

**EXPEDIENTE PARA LA CONTRATACIÓN DEL SERVICIO
DE MANTENIMIENTO INTEGRAL Y SOPORTE
EVOLUTIVO DEL SITIO WEB CORPORATIVO DE SIGMA
GESTIÓN UNIVERSITARIA, A.I.E. (M.P.)**

Pliego de prescripciones técnicas

**SIGMA GESTIÓN UNIVERSITARIA,
A.I.E. (M.P.)**



1. Objeto del contrato y necesidades a cubrir

El presente Pliego de Prescripciones Técnicas (PPT) tiene por objeto definir las condiciones técnicas que regirán la contratación del **servicio de mantenimiento integral y soporte evolutivo del nuevo sitio web corporativo de SIGMA Gestión Universitaria AIE (M.P.)** (en adelante, SIGMA). Este servicio es fundamental para asegurar el funcionamiento óptimo, la seguridad, la disponibilidad y la evolución continua de la plataforma web, la cual representa un activo estratégico para la comunicación, la visibilidad y la imagen de la entidad.

La necesidad de este contrato se enmarca en el reciente proceso de renovación de la marca (*rebranding*) de SIGMA, que ha culminado con el desarrollo y puesta en producción de un nuevo sitio web corporativo. Para proteger la inversión realizada y garantizar que el portal se mantenga como una herramienta eficaz y relevante a largo plazo, es imprescindible contar con un servicio especializado que cubra todas las facetas de su ciclo de vida técnico. El servicio deberá asegurar que el sitio web no solo funcione correctamente, sino que también se adapte a los futuros desafíos tecnológicos y a las necesidades cambiantes de la organización y de su ecosistema de universidades.

Los objetivos clave que se persiguen con la contratación de este servicio son:

- **Garantizar la funcionalidad y la disponibilidad del servicio:** Asegurar que el sitio web esté operativo y accesible de forma permanente (24x7), minimizando cualquier tiempo de inactividad y proporcionando una experiencia de usuario fluida, rápida y fiable.
- **Asegurar la integridad y la seguridad de la plataforma:** Proteger el sitio web contra todo tipo de amenazas, vulnerabilidades y accesos no autorizados, implementando de forma proactiva las medidas técnicas y organizativas necesarias para preservar la confidencialidad, la integridad y la trazabilidad de la información.
- **Velar por el estricto cumplimiento normativo:** Garantizar que la plataforma web se adhiera en todo momento a la legislación y los estándares vigentes que son de aplicación para SIGMA, con especial atención al Esquema Nacional de Seguridad (ENS), el Reglamento General de Protección de Datos (RGPD) y la normativa sobre accesibilidad digital (RD 1112/2018).
- **Facilitar la evolución y la adaptación continua:** Proveer un marco de trabajo flexible que permita implementar mejoras funcionales, optimizaciones de rendimiento, cambios de diseño e integraciones con otros sistemas, asegurando que el sitio web evolucione en paralelo a la estrategia de SIGMA.

En resumen, el objeto de este contrato es la prestación de un servicio experto que abarque el mantenimiento **correctivo** (resolución de incidencias), **preventivo** (monitorización y actualizaciones) y **evolutivo** (implementación de mejoras), garantizando que el sitio web corporativo de SIGMA se mantenga como una herramienta segura, fiable y alineada con los altos estándares de calidad que rigen la actividad de la entidad.

Con la mera presentación de su oferta, la empresa licitadora acepta las prescripciones técnicas

establecidas en este pliego. Cualquier propuesta que no se ajuste a los requerimientos mínimos establecidos en este pliego quedará automáticamente excluida de la licitación.

2. Alcance y descripción de los servicios

El alcance de los servicios se estructura en dos ejes complementarios: un servicio de mantenimiento básico de carácter recurrente, destinado a garantizar la estabilidad y la seguridad de la plataforma, y una bolsa de horas para soporte evolutivo, concebida para atender demandas de mejora y nuevas funcionalidades bajo pedido.

A continuación, se detallan las prestaciones incluidas en cada una de estas modalidades.

2.1. Servicio de mantenimiento básico

Esta modalidad de servicio, de carácter recurrente y proactivo, tiene como objetivo principal garantizar la estabilidad, la seguridad y el rendimiento óptimo del sitio web. Las tareas incluidas en este servicio serán ejecutadas de forma regular por el adjudicatario y cubiertas por una cuota fija. Las prestaciones concretas son las siguientes:

- **Monitorización y Disponibilidad:** El adjudicatario deberá implementar un sistema de **monitorización proactiva 24x7x365** que vigile constantemente la disponibilidad del servicio (uptime), los tiempos de respuesta del servidor y de la aplicación, y el consumo de recursos clave (CPU, memoria, espacio en disco). Este sistema deberá generar alertas automáticas ante la detección de anomalías, errores o posibles degradaciones del servicio, permitiendo una intervención rápida antes de que afecten la experiencia del usuario final.
- **Gestión de Copias de Seguridad:** Se establece la obligación de realizar **copias de seguridad diarias y completas** de la plataforma. El alcance de la copia debe incluir, como mínimo, la base de datos completa, todos los archivos que componen la aplicación web (imágenes, documentos, etc.) y el código fuente de la última versión en producción. Se deberá definir y aplicar una política de retención que garantice la conservación de las copias durante un mínimo de 30 días naturales. Además, el adjudicatario deberá realizar pruebas de restauración periódicas, como se detallará en el apartado de continuidad del servicio, para verificar la integridad y la viabilidad de las copias.
- **Actualizaciones y Gestión de Vulnerabilidades:** Esta prestación es crítica para la seguridad de la plataforma. El adjudicatario será responsable de aplicar todas las **actualizaciones de seguridad** que afecten al núcleo (core) del gestor de contenidos **Strapi**, así como a sus plugins, librerías y dependencias de terceros. Esto incluye la aplicación de parches de seguridad críticos publicados por los desarrolladores para corregir vulnerabilidades conocidas. Estas actualizaciones deberán planificarse y ejecutarse de manera controlada, realizando previamente las pruebas necesarias en un entorno de preproducción para asegurar que no generen conflictos ni regresiones funcionales.
- **Soporte Técnico y Resolución de Incidencias:** El adjudicatario proporcionará un canal de soporte técnico para la notificación y resolución de incidencias, entendiendo como incidencia cualquier evento que provoque una interrupción no planificada, una degradación de la calidad

