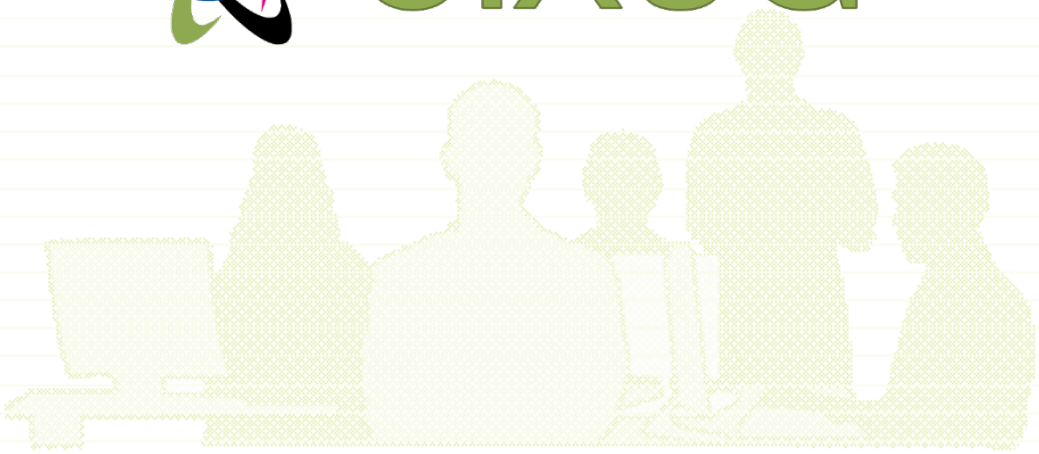

Pliego de Prescripciones Técnicas

Suministro y Cesión de Derechos de Uso para la plataforma SIEM (Security Information and Event Management), en modalidad SaaS de la herramienta Splunk o equivalente

CPV 48730000-4

Paquetes de software de seguridad

Julio, 2024

UNIVERSIDADE DA CORUÑA

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Universidade Vigo

ÍNDICE

1 Objeto del Contrato

El objeto del contrato consiste en el suministro y cesión de derechos de uso del actual **tenant de Splunk Cloud Platform o equivalente** para las tres universidades públicas (Universidad da Coruña, Universidad de Santiago de Compostela y Universidad de Vigo) del Sistema universitario gallego (en adelante SUG) a través del Consorcio para o desenvolvemento de aplicacións de xestión universitaria (en adelante CIXUG).

Esta licencia deberá contar con un mínimo de **10 unidades SVCs (Splunk Virtual Compute)**, capacidad para recibir y procesar **150 GBytes diarios** y ofrecer **13.500 GBytes de almacenamiento de tipo Dynamic Data Active Searchable (DDAS)** y **41.500 GBytes de almacenamiento de tipo Dynamic Data Active Archive (DDAA).**

La duración de la licencia será de **2 años, con posibilidad de prórroga** según los términos del PCAP. La solución, entregada en **formato SaaS nativo** por el fabricante, será dedicada y exclusiva para el SUG, **sin compartir con otros clientes**. El licitante deberá incluir el **SLA de disponibilidad de la plataforma** y asegurar la conservación de todos los datos existentes en la instancia actual.

Además, se suministrará licencia de uso del **software Cribl Stream, en cada universidad**, y se llevarán a cabo las tareas necesarias de **administración y mantenimiento de los servidores y del software on premise que sean necesarios**.

2 Antecedentes

Las universidades públicas gallegas cuentan con una gran cantidad de sistemas informáticos y de comunicaciones para la prestación de los servicios telemáticos que proveen. Cada uno de estos sistemas generan numerosos registros de auditoría, también denominados eventos o logs, que indican los hechos relevantes de cada uno de los procesos que ejecutan.

Habitualmente estos registros se almacenan en el propio sistema que los origina que, en la mayor parte de casos, no suele ofrecer herramientas para la explotación masiva de esta información.

Existe, por tanto, una clara necesidad de centralizar el almacenamiento de estos registros para facilitar su protección, explotación y análisis ya sea en tiempo real o a posteriori, de una forma sencilla y eficiente.

