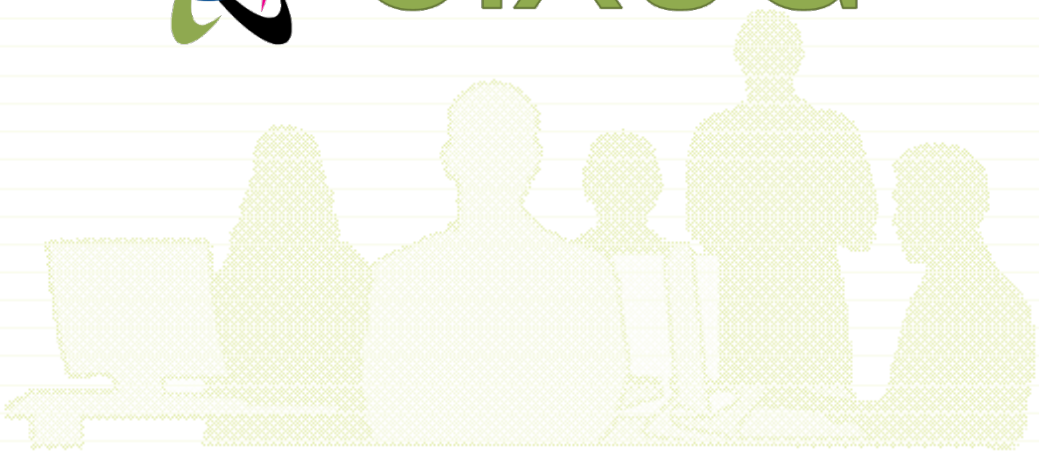

Prego de Prescricións Técnicas

Subministración e Cesión de Dereitos de Uso para a plataforma SIEM (Security Information and Event Management), en modalidade SaaS da ferramenta Splunk ou equivalente

CPV 48730000-4

Paquetes de software de seguridade

Xullo, 2024

UNIVERSIDADE DA CORUÑA

USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Universidade Vigo

ÍNDICE

1 Obxecto do Contrato

O obxecto do contrato consiste na subministración e cesión de dereitos de uso do actual **tenant de Splunk Cloud Platform ou equivalente** para as tres universidades públicas (Universidade da Coruña, Universidade de Santiago de Compostela e Universidade de Vigo) do Sistema universitario galego (en adiante SUG) a través do Consorcio para o desenvolvemento de aplicacións de xestión universitaria (en adiante CIXUG).

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

A duración da licenza será de **2 anos, con posibilidade de prórroga** segundo os termos do PCAP. A solución, entregada en **formato SaaS nativo** polo fabricante, será dedicada e exclusiva para o SUG, **sen compartir con outros clientes**. O licitante deberá incluír o **SLA de dispoñibilidade da plataforma** e asegurar a conservación de todos os datos existentes na instancia actual.

Ademais, subministrarase a licencia de uso do **software Cribl Stream, en cada universidade**, e levaranse a cabo as tarefas necesarias de **administración e mantemento dos servidores e do software on premise que sexan necesarios**.

2 Antecedentes

As universidades públicas galegas contan con unha gran cantidade de sistemas informáticos e de comunicacións para a prestación dos servizos telemáticos que proveen. Cada un destes sistemas xera numerosos rexistros de auditoría, tamén denominados eventos ou logs, que indican os feitos relevantes de cada un dos procesos que executa.

Habitualmente estes rexistros almacénanse no propio sistema que os orixina que, na maior parte dos casos, non adoitan ofrecer ferramentas para a explotación masiva desta información.

Existe, por tanto, unha clara necesidade de centralizar o almacenamento destes rexistros para facilitar a súa protección, explotación e análise xa sexa en tempo real ou a posteriori, dunha forma sinxela y eficiente.

Por outra parte, o análise continuo e automatizado dos eventos que os sistemas xeran, unido a outra información que poida incorporarse de fontes externas, é imprescindible para detectar, no menor tempo posible, anomalías que puideran derivar nun incidente de seguridade.

