



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

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HAN DE REGIR PARA LA REALIZACIÓN DE UN CONTRATO MIXTO DE SUMINISTRO DE LICENCIAS PARA UNA HERRAMIENTA DE GOBIERNO, RIESGO Y CUMPLIMIENTO CORPORATIVO Y DE LOS SERVICIOS PARA IMPLANTARLA, CON CARGO AL PLAN DE RECUPERACIÓN TRANSFORMACIÓN Y RESILIENCIA DEL GOBIERNO DE ESPAÑA – FINANCIADO POR LA UNION EUROPEA – NEXTGENERATIONEU (C11.I03.P14.S13)

ÍNDICE

1	INTRODUCCIÓN.....	3
2	OBJETO	4
3	DESCRIPCIÓN DEL SUMINISTRO	4
4	CARACTERÍSTICAS Y FUNCIONALIDADES DEL PRODUCTO.....	5
4.1	CARACTERÍSTICAS DE LA HERRAMIENTA A SUMINISTRAR	5
4.2	ADQUISICIÓN DE LA LICENCIA.....	12
4.3	IMPLANTACIÓN DE LA SOLUCIÓN OFERTADA.....	12
4.3.1	<i>Revisión de requisitos y diseño de la solución.....</i>	<i>12</i>
4.3.2	<i>Instalación y configuración de la solución.....</i>	<i>13</i>
4.3.3	<i>Documentación de la solución y transferencia de conocimiento</i>	<i>13</i>
4.3.4	<i>Formación.....</i>	<i>13</i>
4.3.5	<i>Garantía del producto</i>	<i>14</i>
5	CONDICIONES GENERALES DE ENTREGA	14
5.1	SEGURIDAD.....	14
5.2	AUDITORÍAS.....	15
5.3	HERRAMIENTAS	15
5.4	REPOSITORIO DE DOCUMENTACIÓN	16
6	FASES DE LA PRESTACIÓN DE LA PUESTA EN MARCHA	16
7	REQUISITOS Y CUALIFICACIÓN DE LOS PERFILES.....	17
8	HORARIO Y LUGAR DE PRESTACIÓN DEL SERVICIO	19
9	GARANTIA.....	19
10	PROPIEDAD INTELECTUAL	20
11	TRANSFERENCIA DE CONOCIMINETO.....	20
	ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA.....	21
A.	OBLIGACIONES GENERALES APLICABLES A TODOS LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA	21
B.	OBLIGACIONES GENERALES APLICABLES A LOS CONTRATOS FINANCIADOS CON CARGO AL PRTR	22

1 INTRODUCCIÓN

El Plan de Recuperación, Transformación y Resiliencia (PRTR) representa en España el instrumento para la implementación del proyecto “NextGeneration EU” (NEGEU), concebido con el objetivo de relanzar la actividad económica tras la crisis sanitaria provocada por COVID 19.

Los objetivos en torno a los que se estructura el PRTR se concretan en diferentes políticas Palanca y Componentes, los cuales se dividen a su vez en Reformas e Inversiones. Como refleja la siguiente tabla, el Plan de Transformación Digital de la Atención Primaria (AP) pertenece a unas de las seis líneas estratégicas en las que a su vez se subdividen las diferentes inversiones, en concreto a la Línea Estratégica 6 (Sanidad).

NextGeneration EU	Mecanismo Europeo de Recuperación y Resiliencia (MRR) / Plan de Recuperación para Europa
PRTR	Plan de Recuperación, Transformación y Resiliencia
Palanca IV	Una Administración para el Siglo XXI
Componente 11	Modernización de las Administraciones Públicas
Inversión 3	Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones Públicas de las CCAA y las EELL
Línea Estratégica 6	Sanidad / Plan de Transformación Digital de la Atención Primaria

Proyecto financiado por la Unión Europea a través del Mecanismo de Recuperación y Resiliencia-NextGeneration EU, instrumento financiero de la inversión C11.I3. Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones Públicas de las CCAA y las EELL, del Plan de Recuperación, Transformación y Resiliencia del Gobierno de España. Línea Estratégica 6: Sanidad. Plan de Transformación Digital de la Atención Primaria.

La realización del presente contrato se enmarca particularmente dentro del Plan de Transformación Digital de la Atención Primaria, que pertenece a una de las 6 líneas estratégicas en las que se subdivide la Inversión 3. En concreto: Línea Estratégica 6: Sanidad. Plan de Transformación Digital de la Atención Primaria. De acuerdo con este encaje, debe contribuir al siguiente hito:

N.º	Tipo	Definición	Indicador	Meta	Plazo máximo
169	Hito	Finalización de todos los proyectos de apoyo a la transformación digital del Ministerio de Hacienda y Función pública y de las Administraciones de las CC.AA. y de los Entes locales.			T2 2026

En particular la ejecución de este contrato colaborará con el ámbito de la transformación digital en términos de ciberseguridad de entre los ámbitos definidos en el objetivo CID 169.

El contrato se debe llevar a cabo bajo el principio del compromiso con el resultado, en línea con el enfoque de ejecución que plantea el Plan de Recuperación, Transformación y Resiliencia. Por ello, deberá asegurarse en todo momento la observancia concreta de los citados hitos, objetivos y plazos temporales. El despliegue del Plan de Transformación Digital de la Atención Primaria se implementa a través de **Proyectos Colaborativos**, concebidos como proyectos escalables a nivel nacional, primando la colaboración y participación de más de una Comunidad Autónoma, alineados con el Modelo de Ejecución Colaborativa por las CC. AA, en coordinación con el Ministerio de Sanidad.

Dentro del Plan de Transformación Digital de la Atención Primaria se establecieron diferentes Grupos de Trabajo y Líneas de Actuación. En cada uno de los Grupos de Trabajo constituidos, existen cuatro roles de participación diferenciados por las CC. AA. Intervinientes: Líder, Participante, Interesado y Alineado.

En el seno del citado Plan de Transformación Digital de la Atención Primaria, la Dirección General de Salud Digital (en adelante, DGSD) desempeña el rol de Comunidad Autónoma de "Participante", adscrito al Grupo de Trabajo **GT1.1 Tecnologías Transversales** y línea de Actuación "**1.1 CiberAP**", cuya licitación consiste en la adquisición de una herramienta de Gobierno corporativo, Riesgo y Cumplimiento (GRC), cumplimiento de medidas de protección de datos y seguridad de la información para el servicio de Salud de la Comunidad de Madrid, el cual será financiado por la Unión Europea con el fondo NextGenerationEU. La puesta en marcha deberá estar incluida dentro de la propia adquisición del producto y consistirá principalmente en la ejecución de las siguientes tareas:

- Implantación de la solución en la organización.
- Formación sobre su uso.
- Garantía del producto.

Con lo que se busca impulsar los sistemas de información y digitalización seguros para la implantación de cuatro acciones en el marco de la Estrategia de Salud Digital, estas son:

- Implementación de herramientas para facilitar la atención sanitaria en centros sanitarios inteligentes.
- Impulso a la atención personalizada adaptada a cada paciente en función de sus circunstancias de vida y de salud.
- Implementación de herramientas digitales evaluadas para el apoyo a los cuidados de personas con enfermedades crónicas y con altas necesidades.
- Impulsar la transformación digital de los procesos de soporte a la gestión para facilitar la evaluación y mejora continua de los servicios, la transparencia y la toma de decisiones basadas en datos.

2 OBJETO

El objeto del presente documento es establecer los requisitos mínimos que han de regir el **suministro, configuración e instalación de una herramienta de Gobierno corporativo, Riesgo y Cumplimiento** del Organismo en la normativa vigente en materia de protección de datos y seguridad de la información. La herramienta de Gobierno, Riesgo y Cumplimiento (GRC) permitirá:

- Optimizar la gestión del cumplimiento alineándolo con la gestión de riesgos internos.
- Entregar valor a corto, medio y largo plazo mediante una aproximación integrada y eficiente a GRC.
- Mejorar los procesos de negocio y las medidas de desempeño.
- Proveer a la gobernanza con información que permita tomar mejores decisiones estratégicas.
- Convertir la administración de riesgos en una fuente de ventaja competitivas.
- Integrar, gestionar y alinear negocio, riesgo y cumplimiento.

El suministro deberá cumplir con todas las especificaciones técnicas que se describen en los siguientes puntos.

3 DESCRIPCIÓN DEL SUMINISTRO

Este contrato tiene como objetivo la adquisición de una solución web para la gestión del riesgo y cumplimiento del Organismo en la normativa vigente en materia de protección de datos, seguridad de la información, continuidad del negocio, gestión de riesgos de terceros y calidad que le son de aplicación.

