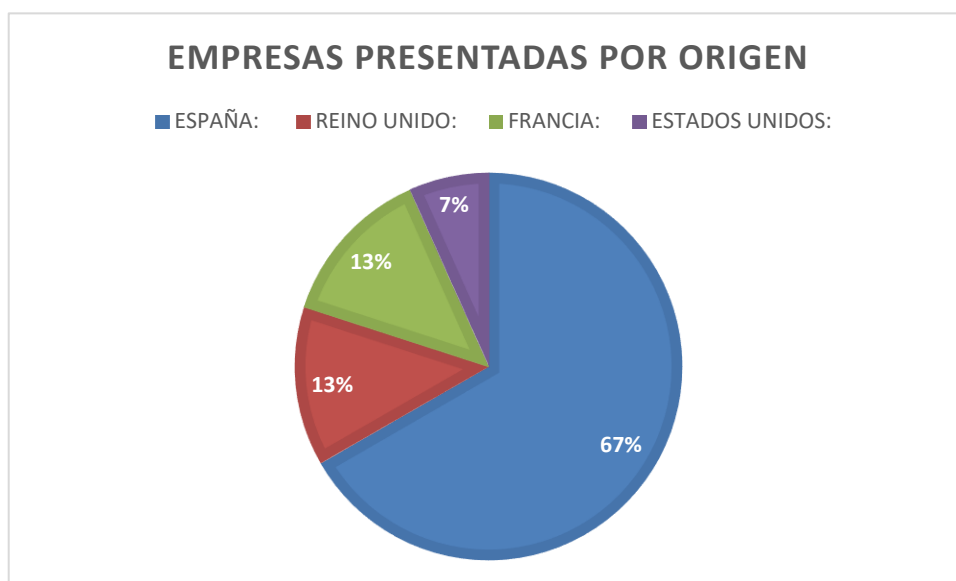


Ilustración 19.- Elaboración propia con los datos del acuerdo marco.

Tamaño de las empresas:

- **Grandes corporaciones:** Hay grandes corporaciones con una amplia presencia en el mercado, como Telefónica Soluciones de Informática y Comunicaciones de España S.A.U., ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L. y PricewaterhouseCoopers Asesores de Negocios, S.L., entre otras.
- **Pymes:** También hay pymes que participan en las licitaciones, como TRC INFORMÁTICA, S.L. y CENTRO REGIONAL DE SERVICIOS AVANZADOS S.A.

Áreas tecnológicas:

- **Consultoría:** Hay empresas especializadas en consultoría, como Deloitte Advisory, S.L. y PricewaterhouseCoopers Asesores de Negocios, S.L., que pueden ofrecer servicios de asesoramiento y análisis en materia de ciberseguridad.
- **Servicios de tecnologías de la información:** Hay empresas especializadas en servicios de tecnologías de la información, como Telefónica Soluciones de Informática y Comunicaciones de España S.A.U., ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L. y EVOLUTIO CLOUD ENABLER S.A., que pueden ofrecer servicios de desarrollo, implantación y mantenimiento de sistemas de ciberseguridad.
- **Integración de sistemas:** Hay empresas especializadas en integración de sistemas, como TRC INFORMÁTICA, S.L. y SISTEMAS INFORMATICOS ABIERTOS, S.A.U., que pueden ofrecer servicios de integración de diferentes soluciones de ciberseguridad.
- **Seguridad de la información:** Hay empresas especializadas en seguridad de la información, como THALES ESPAÑA SISTEMAS, S.A.U., que pueden ofrecer soluciones específicas para la protección de la información.

Conclusión:

Se observa que la participación de empresas es diversa, aunque predominan aquéllas con origen en España y las grandes corporaciones del sector de las TIC. Las pymes se presentan bien por sí mismas o formando UTE con corporaciones de otros países, a un limitado número de lotes en aquéllos más compatible con su actividad.

El acuerdo marco ha despertado el interés de diferentes actores del sector de la ciberseguridad, lo que, teóricamente, puede haber redundado en una mayor competitividad y en la obtención de mejores soluciones para la Administración en un proyecto tan complejo que resulta más manejable para las pymes por la división en lotes o haciendo sinergias presentándose en UTEs con otras empresas que complementan su especialización.

8 RESULTADOS – ANÁLISIS CRÍTICO

Este capítulo final sintetiza los hallazgos obtenidos en el análisis de los procesos de contratación TIC en el Ministerio de Defensa. Además, se presentan recomendaciones concretas para mejorar dichos procesos, con un enfoque en adaptabilidad, seguridad y eficiencia y sostenibilidad.

- **Eficiencia y Optimización de Recursos a través de Acuerdos Marco:**

Los acuerdos marco han demostrado ser una herramienta eficaz para la contratación de TIC en el MINISDEF, centralizando adquisiciones y permitiendo un uso eficiente del presupuesto. Esta metodología ha facilitado la estandarización y cohesión de los sistemas de TIC en todas las unidades del Ministerio, promoviendo la interoperabilidad.

Sin embargo, la estructura rígida de los acuerdos marco puede dificultar la incorporación de tecnologías emergentes y adaptadas a necesidades específicas de cada unidad, limitando la flexibilidad que exige el ámbito de defensa.

Para mejorar la respuesta a las necesidades tecnológicas locales, se sugiere crear **variantes de acuerdos marco** que permitan personalizar los servicios TIC para cada unidad o área específica. Estos acuerdos podrían incluir cláusulas que flexibilicen la implementación en función de las particularidades de cada área, optimizando la capacidad de respuesta ante demandas tecnológicas concretas.

Esta medida permitiría una mayor autonomía en las unidades y aseguraría que los sistemas TIC se adapten mejor a las realidades operativas de cada área, sin perder los beneficios de la centralización.

- **Seguridad y Confidencialidad en Procedimientos Negociados sin Publicidad:**

Los procedimientos negociados sin publicidad han permitido al MINISDEF adquirir tecnologías de alta sensibilidad sin comprometer la seguridad de la información. Esta modalidad ha resultado adecuada para la adquisición de sistemas que requieren confidencialidad en todas las fases del proceso de contratación.

A pesar de su efectividad en términos de seguridad, este enfoque reduce la competencia entre proveedores, lo cual podría limitar la diversidad de soluciones tecnológicas y, en algunos casos, incrementar los costos.

- **Impacto del Aumento Presupuestario en la Transformación Digital y Ciberseguridad:**

El incremento en el presupuesto destinado a TIC ha permitido al MINISDEF avanzar en su transformación digital y mejorar su ciberseguridad. Estos fondos han facilitado la modernización de infraestructuras críticas y la implementación de medidas avanzadas de protección contra amenazas cibernéticas.

Sin embargo, el crecimiento presupuestario exige una planificación y revisión constante para asegurar que los recursos se asignen de manera óptima y alineada con los objetivos estratégicos del MINISDEF, evitando gastos innecesarios o redundantes.

- **Necesidad de Evaluación y Control de Calidad en Contratación TIC:**

Los mecanismos de validación y auditoría han sido efectivos en el control de calidad de los contratos TIC, garantizando que los sistemas contratados cumplan con los requisitos de interoperabilidad y seguridad establecidos.

No obstante, los procesos de evaluación podrían beneficiarse de la implementación de métricas de rendimiento específicas, que permitan evaluar el impacto y la eficiencia de cada proyecto TIC en términos cuantificables, optimizando futuras decisiones de inversión.

- **Retos en la Adopción de Nuevas Tecnologías:**

La rápida evolución de las TIC en defensa y seguridad plantea desafíos para la contratación pública, ya que los procedimientos actuales no siempre permiten adaptarse con rapidez a las innovaciones tecnológicas. Esto puede limitar la capacidad del MINISDEF para implementar tecnologías de vanguardia que mejoren su operatividad y eficiencia.

La falta de flexibilidad en la normativa actual implica una oportunidad de mejora en los procesos de contratación, sobre todo en el contexto de tecnologías emergentes y soluciones de alto impacto.

- **Fomento de la Innovación a través de Procedimientos Flexibles:**

Se recomienda revisar la normativa para facilitar la adopción de tecnologías emergentes, permitiendo procesos de contratación más ágiles y accesibles. La introducción de contratos de innovación o acuerdos marco específicos para soluciones tecnológicas avanzadas podría permitir

al MINISDEF beneficiarse de las últimas innovaciones en ciberseguridad, inteligencia artificial y blockchain.