Por otra parte, el análisis continuo y automatizado de los eventos que los sistemas generan, unido a otra información que pueda incorporarse de fuentes externas, es imprescindible para detectar, en el menor tiempo posible, anomalías que pudieran derivar en un incidente de seguridad.

En el año 2023 las tres universidades públicas gallegas, Universidad de A Coruña (UDC), Universidad de Santiago de Compostela (USC) y Universidad de Vigo (UVigo), firmaron un convenio de colaboración para “la ejecución del proyecto UniSoC (diseño e implantación de un servicio de generación de indicadores de compromiso para prevención

de ciberataques), financiado por el Real Decreto 641/2021, del 27 de julio, por el que se regula la concesión directa de subvenciones a universidades públicas españolas para la modernización y digitalización del sistema universitario español en el marco del Plan de Recuperación, Transformación y Resiliencia financiado por la Unión Europea "NEXT GENERATION EU".

El proyecto UniSOC se plasmó en la adopción de una plataforma SIEM, compuesta por una instancia de Splunk Cloud Platform y una instancia de Splunk heavy forwarder y otra de Cribl Stream desplegadas en cada una de las tres universidades.

Con posterioridad se contrató una asistencia técnica para el análisis de alertas generadas por dicha plataforma SIEM.

Durante la reunión del Consejo de Gobierno del Consorcio CIXUG, celebrada el día 5 de diciembre del 2023, se acordó por unanimidad que, para poder dar continuidad al proyecto, se trasladarían las iniciativas de licitación, contratación y administración al Consorcio desde la Universidad da Coruña, gestionando la contratación final antes del 1 de enero del 2025, fecha cuando se iniciaría el servicio con los proveedores adjudicatarios de la licitación a través del CIXUG.

3 Alcance

3.1 Suministro de licencias

Específicamente, a través del presente proceso se persigue el suministro y cesión de derechos de uso de licencias de la actual instancia (o tenant) **de Splunk Cloud Platform o equivalente**, que deberá cumplir los siguientes requisitos:

- Contará con un mínimo de **10 unidades SVCs** (Splunk Virtual Compute), valorándose un incremento de esta cantidad (criterio C.2).
- Tendrá capacidad de recibir y procesar un mínimo de **150 GBytes diarios**.
- La licencia tendrá una **duración de 2 años**, prorrogables según los términos expuestos en el PCAP.
- Deberá proporcionar un mínimo de **13.500 GBytes** de almacenamiento de tipo **Dynamic Data Active Searchable (DDAS)**, valorándose un incremento de esta cantidad (criterio C.3).
- Deberá proporcionar un mínimo de **41.500 GBytes** de almacenamiento de tipo **Dynamic Data Active Archive (DDAA)** valorándose un incremento de esta cantidad (criterio C.3).
- La solución deberá ser entregada en formato SaaS nativo ofrecido y mantenido directamente por el fabricante de la solución, no siendo válido el montaje a medida de un servicio sobre una nube pública o privada que requiera operación manual de la plataforma.

La plataforma será dedicada y no podrá ser compartida con otros clientes de la plataforma SaaS contratada.

Deberán conservarse todos los datos alojados en la instancia actual.

Se suministrará licencia de uso del software Cribl Stream desplegado en cada una de las universidades para proporcionar funcionalidades adicionales en gestión de eventos y optimización de la licencia contratada.

3.2 Administración de la plataforma SIEM

El adjudicatario deberá realizar las siguientes tareas:

- Administración y mantenimiento de los servidores *on premise* necesarios para el servicio.
- Administración y mantenimiento de la instancia de Splunk Cloud o equivalente:
  - Alta, bajas y modificaciones de usuarios
  - Gestión del espacio de almacenamiento
  - Instalación de technical add-ons necesarios
- Administración y mantenimiento de Cribl Stream:
  - Configuración de mecanismos de agregación y filtrado de logs no necesarios.
  - Eliminación de campos prescindibles o información redundante.
  - Modificación de la extracción de campos según las necesidades del proyecto.