del servicio o un error funcional del sitio web. Este servicio incluye el diagnóstico, el análisis de la causa raíz y la aplicación de las soluciones correctivas necesarias para restablecer el funcionamiento normal de la plataforma en los plazos establecidos en los Acuerdos de Nivel de Servicio (ANS) definidos en este pliego.

2.2. Bolsa de horas

Para complementar el mantenimiento básico, se establece una bolsa de horas anual destinada a cubrir tareas de carácter evolutivo y consultivo que vayan más allá de la corrección de errores y el mantenimiento preventivo. Este mecanismo proporciona a SIGMA la flexibilidad para solicitar mejoras y adaptaciones a la plataforma de manera planificada.

En el primer año de contrato, la bolsa de horas requerida será de 150 horas aproximadamente. En caso de prorrogarse el contrato, se establecerá una bolsa de aproximadamente 25 horas anuales para cada uno de los años adicionales, las cuales serán acumulables durante toda la vigencia del contrato.

El uso de estas horas se gestionará bajo demanda de SIGMA y requerirá la aprobación previa por parte de SIGMA. Los servicios que se podrán financiar con cargo a esta bolsa de horas incluyen, entre otros:

- **Desarrollo de Nuevas Funcionalidades:** Implementación de nuevos componentes, módulos o secciones en el sitio web que no estuvieran previstos en el lanzamiento inicial.
- **Mejoras y Optimizaciones:** Realización de modificaciones sobre funcionalidades existentes para mejorar la experiencia de usuario (UX), el aspecto visual (UI) o la arquitectura de la información. También incluye tareas de optimización del rendimiento (Web Performance Optimization - WPO) y la refactorización de código para mejorar su calidad y mantenimiento.
- **Consultoría Técnica Especializada:** Prestación de servicios de asesoramiento en materias como la optimización para motores de búsqueda (SEO técnico), el análisis de viabilidad de nuevas propuestas tecnológicas, la elaboración de pruebas de concepto o la definición de estrategias técnicas para futuras evoluciones de la web.
- **Integraciones con Sistemas de Terceros:** Desarrollo de conectores o procesos para la integración del sitio web con otros sistemas de información, ya sean internos de SIGMA o externos (por ejemplo, conexión con API de terceros, plataformas de CRM, ERP, etc.).

El procedimiento para el uso de la bolsa de horas será el siguiente: SIGMA realizará una petición de servicio detallando las necesidades. El adjudicatario analizará la petición y presentará una propuesta técnica que incluirá una estimación detallada de las horas necesarias para su ejecución. Una vez SIGMA valide y apruebe formalmente la estimación, el adjudicatario procederá a planificar y ejecutar los trabajos. Las horas invertidas se descontarán de la bolsa de horas y se reportarán de manera transparente en los informes de seguimiento trimestrales.

3. Requisitos técnicos del servicio

Esta sección establece el marco técnico y operativo que deberá regir la prestación del servicio. El adjudicatario deberá cumplir con la totalidad de las especificaciones que se detallan a continuación.

3.1. Entorno tecnológico

El adjudicatario deberá demostrar un conocimiento experto y experiencia contrastada en el entorno tecnológico sobre el cual está construido el sitio web corporativo. La prestación del servicio deberá realizarse respetando en todo momento la arquitectura y las tecnologías definidas, así como los procedimientos de gestión de la configuración y control de versiones establecidos por SIGMA.

La arquitectura tecnológica de referencia se basa en un modelo de **Headless CMS**, utilizando Strapi como gestor de contenidos. El adjudicatario deberá gestionar todos los componentes de esta arquitectura, que incluye, entre otros:

- **Backend:** La aplicación Strapi, desarrollada sobre Node.js.
- **Base de Datos:** El sistema gestor de base de datos asociado a Strapi (por ejemplo, PostgreSQL, MySQL o similar).
- **Frontend:** El código de la capa de presentación que consume la API de Strapi (desarrollado con tecnologías modernas como React, Vue.js, Next.js o similar).
- **Infraestructura de Alojamiento:** Aunque la gestión de la infraestructura subyacente (servidores, red) no es objeto de este contrato, el adjudicatario deberá colaborar estrechamente con los equipos de sistemas de SIGMA para la correcta operación de la aplicación en los entornos definidos.