- **Adopción de Contratos de Innovación para Soluciones Tecnológicas Emergentes:**

Se recomienda la creación de **contratos de innovación** que permitan la incorporación de tecnologías emergentes en el ámbito de defensa. Estos contratos podrían ofrecer una estructura más flexible para adoptar tecnologías como la inteligencia artificial, el big data o el blockchain, que requieren procesos de contratación más ágiles y menos restrictivos.

Este enfoque permitiría al MINISDEF mantenerse a la vanguardia en términos tecnológicos y mejorar la operatividad de sus sistemas de defensa, adaptándose rápidamente a las nuevas herramientas del mercado.

- **Implementación de Indicadores de Rendimiento en Contratos TIC:**

Es fundamental establecer **indicadores de rendimiento** (KPIs) para evaluar la eficiencia y efectividad de los contratos TIC. Estos indicadores podrían incluir métricas como el tiempo de respuesta ante incidencias, la disponibilidad del sistema, el consumo energético y el costo por usuario, ayudando al MINISDEF a optimizar el uso del presupuesto y garantizar la sostenibilidad de sus sistemas tecnológicos.

Con estos indicadores, el MINISDEF podría realizar un seguimiento más detallado del rendimiento de los sistemas TIC y tomar decisiones informadas para futuras contrataciones, asegurando la rentabilidad y la sostenibilidad de sus inversiones tecnológicas.

- **Fortalecimiento de la Seguridad en la Cadena de Suministro TIC:**

Dada la relevancia de la ciberseguridad, es esencial establecer estándares de seguridad más estrictos en la cadena de suministro de TIC. Esto podría incluir requisitos de certificación en ciberseguridad para los proveedores y auditorías de seguridad periódicas para verificar la integridad de los sistemas TIC contratados.

Estas medidas garantizarían que los sistemas TIC cumplan con los estándares de seguridad más altos y reducirían los riesgos de ciberamenazas derivadas de la cadena de suministro.

- **Revisión Continua y Ciclo de Mejora en Procesos de Contratación:**

Se recomienda realizar revisiones periódicas de los procesos de contratación TIC, con base en un ciclo de mejora continua que considere las lecciones aprendidas de proyectos anteriores. Esta revisión podría incluir la actualización de los procedimientos en función de las experiencias previas y de las innovaciones del mercado.

El análisis continuo de los procesos permitiría al MINISDEF adaptarse de manera proactiva a las necesidades de un entorno en constante cambio y optimizaría la eficiencia y efectividad de los contratos TIC.

- **Fomento de Colaboración Internacional en Contratación de TIC:**

Dada la importancia de la interoperabilidad y la compatibilidad en el ámbito de la defensa, se sugiere fomentar la colaboración internacional en la contratación de TIC, especialmente con países aliados y en el contexto de la OTAN. La adquisición conjunta de tecnologías podría generar economías de escala y mejorar la compatibilidad operativa.

Además, la cooperación internacional en TIC permitiría al MINISDEF acceder a soluciones tecnológicas de vanguardia y compartir experiencias y mejores prácticas con otros países en el sector de defensa.

- **Fortalecimiento de la Capacitación en Ciberseguridad y Gestión TIC:**

La capacitación continua en ciberseguridad y en la gestión de tecnologías avanzadas es fundamental para el personal del MINISDEF. Invertir en formación permitirá que el personal esté preparado para manejar de manera adecuada los sistemas TIC y proteja la infraestructura del Ministerio ante posibles ciberamenazas.

Esta formación debería incluir no solo conocimientos técnicos, sino también mejores prácticas en seguridad de la información y procedimientos de respuesta a incidentes, mejorando así la capacidad de reacción del Ministerio ante posibles riesgos.

9 BIBLIOGRAFÍA

1. **Ley 9/2017, de Contratos del Sector Público.** (2017). Boletín Oficial del Estado.
2. **Ley 24/2011, de Contratos del Sector Público en los Ámbitos de Defensa y Seguridad.** (2011).
3. **Ministerio de Defensa.** (2023). *Memoria de Contratación del Ministerio de Defensa 2023.*
4. **Ministerio de Defensa.** (2022). *Guía de Contratación Basada en Acuerdos Marco.*
5. **Orden DEF/2639/2015: Política de Sistemas y Tecnologías de la Información y las Comunicaciones (Política CIS/TIC).** (2015).
6. **Ministerio de Defensa.** (2016). *Arquitectura Global de Sistemas y Tecnologías de la Información y Comunicaciones (AG CIS/TIC).*
7. **Ministerio de Defensa.** (2023). *Plan de Transformación Digital del MINISDEF.*
8. **Ministerio de Hacienda.** (2023). *Presupuestos Generales del Estado 2023.*
9. **Unión Europea.** (2021). *Reglamento 2021/241 por el que se establece el Mecanismo de Recuperación y Resiliencia.* Diario Oficial de la Unión Europea. Recuperado de <https://eur-lex.europa.eu> .
10. **Estrategia TIC de la Administración General del Estado (AGE).**
11. **Memoria de Contratación Pública del Ministerio de Defensa (2022).**
12. **Estadística de Asuntos Económicos del Ministerio de Defensa (2022).**
13. **Guía de Contratación Pública del MINISDEF.**
14. **Marco Estratégico de Sistemas y Tecnologías de la Información y Comunicaciones del MINISDEF.** (2022).
15. **Evolución histórica contratación TIC en el MINISDEF.** Memoria de contratación del Ministerio de Defensa, 2023.
16. https://www.huffingtonpost.es/sociedad/asombro-superpotencias-mundiales-historica-mejora-submarino-espanol-futuro-rp.html?utm_source=chatgpt.com
17. https://www.huffingtonpost.es/sociedad/asombro-superpotencias-mundiales-historica-mejora-submarino-espanol-futuro-rp.html?utm_source=chatgpt.com
18. https://www.huffingtonpost.es/sociedad/luz-verde-gran-puente-ferry-anfibio-apto-tanques-leopard-deseado-ejercito-espanol.html?utm_source=chatgpt.com

Anexo I (glosario de términos)

Término/Abreviatura	Definición
AGE	Administración General del Estado. Órgano de administración pública en España que gestiona y coordina los servicios y políticas del Estado.
AG CIS/TIC	Arquitectura Global de Sistemas y Tecnologías de la Información y Comunicaciones. Marco del MINISDEF que establece los estándares para la interoperabilidad y seguridad de los sistemas TIC en Defensa.
AI	Inteligencia Artificial. Conjunto de tecnologías que permiten a los sistemas realizar tareas que requieren inteligencia humana, como el aprendizaje, la toma de decisiones y el reconocimiento de patrones.
Big Data	Procesamiento y análisis de grandes volúmenes de datos que no pueden gestionarse con herramientas tradicionales debido a su tamaño, velocidad y variedad.
Blockchain	Tecnología de registro distribuido que garantiza la seguridad y transparencia de las transacciones de datos a través de una cadena de bloques verificable y descentralizada.
CESTIC	Centro de Sistemas y Tecnologías de la Información y Comunicaciones. Unidad del MINISDEF encargada de gestionar, supervisar y mantener la infraestructura TIC en el Ministerio.
Ciberseguridad	Conjunto de prácticas y tecnologías destinadas a proteger sistemas, redes y datos de accesos no autorizados y ciberataques.
Contrato de Innovación	Contrato público que facilita la adquisición de soluciones tecnológicas innovadoras, permitiendo flexibilidad en los procesos de contratación para integrar nuevas tecnologías.
DFARS	Defense Federal Acquisition Regulation Supplement. Normativa de contratación del Departamento de Defensa de los Estados Unidos, que regula la adquisición de bienes y servicios para defensa.

