

Edgar Neville 3, Planta Baja
28020 Madrid
Teléfonos: 914 361 590
Fax: 915 770 150



Este documento se ha obtenido directamente del original que contenía todas las firmas auténticas y se han ocultado los datos personales protegidos y los códigos que permitirían acceder al original.

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES QUE HA DE REGIR EN EL “CONTRATO DE SERVICIO DE ACOMPAÑAMIENTO, MANTENIMIENTO Y AUDITORÍA PARA LA RENOVACION DE LA CERTIFICACIÓN ENS 2025-2027 PARA PLANIFICA MADRID, PROYECTOS Y OBRAS, M.P., S.A”.

La autenticidad de este documento se puede comprobar en <https://gestion.comunidad.madrid/csv> mediante el siguiente código seguro de verificación:

ÍNDICE

1. OBJETO DEL CONTRATO
2. MARCO NORMATIVO Y GUÍAS DE REFERENCIA
3. ALCANCE DEL SERVICIO Y FASES
4. ENTORNO ACTUAL Y EVIDENCIAS DISPONIBLES
5. REQUISITOS FUNCIONALES Y TÉCNICOS
6. EQUIPO MÍNIMO Y DEDICACIÓN
7. ENTREGABLES MÍNIMOS
8. NIVELES DE SERVICIO (SLA)
9. PLAN DE TRABAJOS Y CRONOGRAMA DE REFERENCIA
10. COORDINACIÓN, REUNIONES Y COMUNICACIONES
11. PROTECCIÓN DE DATOS Y CONFIDENCIALIDAD
12. CRITERIOS DE ACEPTACIÓN
13. SUPUESTOS Y DEPENDENCIAS
14. PROPIEDAD INTELECTUAL Y CUSTODIA DE EVIDENCIAS
15. SUBCONTRATACIÓN Y AUDITORÍA EXTERNA
16. RIESGOS Y MEDIDAS DE MITIGACIÓN

1. OBJETO DEL CONTRATO

Definir las prescripciones técnicas para la contratación de un servicio de asistencia técnica especializada que garantice el mantenimiento, actualización y mejora del SGSI conforme al Esquema Nacional de Seguridad (ENS), la realización de la auditoría interna obligatoria y el acompañamiento hasta la superación de la auditoría externa prevista para abril de 2027. La certificación actual se obtuvo en abril de 2025 y el sistema está categorizado en Media.

2. MARCO NORMATIVO Y GUÍAS DE REFERENCIA

- Real Decreto 311/2022, por el que se regula el ENS.
- CCN-STIC 808 – Verificación del cumplimiento del ENS (incluida su Tabla de Verificación del Cumplimiento).
- CCN-STIC 802 – Auditoría ENS.
- CCN-STIC 804/806 – Medidas e implantación y Plan de adecuación.
- CCN-STIC 815 y 824 – Métricas e INES.
- Catálogo CPSTIC y guías específicas aplicables (perímetro, correo, web, SaaS, VPN, etc.).

3. ALCANCE DEL SERVICIO Y FASES

El adjudicatario ejecutará todas las actividades necesarias para mantener la conformidad ENS y preparar la renovación, estructuradas en cuatro fases con entregables definidos:

- **Fase 1 – Revisión inicial y planificación (mes 1)**
 - Revisión integral del SGSI-ENS y análisis de brechas.
 - Actualización de categorización, riesgos y Declaración de Aplicabilidad (DA).
 - Plan de Trabajo 2026 con hitos, responsables y calendario hasta auditoría externa (abril 2027).
 - Inventario de evidencias existentes y mapa control-evidencia.
- **Fase 2 – Mantenimiento operativo y generación de evidencias (meses 2 a 8)**
 - Actualización de políticas, procedimientos y registros.
 - Custodia y clasificación de evidencias por medida ENS.
 - Implantación de configuraciones técnicas necesarias en coordinación con el personal interno (hardening, revisión de GPOs, configuración de controles de acceso, revisión de sistemas de monitorización y explotación de registros, etc.).
 - Programa de vulnerabilidades y parcheo (plan, escaneos, remediación, informes).
 - Programa de métricas/KPIs ENS e informes mensuales.
- **Fase 3 – Auditoría interna ENS (meses 8 a 9)**
 - Plan de auditoría interna conforme ENS e ISO 19011.
 - Ejecución de auditoría interna completa (revisión documental y de evidencias, entrevistas, muestreos).
 - Informe de auditoría interna con hallazgos y plan de acciones correctoras (PAC).