Una obligación fundamental del servicio es el **Control de la Configuración**. El adjudicatario será responsable de crear y mantener actualizado un inventario detallado de todos los elementos de configuración del software que componen el sitio web. Este inventario, que deberá ser gestionado a través de la herramienta que SIGMA designe a tal efecto (por ejemplo, GLPI), deberá incluir, como mínimo:

- La versión exacta del núcleo de Strapi CMS.
- Un listado de todos los *plugins*, módulos y extensiones de Strapi instalados, con sus respectivas versiones.
- Las librerías y dependencias principales, tanto del *backend* (Node.js) como del *frontend*, con sus versiones correspondientes.
- La versión del intérprete de Node.js utilizado.
- Cualquier otro componente de software relevante para el funcionamiento de la plataforma.

Este inventario es crucial para una correcta gestión de vulnerabilidades, la planificación de actualizaciones y el análisis de impacto ante cualquier cambio. El adjudicatario deberá seguir el **Procedimiento de Gestión de la Configuración** de SIGMA.

Todo el código fuente de la aplicación deberá ser gestionado mediante el sistema de control de versiones **Git**, utilizando el repositorio que SIGMA proporcione. Se exige el seguimiento de una metodología de ramas (como GitFlow o similar) que asegure el aislamiento del desarrollo, la realización de revisiones de código mediante *pull requests* y un registro claro y trazable de los cambios.

3.2. Mantenimiento correctivo y gestión de incidencias

El servicio de mantenimiento tiene como objetivo la resolución de cualquier error, anomalía o comportamiento inesperado que afecte al funcionamiento del sitio web. El adjudicatario deberá seguir el **Procedimiento de Gestión de Incidencias** de SIGMA, utilizando la herramienta de *ticketing* corporativa para el registro, seguimiento y documentación de todas las actuaciones.

A continuación, se recogen las tipologías de referencias junto con sus correspondientes Acuerdos de Nivel de Servicio (ANS) valorados en horas laborables:

Nivel de Prioridad	Descripción	Tiempo de Atención de las referencias	Tiempo de Resolución Objetivo	% de Cumplimiento Exigido
Crítica (Extrema)	Caída completa del servicio. Pérdida de acceso para todos los usuarios. Vulnerabilidad de seguridad grave con impacto confirmado. Corrupción de datos.	1 hora	10 horas	95%
Alta (Prioritaria)	Una funcionalidad principal no opera correctamente (ej: formularios de contacto, buscador). Error que impide la publicación de contenido crítico. Degradación severa del rendimiento.	2 horas	70 horas	90%
Media (Ordinaria)	Error en una funcionalidad secundaria o que afecta a un grupo reducido de usuarios. Problemas de visualización en navegadores específicos (no mayoritarios). Existe una solución temporal viable.	3 horas	120 horas	90%
Baja (Leve)	Errores cosméticos menores	4 horas	11 meses	90%

	(desalineaciones, erratas). Enlaces rotos no críticos. Funcionalidad con comportamiento no óptimo pero que no impide su uso.			
Consulta Técnica	Solicitudes de información, asesoramiento técnico o dudas sobre el funcionamiento de la plataforma que no implican un error.	4 horas	20 horas	90%

El **tiempo de respuesta** se define como el período máximo entre la notificación de la incidencia por parte de SIGMA y el inicio de las tareas de diagnóstico por parte del adjudicatario, con la correspondiente comunicación a SIGMA. El **tiempo de resolución** es el período máximo desde la comunicación para la implementación de una solución definitiva o, si no fuera posible, una solución de contorno aceptada por SIGMA. Todos los tiempos se deben contabilizar dentro del horario de soporte establecido en este pliego.

El adjudicatario deberá mantener una comunicación fluida y proactiva con SIGMA durante todo el ciclo de vida de las incidencias, especialmente en las de criticidad Crítica y Alta.

En caso de producirse una caída de la página web, el adjudicatario deberá de disponer de un entorno redundado en HA para seguir ofreciendo el servicio, o bien, permitir el acceso al SPortal de SIGMA desde el exterior a través de la URL de la web.

3.3. Mantenimiento Preventivo

El mantenimiento preventivo comprende el conjunto de tareas proactivas y planificadas destinadas a garantizar la seguridad, la estabilidad y el rendimiento óptimo del sitio web, así como a minimizar la probabilidad de que se produzcan incidencias. El adjudicatario deberá ejecutar estas tareas de forma recurrente, según un calendario acordado con SIGMA.

Las tareas de mantenimiento preventivo incluirán, como mínimo, las siguientes:

- **Monitorización continua del servicio:** Supervisión 24/7 de la disponibilidad de la web y el rendimiento de sus componentes clave (tiempos de respuesta del servidor, uso de CPU y memoria, estado de la base de datos). El adjudicatario deberá integrarse con las herramientas de monitorización de SIGMA.
- **Gestión de actualizaciones de software:** Vigilancia activa de la publicación de nuevas versiones y parches de seguridad para todos los componentes del entorno tecnológico (núcleo de Strapi, *plugins*, librerías, etc.). El adjudicatario será responsable de analizar el impacto de cada actualización, probarla exhaustivamente en un entorno de preproducción y planificar su

instalación en producción, previa autorización de SIGMA. Las actualizaciones de seguridad críticas deberán gestionarse con carácter de urgencia.