Término/Abreviatura	Definición
DoD	Department of Defense. Ministerio de Defensa de los Estados Unidos, responsable de la seguridad nacional y la defensa de ese país.
FAR	Federal Acquisition Regulation. Normativa que regula las contrataciones del gobierno de los Estados Unidos, incluyendo los contratos en el ámbito de defensa.
I3D	Infraestructura Integral de Información para la Defensa. Sistema del MINISDEF que unifica y centraliza los servicios TIC en todas las unidades del Ministerio.
IDS	Intrusion Detection System (Sistema de Detección de Intrusiones). Herramienta de ciberseguridad que monitoriza la red en busca de actividades sospechosas y posibles amenazas.
Interoperabilidad	Capacidad de los sistemas y organizaciones para operar conjuntamente y compartir información de manera efectiva y segura. Es esencial en el ámbito de defensa para la colaboración entre diferentes unidades y países.
KPI	Key Performance Indicator (Indicador Clave de Desempeño). Métrica utilizada para evaluar la eficacia y el rendimiento de un proceso o inversión.
Ley 9/2017	Ley de Contratos del Sector Público en España. Regula la contratación pública para fomentar la transparencia y la eficiencia en el uso de los recursos públicos.
Ley 24/2011	Ley de Contratos del Sector Público en los ámbitos de Defensa y Seguridad. Normativa española que adapta la contratación en defensa a requisitos de seguridad y confidencialidad.
MINISDEF	Ministerio de Defensa de España. Órgano gubernamental encargado de la política de defensa y la seguridad nacional.
MOD	Ministry of Defence (Ministerio de Defensa). Nombre del Ministerio de Defensa en el Reino Unido.

Término/Abreviatura	Definición
OTA	Other Transaction Authority. Procedimiento de contratación en Estados Unidos que permite la colaboración directa con empresas de innovación sin los requisitos formales de contratación pública.
OTAN	Organización del Tratado del Atlántico Norte. Alianza de defensa intergubernamental que incluye a varios países, incluyendo España, y fomenta la cooperación y defensa conjunta.
PPT	Pliego de Prescripciones Técnicas. Documento contractual que detalla los requisitos técnicos y operativos de un contrato, incluyendo los estándares de calidad y seguridad.
ROI	Return on Investment (Retorno de la Inversión). Indicador financiero que mide la rentabilidad de una inversión en relación con su costo.
SOC	Security Operations Center (Centro de Operaciones de Seguridad). Equipo responsable de monitorizar y gestionar la seguridad de las redes y sistemas de una organización.
TIC	Tecnologías de la Información y Comunicaciones. Conjunto de tecnologías dedicadas a gestionar, transmitir y almacenar información. Incluye sistemas informáticos, redes de comunicación y soluciones de ciberseguridad.

Anexo II (Cuestionario empresas)

Contratación Pública de Recursos TIC en el Ministerio de Defensa

Objeto.- Obtener información sobre la percepción de las empresas privadas de proceso de obtención de recursos TIC en el Ministerio de Defensa a través de la contratación pública. Esa información se utilizará en el trabajo fin de máster en Dirección TIC para la Defensa “PARTICULARIDADES DE LA OBTENCIÓN DE RECURSOS TIC A TRAVÉS DE LA CONTRATACIÓN PÚBLICA EN EL ÁMBITO DEL MINISTERIO DE DEFENSA”, cuyo autor es el Capitán de Corbeta de la Armada Víctor Manuel Grande Corral.

Se tratará de identificar áreas de mejora en el proceso de contratación pública para facilitar el desarrollo de estrategias más efectivas y transparentes.

Tratamiento.- La información obtenida se empleará a los exclusivos efectos de documentar el trabajo descrito, respetándose el anonimato de las empresas que proporcionen la información en caso de que aquéllas no quieran figurar como fuente.

Información General

1. **Nombre de la Empresa:** Haga clic o pulse aquí para escribir texto.
2. **Nombre del Contacto:** Haga clic o pulse aquí para escribir texto.
3. **Cargo del Contacto:** Haga clic o pulse aquí para escribir texto.
4. **Teléfono y Correo Electrónico:** Haga clic o pulse aquí para escribir texto.
5. **Fecha:** Haga clic aquí o pulse para escribir una fecha.

Sección A: Participación en Concursos Públicos del Ministerio de Defensa

1. ¿Ha participado su empresa en concursos públicos del Ministerio de Defensa para la contratación de recursos TIC?
 - ☐ Sí
 - ☐ No
2. Si la respuesta es "Sí", ¿con qué frecuencia participa su empresa en estos concursos?
 - ☐ Regularmente (varias veces al año)
 - ☐ Ocasionalmente (una vez al año)
 - ☐ Raramente (menos de una vez al año)
 - ☐ Otra (especifique): Haga clic o pulse aquí para escribir texto.
3. ¿Cuáles considera que son los principales beneficios de participar en estos concursos? (Seleccione los que apliquen)
 - ☐ Ampliar el mercado de la empresa
 - ☐ Acceso a contratos de gran volumen

- ☐ Oportunidad de innovación en TIC
- ☐ Fortalecer la relación con el sector público
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

Sección B: Proceso de Participación y Evaluación de Ofertas

4. ¿Cómo evaluaría el proceso de participación en concursos públicos en cuanto a simplicidad y transparencia?
 - ☐ Muy Satisfactorio
 - ☐ Satisfactorio
 - ☐ Neutral
 - ☐ Insatisfactorio
 - ☐ Muy Insatisfactorio
5. ¿Considera que los requisitos de los pliegos técnicos son claros y específicos?
 - ☐ Sí, completamente
 - ☐ Sí, en la mayoría de los casos
 - ☐ A veces
 - ☐ No, suelen ser ambiguos
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.
6. ¿Cómo considera la competitividad en estos concursos?
 - ☐ Muy Alta
 - ☐ Alta
 - ☐ Moderada
 - ☐ Baja
7. ¿Cuál es su nivel de satisfacción con la transparencia en los criterios de evaluación y adjudicación?
 - ☐ Muy Satisfecho
 - ☐ Satisfecho
 - ☐ Neutral
 - ☐ Insatisfecho
 - ☐ Muy Insatisfecho

Sección C: Normativas y Requisitos Específicos de Defensa

8. En su experiencia, compare cómo de exigentes son los requisitos de seguridad y confidencialidad en comparación con otros concursos de TIC en el sector público?
- ☐ Mucho más exigentes
 - ☐ Algo más exigentes
 - ☐ Similares
 - ☐ Menos exigentes
9. ¿Considera que su empresa cumple fácilmente con los requisitos específicos del Ministerio de Defensa?
- ☐ Sí, completamente
 - ☐ Sí, en la mayoría de los casos
 - ☐ No, algunos requisitos son difíciles de cumplir
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.
10. ¿Cree que los procedimientos de contratación del Ministerio de Defensa facilitan la incorporación de innovaciones tecnológicas?
- ☐ Sí, totalmente
 - ☐ Sí, en algunos casos
 - ☐ No, es difícil innovar
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

Sección D: Desafíos y Mejora del Proceso de Contratación

11. ¿Cuáles son los principales desafíos que su empresa enfrenta al participar en concursos del Ministerio de Defensa? (Seleccione los que apliquen)
- ☐ Complejidad en los requisitos de seguridad
 - ☐ Falta de claridad en los pliegos técnicos
 - ☐ Competencia de grandes empresas del sector
 - ☐ Proceso largo y burocrático
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

12. En su opinión, ¿qué mejoras se podrían implementar en el proceso de contratación de TIC en el Ministerio de Defensa?

- Respuesta libre: Haga clic o pulse aquí para escribir texto.

13. ¿Hay algún aspecto específico de la contratación de TIC en Defensa que le gustaría que mejorara? (especificar)

Haga clic o pulse aquí para escribir texto.

Sección E: Opinión sobre la Estrategia de Contratación de TIC en Defensa

14. ¿Cree que el Ministerio de Defensa fomenta adecuadamente la participación de empresas tecnológicas nacionales?

- ☐ Sí
- ☐ No
- ☐ No tengo una opinión formada

15. ¿Considera que las estrategias de contratación de TIC actuales del Ministerio de Defensa están alineadas con las necesidades tecnológicas actuales del sector?

- ☐ Sí, completamente
- ☐ Sí, en algunos aspectos
- ☐ No, existen áreas de mejora
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

16. Comentarios adicionales sobre la contratación pública de TIC en el Ministerio de Defensa:

- Respuesta libre: Haga clic o pulse aquí para escribir texto.

*Anexo III (CSA)***Contratación Pública de Recursos TIC en el Ministerio de Defensa**

Objeto.- Obtener información sobre la percepción de las empresas privadas de proceso de obtención de recursos TIC en el Ministerio de Defensa a través de la contratación pública. Esa información se utilizará en el trabajo fin de máster en Dirección TIC para la Defensa “PARTICULARIDADES DE LA OBTENCIÓN DE RECURSOS TIC A TRAVÉS DE LA CONTRATACIÓN PÚBLICA EN EL ÁMBITO DEL MINISTERIO DE DEFENSA”, cuyo autor es el Capitán de Corbeta de la Armada Víctor Manuel Grande Corral.