No ano 2023 as tres universidades públicas galegas, Universidade de A Coruña (UDC), Universidade de Santiago de Compostela (USC) e Universidade de Vigo (UVigo), asinaron un convenio de colaboración para “a execución do proxecto UniSoC (deseño e implantación dun servizo de xeración de indicadores de compromiso para prevención de

ciberataques), financiado polo Real Decreto 641/2021, do 27 de xullo, polo que se regula a concesión directa de subvencións a universidades públicas españolas para a modernización e dixitalización do sistema universitario español no marco do Plan de Recuperación, Transformación e Resiliencia financiado pola Unión Europea "NEXT GENERATION EU".

O proxecto UniSOC plasmouse na adopción dunha plataforma SIEM, composta por unha instancia de Splunk Cloud Platform e unha instancia de Splunk heavy forwarder e outra de Cribl Stream despregadas en cada unha das tres universidades.

Con posterioridade contratouse unha asistencia técnica para o análise de alertas xeradas pola dita plataforma SIEM.

Durante a reunión do Consello de Goberno do Consorcio CIXUG, celebrada o día 5 de decembro do 2023, acordouse por unanimidade que, para poder dar continuidade ao proxecto, trasladaríanse as iniciativas de licitación, contratación e administración ao Consorcio CIXUG desde a Universidade da Coruña, xestionando a contratación final antes do 1 de xaneiro do 2025, data cando se iniciaría o servicio cos provedores adxudicatarios da licitación a través do CIXUG.

3 Alcance

3.1 Subministración de licenzas

Especificamente, a través do presente proceso perséguese a subministración e cesión de dereitos de uso de licencias da actual instancia (ou tenant) **de Splunk Cloud Platform ou equivalente**, que deberá cumprir os seguintes requisitos:

- Contará cun mínimo de **10 unidades SVCs** (Splunk Virtual Compute), valorándose un incremento desta cantidade (criterio C.2).
- Terá capacidade de recibir e procesar un mínimo de **150 GBytes diarios**.
- A licenza terá unha **duración de 2 anos**, prorrogables segundo os termos expostos no PCAP.
- Deberá proporcionar un mínimo de **13.500 GBytes** de almacenamento de tipo **Dynamic Data Active Searchable (DDAS)**, valorándose un incremento desta cantidade (criterio C.3).
- Deberá proporcionar un mínimo de **41.500 GBytes** de almacenamento de tipo **Dynamic Data Active Archive (DDAA)** valorándose un incremento desta cantidade (criterio C.3).
- A solución deberá ser entregada en formato SaaS nativo ofrecido e mantido directamente polo fabricante da solución, non sendo válido o montaxe a medida dun servicio sobre unha nube pública ou privada que requira operación manual da plataforma.

A plataforma será dedicada e non poderá ser compartida con outros clientes da plataforma SaaS contratada.

Deberán conservarse todos os datos aloxados na instancia actual.

Subministrarase licenza de uso do software Cribl Stream despregado en cada unha das universidades para proporcionar funcionalidades adicionais en xestión de eventos e optimización da licenza contratada.

3.2 Administración da plataforma SIEM

O adxudicatario deberá realizar as seguintes tarefas:

- Administración e mantemento dos servidores *on premise* necesarios para o servizo.
- Administración e mantemento da instancia de Splunk Cloud ou equivalente:
  - Altas, baixas e modificacións de usuarios.
  - Xestión do espazo de almacenamento.
  - Instalación de technical add-ons necesarios.
- Administración e mantemento de Cribl Stream:
  - Configuración de mecanismos de agregación e filtrado de logs non necesarios.
  - Eliminación de campos prescindibles ou información redundante.
  - Modificación da extracción de campos segundo as necesidades do proxecto.