La licitación consiste en la adquisición de la licencia de una herramienta de GRC y su respectiva puesta en marcha para la Dirección General de Salud Digital (DGSD) y en quien delegue y el Servicio Madrileño de

Salud (SERMAS), y no se trata del desarrollo de un software a medida. La puesta en marcha deberá estar incluida y consistirá principalmente en la ejecución de las siguientes tareas:

- **Implantación de la solución en la organización:** Instalación y configuración de la herramienta GRC para su uso por la DGSD y el SERMAS.
- **Formación sobre su uso:** Sesiones de formación a los usuarios finales de la solución, incluyendo responsables de procesos y controles, así como al resto de personal involucrado. La formación se realizará en español, en modalidad presencial y/u online a través de la plataforma TEAMS, con una duración mínima de 20 horas.
- **Garantía del producto:** Sesión de apoyo para el arranque inicial, revisión trimestral de la plataforma, actualización y acompañamiento para el uso de la herramienta según recomendaciones del fabricante de la solución, y atención y resolución de incidencias relacionadas con el funcionamiento de la herramienta suministrada.

La herramienta debe cumplir con una serie de características técnicas y funcionales, incluyendo la gestión de riesgos, protección de datos personales, continuidad en el negocio, auditoría normativa, y la incorporación de normativa específica como el Esquema Nacional de Seguridad (ENS), RGPD, LOPDGDD, LPIC, ISO 27001, ISO 27002, ISO 22301, NIS2.

4 CARACTERÍSTICAS Y FUNCIONALIDADES DEL PRODUCTO

A continuación, se indican las características y funcionalidades de la herramienta, se deberán tener en cuenta los siguientes requerimientos.

4.1 Características de la herramienta a suministrar

1. Características técnicas de la herramienta:

- La herramienta debe contar con un modelo de arquitectura multi-entidad, incorporando dependencias e interrelaciones entre las diferentes gerencias territoriales que componen la Consejería de Sanidad (Salud pública, innovación y docencia, por ejemplo) y la Consejería de Digitalización (DGSD y Agencia de Ciberseguridad, por ejemplo).
- Acceso mediante interfaz basada en entorno web multiplataforma/navegador, con diseño responsive y alto nivel de usabilidad. Los navegadores soportados serán al menos Chrome, Microsoft Edge y Firefox ESR.
- Acceso por autenticación y autorización con usuario y contraseña, integrado con el sistema de autenticación del organismo/Single Sign On (SSO, OAUTH, SAML).
- Configuración multi-SAML, es decir, la posibilidad de disponer de más de una configuración SAML para integrarse con varios proveedores de identidad (IdP) en la misma plataforma.
- La plataforma debe permitir el acceso con doble factor de autenticación, el cual debe estar integrado en el Single Sign On Corporativo.
- La solución propuesta permitirá la integración con los directorios activos de la entidad, de forma que se haga más sencilla el alta y baja de usuarios.
- La autenticación y autorización deberá estar delegada en el sistema de Single Sign On del cliente.
- La creación de los usuarios se gestionará en el primer login del usuario en el sistema.
- Será una herramienta modular que no requiera hacer login cada vez que se cambia de módulo y que comparta información entre los módulos, al menos activos, terceros, catálogos de riesgos y metodologías de trabajo, catálogo de controles...
- La herramienta deberá ofrecerse en modalidad SaaS.
- La solución propuesta proporcionará una API de gestión de usuarios.
- La herramienta debe ser capaz de gestionar un sistema multiusuario que facilite realizar perfilado de usuarios en base a módulos/funciones.

- La solución deberá permitir el acceso a todos los módulos de la herramienta a los que tenga acceso (permisos) desde una misma sesión, sin que requiera del usuario múltiples autentificaciones.
- Deberá ser capaz de una integración con otros sistemas de información corporativos (CMDB basado en GLPI, sistema de ticketing corporativo basado en OTRS, correo electrónico mediante relay, suite ofimática de Office 365) a través de servicios web y/o APIs.
- Se valorará la integración con las herramientas CCN-CERT (como, por ejemplo, PILAR).
- La solución debe estar disponible en idioma español.

2. Características **funcionales** generales que debe incorporar como mínimo la solución ofertada:

- Los requisitos básicos que debe cumplir son:
 - o Inventario de activos y valoración.
 - o Metodología de evaluación de riesgos configurable.
 - o Categorización del sistema ENS.
 - o Declaración de aplicabilidad parcial y definitiva
 - o Evaluación de riesgos de seguridad, privacidad y continuidad de negocio.
 - o Gestión documental.
 - o Planes de tratamiento de riesgo.
 - o Auditorías internas.
 - o Planes de Acción Correctivas.
 - o Objetivos y mejoras.
 - o Indicadores.
 - o Análisis de Impacto en el Negocio.
 - o Planes de Continuidad.
 - o Programa de ejercicios y pruebas.
 - o Registro de incidentes.
 - o Gestión de roles y competencias.
 - o Gestión de reuniones, informes y actas.
 - o Registro de actividades de tratamiento.
 - o Gestión de ejercicios de derechos.
 - o Incorpora las siguientes regulaciones, normas y estándares: ENS, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, ISO 22301, NIST Cybersecurity Framework (CSF), DORA, Ley de Protección de Infraestructuras Críticas / Reglamento de Contenidos mínimos, LOPD y RGPD.
- Mapeo automático entre las normas, estándares o regulaciones incluidas en la herramienta, así como otras de interés, incluyendo al menos: ISO/IEC 27001, ISO/IEC 27002, ISO 22301, NIS2, ENS, RGPD, NIST CSF, ISO 42001.
- Mapeo con otras normas o regulaciones internacionales: Secure Control Framework (SCF), CIS Controls, HIPAA, NIST AI.
- Creación de normativas o frameworks de control por parte del usuario a través de la aplicación o plantilla.
- Gestión independiente de varias organizaciones u entidades, de modo que cualquier información que se registre o gestione en la plataforma estará asociada a una entidad. La herramienta permitirá establecer una entidad principal y otras secundarias.
- La herramienta debe permitir describir una supraentidad desde la cual se establezcan los marcos de control aplicables a cada entidad dependiente, el lanzamiento de los procesos en forma de planes y obtenga información sobre la situación del sistema a nivel global y en detalle. Las entidades dependientes se encargarán de ejecutar los planes establecidos desde la supraentidad.

- Permite jerarquía de activos, de tal forma que se pueda establecer una entidad principal que pueda trasladar activos a las secundarias, y sincronizar la información de dichos activos en el tiempo.
- La herramienta debe permitir que se incorporen a usuarios externos o con participación “puntual” en el sistema.
- Permita la gestión de terceros (proveedores) y los riesgos asociados.
- Tenga capacidades de carga y extracción de información y, eventualmente, de terceros a través de formatos de uso común como .csv.
- Tenga capacidad para ejecutar cargas de información por lotes.
- Sea escalable, tanto en número de usuarios como de soluciones/funcionalidades, permitiendo la incorporación de otros módulos.
- La solución debe contar con un gestor de procesos o capacidad para integrarse con gestores de procesos que permitan el diseño y despliegue de flujos de trabajo y planes de acción.
- Sea flexible a la hora de establecer normas y desplegar marcos de control a medida de las necesidades de la Comunidad de Madrid.
- Tenga capacidad de generar, de forma automatizada, un inventario y control de activos (tratamientos, sistemas de información, riesgos, amenazas, etc.). Y que pueda valorar estos activos.
- Disponga de mecanismos y conservación de trazabilidad (actividad de usuarios), generación de informes, plantillas, control de avisos y notificaciones.
- Sea capaz de generar un workflow, facilitando la cumplimentación de cuestionarios por personal propio o externo, incorporación de la documentación acreditativa (evidencias) y visualización de los objetivos de control, controles y visualización y corrección de riesgos asociados.
- La aplicación deberá permitir el envío de correos electrónicos configurables a modo de notificaciones, con un enlace para acceder al hito que lo ha generado.
- Sea capaz de incorporar mecanismos que ayuden y dinamicen a los profesionales especializados o no en esta cuestión: notificaciones, recordatorios, etc.
- Periódicamente detectará la información pendiente de introducir, agrupándola por responsable y enviará aviso mediante correo electrónico.
- Preste soporte general al cumplimiento del ENS.
- Preste soporte a la implantación de la LPIC en el organismo.
- Permita la elaboración y mantenimiento de los planes de operador y planes de protección específico en el marco de la LPIC.
- Permitirá que las acciones del plan de acción puedan referenciar y actualizar el estado de los controles del ENS u otras normas soportadas en la plataforma, incluidas las definidas por el usuario.
- Registro de incidentes, con posibilidad de parametrización de sus clases y tipología, pudiendo remitir cualquier incidente a cuentas de correo externas, previamente configuradas.
- La herramienta realizará un registro de actividad de usuario, pudiéndose mostrar a administradores, tanto a nivel general como por cada usuario.
- Carga de valores para el cálculo de indicadores desde documentos externos, por ejemplo, Excel, pudiendo automatizar los procesos de carga desde distintas fuentes: como mínimo SFTP y repositorio en SharePoint.
- La herramienta debe permitir la evaluación o auditoría del ENS, siendo posible a nivel de control o a nivel de los subrequisitos/subcláusulas de cada control.
- La herramienta debe permitir evaluaciones de prePIA parametrizables en base a un conjunto de tratamientos tipo configurables.
- La herramienta debe permitir trazar procesos/subprocesos/actividades/activos esenciales y activos de soporte, así como aportar vista de riesgos por activos, activos esenciales, actividades y/o procesos

