Premios Socinfo Digital:
CIBERSEGURIDAD AAPP

Título de la candidatura:	**Proyecto de Implantación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS)**
Categoría:	**Ciberseguridad disruptiva**
Entidad proponente:	**Secretaría General de Administración Digital** Secretaría de Estado de Función Pública Ministerio para la Transformación Digital y de la Función Pública
Datos de contacto:	**Miguel A. Amutio Gómez** Director de Planificación y Coordinación de Ciberseguridad Secretaría General de Administración Digital Ministerio para la Transformación Digital y de la Función Pública Manuel Cortina 2 despacho D515 28071 Madrid Tel. 91 273 2990 / 629 794 862 miguel.amutio@digital.gob.es

Contenido

1. DESCRIPCIÓN DEL PROYECTO

Descripción

El proyecto presentado como candidatura a la categoría de '*ciberseguridad disruptiva*' **tiene por objeto** el diseño, construcción, implantación, migración e integración de entidades, la operación, y el apoyo a la gestión y dirección del **Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS)**. El proyecto del COCS incluye la provisión de los medios necesarios para soportar la operativa de prestación de servicios transversales de ciberseguridad a las entidades de la Administración General del Estado en su alcance, 122 entidades a la fecha de redacción de este documento.

El proyecto del COCS se lleva adelante con fondos del Plan de Recuperación, Transformación y Resiliencia, en particular de la línea 5 'Ciberseguridad' de la Inversión 1 del Componente 11.

La ejecución del proyecto del COCS **se inició en marzo de 2022**. El alcance temporal para sus construcción e implantación, junto con la integración de las entidades en sus servicios, es **de 3 años**, si bien se contemplan fases posteriores para su consolidación y evolución.

El proyecto del COCS es responsabilidad de la **Secretaría General de Administración Digital (SGAD)** que asume la dirección técnica y estratégica del servicio. Como socio estratégico y colaborador clave en el proyecto, el **Centro Criptológico Nacional (CCN)** pone a disposición del proyecto su apoyo al despliegue del COCS, sus capacidades de ciberseguridad, herramientas y soluciones de ciberseguridad, así como sus capacidades de ciberinteligencia, investigación y respuesta experta ante incidentes de seguridad complejos, más las de ciberdefensa activa; así mismo, apoya a la SGAD en la dirección técnica y estratégica del servicio y en el seguimiento y ejecución del contrato para su implantación.

El proyecto del COCS está previsto en la Medida 9 del **Plan de Digitalización de las Administraciones Públicas 2021 – 2025**. Además, la creación del COCS se alinea con la **Estrategia Nacional de Ciberseguridad 2019**, respondiendo a la medida 5 de la Línea de Acción 2 ("Garantizar la seguridad y resiliencia de los activos estratégicos para España").

El **COCS es una infraestructura**, una capacidad, **dotada de hardware, software y servicios alojada en los centros de proceso de datos** de la Secretaría General de Administración Digital, integrada con las infraestructuras que permiten a dicha Secretaría la prestación de los servicios, hasta el punto de llevar aparejada la integración de las infraestructuras de ciberseguridad de las entidades en su alcance.

Se trata, por tanto, de una infraestructura **estrechamente ligada e imbricada con el Servicio Unificado de Comunicaciones** de la Administración General del Estado, especialmente con algunos de sus servicios como el de protección contra ataques de denegación de servicio (AntiDDoS) configurando un escudo global de las entidades en