- **Análisis de vulnerabilidades:** Realización de escaneos periódicos (como mínimo, trimestrales) del código de la aplicación y sus dependencias para la detección de posibles vulnerabilidades de seguridad. El adjudicatario deberá presentar un informe con los resultados y un plan de mitigación para las vulnerabilidades detectadas.
- **Revisión y optimización del rendimiento:** Análisis periódico del rendimiento general del sitio web, incluyendo la optimización de consultas a la base de datos, la mejora de los tiempos de carga de las páginas y la identificación de posibles cuellos de botella.
- **Revisión de registros (logs):** Inspección proactiva de los registros de la aplicación y del servidor web en busca de patrones de error recurrentes, intentos de acceso no autorizados u otras anomalías que puedan indicar un problema latente.
- **Verificación de integridad:** Ejecución de comprobaciones automatizadas para detectar enlaces rotos, imágenes que no cargan y otros problemas de integridad del contenido.
- **Mantenimiento de la base de datos:** Tareas de optimización y limpieza de la base de datos, siempre de forma planificada y controlada para asegurar la integridad de los datos.

4. Requisitos de seguridad y continuidad del servicio

Esta sección establece el marco obligatorio de medidas técnicas y organizativas que la empresa adjudicataria deberá implementar y mantener durante toda la vigencia del contrato para asegurar un nivel de seguridad y continuidad adecuado a las exigencias de SIGMA y a la normativa aplicable.

El adjudicatario será responsable de garantizar que el servicio prestado cumple con todas las especificaciones descritas a continuación, actuando de manera proactiva en la identificación y mitigación de riesgos y colaborando estrechamente con los equipos técnicos y de seguridad de SIGMA.

4.1. Cumplimiento del Esquema Nacional de Seguridad (ENS)

El servicio objeto de este contrato está sujeto al Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS). La naturaleza de la información gestionada y los servicios ofrecidos a través del sitio web corporativo requieren su encuadramiento en una categoría de seguridad que garantice la protección adecuada de las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

El adjudicatario deberá acreditar estar en posesión del **certificado de conformidad con el Esquema Nacional de Seguridad para la categoría MEDIA**, expedido por una entidad de certificación acreditada. Esta certificación deberá mantenerse vigente durante toda la duración del contrato, siendo motivo de resolución su incumplimiento.

Además de la certificación propia, el adjudicatario deberá integrarse y adherirse plenamente al marco normativo de seguridad de SIGMA, el cual incluye, entre otros, los documentos siguientes:

- **Política de Seguridad de la Información (POL001_Politica de Seguridad):** Documento marco que establece los principios rectores, responsabilidades y el compromiso de la organización con la seguridad.
- **Normativa de uso del sistema web (NORM001_Normativa de Seguridad):** Reglas específicas que aplican al uso y gestión de la plataforma tecnológica del sitio web.

El adjudicatario deberá colaborar activamente en los procesos de seguridad gestionados por SIGMA, especialmente en los siguientes ámbitos:

- **Análisis y Gestión de Riesgos:**

El adjudicatario participará activamente en el proceso de análisis de riesgos de la plataforma, conforme al procedimiento interno de SIGMA (PROC002_Análisis de Riesgos). Esta colaboración implicará la identificación de nuevas amenazas y vulnerabilidades específicas del entorno tecnológico de la web (Strapi, librerías, integraciones), la evaluación de su impacto y probabilidad, y la propuesta de salvaguardas técnicas y procedimentales para mitigar los riesgos a un nivel aceptable. Este análisis se revisará de manera periódica, como mínimo anualmente, o siempre que se produzcan cambios significativos en la plataforma.

- **Gestión de Vulnerabilidades:**

Será responsabilidad del adjudicatario implementar un proceso de gestión de vulnerabilidades continuo y proactivo. Este proceso incluirá, como mínimo, las siguientes tareas:

- **Escaneo de vulnerabilidades:** Realización de escaneos periódicos, tanto a nivel de infraestructura como de aplicación, para identificar debilidades de seguridad.
- **Clasificación y priorización:** Las vulnerabilidades identificadas serán clasificadas según su nivel de criticidad (p. ej., utilizando el estándar CVSS) y priorizadas para su corrección.
- **Aplicación de parches y actualizaciones:** El adjudicatario será responsable de aplicar todos los parches de seguridad críticos e importantes para el CMS Strapi, sus conectores (*plugins*), las librerías de terceros y el software base, dentro de los plazos establecidos en el Acuerdo de Nivel de Servicio (ANS).
- **Informes de seguimiento:** Se generarán informes mensuales que detallen las vulnerabilidades detectadas, su estado y las acciones de remediación aplicadas.

- **Monitorización y Respuesta a Incidentes:**

El adjudicatario deberá monitorizar activamente la plataforma para detectar posibles incidentes de seguridad, como intentos de acceso no autorizado, ataques de denegación de servicio (DDoS), inyección de código o fugas de información. Cualquier incidente de seguridad detectado deberá ser notificado al equipo de seguridad de SIGMA de manera inmediata, siguiendo el procedimiento de gestión de incidencias establecido. El adjudicatario deberá colaborar en el análisis, contención, erradicación y recuperación del incidente, así como en el análisis forense posterior si fuera

necesario.

4.2. Gestión de copias de seguridad y plan de continuidad del servicio

Para garantizar la resiliencia del servicio y la capacidad de recuperación ante un incidente grave o desastre, el adjudicatario deberá implementar una política robusta de copias de seguridad y un plan de continuidad del servicio.