- La herramienta debe permitir el cálculo dinámico de riesgos basado en el riesgo estimado y también basado en las posibles vulnerabilidades que afecten a cada activo.
- La herramienta debe permitir la generación de planes de continuidad de negocio en formato Word basado en plantilla, en base a la información recogida en el BIA.

3. En cuanto a **riesgos de terceros**, la herramienta deberá:

Permitir que terceros puedan identificarse como un activo en el sistema y vincularse con una tercera parte y su documentación asociada. Los riesgos de dicho activo podrán ser analizados, de acuerdo con las amenazas asignadas a dicho tipo de activo.

La herramienta permitirá mantener un inventario de terceras partes, junto a los documentos e interacciones relevantes.

La herramienta tiene que disponer de funcionalidades adicionales, como son:

- Gestión de cuestionarios para homologación de proveedores.
- Gestión de proyectos o contratos de terceros, cuestionarios de evaluación de proyectos y evaluación de riesgos de dichos contratos o proyectos.
- Evaluación de riesgos generales del tercero.

4. En cuanto a la **gestión de procesos**, la herramienta deberá:

Tener que dar la posibilidad de la creación de un árbol de servicios y un árbol de procesos con al menos 5 niveles de profundidad (incluyendo el nodo raíz). Permitiendo registrar sus actividades o subprocesos dependientes.

Por cada subproceso o actividad se tiene que poder detallar la siguiente información: Información general, Personas, TIC, Sistemas y otros activos, Instalaciones, Dependencias internas, Terceras partes, Otros recursos, Comunicaciones, Documentos.

5. En cuanto a la **capacidad de reporte**, la herramienta deberá:

- Hacer que todos los formularios que sean en modo tabla de la aplicación permitan la generación y gestión de vistas de datos, que podrán ser exportadas a ficheros en diversos formatos como csv, xlsx, json, pdf, etc.
- Incorporará capacidades de reporting avanzadas que permitan ver la evolución del sistema, facilitando el conocimiento general y de detalle de la situación, así como la incorporación de mecanismos de alerta a usuarios de acuerdo con su perfil.
- Tener capacidad de proveer cuadros de mando, indicadores y herramienta de análisis de datos, personalizados por perfil de acceso, que permitan identificar la exposición al riesgo de la organización, medir el progreso de implementación de los planes de acción o de una legislación concreta (entre otros).
- Integración a través de una API propia con PowerBI. Que permita generar un cuadro de mando en PowerBI integrado a través de API con la herramienta que recoja el nivel de madurez de los controles de normativa.
- Informes ad-hoc, y adicionalmente, incorporará informes específicos. Permitirá la creación de informes basados en plantillas Word.
- Generación en formato editable Word basado en plantillas, de informes de revisión por la dirección en base a los requisitos de los sistemas de gestión según ISO/IEC 27001 e ISO 22301.
- Las alertas tienen que poder ser generadas manual o automáticamente. En este último caso, al menos en los siguientes eventos: al registrar un ejercicio de derechos, cuando usuarios son asignados a controles, cuando se asignan acciones y/o tareas, cuando un usuario es asignado a un

indicador, cuando un usuario es asignado a un incidente, cuando un usuario es asignado a un hallazgo o no conformidad.

- Tiene que permitir edición de las alertas por parte del usuario de aspectos como: planificación, documentos adjuntos a la alerta, usuarios notificados. Las comunicaciones de la alerta se realizarán de acuerdo con la configuración que se establezca, bien entre fechas, diariamente, en determinados días de la semana, días del mes, o del año. El texto incluido en las comunicaciones de alerta tiene que ser configurable.
- Permite emitir comunicaciones vía e-mail en determinadas ocasiones:
 - Cuando se publica un documento.
 - Cuando un usuario contesta a un conjunto de controles.
 - Comunicación de agenda a los miembros de un comité o grupo.
 - Comunicación de convocatoria de ejercicio de continuidad de negocio a los participantes.
 - 7 y 3 días antes de que una acción vaya a finalizar de acuerdo con su fecha fin prevista, siempre que no se encuentre en estado finalizado.
- La herramienta permitirá establecer una firma de correo electrónico que acompañará a cualquier email enviado desde la plataforma, y deberá permitir configurar una cuenta de correo corporativa para dichos envíos.

6. En cuanto a la **gestión documental**, la solución debe tener:

- Un gestor documental o capacidad para integrarse con gestores documentales, especialmente con la suite de Microsoft Office 365, que permita la recogida de evidencias en los procesos de control.
- Tiene que almacenar documentos asociados a las siguientes funcionalidades:
 - Terceros:
 - Documentación relativa a cada tercero, p.ej. contratos, anexos, certificaciones, cláusulas, etc.
 - Interacciones realizadas con terceros como correos electrónicos y sus anexos.
 - Documentación adjunta por tercero en cada pregunta de los cuestionarios diseñados.
 - Roles y competencias:
 - Evidencias de asignación y/o comunicación de los roles.
 - Evidencias de cumplimiento de competencias, como certificados de formación, CV, diplomas u otros.
 - Evaluaciones y auditorías:
 - Informes de auditoría interna/externa.
 - Evidencias recopiladas en cada uno de los controles de la regulación, normativa o estándar evaluado o auditado.
 - Registro de Actividades de Tratamiento:
 - Formularios, formatos u otras evidencias de obtención de información.
 - Contratos/Clausulas legales.
 - Informe EIPD/PIA, EIL, u otros
 - Ejercicios de derechos:
 - Solicitudes de acceso y adjuntos.
 - Comunicaciones y emails intercambiados por el solicitante.
 - Comunicados y emails intercambiados internamente.
 - Comunicación de respuesta al solicitante.
 - Evaluaciones de riesgos de seguridad de la información y/o privacidad:
 - Informe de riesgos resultante.
 - Evaluaciones de riesgos empresariales (continuidad, etc.):
 - Informe de riesgos resultante.



- Gestión de cambios:
 - Documento de solicitud.
 - Evidencia de revisión.
 - Evidencia de aprobación.
 - Documento de requisitos de cambios.
 - Planes de continuidad de negocio:
 - Planes de continuidad y recuperación.
 - Programa de ejercicio:
 - Informes post-ejercicio.
 - Planes de acción:
 - Documentación relacionados con la acción o proyecto.
 - Gestión de incidentes:
 - Documentación relacionada con el incidente.
 - Evidencia de comunicación a regulador.
 - Evidencia de comunicación a sujetos (RGPD).
 - Evidencia de comunicación a responsable o encargado.
 - Comités:
 - Informes de revisión.
 - Actas de comité.
 - Además, debe permitir el registro y mantenimiento de documentos necesarios para la gestión.
 - Compartición de documentos tanto a usuarios internos como externos, con la posibilidad de tener registro, en ambos casos, de lectura de dichos documentos.
 - Posibilidad de decidir documentos que son compartidos dentro de cada organización o para usuarios de cualquier organización, sin necesidad de duplicar el documento por cada entidad.
 - Permite almacenar por cada documento: Tipo de documento, Nombre de documento, Versión, Fecha, Documento, Carpeta donde se ubica, Comentarios o metadatos, Elaborador, Aprobador, Estándares relacionados con el documento, Lista de distribución a usuarios de la plataforma, Lista de distribución a correos electrónicos externos o internos, Histórico de versiones, Histórico de revisiones.
7. Sobre el **sistema de gestión**, la solución ofertada deberá:
- Tener capacidad de contemplar la gestión y actividad de diferentes Comités de seguridad y protección de datos pertenecientes a las distintas entidades que componen el Servicio de Salud de la Comunidad de Madrid.
 - Todos estos análisis y recogida de evidencias se han de poder vincular entre si evidenciado aquellas relaciones “causa – efecto” existentes (GRC, riesgos penales, etc.)
 - Elaboración de planes directores de seguridad en base a recomendaciones de auditorías.
 - Ayude en la gestión y control durante procesos de certificación (ENS, ISO 27001, etc).
 - Facilite la Gestión del SGSI.
8. Sobre la **gestión de riesgos**, será necesario que el producto tenga:
- Capacidad de importar análisis de riesgos preconfigurados con metodologías reconocidas y estandarizadas para evaluar las amenazas y el impacto.
 - Disponibilidad de un catálogo de amenazas actualizado para implantar los controles necesarios con el objetivo de mitigar los riesgos. Al menos deberá incorporar la relativa a ENS nivel alto para AARR: Refuerzo 2.
 - Soportará MAGERIT como metodología de riesgo, entre otras.
 - Los niveles y valores de riesgo serán configurables. Y la asociación de clases de activos, amenazas y controles parametrizados en la herramienta, será personalizable.
9. En cuanto a la **protección de datos personales**, la herramienta deberá:
- Dar soporte general al cumplimiento del RGPD.