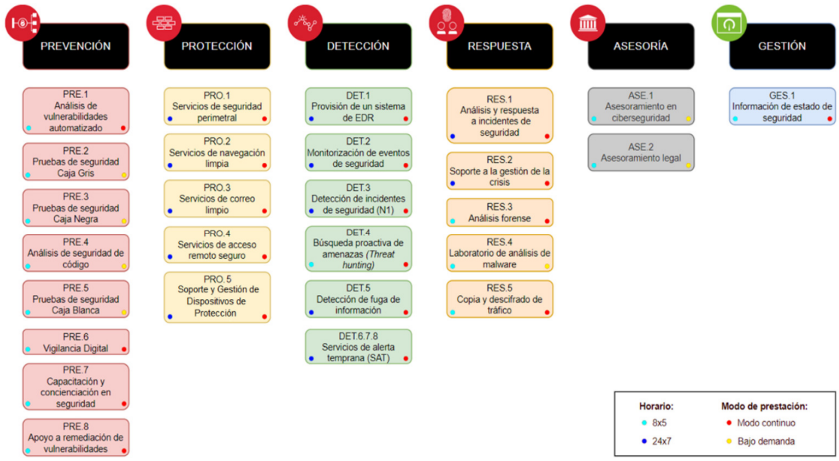
su alcance, así como con la nube híbrida securizada para el acceso y prestación de los diversos servicios comunes, compartidos y transversales.

También se encuentra el COCS integrado en la **Red Nacional de Centros de Operaciones de Ciberseguridad** promovida por el Centro Criptológico Nacional, siendo uno de los contribuyentes principales de información reutilizable para la gestión de incidentes de ciberseguridad.

El proyecto del COCS persigue la protección de la seguridad de la Administración General del Estado y sus Organismos Públicos frente a ciberamenazas, y supone la evolución hacia un modelo integral que favorece la coordinación interdepartamental ante incidentes de seguridad complejos, y la compartición e intercambio de información de inteligencia de ciberseguridad. El modelo centralizado facilitará la excelencia y optimización de los recursos humanos y técnicos a disposición de las entidades en su alcance, y conseguirá mejorar sus capacidades de defensa a la vez que reducirá el coste global de operación de ciberseguridad del conjunto de la Administración General del Estado.

Se encuentran en el **alcance del COCS** la totalidad de las entidades usuarias del Servicio Unificado de Comunicaciones de la Administración General del Estado, más otras entidades que cuentan con conexión directa a un nodo de interconexión de Red SARA. Eso supuso al comienzo del proyecto un alcance inicial de 106 entidades, que en la actualidad ha evolucionado hasta un **alcance de 122 entidades, que ofrecen un escenario de enorme diversidad en cuanto a sus características, tipología, capacidades y cometidos**.

Las capacidades de ciberseguridad del COCS se articulan en torno a un **catálogo de servicios horizontales de ciberseguridad,** que actualmente comprende **27 servicios**.



Los servicios se organizan en torno a **familias**, según su naturaleza, y cuentan con su propia codificación:

- **Servicios de prevención**, orientados a minimizar la probabilidad de materialización de amenazas (servicios de auditorías técnicas de seguridad, análisis de vulnerabilidades, vigilancia digital, apoyo a la remediación de vulnerabilidades, concienciación y formación).

- **Servicios de protección** frente a las amenazas (servicios de seguridad perimetral, navegación limpia, correo limpio, acceso remoto seguro, operación de ciberseguridad).
- **Servicios de detección** de las amenazas (provisión de agente de seguridad de punto final (Endpoint Detection and Response -EDR-), monitorización de seguridad, *threat hunting*, etc.).
- **Servicios de respuesta** ante incidentes de seguridad, que aseguren una gestión y reacción lo más eficaz posible ante su materialización, incluyendo análisis forense, análisis de malware, copia y descifrado del tráfico.
- **Servicios de asesoramiento** en ciberseguridad, tanto en aspectos generales de ciberseguridad como en el plano legal.
- **Servicios de información de estado de seguridad**, consistente en cuadros de mando que midan tanto el grado de integración en el COCS de las entidades como su estado general de ciberseguridad.

Cada servicio del catálogo tiene su definición y diseño detallado estandarizado, que incluye su modelo de integración, sus procedimientos y sus condiciones de servicio. Existen diversas **modalidades** de prestación (servicios bajo demanda y en modo continuo) y **horarios** (8x5, 24x7).

El **modelo de implantación de los servicios** del catálogo se basa en "disponibilizar" e incrementar su madurez:

- Por un lado, se han ido desplegando los servicios hasta alcanzar un punto en el cual se aprueba su paso a "disponible" para su uso por parte de las entidades.
- Por otro lado, cada servicio va evolucionando en su madurez y prestaciones a lo largo de la vida del proyecto, con mejoras de las que se van beneficiando las entidades que los usan.