Política de Copias de Seguridad:

El adjudicatario definirá y ejecutará una política de copias de seguridad que asegure la protección de todos los componentes críticos del sitio web. Esta política deberá incluir, como mínimo:

- **Alcance de las copias:** Las copias de seguridad deberán incluir la totalidad de los elementos necesarios para una restauración completa del servicio:
 - Base de datos del CMS Strapi.
 - Código fuente completo de la aplicación y sus configuraciones.
 - Todos los archivos y contenidos multimedia subidos por los usuarios (assets).
- **Frecuencia y Tipología:**
 - **Copias de seguridad completas semanales**, a realizar durante una ventana de bajo impacto (p. ej., fin de semana).
 - **Copias de seguridad incrementales o diferenciales diarias**, para minimizar la pérdida de datos (RPO).
- **Retención:** Se establecerá un período de retención mínimo de 30 días para las copias diarias, 12 semanas para las semanales y 6 meses para las mensuales.
- **Almacenamiento:** Las copias de seguridad se almacenarán en un repositorio **seguro, cifrado y en una ubicación geográfica diferente** del centro de datos principal donde se aloja el servicio, para garantizar su disponibilidad en caso de un desastre local.

Plan de Continuidad y Pruebas de Recuperación:

El adjudicatario deberá desarrollar y mantener un **Plan de Continuidad del Servicio** que documente detalladamente los procedimientos técnicos y organizativos para la recuperación del servicio ante diferentes escenarios de fallo. Este plan deberá estar alineado con los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO) que se acuerden contractualmente con SIGMA.

Para garantizar la eficacia y viabilidad de este plan, será obligatorio realizar **pruebas periódicas de recuperación**.

- **Frecuencia:** Las pruebas de restauración completas se ejecutarán con una periodicidad mínima **semestral**.
- **Metodología:** Las pruebas consistirán en la restauración completa del servicio en un entorno de ensayo aislado, a partir de uno de los juegos de copias de seguridad. Se verificará la integridad de los datos, la funcionalidad de la aplicación y el tiempo necesario para la recuperación.
- **Entregables:** Tras cada prueba, el adjudicatario entregará a SIGMA un **informe de resultados**

10

que incluya las métricas obtenidas (RTO y RPO reales), las incidencias detectadas durante el proceso y un plan de acciones correctoras para mejorar el procedimiento.

4.3. Control de acceso seguro y gestión de registros

El control estricto sobre quién accede a la plataforma y qué hace es un requisito de seguridad fundamental. El adjudicatario deberá implementar medidas robustas para la gestión de identidades, el control de acceso y la trazabilidad de las acciones.

4.3.1. Gestión de Identidades y Control de Acceso:

- **Integración con el Directorio Activo de SIGMA:** Todo acceso con privilegios a los entornos de gestión del sitio web (backend del CMS Strapi, acceso a servidores, paneles de control de infraestructura, etc.) deberá realizarse **exclusivamente** mediante la federación de identidades con el Directorio Activo (Active Directory) de SIGMA. Queda expresamente prohibido el uso de cuentas de usuario locales, genéricas o compartidas.
- **Autenticación Multifactor (MFA):** El uso de mecanismos de **Autenticación Multifactor (MFA)** será **obligatorio** para todos los accesos a entornos con privilegios de administración o gestión de contenidos. La configuración del MFA se integrará con la solución corporativa de SIGMA.
- **Principio de Mínimo Privilegio:** El adjudicatario garantizará que los permisos asignados a cada usuario sean los mínimos necesarios para desarrollar sus funciones (lectura, escritura, publicación, administración). Los roles y permisos serán revisados periódicamente, como mínimo de forma anual, junto con SIGMA.

4.3.2. Gestión de Registros (Logs) e Integración con SIEM:

Para garantizar la trazabilidad de las acciones y facilitar la detección y análisis de incidentes, el adjudicatario deberá asegurar una gestión exhaustiva de los registros de actividad.

- **Recolección de registros:** Se deberán generar, centralizar y custodiar de forma segura los registros provenientes de todas las fuentes relevantes, incluyendo:
 - Registros de acceso al servidor web y a la aplicación.
 - Registros de autenticación (éxitos y fallos).
 - Registros de acciones administrativas realizadas en el backend del CMS (creación, modificación o eliminación de contenidos, usuarios o configuraciones).
 - Registros de errores de la aplicación y del sistema.
 - Registros del cortafuegos de aplicaciones web (WAF) y otros sistemas de seguridad perimetral.
- **Envío al SIEM de SIGMA:** Todos los registros de seguridad relevantes deberán ser enviados **en tiempo real y en un formato estandarizado (p. ej., Syslog o CEF)** al sistema de Gestión de Información y Eventos de Seguridad (**SIEM**) de SIGMA. El adjudicatario será responsable de configurar y mantener el correcto funcionamiento de este envío, colaborando con el equipo de SIGMA para definir los filtros y formatos adecuados. Esta integración permitirá a SIGMA correlacionar eventos de seguridad del sitio web con el resto de sistemas de su infraestructura y mejorar la capacidad de detección y respuesta.

- **Retención y protección:** Los registros serán almacenados durante el período que estipule la normativa de seguridad de SIGMA, garantizando su integridad y confidencialidad para futuras auditorías o análisis forenses.

5. Normativa y Certificaciones

La prestación del servicio objeto de este pliego debe garantizar el cumplimiento estricto de un conjunto de normativas, estándares y certificaciones que son de obligado cumplimiento para SIGMA. El adjudicatario será responsable de asegurar que todas sus actuaciones y los resultados de las mismas se adecúen plenamente a los requisitos que se detallan a continuación, manteniendo su vigencia durante toda la duración del contrato.