- Realizar el registro de actividades de tratamiento de datos por parte del servicio de salud.
- Llevar un control de las transferencias internacionales de datos.
- Gestionar la atención de derechos, solicitudes, consultas y reclamaciones al DPD.
- Evaluaciones de impacto y riesgos de privacidad sobre las actividades de tratamiento.
- Realizar análisis de necesidad de elaborar evaluaciones de Impacto de Privacidad.
- Gestionar y Notificar brechas de seguridad en lo que respecta a datos.
- Indicadores y cuadros de mandos relativos a los procesos de privacidad.
- Gestión de reuniones de comités de privacidad o de grupos internos con responsabilidad sobre la privacidad.
- Generación de informes de evaluaciones de interés legítimo y evaluaciones de transferencias internacionales, evaluaciones de impacto en la privacidad, y vista resumida del Registro de Actividades de Tratamiento (RAT), en formato editable Word basado en plantillas.

10. Con respecto a la **continuidad de negocio**, la herramienta deberá:

- Elaboración y gestión de Análisis de Impacto en el Negocio a nivel de proceso y establecimiento de requisitos de recuperación a nivel de subproceso o actividad.
- Elaboración y gestión de planes de continuidad.
- Gestión y planificación de planes de pruebas y ejercicios de continuidad.
- Generación de informes BIA en formato .docx.
- Definición de estrategias de recuperación y generación de informe en formato .docx.
- Posibilidad de almacenamiento de planes elaborados por el contratante.
- Gestión de programas de ejercicios y pruebas, pudiendo definir y planificar diversos tipos de pruebas, e incorporando las siguientes funcionalidades:
 - o Inclusión de los planes.
 - o Inclusión de las personas críticas convocadas para cada ejercicio y comunicación vía e-mail.
 - o Posibilidad de incluir un checklist por cada plan para su cumplimentación.
 - o Generación de informe post-ejercicio en formato .docx.
 - o Registro de acciones de mejora en base a los resultados obtenidos.

11. Sobre la **auditoría normativa**:

- Creación de planes de auditoría
- Soporte a auditorías de cumplimiento normativo, en especial del Esquema Nacional de Seguridad y RGPD.
- Realización de auditorías colaborativas (distribución de cuestionarios) entre todos los roles implicados en la misma sin necesidad de dar de alta a todos los agentes en la solución, pudiendo además adjuntar evidencias.
- Elaboración de informes de auditoría.
- Gestión de resultados de auditoría a través del Plan de Acción.
- Elaboración de Plan de Acciones Correctivas en base a las deficiencias encontradas.
- Para cada informe de auditoría se generará de forma automática un plan de acciones y seguimiento de cada una de las recomendaciones, incidencias, limitaciones o salvedades en plazos y cantidades, de informe de finalización y de aprobación por parte de la auditoría.
- Gestión y seguimiento de recomendaciones. Retroalimentación de auditoría previas incluyendo también la información actualizada de las recomendaciones aplicadas.
- Introducción de resultados en forma de hallazgos.
- Posibilidad de enviar auditorías a terceros, seleccionando previamente los controles que son aplicables.
- Auditorías colaborativas que permitan que distintos usuarios o roles accedan al sistema y contesten sólo a los controles a los que han sido asignados.
- Obtención de informes tabulares, gráficos y un informe de auditoría en formato .docx.
- Posibilidad de que un usuario asignado a un control, re-asigne a otro usuario.

A continuación, se indica la **normativa** que debe incorporar la herramienta:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). o Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (LPIC).
- UNE-ISO/IEC 27001, Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (ISO 27001).
- UNE-ISO/IEC 27002, Código de buenas prácticas para la Gestión de la Seguridad de la información (ISO 27002).
- UNES-ISO/IEC 22301, Sistema de Gestión de la Continuidad de Negocio (ISO 22301).
- Durante la vigencia de las licencias, la empresa adjudicataria será responsable de mantener actualizado el marco normativo atendiendo a cualquier cambio que pudiera sufrir dicha normativa.

4.2 Adquisición de la licencia

Se suministrará una licencia corporativa para cubrir todas las necesidades del Servicio Madrileño de Salud para disponer de una herramienta Gobierno corporativo, Riesgo y Cumplimiento (GRC), que cumpla con todos los requisitos indicados anteriormente en este mismo documento, y, además, se debe incorporar el mantenimiento durante la ejecución del proyecto.

No habrá límite de usuarios, entidades y servicios/departamentos para su uso durante un plazo de 4 años. Los usuarios tendrán que pertenecer a la Consejería de Digitalización o a la Consejería de Sanidad, incluidos los terceros que les puedan estar prestando servicio para la atención al Servicio Madrileño de Salud o a la DGSD.

Las licencias, por cuatro años, deben estar disponibles desde el arranque del proyecto.

4.3 Implantación de la solución ofertada

Para la puesta en marcha del producto, y como parte fundamental de la propia adquisición de la licencia, será necesaria la implantación y el despliegue de esta en la organización. Para ello, se deberán tener en cuenta:

4.3.1 Revisión de requisitos y diseño de la solución.

- A partir de la firma del contrato, se realizará la reunión de lanzamiento que supondrá el inicio del periodo de puesta en marcha de la solución.
- Se realizará una revisión de los requisitos para la cual, el adjudicatario contará con alta participación de la DGSD o quien ella designe. En esta revisión de requisitos se deberán analizar, las necesidades el cumplimiento de los requisitos técnicos y funcionales de la herramienta indicados en este documento.
- El proceso de revisión de requisitos técnicos y funcionales deberá incluir los roles, el establecimiento de marcos normativos y perfiles de cumplimiento, etc.

- Como parte de los trabajos realizados previo al despliegue y configuración, el adjudicatario también deberá elaborar:
 - o Plan de implantación herramienta GRC.
 - o Plan general del proyecto.

4.3.2 Instalación y configuración de la solución.

Atendiendo al diseño y configuración propuestos y validado por la DGSD, siguiendo el plan de actuación acordado por ambas partes, el adjudicatario tendrá que ejecutar las siguientes actividades:

- Diseño y despliegue de la solución para el SERMAS.
- Configuración y parametrización inicial de la herramienta.
- Carga inicial de información.
- Integración con las herramientas corporativas.

En la fase de implantación, el adjudicatario deberá informar del avance de la implantación, elaborando un acta de contenido tratado y acuerdos alcanzados. Sin perjuicio de eventuales pruebas unitarias y funcionales, se realizará una completa simulación de auditoría al término de la implantación para confirmar el correcto funcionamiento del sistema.

4.3.3 Documentación de la solución y transferencia de conocimiento

El adjudicatario deberá documentar la solución desplegada para una correcta operación del producto. Dicha documentación, deberá constar de:

- Descripción y diseño de la solución.
- Inventario de los activos.
- Documentación técnica, incluyendo la documentación relacionada con el traspaso de la gestión del producto.
- Gestión del producto, dando respuesta a los siguientes conceptos de gestión: conocimientos, activos, configuración, copias de seguridad, eventos, peticiones, incidencias, disponibilidad, reporte, cambio, continuidad y capacidad.
- Cumplimiento de los requisitos acordados.

Toda documentación debe ser entregada tras finalizar la implantación de la herramienta en la organización. Además, debe mantenerse actualizada en función de que el producto vaya evolucionando.