3.3 Consultaría e formación

- As ofertas deberán incluír un servizo de consultaría para a inxesta de logs de novos sistemas, cun mínimo de 5 tipos de sistemas ao ano.
- As propostas deberán incluír un **curso** dirixido a analistas e persoal técnico de ciberseguridade das universidades do SUG. Deberá ser un curso oficial do fabricante da solución. Realizarase unha edición para un mínimo de 15 participantes.
- Valoraranse aquelas propostas que inclúan **servizos de consultaría** que aporten valor engadido ao servizo, tales como despregue de casos de uso, a integración con sistemas de seguridade para conseguir automatizacións ou a incorporación de novas ferramentas á plataforma, todo elo con fins de mellorar a detección, prevención e recuperación ante incidentes (criterio B.1).

3.4 Soporte e mantemento

O soporte e mantemento cubrirá todos os elementos da plataforma SIEM excluíndo, unicamente, o soporte do hardware proporcionado polas tres universidades do SUG.

O adxudicatario levará a cabo as seguintes tarefas que afectan ao equipamento e todo o software despegado *on premise*:

- Mantemento preventivo: revisión periódica do estado do sistema operativo e aplicacións ou paquetes instalados, aplicando novas versións que corrixan vulnerabilidades.

- Mantemento evolutivo: instalación de novas versións das aplicacións con novas funcionalidades ou casos de uso, se procede. Deberán documentarse adecuadamente as modificacións realizadas na configuración de cada un dos compoñentes da ferramenta.
- Mantemento correctivo: cubrirá as intervencións necesarias fronte ao mal funcionamento de calquera compoñente da plataforma, a excepción do hardware que proporcionaran as universidades.
- Os licitantes deberán indicar nas súas propostas o acordo de nivel de servizo (SLA) para as tarefas anteriores.

Os requisitos mínimos para resolución de incidencias (tempo que transcorra desde a comunicación da incidencia hasta a reposición do servicio) serán os seguintes:

- Tempo máximo de resolución de incidencias non críticas, entendendo como tales aquelas que só afectan a algunhas funcionalidades da ferramenta, non impedindo a inxesta de eventos nin as buscas: 96 horas.
- Tempo máximo de resolución de incidencias críticas, entendendo como tales aquelas que impidan a inxesta de eventos ou as buscas: 12 horas.
- Nos anteriores tempos máximos só se considerarán os problemas que afecten aos sistemas instalados *on premise.*
- Para servizos na nube o adxudicatario deberá realizar a xestión dos Service Level Credit que ofrece o fabricante como compensación dun posible incumprimento do seu SLA.

O adxudicatario proporcionará o servizo de soporte a través dunha ferramenta de ticketing que permita realizar unha xestión eficiente das tarefas necesarias. Habilitará tamén un número de teléfono para a comunicación de incidentes especialmente graves.

O soporte deberá prestarse de luns a venres, de 9:00 a 17:00, excepto festivos nacionais e autonómicos da comunidade autónoma de Galicia.

Presentarase un informe trimestral sobre o cumprimento do SLA proposto, incluíndo, como mínimo, tempos medios de resolución de incidencias e tempo de dispoñibilidade da plataforma SaaS.

O adxudicatario proporcionará o soporte de primeiro nivel nas incidencias relativas aos servizos contratados na nube, xestionando as solicitudes necesarias có fabricante. Para elo deberá contratar o soporte oficial deste, aportando evidencias documentais. As universidades do SUG poderán facer uso deste servizo de soporte directamente, ademais do que ofreza o adxudicatario.

4 Requisitos

4.1 Condición de partner

Os licitantes deberán acreditar a súa condición de partner do fabricante Splunk.

4.2 Equipo de traballo

O licitante deberá propoñer un equipo de traballo composto, polo menos, polos seguintes perfís:

4.2.1 Xefe/a de proxecto

Cuxo perfil deberá cumprir os seguintes requisitos mínimos:

- Contar cunha das seguintes titulacións: Enxeñeiro/a de Telecomunicación ou Informática, Licenciado en Informática, enxeñeiro/a técnico/a de Telecomunicación ou Informática, graduado/a ou mestrado en áreas de Enxeñaría de Telecomunicación ou Enxeñaría Informática.
- 10 anos de experiencia en traballos técnicos ou de consultaría en ciberseguridade ou xestión de sistemas TIC.
- Experiencia contrastable en proxectos do mesmo ámbito.