- La auditoría interna será realizada por personal de la adjudicataria que no haya participado en ninguna de las actividades de implantación, mantenimiento o adecuación del sistema objeto del contrato, garantizando la independencia funcional conforme a lo establecido en la guía CCN-STIC 802.
- **Fase 4 – Preparación y acompañamiento a auditoría externa (meses 10 a 12)**
 - Cierre de no conformidades y verificación de evidencias.
 - Preparación de carpeta final y simulacro de auditoría.
 - Acompañamiento durante la auditoría externa de certificación prevista para abril de 2027.
 - La adjudicataria asumirá la contratación y el coste del auditor externo acreditado (Entidad de Certificación), incluyendo tasas y desplazamientos si aplica.

4. ENTORNO ACTUAL Y EVIDENCIAS DISPONIBLES

PLANIFICA MADRID dispone de un repositorio estructurado por dominios ENS

- Marco organizativo.
- Marco operacional y Medidas de protección: con documentos clave
- Política de Seguridad firmada, Normativa aceptada por usuarios

Categorización y DA, Análisis de riesgos 2025, INES, informes de auditorías interna/externa, GPOs, hardening Windows/Linux, inventario de activos, gestión de incidentes, KPIs y vigilancia (XDR, pruebas EICAR). Se han detectado áreas a completar (continuidad de negocio y pruebas, autenticación externos/internos con evidencias actualizadas, programa de protección frente a código dañino, libro de gestión de incidentes, cadena de suministro e interconexión, sello de tiempo, criptografía/ciclo de vida de certificados, y gestión formal de vulnerabilidades y parches).

5. REQUISITOS FUNCIONALES Y TÉCNICOS

1. Gobierno ENS: mantenimiento del Comité de Seguridad, actas y roles; actualización de PSI, normativa y procedimientos.
2. Gestión de riesgos: metodología, reevaluación 2026, plan de tratamiento y actas de aceptación.
3. Control de accesos: principios de mínimo privilegio, segregación de funciones, MFA/SSO, registro y revisión periódica.
4. Hardening y configuración segura: sistemas Windows/Linux, dispositivos de red, perímetro, correo y web; GPOs sin avisos pendientes.
5. Registro y correlación: explotación de logs y retención; evidencias de supervisión continua.
6. Código dañino: política AV/EDR, cobertura, firmas, excepciones y reportes.
7. Continuidad: BIA, PCN/DRP, medios alternativos y al menos 1 prueba ejecutada con acta en 2026.
8. Gestión de incidentes: proceso extremo a extremo, libro de incidentes y lecciones aprendidas.

9. Proveedores y nube: evaluación de riesgos de terceros, cláusulas ENS, interconexión segura, certificados de conformidad cloud y controles complementarios.
10. Vulnerabilidades y parches: calendario de escaneos, SLAs de remediación y evidencias de cierre.
11. Criptografía y certificados: inventario, ciclo de vida, rotación y respaldo de claves; alineación con CPSTIC.
12. Métricas e INES: cuadro de mando con indicadores y envíos/actualizaciones según corresponda.

6. EQUIPO MÍNIMO Y DEDICACIÓN

El equipo mínimo que el contratista ha de dedicar al contrato es el siguiente, configurándose como una obligación esencial a los efectos previstos en el artículo 211.1.f) de la LCSP:

- Un Director/a de Proyecto ENS: Técnico con titulación universitaria superior (grado o equivalente MECES nivel 2 o superior), en Ingeniería Informática, Ingeniería de Telecomunicaciones, Ingeniería Industrial o afines), con una experiencia de al menos tres años en implantación, mantenimiento o auditoría ENS y haber dirigido al menos dos proyectos ENS de categoría media o superior. Con experiencia en gestión de auditorías internas y externas ENS y en seguimiento de planes de tratamiento de riesgos y planes de adecuación y conocimiento del RD 311/2022, CCN-STIC 802, 808, 804/806, 815 y CPSTIC.
- Un Consultor/a ENS: Técnico con titulación universitaria superior (grado o equivalente MECES nivel 2 o superior), en Ingeniería Informática, Ingeniería de Telecomunicaciones, Ingeniería Industrial o afines, con una experiencia de al menos dos años en consultoría ENS y haber participado al menos en dos proyectos ENS en tareas de custodia de evidencias, actualización documental, revisiones de conformidad y análisis de brechas. Con conocimiento en CCN-STIC 808, 804/806 y 815/824.
- Un Especialista técnico en ciberseguridad: Con enfoque en hardening, GPOs, EDR/SIEM y continuidad. Con titulación de grado TIC o FP superior y experiencia de al menos dos años en sistemas Windows/Linux, AD/GPOs, SIEM/XDR/EDR, y administración de firewalls/VPN.