4.3.4 Formación

Dentro de la puesta en marcha del producto y como tarea de la propia adquisición de este se deben realizar sesiones de formación tanto a los usuarios finales de la solución, como a los gestores de la plataforma.

En relación con estas sesiones formativas, se deberán tener en cuenta las siguientes consideraciones:

- La formación deberá realizarse una vez concluidos los trabajos de implantación de la herramienta y dentro de los 4 meses planificados para la puesta en marcha del producto.
- La formación incluirá a los responsables de los procesos y los responsables de los controles, así como al resto de personal implicado en los procesos.
- La formación implicará al personal que indique la DGSD y deberá incluir todos los aspectos ligados a la configuración y uso de la herramienta.
- La formación se realizará en español.
- La formación se realizará en modalidad presencial y/u online vía TEAMS, donde podrán ser grabada con previo consentimiento por los asistentes de la sesión formativa.
- La formación tendrá una duración mínima de 20 horas.

4.3.5 Garantía del producto

Corresponde al adjudicatario, como parte del suministro de las licencias, la garantía y mantenimiento de esta una vez puesta en marcha en el organismo durante el plazo de vigencia de estas. Para ello, se contemplan como mínimo las siguientes actividades:

- Sesión de apoyo y acompañamiento en el arranque inicial.
- Revisión trimestral de la herramienta.
- Actualizaciones de la herramienta según recomendación del fabricante y en coordinación con las necesidades de la DGSD.
- Atención y resolución de incidencias relacionadas con el funcionamiento de la herramienta.

5 CONDICIONES GENERALES DE ENTREGA

5.1 Seguridad

En materia de seguridad de la información, es fundamental que el adjudicatario alcance entre otros, los siguientes objetivos:

- Garantizar un adecuado nivel de seguridad de la configuración de la herramienta suministrada. El adjudicatario tendrá que contemplar la seguridad en los diferentes momentos del ciclo de vida de la herramienta. Estas actuaciones permitirán gestionar los riesgos de seguridad en todo momento, y tomar las decisiones que se consideren oportunas.
- Garantizar la correcta implantación del modelo de seguridad en herramienta suministrada, marcado por el Servicio de Seguridad de Sistemas de Información de la DGSD y por la Agencia de Ciberseguridad de la Comunidad de Madrid, involucrando a los equipos de seguridad desde el inicio de los trabajos de diseño y configuración de la herramienta, haciendo las pruebas que sean necesarias, garantizando en todo caso las medidas de ciberseguridad y seguir las pautas marcadas en general.
- Cumplir con todos los requerimientos que sean de aplicación de acuerdo en el marco normativo de seguridad vigente de la Comunidad de Madrid y de todas las actualizaciones posteriores que se produzcan, así como en todo el marco legal en materia de ciberseguridad que sea de aplicación (por ejemplo, Esquema Nacional de Seguridad y Reglamento General de Protección de Datos).
- Disponer de los recursos adecuados para llevar a cabo la ejecución de las tareas que le correspondan en el modelo de cumplimiento, dando respuesta en los plazos marcados por el Servicio de Seguridad de Sistemas de Información.
- Dar cumplimiento como encargado de tratamiento a aquello establecido en el Reglamento General de Protección de Datos. Por lo que hace la seguridad en el tratamiento de las mismas, el adjudicatario implementará las medidas de seguridad establecidas por el Servicio de Seguridad de Sistemas de Información y la Agencia de Ciberseguridad de la Comunidad de Madrid en el marco de Ciberseguridad para la Protección de Datos. Esta implementación y nivel de cumplimiento serán incorporados al modelo de cumplimiento normativo de la Comunidad de Madrid.
- Asumir la corrección de todas aquellas vulnerabilidades de seguridad para cumplir con los umbrales solicitados por el Servicio de Seguridad de Sistemas de Información, a partir de los cuales la herramienta podrá ser utilizada.

- Asumir la corrección de todas aquellas vulnerabilidades de seguridad detectadas en los análisis de seguridad. El Servicio de Seguridad de Sistemas de Información podrá ejecutar en cualquier momento los análisis de seguridad que considere oportunos.
- Garantizar el despliegue efectivo de la estrategia de ciberseguridad determinada por el Servicio de Seguridad de Sistemas de Información, velando por la implementación efectiva de los diferentes servicios, procesos y tecnologías que la componen.

5.2 Auditorías

La Agencia de Ciberseguridad de la Comunidad de Madrid, el Servicio de Seguridad de Sistemas de Información (OSSl) o cualquier organismo competente de la Comunidad de Madrid podrán revisar o auditar la correcta ejecución de los procesos de seguridad con la periodicidad que consideren necesaria.

En todos aquellos casos en que se decida la realización de una auditoría, el adjudicatario tendrá que garantizar el acceso total, incondicional e irrevocable a los documentos y herramientas existentes que estén relacionadas con las prestaciones de los servicios.

El adjudicatario proporcionará la asistencia y la información que requieran las auditorías, sin cargo adicional para la Consejería de Digitalización. La información se proporcionará en la forma y tiempos requeridos.

La realización de la auditoría en ningún momento eximirá al adjudicatario del cumplimiento de los compromisos derivados de la licitación.

En la finalización de la auditoría las partes revisarán las desviaciones y/u observaciones detectadas, elaborando un plan de acción. El conjunto del resultado será firmado por ambas partes.

El adjudicatario, de acuerdo con el calendario establecido en el plan de acción, se compromete a informar del estado y a llevar a cabo las actividades establecidas en el plan de acción. La DGSD podrá verificar que el plan de acción se ha implementado correctamente.

5.3 Herramientas

La DGSD determinará y/o proporcionará las herramientas que soportan los procesos para gestionar y gobernar los servicios TIC. Se tendrán que cumplir los siguientes condicionantes:

- El adjudicatario tendrá que usar las herramientas propuestas por la DGSD en las condiciones que este establezca.
- El adjudicatario se hará cargo (en caso de que haya) de los costes asociados al uso de estas herramientas (acceso, licenciamiento, integración, etc..). Con el fin de asegurar la operativa de los procesos de gobernanza, la DGSD podrá establecer unos volúmenes mínimos de licencias a adquirir para ciertas de las herramientas.
- El adjudicatario podrá proponer modificaciones en las herramientas para obtener una mejor eficiencia y calidad en el servicio, siempre que se asegure la continuidad de los acuerdos de nivel del servicio. Cualquier petición de cambio tendrá que estar documentada previamente para que la DGSD pueda analizar y autorizar la conveniencia de su implantación.
- El adjudicatario podrá hacer uso de herramientas adicionales, previa autorización de la DGSD. Eso no lo exime del cumplimiento y del uso de las herramientas que haya determinado la DGSD. El uso de estas herramientas adicionales no puede deteriorar el servicio o suponer un sobre coste.

El uso de estas herramientas adicionales no puede poner en riesgo la continuidad del servicio después de la finalización de la relación contractual.

- La DGSD podrá evolucionar las herramientas escogidas en cualquier momento de la duración del contrato.
- Se reserva el derecho de incorporar nuevas herramientas. En cualquier caso, se dará un preaviso a los proveedores de un mínimo de 2 meses antes de su implantación.

5.4 Repositorio de Documentación

Se pondrá a disposición del adjudicatario un repositorio donde intercambiar la documentación en lo referente a la provisión del servicio y los procesos de gobernanza de este. En esta herramienta el adjudicatario guardará también los documentos entregables resultantes de la ejecución del servicio y de los proyectos relacionados.

Este repositorio será la fuente única de documentos entregables, y el resto de las herramientas de gobernanza tendrán que hacer referencia a este repositorio. El adjudicatario será el responsable de mantener la información actualizada y siguiendo las políticas, nomenclatura y control de versiones determinados por la Oficina Técnica correspondiente.

6 FASES DE LA PRESTACIÓN DE LA PUESTA EN MARCHA

Las fases que se consideran necesarias para la puesta en marcha de la herramienta son:

- **Fase de revisión de requisitos y diseño de la solución**

En la que las principales tareas son:

- Analizar las necesidades y el cumplimiento de los requisitos técnicos y funcionales de la herramienta indicados en este documento.
- Realizar la revisión de los requisitos técnicos y funcionales, de los roles necesarios, el establecimiento de los marcos normativos y los perfiles de cumplimiento, etc.
- Como parte de los trabajos realizados previo al despliegue y configuración, el adjudicatario también deberá elaborar:
 - Plan de implantación.
 - Plan general del proyecto.

Plazo estimado para esta fase: máximo 1 mes.