As súas funcions serán as seguintes:

- Actuar de interlocución, por parte do adxudicatario, coa dirección técnica.
- Coordinar as tarefas contempladas na proposta técnica e aquelas que se deriven das distintas fases que compoñen o proxecto.
- Coordinar aos membros do seu equipo de traballo.
- Realizar un seguimento continuo do avance do proxecto segundo a planificación prevista, adoptando medidas correctivas, tras ser consensuadas coa dirección do proxecto se procede, en caso de desviacións significativas.
- Realizar o control de calidade de toda a documentación que vaia a entregarse á dirección do proxecto.
- Asistir ás reunións de seguimento que a dirección do proxecto convoque, redactando o acta correspondente, que deberá ser enviada á dirección do proxecto nun prazo non maior a dous días hábiles.

4.2.2 Equipo técnico

Composto polo número de técnicos/as que o licitador considere necesario.

Deberán cumprir os seguintes requisitos mínimos:

- Contar cunha das seguintes titulacións: enxeñeiro/a de Telecomunicación ou Informática, enxeñeiro/a técnico/a de Telecomunicación ou Informática, graduado/a ou mestrado en áreas de Enxeñaría de Telecomunicación ou Enxeñaría Informática, titulacións de formación profesional de grao superior no ámbito da Informática e Comunicacións.
- 2 anos de experiencia en traballos técnicos ou de consultaría en ciberseguridade ou xestión de sistemas TIC.
- Experiencia contrastable en proxectos do mesmo ámbito.

Calquera cambio que o adxudicatario realice en calquera dos equipos de traballo

deberá contar coa autorización expresa da dirección técnica e en ningún caso poderá modificar a acreditación aportada na solvencia técnica. O dito cambio deberá ser notificado á persoa responsable do contrato con, polo menos, quince días de antelación e sempre có tempo suficiente para levar a cabo a transferencia de coñecemento entre os membros do equipo.

5 Condicións relativas á xestión da seguridade da información tratada

O adxudicatario deberá acreditar o cumprimento das obrigacións có Esquema Nacional de Seguridade, mediante algunha das seguintes condicións:

Acreditación de estándares de seguridade similares ao ENS, como ISO/IEC 27001.

Acreditación de esquemas de certificación de seguridade europeos.

Acreditación do cumprimento das medidas de seguridade conforme ao Anexo II do Real Decreto 311/2022, presentando unha Declaración de aplicabilidade conforme ao anexo II do ENS no que o licitador especifique a medida no seu sistema e como a aplica.

5.1 Persoa de contacto

O adxudicatario deberá informar ao CIXUG, trala firma do contrato, da persoa de contacto para a seguridade da información tratada e do servizo prestado, segundo os termos indicados no artigo 13 do Real Decreto 311/2022, ou lexislación futura vixente.

A dita persoa deberá ser o responsable de seguridade da organización, formar parte da súa área ou ter comunicación directa coa mesma.

Encargarase de canalizar e supervisar ao cumprimento dos requisitos de seguridade do servizo ou solución implicados no contrato, realizar as comunicacións relativas a seguridade da información e a coordinación e xestión dos incidentes que puideran suceder.

Calquera cambio na persoa designada para estas funcións deberá ser notificado ao CIXUG.

5.2 Xestión de incidentes de seguridade

O adxudicatario notificará ao CIXUG, con carácter urxente, a existencia de calquera incidencia, que puidera afectar á seguridade da información, que coñecera no desenvolvemento das tarefas obxecto do contrato e que puideran afectar á seguridade dos Sistemas de Información da entidade contratante.

Será obrigatorio que a entidade adxudicataria, dispoña dun rexistro operativo aos efectos de rexistro de incidencias e peticións, e deberá cumprir as premisas establecidas na normativa de protección de datos.