El uso efectivo de los servicios se formaliza en el proyecto del COCS mediante el concepto de **integración de las entidades en los servicios** (el par entidad-servicio), base para la medición de objetivos del proyecto, así como para la facturación del contrato de implantación del COCS, que requiere la **certificación** por parte de una entidad auditora independiente de las integraciones efectivamente producidas, es decir, de cada par entidad-servicio.

Los servicios previamente indicados se ponen a disposición de las **entidades incluidas en el alcance de proyecto**, que inicialmente fueron aquellas incluidas en el alcance del Contrato Unificado de Comunicaciones de la AGE (106), si bien actualmente ya se cuenta con **122 entidades**, pues se han incorporado 16 nuevas entidades a finales de 2023.

Otros **aspectos relevantes** en cuanto a la implantación **del proyecto** son los siguientes:

- Instalación de herramientas en los centros de procesos de datos e **infraestructuras de la Secretaría General de Administración Digital**.
- Para el suministro de licencias del **agente de seguridad de punto final EDR** y su despliegue en 150.000 puestos de las entidades de la Administración General del Estado se realizó contratación en paralelo al proyecto del COCS. A medida que se va implantando en cada entidad el agente de seguridad de punto final se va

realizando el trasvase de su gestión al Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (servicio DET.1).

- Disponibilidad de un **sistema integrado de gestión**, formado por componentes como cuadros de mando, herramientas de *ticketing*, herramientas de gestión de incidentes, base de datos de configuración, etc.
- Un modelo de implantación que tiene en cuenta desde el principio el **cumplimiento** de requisitos del **Esquema Nacional de Seguridad** (ENS).
- **Importancia de la comunicación, tanto de progreso del proyecto como de operación de ciberseguridad**, hacia el alto nivel, hacia la dirección del proyecto del COCS, hacia las entidades y a hacia sus responsables de tecnología de la información y las comunicaciones: logotipo e imagen corporativa, *newsletter* semanal, boletines periódicos, formaciones *ad-hoc*, cuadro de mando con perspectivas para el alto nivel, para la dirección del proyecto y para las entidades, presentaciones periódicas al Comité de Dirección de las Tecnologías de la Información y las comunicaciones, otras acciones de difusión.
- El proyecto del COCS ha suscitado interés en otros países de la Unión Europea y se viene presentando en relaciones bilaterales en visitas de estudio (Austria, Ucrania y Noruega).

Contexto de ciberseguridad y antecedentes

A continuación, un apunte breve sobre el contexto de ciberseguridad y los antecedentes que motivan el proyecto del COCS.

En primer lugar, el avance de la digitalización en la Administración General del Estado ha venido a ampliar la superficie de ataque por parte de posibles agresores, en un contexto geopolítico complejo, y con extensión de la ciberdelincuencia que le convierten en un objetivo señalado de cara la disrupción de los servicios, a la sustracción de la información o a ambos, a menudo con el intento añadido de extorsión, e incluso como actividad rutinaria de agresión. El aumento de los ciberataques que se vienen registrando en términos de número, alcance, sofisticación y severidad del impacto, así como su transversalidad, hace que sea necesario reforzar las capacidades de ciberseguridad de la Administración General del Estado y sus Organismos Públicos con capacidades como las proporcionadas por el proyecto del COCS que permitan la prevención protección, detección, respuesta y la acción conjunta ante este escenario de ciberamenazas y ciberataques.