3.3 Consultoría y formación

- Las ofertas deberán incluir un servicio de consultoría para la ingesta de logs de nuevos sistemas, con mínimo de 5 tipos de sistemas al año.
- Las propuestas deberán incluir un **curso** dirigido a analistas y personal técnico de ciberseguridad de las universidades del SUG. Deberá ser un curso oficial del fabricante de la solución. Se realizará una edición para un mínimo de 15 participantes.
- Se valorarán aquellas propuestas que incluyan **servicios de consultoría** que aporten valor añadido al servicio, tales como despliegue de casos de uso, la integración con sistemas de seguridad para conseguir automatizaciones o la incorporación de nuevas herramientas a la plataforma, todo ello con fines de mejorar la detección, prevención y recuperación ante incidentes (criterio B.1).

3.4 Soporte y mantenimiento

El soporte y mantenimiento cubrirá todos los elementos de la plataforma SIEM excluyendo, únicamente, el soporte del hardware proporcionado por las tres universidades del SUG.

El adjudicatario llevará a cabo las siguientes tareas que afectan al equipamiento y todo el software desplegado *on premise*:

- Mantenimiento preventivo: revisión periódica del estado del sistema operativo y aplicaciones o paquetes instalados, aplicando nuevas versiones que corrijan vulnerabilidades.

- Mantenimiento evolutivo: instalación de nuevas versiones de las aplicaciones con nuevas funcionalidades o casos de uso, si procede. Deberán documentarse adecuadamente las modificaciones realizadas en la configuración de cada uno de los componentes de la herramienta.
- Mantenimiento correctivo: cubrirá las intervenciones necesarias frente a mal funcionamiento de cualquier componente de la plataforma, a excepción del hardware que hayan proporcionado las universidades.
- Los licitantes deberán indicar en sus propuestas el acuerdo de nivel de servicio (SLA) para las tareas anteriores.

Los requisitos mínimos para resolución de incidencias (tiempo que transcurra desde la comunicación de la incidencia hasta la reposición del servicio) será los siguientes:

- Tiempo máximo de resolución de incidencias no críticas, entendiendo como tales aquellas que sólo afectan a algunas funcionalidades de la herramienta, no impidiendo la ingesta de eventos ni las búsquedas: 96 horas.
- Tiempo máximo de resolución de incidencias críticas, entendiendo como tales aquellas que impidan la ingesta de eventos o las búsquedas: 12 horas.
- En los anteriores tiempos máximos solo se considerarán los problemas que afecten a los sistemas instalados *on premise.*
- Para servicios en la nube el adjudicatario deberá realizar la gestión de los Service Level Credit que ofrece el fabricante como compensación de un posible incumplimiento de su SLA.

El adjudicatario proporcionará el servicio de soporte a través de una herramienta de ticketing que permita realizar una gestión eficiente de las tareas necesarias. Habilitará también un número de teléfono para la comunicación de incidentes especialmente graves.

El soporte deberá prestarse de lunes a viernes, de 9:00 a 17:00, excepto festivos nacionales y autonómicos de la comunidad autónoma de Galicia.

Se presentará un informe trimestral sobre el cumplimiento del SLA propuesto, incluyendo, como mínimo, tiempos medios de resolución de incidencias y tiempo de disponibilidad de la plataforma SaaS.

El adjudicatario proporcionará el soporte de primer nivel en las incidencias relativas a los servicios contratados en la nube, gestionando las solicitudes necesarias con el fabricante. Para ello deberá contratar el soporte oficial de éste, aportando evidencias documentales. Las universidades del SUG podrán hacer uso de este servicio de soporte directamente, además del que ofrezca el adjudicatario.

4 Requisitos

4.1 Condición de partner

Los licitantes deberán acreditar su condición de partner del fabricante Splunk.

4.2 Equipo de trabajo

El licitante deberá proponer un equipo de trabajo compuesto, al menos, por los siguientes perfiles:

4.2.1 Jefe/a de proyecto

Cuyo perfil deberá cumplir los siguientes requisitos mínimos:

- Contar con una de las siguientes titulaciones: Ingeniero/a de Telecomunicación o Informática, Licenciado en Informática, ingeniero/a técnico/a de Telecomunicación o Informática, graduado/a o máster en áreas de Ingeniería de Telecomunicación o Ingeniería Informática.
- 10 años de experiencia en trabajos técnicos o de consultoría en ciberseguridad o gestión de sistemas TIC.
- Experiencia contrastable en proyectos del mismo ámbito.