Se tratará de identificar áreas de mejora en el proceso de contratación pública para facilitar el desarrollo de estrategias más efectivas y transparentes.

Tratamiento.- La información obtenida se empleará a los exclusivos efectos de documentar el trabajo descrito, respetándose el anonimato de las empresas que proporcionen la información en caso de que aquéllas no quieran figurar como fuente.

Información General

6. **Nombre de la Empresa:** CSA
7. **Nombre del Contacto:** Elena Casado
8. **Cargo del Contacto:** Desarrollo de negocio
9. **Teléfono y Correo Electrónico:** elena.casado@csa.es
10. **Fecha:** 18/11/2024

Sección A: Participación en Concursos Públicos del Ministerio de Defensa

4. ¿Ha participado su empresa en concursos públicos del Ministerio de Defensa para la contratación de recursos TIC?
 - ☒ Sí
 - ☐ No
5. Si la respuesta es "Sí", ¿con qué frecuencia participa su empresa en estos concursos?
 - ☒ Regularmente (varias veces al año)
 - ☐ Ocasionalmente (una vez al año)
 - ☐ Raramente (menos de una vez al año)
 - ☐ Otra (especifique): Haga clic o pulse aquí para escribir texto.
6. ¿Cuáles considera que son los principales beneficios de participar en estos concursos? (Seleccione los que apliquen)
 - ☒ Ampliar el mercado de la empresa
 - ☐ Acceso a contratos de gran volumen
 - ☒ Oportunidad de innovación en TIC

- ☒ Fortalecer la relación con el sector público
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

Sección B: Proceso de Participación y Evaluación de Ofertas

8. ¿Cómo evaluaría el proceso de participación en concursos públicos en cuanto a simplicidad y transparencia?
- ☐ Muy Satisfactorio
 - ☒ Satisfactorio
 - ☐ Neutral
 - ☐ Insatisfactorio
 - ☐ Muy Insatisfactorio
9. ¿Considera que los requisitos de los pliegos técnicos son claros y específicos?
- ☒ Sí, completamente
 - ☐ Sí, en la mayoría de los casos
 - ☐ A veces
 - ☐ No, suelen ser ambiguos
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.
10. ¿Cómo considera la competitividad en estos concursos?
- ☒ Muy Alta
 - ☐ Alta
 - ☐ Moderada
 - ☐ Baja
11. ¿Cuál es su nivel de satisfacción con la transparencia en los criterios de evaluación y adjudicación?
- ☐ Muy Satisfecho
 - ☒ Satisfecho
 - ☐ Neutral
 - ☐ Insatisfecho
 - ☐ Muy Insatisfecho

Sección C: Normativas y Requisitos Específicos de Defensa

11. En su experiencia, compare cómo de exigentes son los requisitos de seguridad y confidencialidad en comparación con otros concursos de TIC en el sector público?
- ☐ Mucho más exigentes
 - ☐ Algo más exigentes
 - ☒ Similares
 - ☐ Menos exigentes
12. ¿Considera que su empresa cumple fácilmente con los requisitos específicos del Ministerio de Defensa?
- ☒ Sí, completamente
 - ☐ Sí, en la mayoría de los casos
 - ☐ No, algunos requisitos son difíciles de cumplir
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.
13. ¿Cree que los procedimientos de contratación del Ministerio de Defensa facilitan la incorporación de innovaciones tecnológicas?
- ☐ Sí, totalmente
 - ☒ Sí, en algunos casos
 - ☐ No, es difícil innovar
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

Sección D: Desafíos y Mejora del Proceso de Contratación

14. ¿Cuáles son los principales desafíos que su empresa enfrenta al participar en concursos del Ministerio de Defensa? (Seleccione los que apliquen)
- ☐ Complejidad en los requisitos de seguridad
 - ☐ Falta de claridad en los pliegos técnicos
 - ☐ Competencia de grandes empresas del sector
 - ☒ Proceso largo y burocrático
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

15. En su opinión, ¿qué mejoras se podrían implementar en el proceso de contratación de TIC en el Ministerio de Defensa?

- Respuesta libre: Haga clic o pulse aquí para escribir texto.

16. ¿Hay algún aspecto específico de la contratación de TIC en Defensa que le gustaría que mejorara? (especificar)

Haga clic o pulse aquí para escribir texto.

Sección E: Opinión sobre la Estrategia de Contratación de TIC en Defensa

17. ¿Cree que el Ministerio de Defensa fomenta adecuadamente la participación de empresas tecnológicas nacionales?

- ☐ Sí
- ☐ No
- ☒ No tengo una opinión formada

18. ¿Considera que las estrategias de contratación de TIC actuales del Ministerio de Defensa están alineadas con las necesidades tecnológicas actuales del sector?

- ☐ Sí, completamente
- ☒ Sí, en algunos aspectos
- ☐ No, existen áreas de mejora
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

19. Comentarios adicionales sobre la contratación pública de TIC en el Ministerio de Defensa:

- Respuesta libre: Haga clic o pulse aquí para escribir texto.

Anexo IV (COMPUSOF)

Contratación Pública de Recursos TIC en el Ministerio de Defensa

Objeto.- Obtener información sobre la percepción de las empresas privadas de proceso de obtención de recursos TIC en el Ministerio de Defensa a través de la contratación pública. Esa información se utilizará en el trabajo fin de máster en Dirección TIC para la Defensa “PARTICULARIDADES DE LA OBTENCIÓN DE RECURSOS TIC A TRAVÉS DE LA CONTRATACIÓN PÚBLICA EN EL ÁMBITO DEL MINISTERIO DE DEFENSA”, cuyo autor es el Capitán de Corbeta de la Armada Víctor Manuel Grande Corral.

Se tratará de identificar áreas de mejora en el proceso de contratación pública para facilitar el desarrollo de estrategias más efectivas y transparentes.

Tratamiento.- La información obtenida se empleará a los exclusivos efectos de documentar el trabajo descrito, respetándose el anonimato de las empresas que proporcionen la información en caso de que aquéllas no quieran figurar como fuente.

Información General

- 11. **Nombre de la Empresa:** COMPUSOF, S.A.
- 12. **Nombre del Contacto:** Jaime Sampedro y Bosch
- 13. **Cargo del Contacto:** Account Manager
- 14. **Teléfono y Correo Electrónico:** 677 933 163 / Jaime_sampedro@compusof.com
- 15. **Fecha:** 18/11/2024

Sección A: Participación en Concursos Públicos del Ministerio de Defensa

- 7. ¿Ha participado su empresa en concursos públicos del Ministerio de Defensa para la contratación de recursos TIC?
 - ☒ Sí
 - ☐ No
- 8. Si la respuesta es "Sí", ¿con qué frecuencia participa su empresa en estos concursos?
 - ☒ Regularmente (varias veces al año)
 - ☐ Ocasionalmente (una vez al año)
 - ☐ Raramente (menos de una vez al año)
 - ☐ Otra (especifique): Haga clic o pulse aquí para escribir texto.
- 9. ¿Cuáles considera que son los principales beneficios de participar en estos concursos? (Seleccione los que apliquen)
 - ☒ Ampliar el mercado de la empresa
 - ☒ Acceso a contratos de gran volumen
 - ☒ Oportunidad de innovación en TIC

- ☒ Fortalecer la relación con el sector público
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

Sección B: Proceso de Participación y Evaluación de Ofertas

12. ¿Cómo evaluaría el proceso de participación en concursos públicos en cuanto a simplicidad y transparencia?

- ☐ Muy Satisfactorio
- ☒ Satisfactorio
- ☐ Neutral
- ☐ Insatisfactorio
- ☐ Muy Insatisfactorio

13. ¿Considera que los requisitos de los pliegos técnicos son claros y específicos?

- ☐ Sí, completamente
- ☒ Sí, en la mayoría de los casos
- ☐ A veces
- ☐ No, suelen ser ambiguos
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

14. ¿Cómo considera la competitividad en estos concursos?

- ☒ Muy Alta
- ☐ Alta
- ☐ Moderada
- ☐ Baja

15. ¿Cuál es su nivel de satisfacción con la transparencia en los criterios de evaluación y adjudicación?