5.1. Certificaciones del proveedor

La empresa adjudicataria deberá acreditar y mantener durante toda la vigencia del contrato, estar certificada, como mínimo, en la **categoría MEDIA del Esquema Nacional de Seguridad**, de acuerdo con el Real Decreto 311/2022, de 3 de mayo. Esta certificación debe amparar los servicios de desarrollo y mantenimiento de software o similares, que son objeto de este contrato. El adjudicatario deberá aportar el certificado en vigor y garantizar su renovación durante toda la duración del servicio.

El cumplimiento del ENS es un requisito fundamental para asegurar que los sistemas de información de SIGMA se desarrollan y mantienen bajo un marco de seguridad robusto y homogéneo.

Asimismo, se valorará positivamente que el adjudicatario disponga de certificaciones adicionales que acrediten su madurez en la gestión de la seguridad de la información y de los servicios tecnológicos, tales como:

- Certificación ISO/IEC 27001
- Certificación ISO/IEC 20000-1:2018

La documentación acreditativa de estas certificaciones deberá ser presentada junto con la oferta. La ausencia o pérdida de vigencia de la certificación ENS durante la ejecución del contrato podrá ser causa de resolución del mismo.

5.2. Accesibilidad Web

El sitio web corporativo de SIGMA debe garantizar el acceso a la información y a los servicios a todas las personas, independientemente de sus capacidades técnicas, físicas, sensoriales o cognitivas. Por lo tanto, el adjudicatario será responsable de asegurar que tanto el sitio web actual como cualquier desarrollo o modificación realizados en el marco del servicio de mantenimiento evolutivo cumplan con la normativa vigente en materia de accesibilidad.

El marco normativo de referencia es el **Real Decreto 1112/2018, de 7 de septiembre**, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. Concretamente, todas las páginas y contenidos del sitio web deberán alcanzar, como mínimo, el **nivel de conformidad AA de las Pautas de Accesibilidad para el Contenido Web (WCAG) 2.1**, publicadas por el World Wide Web Consortium (W3C), según el estándar técnico europeo UNE-EN 301 549.

El cumplimiento de este requisito implica, entre otros aspectos, que el sitio web sea:

- **Perceptible:** Ofreciendo alternativas textuales para contenidos no textuales, subtítulos para vídeos, un contraste de color suficiente (mínimo 4.5:1 para texto normal), y permitiendo redimensionar el texto hasta un 200% sin pérdida de contenido o funcionalidad.
- **Operable:** Garantizando una navegación completa mediante el teclado, con un indicador de foco siempre visible, sin "trampas de teclado", y evitando contenidos que puedan provocar ataques epilépticos.
- **Comprensible:** Utilizando un lenguaje claro y sencillo, proporcionando una navegación consistente, etiquetas claras en los formularios y mensajes de error que sean útiles y orienten a la corrección.
- **Robusto:** Empleando un código HTML semánticamente correcto, que asegure la máxima compatibilidad con las tecnologías de asistencia actuales y futuras, como los lectores de pantalla, y haciendo un uso adecuado de los atributos ARIA cuando sea necesario.

El adjudicatario deberá realizar validaciones periódicas de accesibilidad, tanto automáticas como manuales, y entregar los informes correspondientes. Asimismo, será responsable de generar y mantener actualizada la **Declaración de Accesibilidad** del sitio web, siguiendo el modelo oficial, donde se indique el nivel de cumplimiento y, en su caso, los contenidos no accesibles y la justificación correspondiente.

5.3. Protección de datos

El servicio de mantenimiento deberá garantizar el cumplimiento íntegro de la normativa de protección de datos personales, concretamente el **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD)** y la **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**. El adjudicatario actuará como **Encargado del Tratamiento** respecto a los datos personales a los cuales pueda tener acceso durante la prestación del servicio. Esta relación se formalizará mediante la firma de un contrato de encargo de tratamiento.

El adjudicatario deberá implementar las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado al riesgo, protegiendo los datos personales contra la destrucción, pérdida o alteración accidental o ilícita, así como contra la comunicación o acceso no autorizados.

En relación con el sitio web, el adjudicatario será responsable de asegurar lo siguiente:

- **Formularios de recogida de datos:** Todos los formularios que recojan datos personales (contacto, "trabaja con nosotros", etc.) deberán incluir una primera capa informativa (cláusula resumida) clara y concisa, que informe sobre los aspectos básicos del tratamiento, y un enlace a la política de privacidad completa (segunda capa). Se deberá informar de la finalidad, la base de legitimación, los destinatarios y los derechos del interesado.
- **Política de Privacidad:** El proveedor deberá garantizar que la política de privacidad del sitio web es completa, precisa y fácilmente accesible. Esta deberá detallar todas las finalidades de los tratamientos, las bases de legitimación correspondientes, los plazos de conservación, la existencia o no de transferencias internacionales y los procedimientos para que los usuarios puedan ejercer sus derechos.
- **Política de Cookies:** El sitio web debe disponer de un mecanismo para la gestión del consentimiento de cookies que cumpla con las directrices de la Agencia Española de Protección de Datos (AEPD). El banner de cookies debe permitir al usuario aceptar, rechazar o configurar las cookies de manera granular. La política de cookies deberá proporcionar información detallada sobre cada cookie utilizada (propietario, finalidad, tipo y duración), redactada de forma clara y transparente para evitar interpretaciones equívocas y reforzar la confianza del usuario.