Con la entrega de la documentación de esa fase y la disponibilidad de la licencia de la herramienta GRC se dará por concluido el hito 1 una vez certificado por la DGSD.

- **Fase de implantación, configuración de la solución y transferencia del conocimiento:**

En la que las principales tareas son:

- Diseño y despliegue de la solución para el SERMAS.
- Configuración y parametrización inicial de la herramienta.
- Carga inicial de información.
- Integración con las herramientas corporativas necesarias.
- Formación a los usuarios según los requisitos indicados en el apartado 4.3.4. de este documento.
- Documentación de la solución implantada.

Plazo estimado para esta fase: máximo 3 mes.

Con la finalización de los trabajos y tareas de estas dos fases, se dará por finalizado el hito 2 tras su certificación por la DGSD.

7 REQUISITOS Y CUALIFICACIÓN DE LOS PERFILES

Los equipos que prestan el servicio objeto de este contrato tienen que disponer de los conocimientos funcionales y tecnológicos específicos relacionados con el contexto funcional, así como sobre las plataformas tecnológicas que utilizan, con las herramientas de gestión y/o con las normativas y estándares de la DGSD.

Para la prestación de los servicios se considera la siguiente estimación de recursos por perfil:

Perfil	Nº de personas	Número de horas totales por perfil
Jefe de Proyecto	1	656
Consultor	1	656
Analista	1	656
Total	3	1.968

Los requisitos mínimos de titulación académica, formación y experiencia profesional que deben cumplir los perfiles se detallan a continuación:

Para el cumplimiento de los requisitos exigidos en materia de titulación en el presente pliego, se tomará como referencia el Marco Español de Cualificaciones para la Educación Superior (MECES), el catálogo de Títulos Universitarios "Pre-Bolonia" y el Marco Europeo de Cualificaciones (EQF, European Qualifications Framework):

- **Titulación de Máster:** MECES nivel 3 (equivalente a EQF nivel 7). Titulación oficial académica de Máster Universitario, Licenciado o Ingeniero.
- **Titulación de Grado:** MECES nivel 2 (equivalente a EQF nivel 6). Titulación oficial académica de Grado, Diplomado Universitario o Ingeniero Técnico.
- **Titulación de Técnico Superior en Formación Profesional:** MECES nivel 1 (equivalente a EQF nivel 5). Titulación oficial académica de ciclo formativo de técnico superior o equivalente.

Cada nivel MECES engloba a todos los niveles inferiores, por lo que se aceptará cumplido el requisito de titulación cuando se presente una titulación igual o superior a la requerida.

Perfil JEFE DE PROYECTO
Titulación Académica
<ul style="list-style-type: none"> • <u>Antes de Bolonia:</u> Licenciado o Ingeniero Superior o todas sus equivalencias. • <u>Después de Bolonia:</u> Nivel 3 (Máster) MECES o Nivel 7 EQF o todas sus equivalencias. • Alternativamente, se admitirá la titulación universitaria de Diplomado o Ingeniero Técnico o todas sus equivalencias (antes de Bolonia), o Nivel 2 (Grado) MECES o Nivel 6 EQF o todas sus equivalencias, en las áreas citadas, siempre y cuando se acrediten <u>24 meses de actividad adicional a la solicitada</u> en la experiencia profesional mínima requerida.
Experiencia Profesional
<ul style="list-style-type: none"> • Experiencia mínima de 5 años como jefe de proyecto de proyectos de ciberseguridad, gestión de riesgos o compliance.

Perfil Consultor
Titulación Académica
<ul style="list-style-type: none"> • <u>Antes de Bolonia:</u> Licenciado o Ingeniero Superior o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o ciencias.

<ul style="list-style-type: none"> • <u>Después de Bolonia</u>: Nivel 3 (Máster) MECES o Nivel 7 EQF o todas sus equivalencias, en las áreas de ingeniería, informática o ciencias. • Alternativamente, se admitirá la titulación universitaria de Diplomado o Ingeniero Técnico o todas sus equivalencias (antes de Bolonia), o Nivel 2 (Grado) MECES o Nivel 6 EQF o todas sus equivalencias, en las áreas citadas, siempre y cuando se acrediten <u>24 meses de actividad adicional a la solicitada</u> en la experiencia profesional mínima requerida.
Experiencia Profesional
<ul style="list-style-type: none"> • Experiencia mínima de 3 años en proyectos para organizaciones vinculados con la gestión y mitigación de riesgos, el aseguramiento del cumplimiento normativo y la mejora de la gobernanza. • Experiencia mínima de 1 año en implantación de herramientas de GRC.
Perfil ANALISTA
Titulación Académica
<ul style="list-style-type: none"> • <u>Antes de Bolonia</u>: Diplomado o Ingeniero técnico o todas sus equivalencias en cualquiera de las áreas de ingeniería, informática o ciencias (física, matemáticas, química, etc.). • <u>Después de Bolonia</u>: Nivel 2 (Grado) MECES o Nivel 6 EQF o todas sus equivalencias, en las áreas de ingeniería, informática o ciencias. • Alternativamente, se admitirá la Titulación de Técnico Superior en Formación Profesional cuando se acrediten <u>12 meses adicionales de actividad adicional</u> a la solicitada en la experiencia profesional mínima requerida.
Experiencia Profesional
<ul style="list-style-type: none"> • Experiencia mínima de 2 años en implantación de herramientas GRC. • Experiencia mínima de 1 año en formación a usuarios de herramientas GRC.

Las principales funciones, sin ánimo de ser una lista exhaustiva, de cada perfil serán:

- **Jefe de proyecto**
 - Planificar las actividades del proyecto.
 - Realizar el análisis de las desviaciones del proyecto (alcance, coste y tiempo).
 - Gestionar y hacer seguimiento del proyecto.
 - Gestionar los recursos asignados al proyecto.
 - Gestionar y coordinarse con los proveedores de otros sistemas que tengan dependencias con el proyecto.
 - Gestionar los cambios.
 - Gestionar los riesgos.
 - Establecer acciones de mitigación cuando sean necesarias.
- **Consultor**
 - Toma de requisitos para la configuración de la solución
 - Valoración de alternativas para peticiones de cambios durante la ejecución
 - Diseño de la solución global a implantar
 - Realización de presentaciones sobre las características de la herramienta los usuarios.
 - Resolución de dudas técnicas o funcionales.
- **Analista**
 - Definir las parametrizaciones necesarias y realizar la configuración de la solución.
 - Apoyar en la carga de información en la solución.
 - Realizar actividades formativas a usuarios finales.
 - Realización de pruebas de la solución.

8 HORARIO Y LUGAR DE PRESTACIÓN DEL SERVICIO

Los profesionales que formen parte del servicio estarán ubicados, en su mayor parte, en las instalaciones del adjudicatario, y serán por cuenta del adjudicatario todos los costes asociados a sus puestos de trabajo y su operación y mantenimiento: espacio de oficina, mobiliario, ordenadores personales, infraestructura técnica y de comunicaciones, consumibles y similares.

Las instalaciones, edificios y dependencias utilizados para la localización del servicio tendrán que cumplir en cualquier momento con todos los requisitos de construcción, habitabilidad, seguridad y ergonomía estipulados por la normativa vigente de la Comunidad de Madrid.

Hace falta tener en cuenta que, por necesidades del servicio, se podría solicitar el desplazamiento de cierto personal responsable del adjudicatario a las dependencias que la DGSD determine, bien durante periodos concretos, por coordinación de proyectos o cualquier otra necesidad que se determine. En estos espacios la DGSD proporcionará el mobiliario del puesto de trabajo y conexión en la red LAN y acceso a Internet, y el adjudicatario será el responsable de la provisión del resto de equipamiento necesario (ordenadores sobremesa/portátiles, tablet, terminales de telefonía móvil, etc.) para el desarrollo de las tareas.

Los servicios tienen que estar dimensionados para poder absorber las variaciones de carga y cumplimiento de los plazos establecidos en el presente pliego.

Alguno de los servicios requerirá que determinadas actividades, con el fin de evitar impacto en la continuidad o disponibilidad del sistema, se realicen en días festivos y/o fuera del horario normal. Estas actividades se entienden incluidas dentro del alcance del servicio a prestar para el adjudicatario y no serán objeto de facturación adicional ni de cambio de tarifa. En estos casos, e independientemente del nivel de soporte, se requiere cierta flexibilidad al horario para la realización de actividades extraordinarias que se tengan que realizar fuera del horario establecido en la prestación de cualquiera de los servicios ámbito del contrato.