- ☐ Muy Satisfecho
- ☒ Satisfecho
- ☐ Neutral
- ☐ Insatisfecho
- ☐ Muy Insatisfecho

Sección C: Normativas y Requisitos Específicos de Defensa

14. En su experiencia, compare cómo de exigentes son los requisitos de seguridad y confidencialidad en comparación con otros concursos de TIC en el sector público?
- ☐ Mucho más exigentes
 - ☒ Algo más exigentes
 - ☐ Similares
 - ☐ Menos exigentes
15. ¿Considera que su empresa cumple fácilmente con los requisitos específicos del Ministerio de Defensa?
- ☐ Sí, completamente
 - ☒ Sí, en la mayoría de los casos
 - ☐ No, algunos requisitos son difíciles de cumplir
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.
16. ¿Cree que los procedimientos de contratación del Ministerio de Defensa facilitan la incorporación de innovaciones tecnológicas?
- ☐ Sí, totalmente
 - ☒ Sí, en algunos casos
 - ☐ No, es difícil innovar
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

Sección D: Desafíos y Mejora del Proceso de Contratación

17. ¿Cuáles son los principales desafíos que su empresa enfrenta al participar en concursos del Ministerio de Defensa? (Seleccione los que apliquen)
- ☐ Complejidad en los requisitos de seguridad
 - ☐ Falta de claridad en los pliegos técnicos
 - ☒ Competencia de grandes empresas del sector
 - ☐ Proceso largo y burocrático
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

18. En su opinión, ¿qué mejoras se podrían implementar en el proceso de contratación de TIC en el Ministerio de Defensa?

- Respuesta libre: Haga clic o pulse aquí para escribir texto.

19. ¿Hay algún aspecto específico de la contratación de TIC en Defensa que le gustaría que mejorara? (especificar)

Haga clic o pulse aquí para escribir texto.

Sección E: Opinión sobre la Estrategia de Contratación de TIC en Defensa

20. ¿Cree que el Ministerio de Defensa fomenta adecuadamente la participación de empresas tecnológicas nacionales?

- ☒ Sí
- ☐ No
- ☐ No tengo una opinión formada

21. ¿Considera que las estrategias de contratación de TIC actuales del Ministerio de Defensa están alineadas con las necesidades tecnológicas actuales del sector?

- ☒ Sí, completamente
- ☐ Sí, en algunos aspectos
- ☐ No, existen áreas de mejora
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

22. Comentarios adicionales sobre la contratación pública de TIC en el Ministerio de Defensa:

- Respuesta libre: Haga clic o pulse aquí para escribir texto.

*Anexo V (INETUM)***Contratación Pública de Recursos TIC en el Ministerio de Defensa**

Objeto.- Obtener información sobre la percepción de las empresas privadas de proceso de obtención de recursos TIC en el Ministerio de Defensa a través de la contratación pública. Esa información se utilizará en el trabajo fin de máster en Dirección TIC para la Defensa “PARTICULARIDADES DE LA OBTENCIÓN DE RECURSOS TIC A TRAVÉS DE LA CONTRATACIÓN PÚBLICA EN EL ÁMBITO DEL MINISTERIO DE DEFENSA”, cuyo autor es el Capitán de Corbeta de la Armada Víctor Manuel Grande Corral.

Se tratará de identificar áreas de mejora en el proceso de contratación pública para facilitar el desarrollo de estrategias más efectivas y transparentes.

Tratamiento.- La información obtenida se empleará a los exclusivos efectos de documentar el trabajo descrito, respetándose el anonimato de las empresas que proporcionen la información en caso de que aquéllas no quieran figurar como fuente.

Información General

16. **Nombre de la Empresa:** INETUM ESPAÑA

17. **Nombre del Contacto:** FRANCISCO JOSE MONESMA ALVARO

18. **Cargo del Contacto:** Director de Sector de Defensa

19. **Teléfono y Correo Electrónico:** 683147331, fjose.monesma@inetum.com

20. **Fecha:** 15/11/2024

Sección A: Participación en Concursos Públicos del Ministerio de Defensa

10. ¿Ha participado su empresa en concursos públicos del Ministerio de Defensa para la contratación de recursos TIC?

- ☒ Sí
- ☐ No

11. Si la respuesta es "Sí", ¿con qué frecuencia participa su empresa en estos concursos?

- ☒ Regularmente (varias veces al año)
- ☐ Ocasionalmente (una vez al año)
- ☐ Raramente (menos de una vez al año)
- ☒ Otra (especifique): Varias veces al mes

12. ¿Cuáles considera que son los principales beneficios de participar en estos concursos?
(Seleccione los que apliquen)

- ☒ Ampliar el mercado de la empresa
- ☒ Acceso a contratos de gran volumen
- ☒ Oportunidad de innovación en TIC

- ☒ Fortalecer la relación con el sector público
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

Sección B: Proceso de Participación y Evaluación de Ofertas

16. ¿Cómo evaluaría el proceso de participación en concursos públicos en cuanto a simplicidad y transparencia?

- ☐ Muy Satisfactorio
- ☐ Satisfactorio
- ☒ Neutral
- ☐ Insatisfactorio
- ☐ Muy Insatisfactorio

17. ¿Considera que los requisitos de los pliegos técnicos son claros y específicos?

- ☐ Sí, completamente
- ☐ Sí, en la mayoría de los casos
- ☒ A veces
- ☐ No, suelen ser ambiguos
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

18. ¿Cómo considera la competitividad en estos concursos?

- ☒ Muy Alta
- ☐ Alta
- ☐ Moderada
- ☐ Baja

19. ¿Cuál es su nivel de satisfacción con la transparencia en los criterios de evaluación y adjudicación?

- ☐ Muy Satisfecho
- ☒ Satisfecho
- ☐ Neutral
- ☐ Insatisfecho
- ☐ Muy Insatisfecho

Sección C: Normativas y Requisitos Específicos de Defensa

17. En su experiencia, compare cómo de exigentes son los requisitos de seguridad y confidencialidad en comparación con otros concursos de TIC en el sector público?
- ☒ Mucho más exigentes
 - ☐ Algo más exigentes
 - ☐ Similares
 - ☐ Menos exigentes
18. ¿Considera que su empresa cumple fácilmente con los requisitos específicos del Ministerio de Defensa?
- ☒ Sí, completamente
 - ☐ Sí, en la mayoría de los casos
 - ☐ No, algunos requisitos son difíciles de cumplir
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.
19. ¿Cree que los procedimientos de contratación del Ministerio de Defensa facilitan la incorporación de innovaciones tecnológicas?
- ☐ Sí, totalmente
 - ☒ Sí, en algunos casos
 - ☐ No, es difícil innovar
 - ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

Sección D: Desafíos y Mejora del Proceso de Contratación

20. ¿Cuáles son los principales desafíos que su empresa enfrenta al participar en concursos del Ministerio de Defensa? (Seleccione los que apliquen)
- ☐ Complejidad en los requisitos de seguridad
 - ☒ Falta de claridad en los pliegos técnicos
 - ☒ Competencia de grandes empresas del sector
 - ☐ Proceso largo y burocrático
 - ☒ Otro (especifique): Aavales requeridos en proyectos de alto alcance

21. En su opinión, ¿qué mejoras se podrían implementar en el proceso de contratación de TIC en el Ministerio de Defensa?

- Respuesta libre: 1-La configuración de solicitud de documentos en el portal contratación del Estado debería de coincidir con la especificación de documentos especificada en el pliego. (Debería de coincidir contra el pliego, pero en muchos casos asumimos en que parte debemos de introducir la documentación). 2-Para las ofertas de tamaño grande la el portal de contratación del estado presenta muchos problemas. 3-Hitos de pago más continuos, existen grandes hitos que generan mucha tensión de tesorería en las empresas en proyectos de tamaño grande.

22. ¿Hay algún aspecto específico de la contratación de TIC en Defensa que le gustaría que mejorara? (especificar)

Haga clic o pulse aquí para escribir texto.

Sección E: Opinión sobre la Estrategia de Contratación de TIC en Defensa

23. ¿Cree que el Ministerio de Defensa fomenta adecuadamente la participación de empresas tecnológicas nacionales?

- ☒ Sí
- ☐ No
- ☐ No tengo una opinión formada

24. ¿Considera que las estrategias de contratación de TIC actuales del Ministerio de Defensa están alineadas con las necesidades tecnológicas actuales del sector?