Téngase en cuenta que estos ciberataques son provocados por agentes y actores con mayores capacidades técnicas y operativas y mejor coordinados, que aprovechan la alta dependencia de las tecnologías de la información y las comunicaciones, la gran interconectividad de sistemas y actores, la interdependencia de unos y otros, sus posibles debilidades en protección y, finalmente, tanto la innovación como las vulnerabilidades de la tecnología. Todos los factores anteriores configuran un escenario de ciberseguridad complejo, acentúan el riesgo de propagación rápida, junto con la mayor superficie de exposición que genera la utilización masiva de las tecnologías, a la vez que los potenciales agresores amplían su campo de actuación a todo tipo de organizaciones, individuos y objetos con componente digital. En este escenario de alta

conectividad, la debilidad en una entidad compromete al resto por el alto riesgo y facilidad de propagación de la actuación de los agentes y actores agresores, de forma que una respuesta diligente, eficaz, coordinada y armonizada, que a la vez vaya acompañada de un conocimiento preciso de la situación, así como de su evolución, demanda una mayor coordinación, proporcionada a los requisitos evolutivos y crecientes de la ciberseguridad.

En segundo, lugar la necesidad de un Centro de Operaciones de Ciberseguridad para la Administración General del Estado se había vislumbrado ya con motivo de la Declaración de Servicios Compartidos de 2015. A partir de dicho momento se iniciaron diversos trabajos exploratorios y preparativos, acompañados de diversos actos de apoyo de alto nivel que culminaron con su plasmación en la Estrategia Nacional de Ciberseguridad 2019, en un Acuerdo de Consejo de Ministros de 15 de febrero de 2019, en la Agenda España Digital 2025 y en el Plan de Digitalización de las Administraciones Públicas 2021-2025, pudiéndose ejecutar finalmente gracias a los fondos del Plan de Recuperación, Transformación y Resiliencia.

Objetivos

Como objetivo principal, el proyecto del COCS persigue, mediante la prestación de servicios horizontales de ciberseguridad, reforzar las capacidades de prevención, protección, detección y respuesta ante incidentes de ciberseguridad, de la Administración General del Estado y sus Organismos Públicos, de forma que gracias a la optimización y a las economías de escala se obtenga a la vez una mejor eficacia y eficiencia.

Se contempla también que, además de ayudar a mejorar la ciberseguridad de las entidades en su alcance, el COCS contribuya a facilitar el cumplimiento del Esquema Nacional de Seguridad.

Otros objetivos derivados del objetivo principal a conseguir mediante el desarrollo del proyecto del COCS, son:

- Mejorar el nivel de la ciberseguridad global de la Administración General del Estado, así como la coordinación y la capacidad para enfrentarse a las ciberamenazas y los ciberataques que puedan afectar a entidades individualmente, a varias, o globalmente a todas ellas.
- Disponer de una visión de conjunto de la situación de ciberseguridad de la Administración General del Estado.
- Compartir información para la gestión de incidentes, creando una capacidad para actuar rápidamente ante posibles ciberataques que puedan ir dirigidos contra un colectivo de entidades o que incluso puedan tener un carácter global.
- Facilitar la investigación de incidentes de ciberseguridad a las entidades en el alcance del COCS.
- Contribuir a una mejor aplicación del Esquema Nacional de Seguridad en las entidades en el alcance del COCS. Además, se aprovecha la dinámica de la integración de las entidades en el alcance del COCS para un proyecto paralelo de mejora de la adecuación al Esquema Nacional de Seguridad de las citadas entidades.
- Optimizar el gasto y los esfuerzos en ciberseguridad en un escenario de escasez de recursos.

Retos y riesgos enfrentados

El enfoque y ambición del proyecto del COCS requieren de la gestión de unos **retos y riesgos** identificados desde sus inicios:

- Un plazo temporal ambicioso, que conlleva paralelizar la implantación de los servicios de ciberseguridad junto con la integración de las entidades en dichos servicios. En la práctica, se trata de un “proyecto de proyectos”.
- Un muy elevado número de actores e interlocutores involucrados.
- Una gran complejidad y heterogeneidad en las características de situación técnica y organizativa de las entidades.
- Una cierta diversidad en el grado de colaboración de las entidades.

- Elevada complejidad técnica de la integración en algunos servicios.
- Necesidad de coordinar con las entidades la planificación de su integración en los servicios con sus propias contrataciones en curso en materia de ciberseguridad.
- Elevada exigencia de capacidad de gestión, contando con limitados recursos de personal propio de la Administración.
- Debido a los distintos factores de incertidumbre, necesidad de seguimiento estrecho de las planificaciones y de agilidad para adaptarlas.

