EXP. L3/2026

EXPEDIENTE PARA LA CONTRATACIÓN DE SERVICIOS DE SOPORTE EXTENDIDO DE SEGURIDAD PARA SPRING FRAMEWORK

Pliego de prescripciones técnicas

SIGMA GESTIÓN UNIVERSITARIA,

A.I.E. (M.P.)

helping universities succeed

1. Objeto del contrato y necesidades a cubrir

El presente contrato tiene por objeto la contratación de un **servicio de soporte extendido de seguridad para Spring Framework**, destinado a garantizar la corrección continua de vulnerabilidades, mantenimiento de parches de seguridad y continuidad operativa de las aplicaciones de la plataforma.

El servicio se justifica por la finalización del soporte comunitario oficial de **Spring Framework 5.3.2** desde agosto de 2024, lo que implica ausencia de actualizaciones de seguridad y aumento del riesgo de ciberseguridad.

Por este motivo, resulta necesario contratar un **servicio de extensión de soporte de seguridad**, que garantice la aplicación continua de parches críticos y la protección frente a vulnerabilidades, asegurando así la estabilidad, disponibilidad y cumplimiento de los estándares de seguridad exigidos en entornos productivos.

2. Contexto

Se requiere la contratación de una empresa especializada que proporcione **soporte continuado y extendido para versiones de Spring Framework a partir de la 5.3.2, y superiores** incluyendo mantenimiento de seguridad, corrección de vulnerabilidades y asesoramiento técnico, **con fecha de fin de soporte mínimo hasta final de contrato**, de forma que se garantice la estabilidad de las aplicaciones actuales y futuras, independientemente del ciclo de vida oficial de la comunidad open source, y se asegure la continuidad operativa de los servicios críticos.

La contratación resulta necesaria para:

a) Garantizar la protección frente a vulnerabilidades críticas
b) Asegurar la estabilidad de los servicios productivos
c) Mantener niveles adecuados de ciberseguridad
d) Evitar riesgos operativos derivados de software sin soporte oficial

3. Alcance de la prestación

El adjudicatario deberá proporcionar un servicio integral de soporte extendido para Spring Framework versión 5.3.2 y superiores, que incluya de forma continua la corrección de vulnerabilidades de seguridad, la entrega de parches mediante técnicas de backporting sobre las versiones soportadas, el asesoramiento técnico especializado, así como el acceso seguro a un repositorio privado desde el cual se distribuyan las dependencias parcheadas necesarias para la correcta integración y mantenimiento de la plataforma.

El servicio de soporte extendido deberá cubrir obligatoriamente y de forma integral los siguientes módulos del ecosistema Spring:

- Spring Framework
- Spring Boot

- Spring Security
- Spring Batch
- Spring Data
- Spring Integration

4. Condiciones de licenciamiento

En atención al crecimiento sostenido de la plataforma y a la coexistencia de despliegues en infraestructuras **on-premise** en distintas universidades, se establece como requisito que el modelo de licenciamiento no quede vinculado a métricas de capacidad tales como **CPU/vCPU, número de servidores o entornos**, por tratarse de parámetros variables en el tiempo y dependientes de decisiones operativas de cada institución.

En consecuencia, se requiere un esquema de licenciamiento de tipo **site/developer**, cuantificable de forma objetiva y estable, fijándose en la actualidad en **diecinueve (19) desarrolladores**.

5. Acuerdo de nivel de servicio

La empresa adjudicataria deberá prestar un **servicio de soporte de seguridad continuo para Spring Framework**, garantizando la monitorización permanente, identificación, análisis, priorización y remediación de vulnerabilidades de seguridad que puedan afectar a los componentes incluidos en el alcance del contrato, así como la provisión de las correspondientes actualizaciones, parches o medidas de mitigación necesarias.

A estos efectos, la adjudicataria deberá cumplir los siguientes **plazos máximos de resolución de vulnerabilidades (CVEs)**, establecidos en función de su nivel de criticidad:

- Las vulnerabilidades clasificadas como **críticas o de alto riesgo (High-risk CVEs)** deberán ser corregidas o mitigadas en un plazo máximo de **quince (15) días naturales** desde su publicación oficial o desde su notificación formal.