- ☒ Sí, completamente
- ☐ Sí, en algunos aspectos
- ☐ No, existen áreas de mejora
- ☐ Otro (especifique): Haga clic o pulse aquí para escribir texto.

25. Comentarios adicionales sobre la contratación pública de TIC en el Ministerio de Defensa:

- Respuesta libre: Existe una correcta atención a las llamadas telefónicas y correos electrónicos enviados cuando tenemos alguna problemática. Muy agradecidos

Anexo VI AM Contrato Ciberseguridad I3D



MINISTERIO
DE DEFENSA

SECRETARÍA DE ESTADO
DE DEFENSA

CENTRO DE SISTEMAS Y
TECNOLOGÍAS DE LA INFORMACIÓN
Y LAS COMUNICACIONES

Informe Razonado de la Necesidad de contratación del Acuerdo Marco de herramientas y servicios de ciberseguridad para la Infraestructura Integral de Información para la Defensa (I3D).



MINISTERIO
DE DEFENSA

SECRETARÍA DE ESTADO
DE DEFENSA

CENTRO DE SISTEMAS Y
TECNOLOGÍAS DE LA INFORMACIÓN
Y LAS COMUNICACIONES

INFORME RAZONADO DE LA NECESIDAD

1. OBJETO DEL ACUERDO MARCO

El objeto de esta Memoria es dar los elementos de juicio para efectuar un razonamiento de la necesidad de contratación relativa al *"Acuerdo Marco de herramientas y servicios de ciberseguridad para la Infraestructura Integral de Información para la Defensa (I3D)"* y los correspondientes Contratos Basados derivados del mismo.

El objeto del presente Acuerdo Marco se concreta en la contratación del equipamiento y los servicios para el Nodo de Interconexión de Clase III y del Centro de Operaciones de Ciberseguridad de la Infraestructura Integral de Información para la Defensa (en adelante, COS I3D), junto con las herramientas de ciberseguridad de uso transversal necesarias para fortalecer las capacidades de prevención proactiva y cibervigilancia del Ministerio de Defensa. Del mismo modo también contempla el equipamiento y los servicios destinados a la adecuación al Esquema Nacional de Seguridad de la Infraestructura Integral de Información para la Defensa (I3D).

Para dar respuesta a las necesidades descritas y en base a la diferente naturaleza y tipología de los suministros y servicios de ciberseguridad a contratar se ha establecido la siguiente división por Lotes:

- Lote 1: Suministros y servicios profesionales para el Nodo de Interconexión de Clase III de la I3D.
- Lote 2: Suministros y servicios profesionales para la gestión de eventos de seguridad de la I3D.
- Lote 3: Suministros y servicios profesionales para la interoperabilidad y coordinación en la prevención, detección y respuesta de amenazas en la I3D.
- Lote 4: Suministros y servicios profesionales para el Centro de Operaciones de Seguridad de la I3D.
- Lote 5: Suministros y servicios de ciberseguridad transversales de la I3D.
- Lote 6: Suministros y servicios profesionales para la gestión y adecuación al Esquema Nacional de Seguridad en la I3D.

2. JUSTIFICACIÓN DE LA NECESIDAD

En la actualidad el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC), tiene asumidas las responsabilidades de la gestión y explotación de los Sistemas de Información, de la plataforma informática y de las Telecomunicaciones del Ministerio de Defensa en el entorno de la I3D, así como de su seguridad, tanto en el entorno clasificado como en el no clasificado.

En el Real Decreto 372/2020, de 18 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa, se determina que depende directamente de la Secretaría de Estado de Defensa, con rango de subdirección general, el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC), al que le



corresponde la planificación, desarrollo, programación y gestión de las políticas relativas a los sistemas y tecnologías de la información y las comunicaciones, la transformación digital y seguridad de la información, así como la supervisión y dirección de su ejecución. A estos efectos, dependen funcionalmente de este centro los órganos competentes en las citadas materias de las Fuerzas Armadas y de los organismos autónomos del Ministerio de Defensa.

Como un elemento indisoluble de la taxonomía de Servicios CIS/TIC del MDEF (definida en la Política CIS/TIC y en la Arquitectura Global CIS/TIC) se incluyen los Servicios de Seguridad CIS/TIC (o Servicios de Ciberseguridad, tal y como se denominan en la propia AG CIS/TIC), que junto a la gestión única constituyen capacidades transversales para garantizar la robustez, resiliencia y coherencia técnica necesarias en el ámbito CIS/TIC.

Estos Servicios CIS/TIC, y por tanto los Servicios de Ciberseguridad, podrán ser Permanentes (I3D) o Desplegables. Como directriz general para la delimitación de competencias en este ámbito, se establece que el CESTIC será responsable de los Servicios de Ciberseguridad de la I3D.

Según la Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de sistemas y Tecnologías de la Información y Comunicaciones (AG CIS/TIC) del MDEF, se establece en su apéndice II el concepto de Ciberseguridad entendida como la capacidad de proteger adecuadamente la confidencialidad, integridad y disponibilidad de sistemas (CIS/TIC) y la información procesada, almacenada o transmitida, mediante la aplicación de las medidas necesarias. En la AG CIS/TIC se utiliza indistintamente "Ciberseguridad" y "Seguridad CIS/TIC". En esta línea la OM 76/2006 establece en su artículo primero como objeto de esta política, el alcanzar la protección adecuada (...) proporcionada y razonable de la Información del MDEF (...) mediante la preservación de sus requisitos básicos de seguridad: confidencialidad, integridad y disponibilidad. Responsabilidad del COS I3D (CESTIC).

Los Servicios de Ciberseguridad de la Información del COS de la I3D deben asegurar la protección y defensa de la información y los Servicios CIS/TIC, garantizando su disponibilidad, integridad, autenticación, confidencialidad y no repudio. Incluyen la restauración de los sistemas de información y proporcionan las funciones necesarias para garantizar y asegurar la información almacenada, durante el transporte y la que se está procesando. Así mismo, aseguran que sólo los usuarios autorizados tienen acceso seguro a la información, a los servicios y a los sistemas, y que los componentes CIS/TIC operan como se espera y actúan eficazmente en su propia defensa.

Por otra parte, entre los ejes estratégicos fijados al CESTIC figura el avanzar hacia una única Infraestructura Integral de Información para la Defensa (I3D), gestionada por el Centro de Sistemas y Tecnologías de la Información y las Comunicaciones, con un único punto de interconexión con las redes externas y una panoplia de herramientas que garanticen un adecuado nivel de seguridad entre los usuarios de la red, además de aquellas que garantizan un nivel de adecuación al ENS y a la LOPD conforme a la Ley y a los cometidos asignados al CESTIC a través del plan de actuación departamental Seginfo.