6. Metodología de trabajo y entregables

En este apartado se describe el marco operativo, los procedimientos de gestión y los mecanismos de comunicación que regirán la colaboración entre la empresa adjudicataria y SIGMA durante toda la vigencia del contrato.

6.1. Gestión del servicio y procedimientos

El adjudicatario deberá proporcionar una plataforma centralizada de gestión de servicios (Service Management Tool) para la comunicación y el registro de todas las peticiones, incidencias y consultas. Esta herramienta será el **canal principal y preferente** para todas las comunicaciones formales relacionadas con la ejecución del servicio. El correo electrónico se podrá utilizar para comunicaciones de carácter general o informativo, mientras que el contacto telefónico quedará reservado para la notificación de incidencias críticas o situaciones urgentes que requieran una atención inmediata.

El procedimiento para la **gestión de cambios y evolutivos**, que se gestionarán mediante la bolsa de horas, seguirá un flujo de trabajo formal y trazable. Cualquier solicitud de mejora o nueva funcionalidad deberá ser registrada en la herramienta de gestión de servicios por parte de SIGMA. El adjudicatario realizará un análisis inicial de la petición y presentará una valoración técnica y una estimación detallada de las horas necesarias para su ejecución. Una vez SIGMA valide y apruebe

formalmente esta estimación, el adjudicatario procederá a la planificación y ejecución de la tarea. Antes del paso a producción, cualquier desarrollo deberá ser validado por SIGMA en un entorno de preproducción.

El adjudicatario será responsable de mantener actualizada toda la **documentación técnica** asociada al sitio web. Esto incluye, pero no se limita a, el inventario de software y versiones (control de la configuración), diagramas de arquitectura, documentación funcional de nuevos desarrollos y manuales técnicos. Esta documentación deberá estar almacenada en un repositorio accesible para el personal autorizado de SIGMA, garantizando así la transferencia de conocimiento y la sostenibilidad de la plataforma.

6.2. Informes de seguimiento

Con una **periodicidad trimestral**, el adjudicatario deberá entregar a SIGMA un informe detallado de seguimiento de la actividad. Este documento, que deberá presentarse durante los primeros cinco (5) días hábiles del mes siguiente al período reportado, deberá incluir, como mínimo, la información siguiente:

- Un resumen ejecutivo de las actividades más relevantes llevadas a cabo durante el mes.
- El estado de todas las incidencias gestionadas: detalle de las incidencias abiertas, en progreso y resueltas, indicando su criticidad, los tiempos de respuesta y resolución, y un análisis comparativo respecto a los Acuerdos de Nivel de Servicio (ANS) definidos.
- El consumo detallado de la bolsa de horas de soporte evolutivo: se desglosarán las horas imputadas a cada tarea, el responsable de la petición, el estado de la tarea y el saldo de horas restante.
- Un registro de todas las acciones de mantenimiento preventivo realizadas, como la aplicación de parches de seguridad, actualizaciones del CMS Strapi, de sus módulos o de las librerías subyacentes.
- Un resumen de los resultados de la monitorización de seguridad, incluyendo las vulnerabilidades detectadas y las medidas correctoras aplicadas.
- Recomendaciones proactivas para la mejora del rendimiento, la seguridad o la funcionalidad del sitio web, así como la advertencia sobre posibles riesgos identificados.

6.3. Reuniones

Se establece un calendario de reuniones para asegurar una comunicación fluida y un seguimiento continuo del servicio. Inicialmente, se realizará una **reunión de lanzamiento (kick-off)** para formalizar el inicio del servicio, presentar los equipos de trabajo de ambas partes, confirmar los canales de comunicación y validar la metodología de trabajo.

Posteriormente, se llevarán a cabo **reuniones de seguimiento ordinarias con una frecuencia trimestral**. Estas reuniones, que preferentemente se celebrarán de manera telemática, tendrán como objetivo principal revisar el contenido del informe mensual, evaluar el cumplimiento de los ANS, planificar las próximas tareas evolutivas y resolver cualquier cuestión operativa o estratégica.

Además, se podrán convocar **reuniones extraordinarias** a petición de cualquiera de las partes para tratar asuntos urgentes, gestionar incidencias de gran impacto o abordar planificaciones complejas que requieran un análisis en profundidad. La asistencia a las reuniones será obligatoria para el Gestor del Servicio del adjudicatario y el responsable del contrato por parte de SIGMA, y podrán incorporarse otros perfiles técnicos si los temas a tratar lo requieren. El adjudicatario será responsable de convocar las reuniones, preparar el orden del día y levantar un acta con los acuerdos alcanzados.

7. Equipo técnico asociado al contrato

La empresa adjudicataria deberá garantizar el cumplimiento de los niveles de calidad, disponibilidad y seguridad exigidos para la plataforma web corporativa de SIGMA.

El adjudicatario designará un **Gestor de Servicio** que actuará como interlocutor único y principal con el responsable del contrato designado por SIGMA. Esta figura será la máxima responsable de la supervisión y coordinación integral del servicio, garantizando la alineación de las actuaciones con los objetivos de SIGMA. Sus funciones incluirán la gobernanza del servicio, el seguimiento y cumplimiento de los Acuerdos de Nivel de Servicio (ANS), la gestión de los recursos humanos y técnicos asignados, la planificación y priorización de las tareas de mantenimiento evolutivo y la preparación y presentación de los informes periódicos de seguimiento. Este perfil deberá acreditar una experiencia mínima demostrable de cinco años en la gestión de servicios tecnológicos complejos, preferiblemente en entornos regulados por el Esquema Nacional de Seguridad (ENS) y bajo marcos de trabajo como ISO/IEC 20000 o ITIL.