Sus funciones serán las siguientes:

- Actuar de interlocución, por parte del adjudicatario, con la dirección técnica.
- Coordinar las tareas contempladas en la propuesta técnica y aquellas que se deriven de las distintas fases que componen el proyecto.
- Coordinar a los miembros de su equipo de trabajo.
- Realizar un seguimiento continuo del avance del proyecto según la planificación prevista, adoptando medidas correctivas, tras ser consensuadas con la dirección del proyecto si procede, en caso de desviaciones significativas.
- Realizar el control de calidad de toda la documentación que vaya a entregarse a la dirección del proyecto.
- Asistir a las reuniones de seguimiento que la dirección del proyecto convoque, redactando el acta correspondiente, que deberá ser enviada a la dirección del proyecto en un plazo no mayor a dos días hábiles.

4.2.2 Equipo técnico

Compuesto por el número de técnicos/as que el licitador considere necesario.

Deberán cumplir los siguientes requisitos mínimos:

- Contar con una de las siguientes titulaciones: ingeniero/a de Telecomunicación o Informática, ingeniero/a técnico/a de Telecomunicación o Informática, graduado/a o máster en áreas de Ingeniería de Telecomunicación o Ingeniería Informática, titulaciones de formación profesional de grado superior en el ámbito de la Informática y Comunicaciones.
- 2 años de experiencia en trabajos técnicos o de consultoría en ciberseguridad o gestión de sistemas TIC.
- Experiencia contrastable en proyectos del mismo ámbito.

Cualquier cambio que el adjudicatario realice en cualquiera de los equipos de

trabajo deberá contar con la autorización expresa de la dirección técnica y en ningún caso podrá modificar la acreditación aportada en la solvencia técnica. Dicho cambio deberá ser notificado a la persona responsable del contrato con, al menos, quince días de antelación y siempre con el tiempo suficiente para llevar a cabo la transferencia de conocimiento entre los miembros del equipo.

5 Condiciones relativas a la gestión de la seguridad de la información tratada

El adjudicatario deberá acreditar el cumplimiento de las obligaciones con el Esquema Nacional de Seguridad, mediante alguna de las siguientes condiciones:

Acreditación de estándares de seguridad similares al ENS, como ISO/IEC 27001.

Acreditación de esquemas de certificación de seguridad europeos.

Acreditación del cumplimiento de las medidas de seguridad conforme al Anexo II del Real Decreto 311/2022, presentando una Declaración de aplicabilidad conforme al anexo II del ENS en el que el licitador especifique la medida en su sistema y cómo la aplica.

5.1 Persona de contacto

El adjudicatario deberá informar al CIXUG, tras la firma del contrato, de la persona de contacto para la seguridad de la información tratada y del servicio prestado, según los términos indicados en el artículo 13 del Real Decreto 311/2022, o legislación futura vigente.

Dicha persona deberá ser el responsable de seguridad de la organización, formar parte de su área o tener comunicación directa con la misma.

Se encargará de canalizar y supervisar el cumplimiento de los requisitos de seguridad del servicio o solución implicados en el contrato, realizar las comunicaciones relativas a seguridad de la información y la coordinación y gestión de los incidentes que pudieran suceder.

Cualquier cambio en la persona designada para estas funciones deberá ser notificado al CIXUG.

5.2 Gestión de incidentes de seguridad

El adjudicatario notificará al CIXUG, con carácter urgente, la existencia de cualquier incidencia, que pudiera afectar a la seguridad de la información, que conociera en el desarrollo de las tareas objeto del contrato y que pudieran afectar a la seguridad de los Sistemas de Información de la entidad contratante.

Será obligatorio que la entidad adjudicataria, disponga de un registro operativo a los efectos de registro de incidencias y peticiones, y deberá cumplir las premisas establecidas en la normativa de protección de datos.

