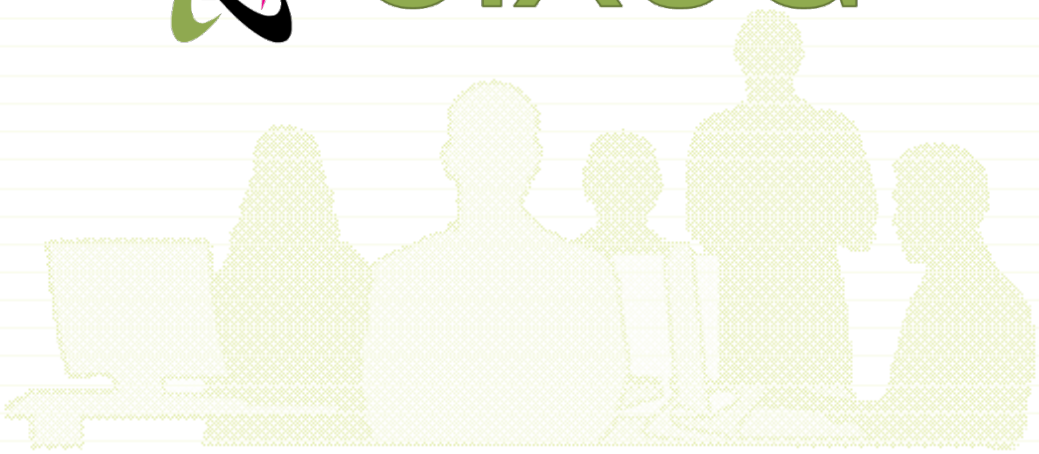

Pliego de Prescripciones Técnicas

Servicio de análisis y gestión de alertas de ciberseguridad en el marco del proyecto UniSOC

CPV 72600000-6

Servicios de apoyo informático y de consultoría

Julio, 2024

UNIVERSIDADE DA CORUÑA

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Universidade Vigo

ÍNDICE

1 Objeto del Contrato

El objeto del contrato consiste en la adjudicación, para las tres universidades públicas (Universidad de A 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 para a xestión universitaria (en adelante CIXUG) de un servicio de asistencia técnica para el análisis y gestión de alertas que produzca la plataforma SIEM del proyecto UniSOC.

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 “NEXTGENERATIONEU”.

El proyecto UniSOC se plasmó en la adopción de una plataforma SIEM, compuesta por un tenant 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 reunión del Consejo de Gobierno del Consorcio CIXUG, formado por las

tres universidades públicas del Sistema Universitario Gallego (SUG), 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 de A 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 Asistencia técnica para el análisis y gestión de alertas de seguridad

Las tareas principales que se llevarán a cabo serán las siguientes:

- Revisión, análisis y priorización de la información y las alertas que produzca la plataforma SIEM. Esta información se obtendrá mediante el acceso directo a la interfaz web de la plataforma, donde se obtendrán los datos de las alertas y los paneles o dashboards, la investigación en profundidad de las alertas mediante las herramientas de búsqueda que proporciona la plataforma o la consulta a fuentes externas para enriquecer el análisis.
- Ejecución de los procedimientos de escalado de incidencias, para las tres universidades, mediante la apertura de tickets en sus respectivas aplicaciones de gestión de incidencias o mediante el envío de notificaciones por correo electrónico.
- Colaboración en la mejora de los casos de uso implementados en la plataforma SIEM.
- Redacción de informes trimestrales del servicio, donde se incluirán estadísticas sobre el número de alertas procesadas agrupadas por criticidad, el tiempo de respuesta, el número de tickets abiertos y un resumen sobre los indicadores de compromiso generados, así como los nuevos casos de uso que se hubieran configurado en la plataforma.

4 Requisitos del servicio

- **Los licitantes deberán acreditar su condición de partner del fabricante Splunk.**
- Se destinará al servicio un/a analista de ciberseguridad principal, a tiempo completo, para llevar a cabo las tareas detalladas en el apartado 3.
- Los licitadores deberán proponer un/a jefe/a de proyecto, con una dedicación estimada al proyecto de 3 horas al mes.
- Horario de prestación del servicio: la asistencia técnica se prestará en horario de lunes a viernes, de 8:00 a 14:00 y de 15:00 a 17:00, excepto festivos nacionales y autonómicos.
- Duración del servicio: La asistencia técnica se prestará por dos años, prorrogables según los términos expuestos en el PCAP.
- Las vacaciones del analista principal se disfrutarán preferentemente entre el 1

y el 15 de agosto y entre el 20 de diciembre y el 6 de enero. Las fechas del resto de días que le corresponda serán acordados con el CIXUG.