Es este enfoque integrado e integrador, que parte de un escenario de ciberseguridad de enorme complejidad, fragmentación y heterogeneidad y que, como se vislumbra en la descripción, objetivos y resultados que cuenta con el máximo grado de ambición, **el que permite calificar al proyecto de implantación y construcción del COCS como disruptivo**.

Como bien nos han reconocido las empresas colaboradoras del proyecto, expertas en la implantación y operación de Centros de Operación de Seguridad (SOC, *Security Operation Center*), numerosos aspectos de este proyecto han constituido para todos un "territorio inexplorado".

2. REPERCUSIÓN PARA LA CIUDADANÍA Y LAS ADMINISTRACIONES

El esfuerzo realizado en el proyecto del COCS incluye una **especial atención a la medición,** tanto del proceso de despliegue de los servicios de ciberseguridad e integración de las entidades en su alcance, como de la operación de ciberseguridad.

Algunos **resultados cuantitativos** destacados conseguidos desde el comienzo del proyecto, en marzo de 2022, son los siguientes, precisados a la fecha de redacción del presente documento:

- 122 entidades de la Administración General del Estado y Organismos Públicos en su alcance.
- Más de 200.000 usuarios en el alcance del COCS.
- 27 servicios de ciberseguridad -prevención, protección, detección, respuesta, asesoramiento y gestión- incluidos en el catálogo del COCS.
- 76% es, a la fecha, la media actual de integración de las entidades en los servicios del COCS.
- Más de 123.000 agentes de seguridad de punto final (Endpoint Detection and Response EDR) en monitorización, correspondientes a 85 entidades con el EDR del COCS; encontrándose 15 entidades en proceso de despliegue del EDR a la fecha. Está previsto desplegar agentes de seguridad de punto final para 150.000 usuarios.

  Esto supone tener el grueso de las entidades de la Administración General del Estado en el alcance del COCS protegidas y monitorizadas de manera uniforme, cuando al comienzo del proyecto un importante número de entidades no disponían de esta defensa de agente de seguridad de punto final. El EDR es un elemento clave de proyecto del COCS, debido a las importantes capacidades de detección y bloqueo de amenazas que proporciona este tipo de soluciones, así como el caudal de información que proporciona a los servicios de búsqueda proactiva de amenazas.
- Con 24.433 incidentes gestionados en 2023, y la correspondiente extracción de Indicadores de Compromiso (IOCs), el COCS se ha convertido en uno de los principales contribuyentes a la Red Nacional de Centros de Operaciones de Ciberseguridad.
- Más de 88 entidades monitorizadas mediante un SIEM (*Security Information and Event Management*), y más de 80 entidades a las que se realiza búsqueda proactiva de amenazas (*threat hunting*) a través de 160 casos de uso.
- Más de 3.000 activos escaneados mensualmente en búsqueda de vulnerabilidades.
- Más de 75 actuaciones de pentesting de caja negra realizados sobre la superficie de exposición en Internet de las entidades en el alcance del COCS.

Pero no menos importantes resultan los **resultados cualitativos** conseguidos:

- **Llevar la ciberseguridad a las entidades sin recursos.**
- Mejorar de forma sustancial la detección y respuesta a los incidentes de ciberseguridad. Gracias a la implantación generalizada del agente de seguridad de punto final EDR se ha multiplicado la capilaridad total en la capacidad de detección y respuesta.
- Poder actuar en respuesta de manera rápida y coordinada ante incidentes que afectan a varias entidades.
- Configurar una visión más completa del estado de la ciberseguridad en la Administración General del Estado.
- Por último y no menos importante, racionalizar el gasto y los esfuerzos en ciberseguridad en un escenario en el que el talento en materia de ciberseguridad resulta escaso.