Con carácter general, se comunicarán mediante llamada de teléfono y correo

electrónico, en el plazo máximo de 24 horas naturales, las incidencias sobre el sistema de información o sobre los datos personales, que se produzcan. Durante todo el proceso de gestión de la incidencia, el adjudicatario deberá emitir informes de seguimiento de la incidencia, detallando todas las medidas de contención y corrección desplegadas, las medidas forenses que se estuvieran desarrollando y las medidas de prevención que se pondrán en marcha para que la incidencia no vuelva a producirse.

El adjudicatario deberá preparar todos los documentos y evidencias que se requieran cuando una autoridad de control requiera al CIXUG más información, colaborando con los equipos de respuesta de incidentes y análisis forense.

5.3 Acuerdo de nivel de servicio

Los licitadores deberán presentar en su oferta los parámetros relativos al nivel de servicio comprometido, según lo solicitado en el apartado “Soporte y mantenimiento” de este pliego.

El adjudicatario deberá presentar un informe trimestral de cumplimiento de los parámetros que componen el SLA.

6 Contenido de las propuestas

Las propuestas técnicas, que se incluirán en el sobre B, deberán contener los siguientes apartados.

Las propuestas no deberán exceder de 30 páginas, con tipo de fuente Arial, tamaño 12, interlineado sencillo y márgenes mínimos superior e inferior de 2,5 cm y de 3 cm a derecha e izquierda. Las propuestas que excedan estas 30 páginas solo se tendrán en cuenta hasta dicha página 30.

1. ÍNDICE
2. RESUMEN EJECUTIVO: Breve descripción de las características principales de la solución ofertada.
3. DESCRIPCIÓN DE LA SOLUCIÓN TÉCNICA OFERTADA
    - Licencia suministrada (sin citar los datos valorables de forma automática).
    - Descripción de la formación ofertada.
    - Descripción de los servicios de consultoría valorables según lo indicado en el apartado “Consultoría y formación” de este pliego.
    - Descripción del equipo de trabajo, incluyendo formación académica, experiencia y certificaciones para cada miembro del equipo.
    - Descripción del servicio de mantenimiento: horario, idioma, formas de contacto, herramienta de ticketing,...

7 Universidades participantes

Las universidades participantes serían las Universidades del SUG a través del Consorcio CIXUG:

- Universidad de A Coruña

- Universidad de Santiago de Compostela
- Universidad de Vigo

8 Duración del contrato, Plazo de ejecución

Dos años más una posible prórroga, a contar desde la fecha de formalización del contrato.

9 Actualizaciones

A lo largo de la duración del contrato y durante el proceso de firma, posterior a la adjudicación, sólo se permitirán actualizaciones, por parte del adjudicatario, de modificación de los productos solicitados en esta que lleven mejoras, tanto en funcionalidades como en nuevas librerías que se incorporen a las actuales, sin que ello suponga mayor coste para el CIXUG.

10 Responsabilidad de la empresa adjudicataria

En lo que se refiere a los términos generales en la prestación de servicios, la empresa adjudicataria debe cumplir los requisitos impuestos en este Pliego y en el Pliego de Cláusulas Administrativas del presente concurso, incluyendo los relativos la protección de datos, confidencialidad, ciberseguridad y propiedad intelectual.

En el marco del presente servicio, la empresa adjudicataria se compromete a:

- Designar a un interlocutor con el CIXUG y a las Universidades del SUG, para labores de coordinación global, así como interlocutores con responsabilidad sobre la prestación de cada uno de los servicios descritos.
- Usar los recursos que el CIXUG y las Universidades del SUG pongan a su disposición con los fines exclusivos que se describen en este documento.
- Realizar un seguimiento de la prestación del servicio, aportando evidencias en forma de indicadores, cumplimiento de niveles de servicio.

11 Incompatibilidades de uso o técnicos

Será excluida cualquier oferta que genere cualquier suerte de incompatibilidad o dificultad técnica y/o de uso con el actual sistema existente en cualquier de las tres universidades. La solución ofertada ha de ser totalmente compatible con lo existente sin que pueda generar ninguna suerte de incompatibilidad y/o dificulta técnica o de uso.

Santiago de Compostela a la fecha de la firma electrónica.

Firmado digitalmente por LOPEZ DIAZ ANTONIO - 76565571C
Fecha: 2024.07.31 13:23:08 +02'00'

D. Antonio López Díaz
Presidente