Haber participado en revisiones técnicas para proyectos de seguridad o ENS.

Se aportarán CVs. La sustitución de los perfiles aportados requerirá aprobación de PLANIFICA MADRID.

- El servicio incluirá una dedicación mínima estimada de 400 horas anuales, distribuidas regularmente durante la vigencia del contrato, incluyendo trabajo documental, técnico, reuniones de seguimiento y auditoría interna.

El reparto aproximado de dichas horas será:

Director ENS → **80 h**
Consultor ENS → **200–250 h**
Técnico → **60–80 h**

7. ENTREGABLES MÍNIMOS

El adjudicatario deberá presentar los siguientes entregables, cuya aprobación por parte de PLANIFICA MADRID será condición necesaria para el abono de las fases correspondientes:

7.1. Documentación de Gestión y Seguimiento

Informe de Revisión Inicial y Gap-Analysis: Estado de situación respecto al ENS 2026.

Plan de Trabajo 2026: Cronograma detallado con hitos, responsables y fechas clave.

Informes Mensuales de Seguimiento: Resumen de actividades, estado de los KPIs de seguridad y actas de las reuniones quincenales.

Índice Maestro Control-Evidencia (Documento Vivo): Matriz que mapea cada medida del ENS con su evidencia documental o técnica, indicando su ruta de acceso y vigencia.

7.2. Entregables Técnicos y Operativos

Cuerpo Normativo Actualizado: Políticas, procedimientos, normas y registros revisados o creados para cumplir con el RD 311/2022.

Programa de Vulnerabilidades y Parcheo: Informes periódicos de escaneo y seguimiento de la remediación (SLA: ≤15 días para críticas, ≤30 días para altas).

Paquete de Continuidad de Negocio (BCP/DRP): Plan de Continuidad y Recuperación ante Desastres actualizado, incluyendo el Acta de la prueba anual realizada en 2026.

Libro de Gestión de Incidentes 2026: Registro completo de incidentes, análisis de causa raíz y lecciones aprendidas.

7.3. Entregables de Auditoría y Certificación

Informe de Auditoría Interna ENS: Ejecutado conforme a la guía CCN-STIC 802, incluyendo el Plan de Acciones Correctoras (PAC) (Plazo de entrega: ≤15 días tras finalizar la auditoría).

Contrato con la Entidad de Certificación: Copia de la orden de servicio/contrato con la certificadora acreditada, gestionado y abonado por el adjudicatario.

Carpeta Final de Certificación: Compendio ordenado de todas las evidencias definitivas para la auditoría externa de abril 2027.

Guía de Defensa de Auditoría: Guía rápida para el personal de PLANIFICA MADRID que explica cómo defender cada control ante el auditor externo.

Certificado de Capacitación y Material Didáctico: Acta de la formación impartida al personal interno y grabaciones de las sesiones de transferencia de conocimiento.

Informe de Acompañamiento y Cierre: Documento final tras la auditoría externa que detalle la resolución de posibles hallazgos hasta la obtención del certificado.

8. NIVELES DE SERVICIO (SLA)

- Respuesta a consultas: ≤ 48 horas laborables.
- Reuniones de seguimiento: quincenales (mínimo), con acta.
- Cierre de “OJO, REVISAR” en GPOs y controles críticos: ≤ 60 días desde inicio.
- PCN/DRP redactado: ≤ 90 días; prueba ejecutada: ≤ 150 días.
- Primer informe de vulnerabilidades y plan de remediación: ≤ 60 días.
- Índice maestro control-evidencia v1: ≤ 30 días; versión final antes de auditoría interna.