MINISTERIO
DE DEFENSA

SECRETARÍA DE ESTADO
DE DEFENSA

CENTRO DE SISTEMAS Y
TECNOLOGÍAS DE LA INFORMACIÓN
Y LAS COMUNICACIONES

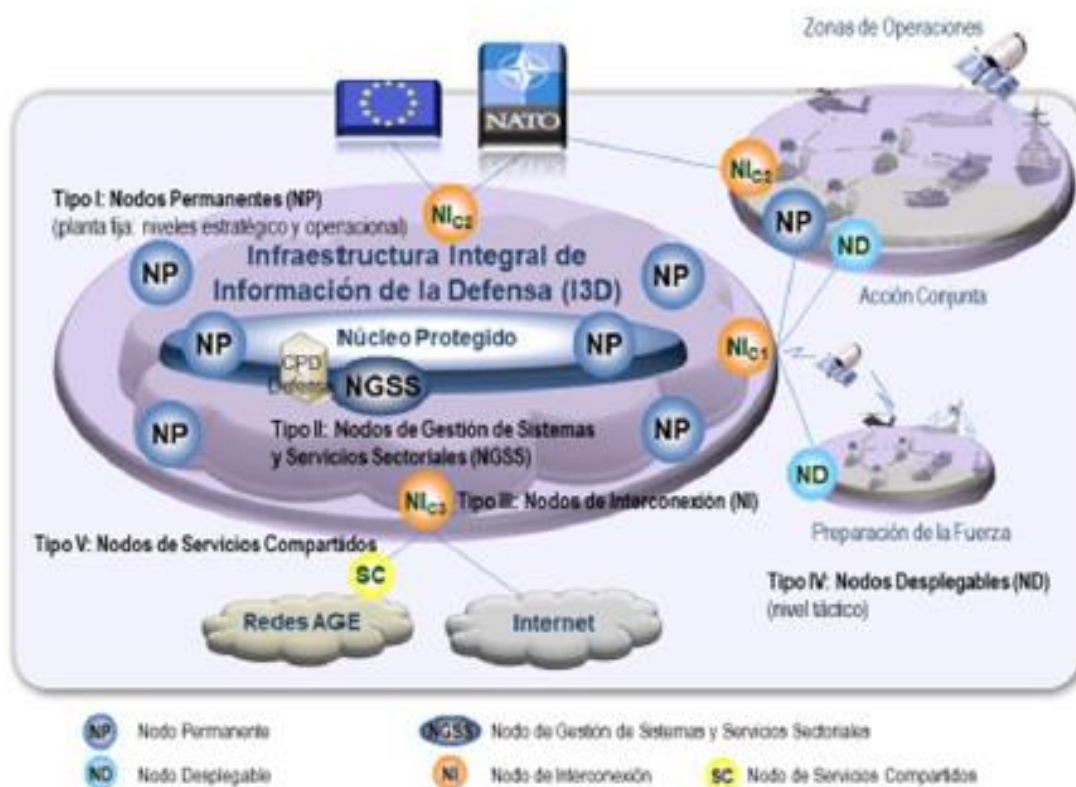


Ilustración 3.- Situación Futura de las Infraestructuras CIS/TIC del Ministerio de Defensa.

Este "Acuerdo Marco de herramientas y servicios de ciberseguridad para la Infraestructura Integral de Información para la Defensa (I3D)", contempla un amplio abanico de soluciones integrales de ciberseguridad para todo el ámbito de la I3D (dominio clasificado y dominio sin clasificar), dado que deben tratarse de manera indisoluble, al compartir las fuentes y activos objetos de protección en función de una única amenaza. Está previsto que este Acuerdo Marco entre en vigor a la finalización del Expediente Contratación Nº 1004219009200 para la "Contratación de los Servicios e Infraestructuras del Nodo de Interconexión de Clase III y el Centro de Operaciones de Ciberseguridad de la I3D" (11-03-2023), siendo este acuerdo marco el catalizador de los anteriores contratos existentes, así como de otros que se venían haciendo sin contar con un marco contractual común.

A raíz de la situación generada por el COVID-19, los ciberdelincuentes han aprovechado esta situación de vulnerabilidad derivada de la generalización del teletrabajo para incrementar sus ataques de todo tipo: ransomware, phishing con el que obtener credenciales de acceso a sistemas, ejecución de código de forma remota, exfiltración de información, etc. Los dos siguientes gráficos muestran los datos de incidentes en 2021, con indicación de su nivel de peligrosidad el primero y del tipo de ciberamenaza el segundo:

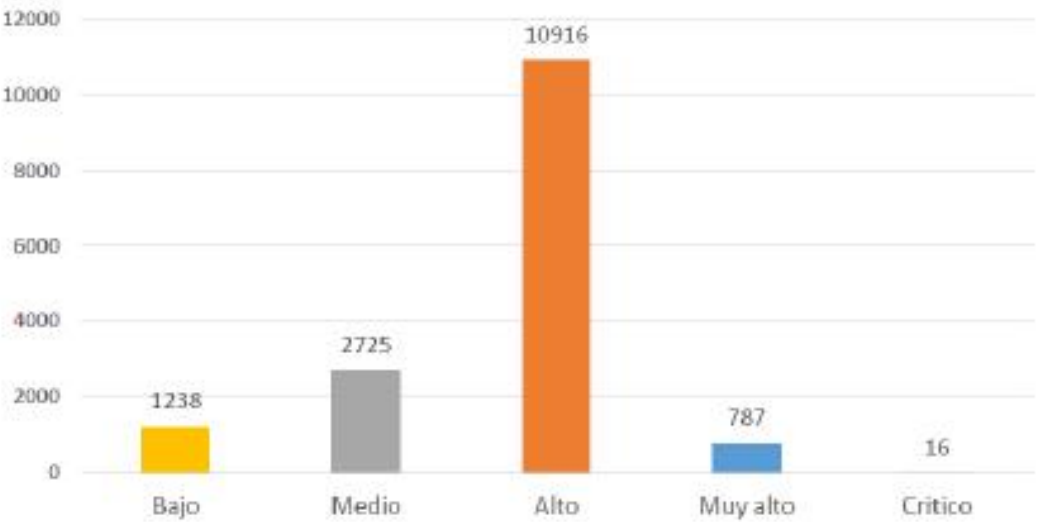


Figura 2. Peligrosidad de los incidentes gestionados por el CCN-CERT en 2021

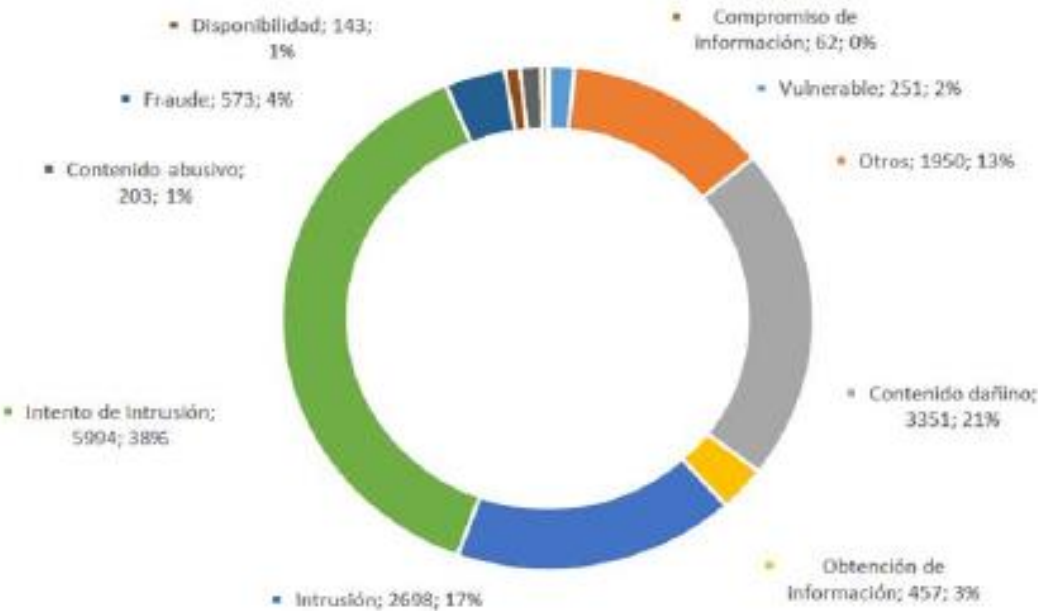


Figura 3. Clasificación de los incidentes gestionados por el CCN-CERT en 2021



MINISTERIO
DE DEFENSA

SECRETARÍA DE ESTADO
DE DEFENSA

CENTRO DE SISTEMAS Y
TECNOLOGÍAS DE LA INFORMACIÓN
Y LAS COMUNICACIONES

Este nivel de amenazas de ciberataques se ha visto incrementado de forma muy considerable con el nuevo escenario bélico en Ucrania.

Durante el mes de marzo del presente 2022 ha tenido lugar una reunión del Foro Nacional de Ciberseguridad, presidido por el Presidente del Gobierno, en La Moncloa. En él se ha destacado la importancia de la labor de colaboración del sector público privado en estos tiempos complicados con un escenario real de guerra híbrida (ciberguerra). En este contexto las soluciones comerciales de ciberseguridad, incluida la inteligencia civil cobran especial importancia en la integración como una parte más de los sistemas militares, y la I3D es uno de ellos.

En dicha reunión, también se ha dado la alarma de un peligro cierto e inminente (fuentes del CNI y del CCN-CERT), consistente en un nuevo ciberataque que se está preparando desde Rusia que volvería a afectar al SEPE, esta vez dejando fuera de funcionamiento el sistema de prestaciones por desempleo para que las personas en situación de recibir una prestación no puedan hacerlo durante este mes, al no poder comunicar el traspaso a los bancos y entidades financieras. Esto supondría un gravísimo perjuicio para la ciudadanía y en este caso, la más vulnerable.