Algunos ejemplos de situaciones en las que es de aplicación son, entre otros:

- Soporte a periodos de alta actividad que requieren de la prolongación del horario habitual (convocatorias, campañas...).
- Soporte asociado a hitos críticos de procesos de negocio.
- Soporte funcional extraordinario por prolongación puntual de la jornada laboral del empleado público.
- Actuaciones en producción fuera de horario de servicio para minimizar el impacto en el servicio.
- Puesta en marcha del aplicativo.
- Migraciones de datos con impacto en el servicio.

Asimismo, el adjudicatario asumirá sin cargo adicional los eventuales costes de desplazamiento que por necesidad del servicio sean requeridos.

9 GARANTIA

Corresponde al adjudicatario, como parte del suministro de las licencias, la garantía y la actualización de la herramienta, una vez puesta en marcha en el organismo, durante el plazo de vigencia de estas.

Durante el periodo de vigencia el adjudicatario se compromete a enmendar cualquier error que pudiera aparecer asociado a la configuración o puesta en marcha realizadas por este, así como a actuar con el fabricante de la herramienta en caso de que exista algún fallo o error que pueda afectar al correcto uso de la misma sin que ello suponga ningún cargo adicional.

10 PROPIEDAD INTELECTUAL

El contratista acepta expresamente que todos los derechos de propiedad intelectual sobre las configuraciones, parametrizaciones, adaptaciones, implementaciones complementarias, estudios, documentos, productos, subproductos, etc., generados al amparo del presente contrato, corresponden únicamente a la DGSD, con exclusividad y a todos los efectos, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el contratista autor material de los trabajos.

Así, podrán ser reutilizados sin coste en cualquier otra implantación en el ámbito del SERMAS o del SNS.

No se incluye en el anterior apartado los derechos de uso sobre los productos protegidos con propiedad intelectual y que se adquieran para la puesta en marcha de los sistemas citados como complemento a esta contratación.

El contratista adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudieran corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de la DGSD.

11 TRANSFERENCIA DE CONOCIMIENTO

Durante la ejecución de los trabajos objeto del contrato, el contratista adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por la DGSD, la información y documentación que soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos. Los trabajos objeto del presente contrato deberán ser convenientemente documentados, para lo que el contratista adjudicatario se compromete a generar toda la documentación que sea aplicable.

Asimismo, el contratista adjudicatario se compromete, previo al final de su contrato, proporcionar a la DGSD toda la documentación relacionada con sus trabajos realizados durante el proyecto, en el formato establecido y compatible con sus herramientas aportadas para gestionar la documentación. A la finalización del contrato el personal de la DGSD y las empresas que ella establezca habrán sido capacitados de forma tal que puedan asumir la gestión autónoma de todos los trabajos incluidos y el pleno conocimiento de la información relacionada.

En relación con este punto, la DGSD y previo a la finalización del contrato con el contratista, podrá requerir de ellos las sesiones de aclaración de cualquier aspecto relacionado con sus trabajos.

La transferencia deberá contemplar tanto el conocimiento tácito como el explícito, por lo que deberán de contemplarse las sesiones de transferencia de conocimiento necesarias entre el contratista adjudicatario y la DGSD.

Madrid,

LA DIRECTORA GENERAL DE SALUD DIGITAL

Firmado digitalmente por: RUIZ HOMBREBUENO NURIA
Fecha: 2025.10.31 14:42

ADENDA PARA LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA

A.OBLIGACIONES GENERALES APLICABLES A TODOS LOS CONTRATOS FINANCIADOS CON CARGO AL PRESUPUESTO DE LA UNIÓN EUROPEA

Resultan de obligado cumplimiento las normas establecidas en el Reglamento Financiero de la UE para los gastos financiados, estableciéndose las siguientes obligaciones:

1. ADECUACIÓN DEL CONTRATO A LAS PREVISIONES ESPECÍFICAS DEL INSTRUMENTO DE PLANIFICACIÓN ESTRATÉGICA

El contrato deberá cumplir las condiciones previstas en el instrumento de programación del acuerdo /programa marco/ programa operativo/eje/criterio para el que resulte seleccionado para apoyo por los fondos o programas.

Específicamente en los contratos financiados con cargo al PRTR deberán cumplirse las obligaciones asumidas en materia de etiquetado verde y etiquetado digital y los mecanismos establecidos para su control en el componente/inversión.

2. PRINCIPIO DO NO SIGNIFICANT HARM (“DNSH”)

El contratista y los posibles subcontratistas garantizarán el respeto al principio de «no causar un perjuicio significativo» (DNSH), exigido por el REGLAMENTO (UE) 2021/241, por el que se establece el Mecanismo de Recuperación y Resiliencia y el artículo 17 del Reglamento (UE) 2020/852 del Parlamento Europeo y del Consejo de 18 de junio de 2020 relativo al establecimiento de un marco para facilitar las inversiones sostenibles y por el que se modifica el Reglamento (UE) 2019/2088 y a las condiciones del componente/inversión del PRTR. En particular se cumplirá con la Comunicación de la Comisión Guía técnica 2021/C 58/01, sobre la aplicación del principio de «no causar un perjuicio significativo».

3. MEDIDAS ANTIFRAUDE Y ANTICORRUPCIÓN

Al presente contrato le resulta de aplicación el Plan de medidas antifraude y anticorrupción, con el contenido mínimo establecido en los sistemas de gestión de las autoridades de los Fondos, Mecanismos o Programas Europeos. En el caso de los contratos del PRTR le será de aplicación lo previsto en la Orden HFP/1030/2021, de 29 de septiembre y el Plan aprobado por el organismo destinatario de la prestación.

4. AUSENCIA DE CONFLICTO DE INTERESES

Al presente contrato le resultan de aplicación las normas que garantizan la prevención de los conflictos de interés, conforme al considerando 104 y al artículo 61 del Reglamento Financiero de la UE, debiendo adoptarse las debidas precauciones durante todas las fases de tramitación y ejecución de los mismos.

En particular, no se considerarán admisibles los intentos de influir indebidamente en el presente procedimiento de adjudicación u obtener información confidencial.

Los participantes en el procedimiento deben cumplimentar la declaración de ausencia de conflicto de interés (DACI) en los términos previstos en los planes de medidas antifraude y anticorrupción. En los contratos sujetos al PRTR, las medidas serán conformes con las disposiciones de la Orden HFP/1030/2021.

5. MEDIDAS DE INFORMACIÓN, COMUNICACIÓN Y VISIBILIDAD DEL PROYECTO

El contrato está sujeto a cuantas medidas de información, comunicación y visibilidad sean requeridas por la normativa que comunitaria y en particular, las medidas que resulten de obligado cumplimiento para las actuaciones y proyectos financiados con cargo al Fondo NextGenerationEU.

6. ACEPTACIÓN DE LOS PRINCIPIOS DE BUENA GESTIÓN FINANCIERA Y SOMETIMIENTO A CONTROLES DE LAS AUTORIDADES PREVISTAS EN LOS FONDOS O MECANISMOS

Todas las actuaciones contractuales deben observar los principios de buena gestión financiera.

El contrato está sujeto a las actuaciones de control que sean de aplicación a las ayudas conforme a la normativa comunitaria, que podrán ser efectuadas por la Comisión Europea, la Oficina de Lucha contra el Fraude (OLAF), el Tribunal de Cuentas Europeo, la Fiscalía Europea, así como a las autoridades nacionales designadas para la gestión o control de los fondos, programas o mecanismos, a los que no podrá denegarse el acceso a la información del contrato.

7. OBLIGACIONES DE DISPONIBILIDAD Y CONSERVACIÓN DE LA INFORMACIÓN

Los beneficiarios deberán conservar la información del expediente de contratación conforme a lo dispuesto en el artículo 132 del Reglamento Financiero de la UE, u otros plazos de disponibilidad que puedan establecerse en los reglamentos comunitarios de los fondos/programas o mecanismos.

En el caso de los contratos financiados en el PRTR los organismos destinatarios se asegurarán de dejar constancia en el expediente de contratación de las actuaciones que acreditan los principios de gestión específicos del Plan, conforme a las recomendaciones contenidas en la Instrucción de la Junta Consultiva de Contratación Pública de 23 de diciembre sobre aspectos a incorporar en los expedientes que se vayan a financiar con fondos procedentes del PRTR.

8. PROHIBICIÓN DE DOBLE FINANCIACIÓN

Conforme al considerando 130 y al artículo 191.3 del Reglamento (UE, Euratom) 2018/1046 del Parlamento Europeo y del Consejo de 18 de julio de 2018 (Reglamento Financiero de la UE), en ningún caso podrán ser financiados dos veces por el presupuesto de la Unión Europea los mismos gastos.