- En caso de bajas o permisos, el adjudicatario deberá sustituir al/a la analista principal por otro/a que cumpla los mismos requisitos, en el plazo no superior a 10 días hábiles. Estos días deberán ser recuperados mediante horas de prestación de servicio de perfiles similares.
- Los trabajos se desarrollarán, de forma general, en dependencias de la UDC. Se preverán desplazamientos a las dependencias de las universidades de Santiago de Compostela o Vigo para el desarrollo de reuniones de coordinación o seguimiento del servicio.
- Una vez el servicio alcance la madurez suficiente el CIXUG podrá autorizar, si lo estima oportuno, que se preste el servicio de forma no presencial, en su totalidad o parcialmente.
- Se valorará (criterio B.1) la existencia de un equipo técnico que pueda dar apoyo al/a la analista destinado al proyecto.
- Acuerdo de nivel de servicio (SLA): los licitantes deberán incluir una propuesta de tiempos objetivo para analizar, investigar y notificar las alertas, distinguiendo entre alertas severas y no severas. También incluirán la cantidad de alertas diarias que, en promedio, se podrán analizar. Esta propuesta se valorará conforme al criterio B.2.

5 Requisitos del equipo de trabajo

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

5.1.1 Jefe/a de proyecto

Se destinará al servicio un/una 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 o título universitario equiparable.
- 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 interlocutor, por parte del adjudicatario, con la dirección técnica.
  - Coordinar a los miembros del 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

- Presentar al CIXUG informes trimestrales de cumplimiento del SLA ofertado.
- Realizar un 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, redactar las actas y remitirlas a la dirección del proyecto en el plazo de 48 horas.

5.1.2 Analista de ciberseguridad

Se destinará al servicio un **analista de ciberseguridad** que deberá 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 o título universitario equiparable.
- 5 años de experiencia como analista de seguridad o en trabajos técnicos o de consultoría en ciberseguridad.
- Experiencia contrastable en proyectos del mismo ámbito.
- Deberá contar con, al menos, una de las siguientes certificaciones:
  - Splunk Core Certified Power User
  - Splunk Cloud Certified Admin
  - Splunk Enterprise Certified Architect
  - Splunk Certified Cybersecurity Defense Analyst

Cualquier cambio que el adjudicatario realice en el personal destinado al proyecto deberá contar con la autorización expresa de la dirección técnica y en ningún caso podrá modificar la acreditación aportada en la solvencia técnica. Dicha petición de cambio deberá ser notificada 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.

6 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.

6.1.1 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.

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.

6.1.2 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.

6.1.3 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 “Requisitos del servicio” de este pliego.

7 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 dicho punto.

- ÍNDICE
- RESUMEN EJECUTIVO: Breve descripción de las características principales del servicio ofertado.
- DESCRIPCIÓN DEL SERVICIO OFERTADO
  - Propuesta metodológica para cumplir los objetivos indicados en este pliego.
  - Perfiles destinados al proyecto: titulación y experiencia.
  - Propuesta de SLA

8 Control de la calidad de los trabajos

La dirección del proyecto del CIXUG llevará a cabo un control de la calidad de los trabajos realizados y podrá rechazar aquellos que no cumplan las condiciones mínimas, todo ello con independencia de las penalizaciones o de una posible resolución contractual contempladas en el PCAP.

Las condiciones mínimas de calidad serán:

- Que los trabajos se realicen conforme a la metodología ofertada.
- Que se respecte el SLA ofertado.
- Que se respete la planificación de los trabajos.
- Que se realicen las reuniones de seguimiento y se entreguen las actas correspondientes en el plazo marcado.

9 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

10 Duración del contrato, Plazo de ejecución

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

11 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.

12 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.

Santiago de Compostela a la fecha de la firma electrónica.

Firmado digitalmente por LOPEZ DIAZ ANTONIO - 76565571C
Fecha: 2024.07.31 14:35:49 +02'00'

D. Antonio López Díaz
Presidente