Por lo tanto, podemos afirmar, que en este escenario de guerra híbrida, Rusia tiene la intención confirmada de realizar el mayor daño posible a todos los países que apoyan a Ucrania en este conflicto. España, como miembro de la OTAN, es uno de ellos y por tanto todos los sistemas de las Fuerzas Armadas son objetivo preferente de los mencionados ciberataques.

Dentro de la infraestructura del Nodo de Interconexión de Clase III de la I3D están instaladas diversas herramientas software que proporcionan servicios de detección y respuesta de amenazas de tipo XDR (Cross Detection and Response). La rápida evolución en las soluciones de ciberseguridad posibilita el uso de nuevas y más potentes funcionalidades, que permiten unos mayores niveles de seguridad y protección ante ciberataques.

Por todo lo anterior, y con el objeto de prestar un servicio de ciberseguridad adecuado a las nuevas amenazas, cada vez más sofisticadas, se hace necesario desarrollar un esfuerzo, si cabe mayor, en la coordinación de los elementos de seguridad, de los que ya dispone nuestra red, además de ampliar aquellos que sean estrictamente necesarios, para afrontar una demanda cada vez más exigente de los usuarios que trabajan fuera del perímetro de nuestra I3D, a través de este Acuerdo Marco propuesto.

3. NATURALEZA DEL ACUERDO MARCO.

Conforme a lo establecido en el artículo 18 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), el presente Acuerdo Marco es Mixto, ya que comprende prestaciones de los contratos de suministros y de servicios.

De igual modo, atendiendo a lo dispuesto en el artículo 18.1. a) este Acuerdo Marco tiene la calificación de Contrato de Suministros, al ser ésta la prestación de más importancia desde el punto de vista económico, siendo el porcentaje atribuido del 62,46% para suministros y el 37,54% para servicios.

3.1 Designación del objeto del Acuerdo Marco según la Nomenclatura CPV

De acuerdo con la nomenclatura del Reglamento (CE) Nº 213/2008 de fecha 28 de noviembre de 2007 por el que se modifica el Reglamento (CE) Nº 2195/2002 del



Parlamento Europeo y del Consejo por el que se aprueba el Vocabulario Común de Contratos Públicos (CPV), las prestaciones objeto de este AM se corresponden con los códigos:

LOTES	CPV
1	48000000-8 Paquetes de software y sistemas de información
	32522000-8 Equipo de telecomunicaciones
	64200000-8 Servicios de telecomunicaciones
	72600000-8 Servicios de apoyo informático y de consultoría.
2	48000000-8 Paquetes de software y sistemas de información
	32522000-8 Equipo de telecomunicaciones
	72600000-8 Servicios de apoyo informático y de consultoría.
3	48000000-8 Paquetes de software y sistemas de información
	32522000-8 Equipo de telecomunicaciones
	72600000-8 Servicios de apoyo informático y de consultoría.
4	48000000-8 Paquetes de software y sistemas de información
	32522000-8 Equipo de telecomunicaciones
	72600000-8 Servicios de apoyo informático y de consultoría.
5	48000000-8 Paquetes de software y sistemas de información
	32522000-8 Equipo de telecomunicaciones
	72600000-8 Servicios de apoyo informático y de consultoría.
6	48000000-8 Paquetes de software y sistemas de información
	72600000-8 Servicios de apoyo informático y de consultoría.

3.2 Designación del objeto del Acuerdo Marco según la Nomenclatura CPA

De acuerdo con la nomenclatura de la Clasificación de Productos por Actividades (CPA) aprobada por Reglamento (UE) N° 1209/2014, de 29 de octubre, por el que se modifica el Reglamento (CE) N° 451/2008, de 23 de abril, las prestaciones objeto de este AM se corresponden con los códigos:

LOTES	CPA
1	58.29.32 Programas de aplicación descargables
	26.30 Equipos de telecomunicaciones
	61.10.20 Servicios de operadores de telecomunicaciones por cable
	62.03.1 Servicios de gestión de los recursos informáticos
2	58.29.32 Programas de aplicación descargables
	26.30 Equipos de telecomunicaciones
	62.03.1 Servicios de gestión de los recursos informáticos
3	58.29.32 Programas de aplicación descargables
	26.30 Equipos de telecomunicaciones
	62.03.1 Servicios de gestión de los recursos informáticos
4	58.29.32 Programas de aplicación descargables
	26.30 Equipos de telecomunicaciones
	62.03.1 Servicios de gestión de los recursos informáticos
5	58.29.32 Programas de aplicación descargables



MINISTERIO
DE DEFENSA

SECRETARIA DE ESTADO
DE DEFENSA

CENTRO DE SISTEMAS Y
TECNOLOGÍAS DE LA INFORMACIÓN
Y LAS COMUNICACIONES

LOTES	CPA
	26.30 Equipos de telecomunicaciones
	62.03.1 Servicios de gestión de los recursos informáticos
6	58.29.32 Programas de aplicación descargables
	62.03.1 Servicios de gestión de los recursos informáticos

4. PLAZO DE EJECUCIÓN DEL ACUERDO MARCO

El plazo de ejecución de las prestaciones incluidas en el presente Acuerdo Marco será de tres (3) años, con posibilidad de prórroga de un (1) adicional.

5. LUGAR DE EJECUCIÓN DEL ACUERDO MARCO Y LOS CONTRATOS BASADOS

Los lugares donde se ejecutarán las prestaciones objeto de los Contratos Basados serán en las ubicaciones señaladas en cada uno de los CB, siendo las ubicaciones previstas las siguientes:

- Las instalaciones del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa, en la calle Arturo Soria 289 (28033 - Madrid).
- Acuartelamiento Capitán Sevillano ubicado en Av. de Radio Televisión, 6 (28223 Pozuelo de Alarcón – Madrid).
- Las instalaciones del Ministerio de Defensa ubicadas en Castellana 109, Madrid.
- Además de las anteriormente relacionadas, en el caso de las prestaciones de servicios, podrán contemplarse los siguientes lugares para su prestación:
- Las instalaciones de la Empresa adjudicataria o los domicilios de los Perfiles ofertados en cada uno de los Lotes, mediante teletrabajo, cuando concurra alguna circunstancia que obligue o aconseje la prestación de los servicios en esta modalidad.
- Las instalaciones de la Empresa adjudicataria o los domicilios de los Perfiles ofertados según lo previsto en el PPT (exclusivamente para los Lotes 5 y 6), mediante teletrabajo.

En este caso las empresas adjudicatarias serán las responsables de dotar a su personal de los equipos informáticos adecuados para poder desempeñar las labores definidas, de acuerdo con cada uno de los perfiles establecidos en el PPT de este expediente. En este caso, será necesario consensuar la utilización de una herramienta de control, que permita comprobar, de forma fehaciente, las horas efectivas trabajadas por cada perfil en dicha circunstancia.

6. VALOR ESTIMADO DEL ACUERDO MARCO

Conforme a lo dispuesto en el artículo 101 de la Ley de Contratos del Sector Público (LCSP), el valor estimado del presente Acuerdo Marco asciende a la cantidad de **SESENTA Y UN MILLONES ONCE MIL TREINTA Y UNO CON SETENTA Y SEIS CÉNTIMOS (61.011.031,76 €)**.



7. RÉGIMEN DE PAGO.

El adjudicatario de los Contratos Basados tendrá derecho al pago del precio, en caso de los suministros, previa recepción y conformidad del suministro, en caso de servicios mediante facturaciones trimestrales, previo Certificado de Conformidad del Responsable del Contrato Basado.

8. FINANCIACIÓN

Para el presente AM no procede la constancia de existencia de crédito, toda vez que del mismo no se derivan obligaciones económicas. Estas serán exclusivamente las que originen los Contratos Basados que se celebren por los diversos órganos de contratación del MINISDEF y cuya financiación será atendida con los créditos presupuestarios puestos a su disposición. Su existencia se justificará por el certificado de Retención de Crédito para Gastos, y en su caso, por el certificado de Retención de Crédito de Tramitación Anticipada, o para Ejercicios Posteriores.

En este sentido se ha planificado que los Contratos Basados en el presente Acuerdo Marco se financien con cargo a los créditos del CESTIC (CRG 037), de los Conceptos y Subconceptos Presupuestarios 660, 668, 22200, 227.06, y 228 de los ejercicios 2023, 2024, 2025 y 2026.

**EL JEFE DE LA DIVISIÓN DE SEGURIDAD DE
LA INFORMACIÓN**

TCol. Jose Francisco García Gil