B. OBLIGACIONES GENERALES APLICABLES A LOS CONTRATOS FINANCIADOS CON CARGO AL PRTR

1. RÉGIMEN JURÍDICO APLICABLE

El contrato, al estar incluido en el PRTR, está sometido al Real Decreto-ley 36/2020, de 30 de diciembre, a la Orden HFP/1030/2021, de 29 de septiembre, a la Orden HFP/1031/2021, de 29 de septiembre, y a cuantas normas de desarrollo se aprueben.

La financiación del contrato se efectúa con cargo a fondos del Mecanismo de Recuperación y Resiliencia de la Unión Europea – Next Generation EU- establecido por el Reglamento (UE) 2020/2094 del Consejo, de 14 de diciembre de 2020, por el que se establece un instrumento de Recuperación de la Unión Europea para apoyar la recuperación tras la crisis de la COVID-19, y regulado según el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia.

2. COMPONENTE E INVERSIÓN Y COMPROMISOS ASUMIDOS POR LA CONTRIBUCIÓN AL ETIQUETADO VERDE Y DIGITAL Y POR EL PRINCIPIO DE NO CAUSAR DAÑO SIGNIFICATIVO AL MEDIOAMBIENTE (DNSH)

El contrato se enmarca en el **Componente 11. Inversión 3. Transformación Digital y Modernización del Ministerio para la Transformación Digital y de la Función Pública y de las Administraciones Públicas de las CCAA y las EELL**, del Plan de Recuperación, Transformación y Resiliencia del Gobierno de España. Línea Estratégica 6: Sanidad. Plan de Transformación Digital de la Atención Primaria.

Conforme al PRTR aprobado esta inversión contribuye en materia de etiquetado verde y digital en los siguientes porcentajes.

Etiquetado verde	Etiquetado digital
0 %	100 %

El PRTR incorpora las obligaciones específicas para la inversión en el Componente/Inversión que deberán cumplirse en la ejecución del presente contrato:

a) Obligaciones del componente/inversión por el **etiquetado verde**:

No Aplica

b) Obligaciones al componente/inversión por el **etiquetado digital**:

No existen obligaciones específicas

c) Condiciones que deben cumplir las prestaciones establecidas en la evaluación de los aspectos del principio de DNSH (*Do No Significant Harm*) con relación los seis objetivos medioambientales definidos en el Reglamento (UE) 2020/852, de 18 de junio de 2020.

Prestación	Objetivo	Condición
Servidores y sistemas de almacenamiento	Mitigación cambio climático Transición a una economía circular	Los equipos que se utilicen cumplirán los requisitos relacionados con el consumo energético establecidos de acuerdo con la Directiva 2009/125/EC
Servidores y sistemas de almacenamiento	Transición a una economía circular	Los equipos no contendrán las sustancias restringidas enumeradas en el anexo II de la Directiva 2011/65/UE.

3.- CLÁUSULA DE MODIFICACIÓN DE LOS CONTRATOS FINANCIADOS EN EL PRTR

Sin perjuicio de las causas de modificación previstas en los pliegos, en caso de estar financiado el presente contrato con cargo al PRTR, podrá ser modificado, si la Autoridad Responsable del mecanismo ordena la adopción de medidas correctoras por haberse evidenciado deficiencias durante la ejecución del contrato que afectan a alguno de los objetivos medioambientales definidos en el Reglamento (UE) 2020/852, de 18 de junio de 2020 que pueden causar un daño significativo al medioambiente.

4.- PENALIDADES POR EJECUCIÓN DEFECTUOSA O INCORRECTA EJECUCIÓN DE LOS CONTRATOS BASADOS FINANCIADOS EN EL PRTR

En caso de incumplimiento o cumplimiento defectuoso por el contratista de los compromisos adquiridos en base a las obligaciones establecidas en este documento de licitación en relación al PRTR, se podrán imponer al contratista las siguientes penalidades conforme a lo previsto en los artículos 192 a 195 de la LCSP:

() No aplica

(X) Por incumplimiento de las obligaciones establecidas para los productos en el etiquetado verde o etiquetado digital. 2%

() Por falta de acreditación a requerimiento del responsable del contrato en el plazo de 10 días hábiles.

(X) Por incumplimiento. 5%

(X) Por incumplimiento de las obligaciones asociadas al DNSH del componente/inversión: 2%

() Otras penalidades

5.- OBLIGACIONES DE ACREDITACIÓN PARA LOS LICITADORES, CONTRATISTAS Y SUBCONTRATISTAS ESTABLECIDAS EN EL PRTR

En el marco de la protección de los intereses financieros de la Unión Europea, y en concreto del Artículo 22 del Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia, la Comisión Europea requiere la identificación de los titulares reales de las entidades contratistas o beneficiarias del Plan de Recuperación, Transformación y Resiliencia, tal y como se define en el artículo 3 punto 6 de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo.

Por ello, en base a lo establecido en el artículo 7 de la Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia, en caso de que no existan datos de titularidad real en las bases de datos de la AEAT de **un participante en el procedimiento de contratación**, el órgano de contratación solicitará a éste la información de su titularidad real. Esta información deberá aportarse al órgano de contratación en el plazo de cinco días hábiles desde que se formule la solicitud de información. La falta de entrega de dicha información en el plazo señalado será motivo de **exclusión** del procedimiento. Los contratistas y, en su caso, subcontratistas están obligados específicamente a cumplir lo previsto en el sistema de gestión del Plan de Recuperación Transformación y Resiliencia, y en lo que les resulta de aplicación, se obligan a lo previsto la adenda. Adicionalmente deberán facilitar los siguientes datos de identificación:

- a) NIF del contratista y, en su caso de los subcontratistas
- b) Nombre o Razón Social
- c) Domicilio fiscal del contratista y, en su caso, subcontratistas
- d) Aceptación de la cesión de datos entre las Administraciones Públicas implicadas para dar cumplimiento a lo previsto en la normativa europea que es de aplicación y de conformidad con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (Modelo Anexo IV.B de la Orden HFP/1030/2021, de 29 de septiembre)
- e) Declaración responsable relativa al compromiso de cumplimiento de los principios transversales establecidos en el PRTR y que pudieran afectar al ámbito objeto de la gestión (Modelo Anexo IV.C de la Orden HFP/1030/2021, de 29 de septiembre)
- f) Los contratistas acreditarán la inscripción en el Censo de empresarios, profesionales y retenedores de la AEAT o en el Censo equivalente de la Administración Tributaria Foral, que debe reflejar la actividad efectivamente desarrollada en la fecha de participación en el procedimiento de licitación.

6.- OBLIGACIONES EN MATERIA DE COMUNICACIÓN

La entidad contratista y subcontratistas, si fuera el caso, estarán obligadas a cumplir las obligaciones de información y publicidad establecidas en el Artículo 9. Comunicación, de la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.

Concretamente, estarán obligados a cumplir las siguientes obligaciones:

- a) En los documentos de trabajo, así como en los informes y en cualquier tipo de soporte que se utilice en las actuaciones necesarias para el objeto del contrato, deberá exhibirse de forma correcta y destacada el emblema de la UE con una declaración de financiación adecuada que diga "financiado por la Unión Europea - NextGenerationEU", junto al logo del PRTR y contener tanto en su encabezamiento como en su cuerpo de desarrollo la siguiente referencia «Plan de Recuperación, Transformación y Resiliencia - Financiado por la Unión Europea – NextGenerationEU»
- b) En las medidas de información y comunicación, sea cual fuere el canal de comunicación que se emplee, se deberá a hacer referencia a que la inversión está financiada por la Unión Europea a través del Mecanismo de Recuperación y Resiliencia-NextGeneration EU, instrumento financiero de la inversión C11.I3. Transformación Digital y Modernización del Ministerio de Política Territorial y Función Pública y de las Administraciones de las CCAA y las EELL. Línea Estratégica 6: Sanidad. Plan de Transformación Digital de la Atención Primaria.

El órgano de contratación proporcionará durante la ejecución del contrato las indicaciones acerca del contenido preciso en cada medio y/o formato.

Cuando proceda, se indicará la siguiente cláusula de exención de responsabilidad: «Financiado por la Unión Europea - NextGenerationEU. Sin embargo, los puntos de vista y las opiniones

expresadas son únicamente los del autor/a o autores y no reflejan necesariamente los de la Unión Europea o la Comisión Europea. Ni la Unión Europea ni la Comisión Europea pueden ser consideradas responsables de las mismas».