9. PLAN DE TRABAJOS Y CRONOGRAMA DE REFERENCIA

El calendario se adaptará a la fecha de inicio del contrato para asegurar el acompañamiento a la auditoría externa de abril de 2027. A título indicativo:

Fase	Hitos principales	Meses	Entregables
1. Revisión y planificación	Gap análisis, DA y riesgos, Plan 2026, Índice maestro v1	1	Informe inicial + Plan 2026
2. Mantenimiento y evidencias	Implantaciones, políticas, evidencias, vulnerabilidades, KPIs, continuidad	2–8	Docs actualizados, informes mensuales, PCN/DRP + prueba
3. Auditoría interna	Ejecución auditoría, informe y PAC	8–9	Informe AI + PAC
4. Preparación, acompañamiento y cierre	Cierre PAC, simulacro, auditoría externa (abril 2027)	10–12	Carpeta final + informe acompañamiento + contratación EC

10. METODOLOGIA DE TRABAJO Y EJECUCION REMOTA

10.1. Régimen de Prestación del Servicio

El servicio se prestará íntegramente en modalidad de teletrabajo, 100% remoto, salvo en casos excepcionales que requieran presencia y previa aprobación de Planifica Madrid. El adjudicatario deberá disponer de los medios tecnológicos necesarios (conectividad, equipos y herramientas de colaboración) para garantizar la continuidad y calidad del servicio sin que ello suponga un coste adicional para PLANIFICA MADRID

10.2. Canales de Comunicación y Disponibilidad

Interlocución Síncrona: El adjudicatario garantizará disponibilidad técnica y de consultoría en horario de 09:00 a 14:00h de lunes a viernes, para la resolución de consultas ágiles vía email/Teams/Helpdesk.

Seguimiento Quincenal: Se establece la obligatoriedad de realizar una videoconferencia de seguimiento cada 15 días naturales. En dicha sesión, el adjudicatario presentará el estado de avance del Índice Maestro de Evidencias y el cronograma actualizado.

Gestión Documental Segura: El intercambio de evidencias y documentos de trabajo se realizará preferentemente a través de la plataforma SharePoint/OneDrive de la empresa o herramienta GRC del licitador, quedando expresamente prohibido el envío de evidencias con datos de carácter personal o configuraciones sensibles a través de correo electrónico sin cifrar.

10.3. Proactividad y Liderazgo del Proyecto

Al tratarse de un servicio remoto, el adjudicatario asume un rol proactivo. Esto implica:

Impulso de agenda: El consultor será responsable de convocar las reuniones necesarias con los responsables de cada área, si fuera necesario, para la captación de evidencias.

Acceso remoto: En caso de requerir revisiones técnicas (hardening, GPOs, revisión de logs), el adjudicatario utilizará los mecanismos de acceso remoto seguro (VPN) proporcionados por PLANIFICA MADRID, cumpliendo estrictamente con la Política de Seguridad de esta.

Grabación de sesiones de transferencia: Las sesiones de transferencia de conocimiento detalladas en el apartado correspondiente deberán ser grabadas y entregadas en formato vídeo como parte de los entregables finales.

10.4. Soporte en Auditoría Externa Remota

Durante los días de ejecución de la Auditoría Externa por parte de la Entidad de Certificación, el equipo del adjudicatario mantendrá una conexión permanente (sala virtual abierta) para dar soporte inmediato a PLANIFICA, realizar la defensa técnica de los controles y localizar evidencias en tiempo real ante el auditor.

11. PROTECCIÓN DE DATOS Y CONFIDENCIALIDAD

Toda la información se tratará como confidencial. Si existe acceso a datos personales, el adjudicatario actuará como encargado del tratamiento, firmando el correspondiente acuerdo conforme RGPD/LOPDGDD. Se seguirá el principio de mínimo privilegio y se respetarán las obligaciones ENS.

12. CRITERIOS DE ACEPTACIÓN

- Todas las medidas ENS aplicables con ≥ 1 evidencia válida, fechada 2026/27 y trazable en el Índice maestro.
- Auditoría interna realizada y PAC ejecutado/cerrado (o con justificación y acordada con PLANIFICA MADRID).
- Carpeta final completa y acompañamiento efectivo durante la auditoría externa.

13. SUPUESTOS Y DEPENDENCIAS

- Disponibilidad de personal clave de PLANIFICA MADRID para entrevistas y validaciones.
- Acceso a repositorios y entornos necesarios validado por personal de PLANIFICA MADRID
- Colaboración de proveedores críticos para evidencias de terceros.
- Calendario alineado con abril 2027 para certificación externa.