Con carácter xeral, comunicaranse mediante chamada de teléfono e correo electrónico, no prazo máximo de 24 horas naturais, as incidencias sobre o sistema de

información ou sobre os datos persoais, que se produzan. Durante todo o proceso de xestión da incidencia, o adxudicatario deberá emitir informes de seguimento da incidencia, detallando todas as medidas de contención e corrección despregadas, as medidas forenses que se estiveran desenvolvendo e as medidas de prevención que se porán en marcha para que a incidencia non volva a producirse.

O adxudicatario deberá preparar todos os documentos e evidencias que se requiran cando unha autoridade de control requira ao CIXUG mais información, colaborando cos equipos de resposta de incidentes e análise forense.

5.3 Acordo de nivel de servizo

Os licitadores deberán presentar na súa oferta os parámetros relativos ao nivel de servizo comprometido, segundo o solicitado no apartado “Soporte e mantemento” deste prego.

O adxudicatario deberá presentar un informe trimestral de cumprimento dos parámetros que compoñen o SLA.

6 Contido das propostas

As propostas técnicas, que se incluirán no sobre B, deberán conter os seguintes apartados.

As propostas non deberán exceder de 30 páxinas, con tipo de fonte Arial, tamaño 12, entreliñado sinxelo e marxes mínimos superior e inferior de 2,5 cm e de 3 cm a dereita e esquerda. As propostas que excedan estas 30 páxinas so se terán en conta ata dita páxina 30.

1. ÍNDICE
2. RESUMO EXECUTIVO: Breve descrición das características principais da solución ofertada.
3. DESCRICIÓN DA SOLUCIÓN TÉCNICA OFERTADA
    - Licencia subministrada (sen citar os datos valorables de forma automática).
    - Descrición da formación ofertada.
    - Descrición dos servizos de consultaría valorables segundo o indicado no apartado “Consultaría e formación” deste prego.
    - Descrición do equipo de traballo, incluíndo formación académica, experiencia e certificacións para cada membro do equipo.
    - Descrición do servizo de mantemento: horario, idioma, formas de contacto, ferramenta de ticketing,...

7 Universidades participantes

As universidades participantes serían as Universidades do SUG a través do Consorcio CIXUG:

- Universidade de A Coruña
- Universidade de Santiago de Compostela
- Universidade de Vigo

8 Duración do contrato. Prazo de execución

Dous anos mais unha posible prórroga, a contar desde a data de formalización do contrato.

9 Actualizacións

Ao longo da duración do contrato e durante o proceso de firma, posterior á adxudicación, so se permitirán actualizacións, por parte do adxudicatario, de modificación dos produtos solicitados nesta que leven melloras, tanto en funcionalidades como en novas librerías que se incorporen ás actuais, sen que elo supoña maior coste para o CIXUG.

10 Responsabilidade da empresa adxudicataria

No que se refire aos termos xerais na prestación de servizos, a empresa adxudicataria debe cumprir os requisitos impostos neste Prego e no Prego de Cláusulas Administrativas do presente concurso, incluíndo os relativos a protección de datos, confidencialidade, ciberseguridade e propiedade intelectual.

No marco do presente servizo, a empresa adxudicataria comprometese a:

- Designar a un interlocutor có CIXUG e coas Universidades do SUG, para labores de coordinación global, así como interlocutores con responsabilidade sobre a prestación de cada un dos servizos descritos.
- Usar os recursos que o CIXUG e as Universidades do SUG poñan a súa disposición cós fins exclusivos que se describen neste documento.
- Realizar un seguimento da prestación do servizo, aportando evidencias en forma de indicadores, cumprimento de niveis de servizo.

11 Incompatibilidades de uso ou técnicos

Será excluída calquera oferta que xere calquera sorte de incompatibilidade ou dificultade técnica e/ou de uso có actual sistema existente en calquera das tres universidades. A solución ofertada será totalmente compatible có existente sen que poida xerar ningunha sorte de incompatibilidade e/ou dificultade técnica ou de uso.

Santiago de Compostela á data da sinatura electrónica.

Firmado digitalmente por LOPEZ DIAZ ANTONIO - 76565571C
Fecha: 2024.07.31 13:19:30 +02'00'

D. Antonio López Díaz
Presidente