El equipo técnico asignado al proyecto deberá estar formado por entre 2 a 4 profesionales con competencias multidisciplinares que cubran todas las necesidades del servicio de mantenimiento. Colectivamente, el equipo deberá demostrar un conocimiento experto en el entorno tecnológico de la plataforma, especialmente en el **CMS Strapi** en sus últimas versiones, incluyendo el desarrollo de plugins personalizados, la gestión de sus API REST/GraphQL y la optimización del rendimiento. Será imprescindible contar con perfiles con experiencia sólida en tecnologías front-end (como React, Vue.js o similar) y back-end (Node.js), así como en la gestión de bases de datos (p. ej., PostgreSQL, MySQL) y sistemas de control de versiones (Git).

Asimismo, y dada la naturaleza del servicio, el equipo deberá poseer conocimientos avanzados en seguridad de sistemas web, gestión de vulnerabilidades, aplicación de parches (patching) y técnicas de securización de aplicaciones e infraestructuras, de acuerdo con los requisitos definidos por el Esquema Nacional de Seguridad.

La empresa licitadora deberá presentar, en su oferta técnica, una descripción detallada del equipo de trabajo propuesto, incluyendo los roles, las responsabilidades y los currículums anonimizados de los perfiles clave que evidencien la experiencia requerida en proyectos de características similares.

8. Condiciones de ejecución del contrato

La prestación del servicio de mantenimiento integral y soporte evolutivo del sitio web corporativo de SIGMA se realizará íntegramente **en remoto**, utilizando los medios telemáticos que acuerden ambas partes. El adjudicatario deberá disponer de la infraestructura técnica y los recursos necesarios para garantizar una comunicación fluida y segura con los sistemas y el equipo de SIGMA, sin que ello implique la necesidad de presencia física en las instalaciones de la entidad, excepto en casos excepcionales y previamente acordados por ambas partes.

El **horario ordinario de soporte** para la gestión de solicitudes evolutivas y consultas será de lunes a viernes laborables, de 9:00 a 18:00 horas (hora peninsular española). Para la resolución de incidencias, se establece un servicio de soporte que garantizará los tiempos de respuesta y resolución definidos en los Acuerdos de Nivel de Servicio (ANS) de este pliego, pudiendo requerir actuaciones fuera del horario ordinario para incidencias clasificadas como críticas o urgentes, según el procedimiento de gestión de incidencias establecido.

Para asegurar una transferencia de conocimiento efectiva y minimizar los riesgos asociados al inicio y la finalización del servicio, el adjudicatario tendrá la obligación de desarrollar y presentar dos documentos clave. En primer lugar, en un plazo máximo de quince (15) días hábiles desde la formalización del contrato, deberá entregar un **Plan de Transición Inicial**. Este documento detallará el cronograma y las acciones previstas para la asunción del servicio, incluyendo la configuración de los sistemas de monitorización, la validación de los accesos y la revisión de la documentación existente.

Asimismo, con una antelación mínima de dos (2) meses respecto a la fecha de finalización del contrato, el adjudicatario deberá presentar un Plan de Transición Final. Este plan describirá de manera exhaustiva el procedimiento para el traspaso del servicio a SIGMA o a un tercero designado por esta. Incluirá, como mínimo, la transferencia completa y actualizada de toda la documentación técnica, las credenciales de acceso, las configuraciones de los entornos y cualquier otro activo o conocimiento generado durante la vigencia del contrato, garantizando una transición ordenada y sin pérdida de información ni degradación del servicio.

9. Propiedad intelectual y confidencialidad

Todos los derechos de propiedad intelectual e industrial derivados de los trabajos realizados en el marco de este contrato serán titularidad exclusiva de SIGMA Gestión Universitaria, AIE. Esta titularidad abarca, sin carácter limitativo, el código fuente de todos los desarrollos, scripts, componentes de software a medida, configuraciones, diseños gráficos y visuales, estructuras de

navegación, wireframes, documentación técnica y funcional, informes y cualquier otro material o elemento creado o generado por el adjudicatario en la ejecución del servicio.

El adjudicatario cede a SIGMA, en exclusiva y con la máxima amplitud permitida por la ley, todos los derechos de explotación sobre los resultados del contrato, incluyendo los derechos de reproducción, distribución, comunicación pública y transformación, para un ámbito territorial mundial y por toda la duración legal de los derechos. El adjudicatario no podrá reutilizar, ceder ni licenciar a terceros ninguno de los elementos desarrollados para SIGMA sin la autorización previa, expresa y por escrito de esta. A la finalización del contrato, el adjudicatario deberá entregar a SIGMA la totalidad del código fuente y la documentación asociada, en un formato accesible y completo.

Asimismo, el adjudicatario y todo su personal adscrito al servicio se comprometen a mantener el **más estricto deber de secreto y confidencialidad** sobre toda la información a la que tengan acceso durante la ejecución del contrato. Se considera información confidencial cualquier dato técnico, operativo, comercial o de seguridad de SIGMA, incluyendo la arquitectura de sistemas, credenciales de acceso, datos de carácter personal, procedimientos internos y cualquier otra información no pública. Esta información solo podrá ser utilizada para los fines estrictos del cumplimiento del contrato. **Este deber de confidencialidad se mantendrá en vigor de forma indefinida**, incluso después de la finalización de la relación contractual por cualquier causa.