La protección de la Administración General del Estado frente a ciberamenazas y ciberataques mediante los servicios de prevención, protección, detección y respuesta del COCS contribuyen de forma decisiva a garantizar el ejercicio de derechos y libertades así como el cumplimiento de deberes por parte de la **ciudadanía**, junto con el normal desenvolvimiento de los cometidos de las entidades en su alcance, en un escenario en el que la Administración Pública es el sector más atacado según los informes disponibles de fuentes como el CCN-CERT y ENISA. Ataques que van dirigidos contra la información (para sustracción, destrucción o alteración), contra los servicios (para disrupción) o a menudo contra ambos con el consiguiente perjuicio en los derechos y libertades de la ciudadanía.

3. EQUIPO DE DESARROLLO Y PROVEEDORES

El equipo de la Administración para el proyecto del COCS está formado por:

- La **Secretaría General de Administración Digital**, que dirige y lidera el proyecto. Incluye dos unidades implicadas:
    - La División de Planificación y Coordinación de Ciberseguridad, que dirige y coordina de forma general el proyecto.
    - La Subdirección General de Infraestructuras y Operaciones, que dirige la implantación de los servicios de Protección, y da las directrices para la implantación de los componentes y herramientas del COCS en la infraestructura de la SGAD.
- El **Centro Criptológico Nacional**, como socio estratégico y colaborador clave en el proyecto, por aportar sus capacidades de ciberseguridad, ciberinteligencia y ciberdefensa activa, más las soluciones del CCN-CERT aplicables al proyecto del COCS.

La Secretaría General de Administración Digital y el Centro Criptológico Nacional colaboran en los diferentes niveles de decisión del proyecto del COCS.

En cuanto a los **proveedores y el soporte para a la implantación del COCS**, los instrumentos contractuales principales son los siguientes:

Instrumento	**Adjudicatario**
Contrato para la construcción e implantación del COCS	UTE Telefónica - Indra
Suministro de licencias de EDR y apoyo en su despliegue	Evolutio
Encargo a medio propio para la Oficina Técnica de apoyo al proyecto de implantación del COCS	ISDEFE

Asimismo, existe un convenio de colaboración con el Centro Criptológico Nacional para su apoyo en la implantación del COCS, así como para el desarrollo de las herramientas de seguridad del Centro Criptológico Nacional usadas para la prestación de los servicios del COCS.

Por último, **es imprescindible la colaboración de las propias entidades** destinatarias de los servicios del COCS, tanto para su adecuada integración, como para facilitar la operación de ciberseguridad, lo que supone un esfuerzo considerable por parte de su personal de tecnologías de la información y comunicaciones y especialmente de ciberseguridad.

Dicho lo anterior, un aspecto especialmente relevante del proyecto del COCS es que **hay que coordinar la participación, en distintos grados, de centenares de actores**:

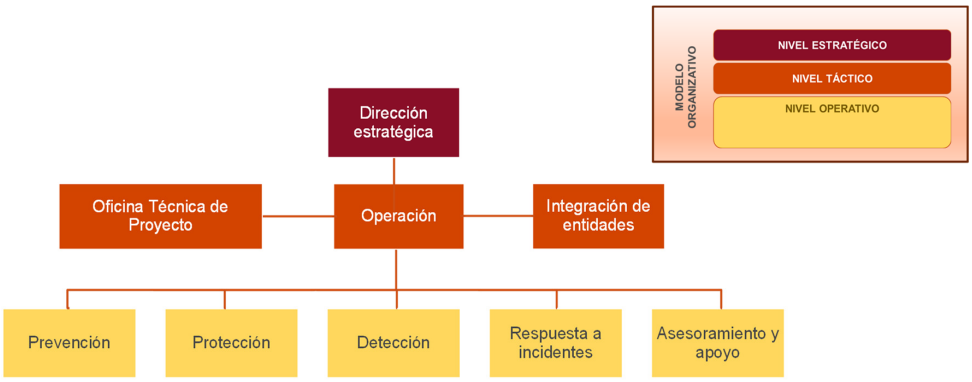
- La Secretaría General de Administración Digital, que dirige y lidera el proyecto.

- El Centro Criptológico Nacional, como socio estratégico y colaborador clave en el proyecto, especialmente en la ciberinteligencia y en la respuesta ante incidentes de seguridad complejos.
- La UTE adjudicataria y el proveedor del EDR.
- La Oficina de proyecto.
- 122 entidades con sus correspondientes contactos.