- Las vulnerabilidades de **riesgo medio (Medium-risk CVEs)** deberán resolverse en un plazo máximo de **sesenta (60) días naturales** desde su publicación oficial o desde su notificación formal.

- Las vulnerabilidades de **riesgo bajo (Low-risk CVEs)** deberán ser corregidas o mitigadas en un plazo máximo de **noventa (90) días naturales** desde su publicación oficial o desde su notificación formal.

El cumplimiento de los plazos indicados tendrá carácter obligatorio y será considerado condición esencial del contrato, formando parte de los niveles mínimos de servicio exigibles en materia de seguridad, mantenimiento y soporte.

4. Consideraciones adicionales de seguridad

La integración de la solución deberá realizarse mediante **acceso seguro a un repositorio privado de Maven**, ya sea a través de credenciales nominativas o **tokens de autenticación**, desde el cual se pongan a disposición las dependencias parcheadas y mantenidas por el proveedor.

Dichas dependencias deberán poder ser **replicadas o consumidas a través de un repositorio corporativo local** (por ejemplo, Artifactory, Nexus u otro equivalente), garantizando la trazabilidad, control de versiones, disponibilidad continua y alineación con las políticas internas de seguridad y despliegue de la organización.

El adjudicatario deberá disponer de medidas organizativas y técnicas adecuadas que garanticen un nivel suficiente de seguridad en la prestación del servicio, en atención a la naturaleza del contrato y los riesgos asociados al mismo.

5. Equipo técnico asociado al contrato

SIGMA nombrará a un interlocutor que realice las funciones de Responsable del contrato y que será el interlocutor con el adjudicatario.

La empresa adjudicataria deberá facilitar al inicio del proyecto dos interlocutores, uno de carácter comercial y otro de carácter técnico, con responsabilidad en cada uno de estos perfiles. El interlocutor que designe la empresa adjudicataria deberá realizar aquellos informes que, a petición de SIGMA, pudiesen servir para conocer la calidad y el nivel de servicio ofertado.

6. Plazos y lugar de entrega y/o ejecución

El contrato tendrá una duración de tres (3) años, a contar desde el día siguiente a la fecha de formalización del contrato.

Asimismo, durante la vigencia del servicio deberá contemplarse la **posibilidad de actualización o cambio de versión de Spring Framework** cuando resulte necesario por motivos técnicos, de seguridad o de evolución de la plataforma, sin que ello suponga la pérdida del soporte contratado ni la aplicación de penalizaciones contractuales desproporcionadas

El proveedor se compromete a la **provisión y activación de las licencias necesarias** para la prestación del servicio en un plazo máximo que, en todo caso, **no podrá exceder del día 1 de** junio del ejercicio correspondiente, constituyendo dicho plazo una condición esencial del contrato. El incumplimiento de este plazo tendrá carácter de incumplimiento esencial.

7. Formas de seguimiento y control de la ejecución de las condiciones

La empresa adjudicataria deberá informar de forma periódica, completa y documentada sobre las versiones de Spring Framework cubiertas por el servicio, así como sobre los parches de seguridad, correcciones y actualizaciones que se vayan entregando durante la vigencia del contrato, incluyendo como mínimo la identificación de las vulnerabilidades corregidas, su nivel de criticidad, el alcance técnico de cada corrección y las versiones afectadas y resultantes, **ya sea mediante la emisión de informes periódicos formales o a través de un portal de acceso privado o público**, garantizando en todo momento la trazabilidad, transparencia y capacidad de verificación por parte de la entidad contratante.

El adjudicatario deberá informar periódicamente mediante

- informes técnicos formales y/o
- portal público o privado

incluyendo:

- versiones cubiertas
- parches entregados
- vulnerabilidades corregidas
- nivel de criticidad
- impacto técnico

8. Documentación técnica que deben aportar las empresas licitadoras

Las especificaciones técnicas propuestas por la empresa licitadora en su oferta se convertirán en condiciones de obligado cumplimiento a lo largo de la ejecución del contrato si ésta se convierte en la adjudicataria.

Con el fin de acreditar el cumplimiento de cada especificación técnica exigida en este pliego, la empresa licitadora debe aportar la siguiente documentación:

- Descripción técnica del servicio
- Modelo de licenciamiento propuesto
- Sistema de entrega de parches