14. PROPIEDAD INTELECTUAL Y CUSTODIA DE EVIDENCIAS

La documentación generada será propiedad de PLANIFICA MADRID. La adjudicataria custodiará evidencias y material de trabajo, asegurando su transferencia ordenada a la finalización del contrato.

15. AUDITORÍAS

La ejecución del servicio se regirá por las siguientes condiciones de responsabilidad y contratación:

- Auditoría Interna: Será ejecutada directamente por el personal especializado de la adjudicataria, garantizando la independencia de funciones respecto a quienes hayan realizado la implantación o mantenimiento previo.
- Auditoría Externa de Certificación: El coste íntegro de la Entidad de Certificación acreditada por ENAC (incluyendo tasas, derechos de examen, emisión de certificado y posibles gastos de gestión) será contratado y abonado directamente por la adjudicataria. La selección de dicha Entidad de Certificación deberá ser propuesta por el adjudicatario con dos opciones posibles y contar con la aprobación expresa de PLANIFICA MADRID antes de su contratación formal.
- Liderazgo y Soporte en la Auditoría: El adjudicatario es el responsable de liderar la defensa técnica y documental durante todo el proceso de auditoría externa. Deberá estar presente de forma síncrona (remota) atendiendo a todas las peticiones del auditor y actuando como interlocutor técnico principal.
- Capacitación del Personal Interno: En el caso de que la presencia del consultor no fuera posible por causas de fuerza mayor, o como medida de refuerzo preventivo, la adjudicataria deberá haber formado previamente a una persona designada por PLANIFICA MADRID en los protocolos de defensa del sistema, proporcionándole la guía de evidencias necesaria para asegurar el éxito del proceso de certificación.

16. RIESGOS Y MEDIDAS DE MITIGACIÓN

- Retrasos en la disponibilidad de evidencias → Plan de captación intensivo y priorización por criticidad.
- Gaps técnicos complejos → Medidas compensatorias CCN-STIC y plan de mejora.
- Cambios organizativos → Actualización de roles y actas del Comité de Seguridad.
- Dependencias de terceros → Cláusulas ENS y plan de seguimiento de proveedores críticos.

Estructuras de trabajo

Tabla de Verificación del Cumplimiento del ENS (CCN-STIC 808)

La matriz oficial de verificación se entregará en formato Excel, con las siguientes columnas mínimas: Medida, Aplicabilidad, Evidencia (ruta/documento), Grado de implantación, Observaciones, Acción/PAC, Responsable, Fecha. La versión final deberá enlazar a las rutas reales del repositorio de evidencias de PLANIFICA MADRID.

Índice maestro control-evidencia

Documento vivo que mapea cada control/medida ENS con su evidencia concreta (uno o varios documentos), responsable y estado (OK / Pendiente / N.A.).

Lista inicial de las carencias detectadas

- Continuidad (PCN/DRP, pruebas, medios alternativos).
- Autenticación (externos/internos) con evidencias actualizadas.
- Protección frente a código dañino (política, cobertura, informes).
- Libro de gestión de incidentes 2026.
- Cadena de suministro e interconexión (evaluaciones, acuerdos, controles).
- Sello de tiempo (aplicabilidad y procedimiento/evidencias).
- Criptografía/certificados (inventario y ciclo de vida).
- Gestión de vulnerabilidades y parches.

Calendario de auditorías

Auditoría interna: dentro del año anterior a la renovación (2026). Auditoría externa: abril de 2027 (fecha a confirmar con la Entidad de Certificación).

TRANSFERENCIA DE CONOCIMIENTO

Durante el último mes de contrato, el adjudicatario realizará sesiones formales de transferencia de conocimiento al personal designado por PLANIFICA MADRID, incluyendo:

- Explicación estructurada del repositorio de evidencias.
- Estado actualizado del cumplimiento ENS.
- Riesgos abiertos y acciones pendientes.
- Recomendaciones de mejora futura.

Se entregará un Manual Operativo ENS actualizado que permita la continuidad del sistema sin dependencia de terceros.

En Madrid, a fecha de la firma.

<p>Firmado digitalmente por: NUÑO SANCHEZ JOSE LUIS Fecha: 2026.04.23 11:48</p> <p>José Luis Nuño Sanchez Jefe de Area de Sistemas</p>	<p>Firmado digitalmente por: BRONCANO JIMENEZ LORENZO MIGUEL Fecha: 2026.04.23 12:07</p> <p>Lorenzo Broncano Jiménez Director de Estrategia y Coordinación.</p>
---	--