Debido a su dimensión, el proyecto del COCS se estructura en **diversas áreas de proyecto**, que se organizan en dos planos interrelacionados:

- Por un lado, el plano organizado en torno a las distintas áreas de prestación de los servicios (prevención, protección, detección, respuesta, asesoramiento y apoyo).
- Por otro lado, el plano organizado en torno a las tareas horizontales de la gestión del propio proyecto (oficina técnica, áreas de gestión de la demanda e integración de entidades, etc.).

Por último, el modelo organizativo cuenta con diversas estructuras (comités, reuniones de seguimiento, etc.) en las que participa distinto personal en función del **nivel de gestión (estratégico, táctico u operativo)**.



Modelo de organización del proyecto

En la práctica el proyecto del COCS se trata de **"un proyecto de proyectos"**, en los que se llegan a abordar en paralelo diversas acciones de implantación de servicios concretos con cada una de las entidades que pueden llegar a contar con las características intrínsecas de un proyecto: planificación, dotación de recursos, gestión de riesgos, etc. Por ello, un aspecto crucial es cómo se realiza la **interacción con las entidades**:

- **Gestión de los contactos** de entidades:
  - Tipificación (responsables de seguridad, TIC, de servicios, etc.).
  - Gestión de autorizaciones.
- **Equipo dedicado y metodología aprobada de integración de entidades.**
  - Reuniones diversas y abundantes: de difusión servicios, de trabajo para la implantación, de seguimiento del servicio, etc.

- **Protocolos de aprobación de documentación** de los subproyectos de integración (diseño técnico, planificación, etc.).
- **Comunicaciones institucionales**, a diversos niveles: emails, presentaciones, envío semanal de una newsletter, etc.

4. VALORACIÓN ECONÓMICA

El proyecto del COCS se financia con fondos del Plan de Recuperación, Transformación y Resiliencia, en particular de la línea 5 'Ciberseguridad' de la Inversión 1 del Componente 11.

Téngase en cuenta que el contrato del COCS se tramitó mediante el procedimiento 'negociado sin publicidad' y que el convenio entre la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado Directora del Centro Nacional de Inteligencia no es objeto de publicidad.

5. PLAZOS DE CUMPLIMIENTO

A la fecha de redacción del presente documento, el proyecto del COCS se encuentra inmerso en su **Fase I**, que comenzó en marzo de 2022, y tiene como horizonte temporal de extensión hasta el final de febrero de 2025. Durante esta fase se cuenta con la vigencia de los contratos actualmente en ejecución, financiados con cargo de los fondos del Plan de Recuperación, Transformación y Resiliencia. **El objetivo principal de esta fase es tener plenamente integradas a las 122 entidades en el alcance del COCS en los servicios del catálogo del COCS**.

Además, aunque, como se ha visto en apartados anteriores, los importantes esfuerzos realizados ofrecen ya resultados visibles, el proyecto del COCS no se concibe como un esfuerzo puntual acotado en el tiempo, sino que tiene vocación de permanencia y de mejora continua. Por tanto, otro importante objetivo a completar durante el resto de la fase I es la consolidación y mejora continua del grado de integración y madurez de los servicios actuales y del modelo de gestión.

Por otro lado, se viene trabajando ya en el diseño de una **Fase II**, con un horizonte temporal que alcanzará hasta el final del segundo trimestre de 2026. Durante este periodo el **objetivo** será **incrementar las capacidades del COCS**, mediante, por ejemplo, el empleo de soluciones basadas en Inteligencia artificial, la mejora en orquestación y automatización en la respuesta ante incidentes, el fomento de la protección de servicios en la nube y de los espacios de datos, las soluciones para mitigar los riesgos de la obsolescencia tecnológica (parcheado virtual), entre otros posibles.

Finalmente, podemos concluir con nuestra **visión** en relación al proyecto de implantación del COCS: constituirnos como todo un **referente a nivel europeo "y más allá"**.