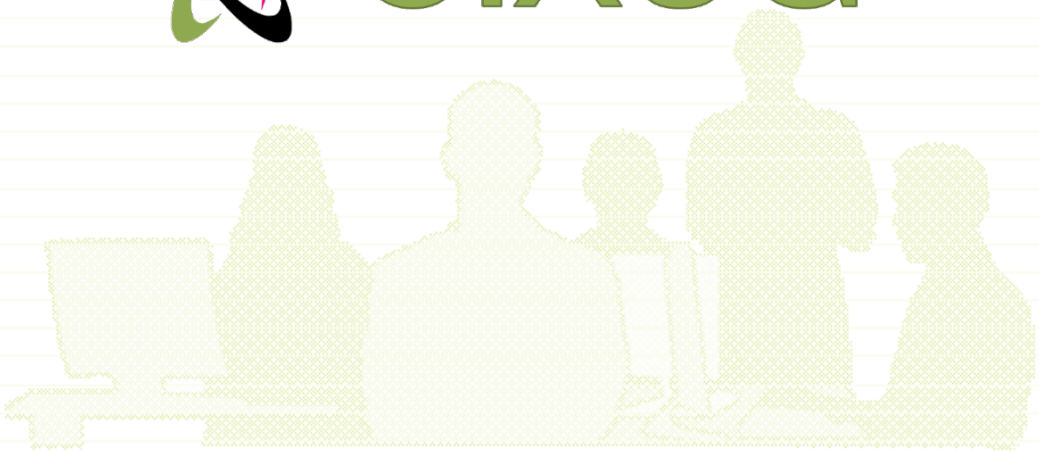

Prego de Prescricións Técnicas

Servizo de análise e xestión de alertas de ciberseguridade no marco do proxecto UniSOC

CPV 72600000-6

Servizos de apoio informático e de consultaría

Xullo, 2024

ÍNDICE

1 Obxecto do Contrato

O obxecto do contrato consiste na adxudicación, para as tres universidades públicas (Universidade de A 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 para a xestión universitaria (en adiante CIXUG) dun servizo de asistencia técnica para o análise e xestión de alertas que produza a plataforma SIEM do proxecto UniSOC.

2 Antecedentes

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

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

Existe, polo 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 e 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 “NEXTGENERATIONEU”.

O proxecto UniSOC plasmouse na adopción dunha plataforma SIEM, composta por un tenant 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 por dita plataforma SIEM.

Durante a reunión do Consello de Goberno do Consorcio CIXUG, formado polas tres universidades públicas do Sistema Universitario Galego (SUG), 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 desde a Universidade de A Coruña, xestionando a contratación final antes do 1 de xaneiro do 2025 data cando se iniciaría o servizo, cós provedores adxudicatarios da licitación, a través do CIXUG.

3 Alcance

3.1 Asistencia técnica para o análise e xestión de alertas de seguridade

As tarefas principais que se levarán a cabo serán as seguintes:

- Revisión, análise e priorización da información e as alertas que produza a plataforma SIEM. Esta información obterase mediante o acceso directo á interface web da plataforma, onde se obterán os datos das alertas e os paneis ou dashboards, a investigación en profundidade das alertas mediante as ferramentas de busca que proporciona a plataforma ou a consulta a fontes externas para enriquecer a análise.
- Execución dos procedementos de escalado de incidencias, para as tres universidades, mediante a apertura de tickets nas súas respectivas aplicacións de xestión de incidencias ou mediante o envío de notificacións por correo electrónico.
- Colaboración na mellora dos casos de uso imprementados na plataforma SIEM.
- Redacción de informes trimestrais do servizo, onde se incluirán estatísticas sobre o número de alertas procesadas agrupadas por criticidade, o tempo de resposta, o número de tickets abertos e un resumo sobre os indicadores de compromiso xerados, así como os novos casos de uso que se configuraran na plataforma.

4 Requisitos do servizo

- **Os licitantes deberán acreditar a súa condición de partner do fabricante Splunk.**
- Destinarase ao servizo un/ha analista de ciberseguridade principal, a tempo completo, para levar a cabo as tarefas detalladas no apartado 3.
- Os licitadores deberán propoñer un/ha xefe/a de proxecto, cunha dedicación estimada ao proxecto de 3 horas ao mes.
- Horario de prestación do servizo: a asistencia técnica prestarase en horario de luns a venres, de 8:00 a 14:00 e de 15:00 a 17:00, excepto festivos nacionais e autonómicos.
- Duración do servizo: A asistencia técnica prestarase por dous anos, prorrogables segundo os termos expostos no PCAP.
- As vacacións do analista principal desfrutaranse preferentemente entre o 1 e o 15 de agosto e entre o 20 de decembro e o 6 de xaneiro. As datas do resto de días que lle correspondan serán acordados có CIXUG.

- En caso de baixas ou permisos, o adxudicatario deberá substituír ao/á analista principal por outro/a que cumpra os mesmos requisitos, no prazo non superior a 10 días hábiles. Estes días deberán ser recuperados mediante horas de prestación de servizo de perfiles similares.
- Os traballos desenvolveranse, de forma xeral, en dependencias da UDC. Preveranse desprazamentos ás dependencias das universidades de Santiago de Compostela ou Vigo para o desenvolvemento de reunións de coordinación ou seguimento do servicio.
- Unha vez o servizo alcance a madurez suficiente o CIXUG poderá autorizar, se o estima oportuno, que se preste o servizo de forma non presencial, na súa totalidade ou parcialmente.
- Valorarase (criterio B.1) a existencia dun equipo técnico que poida dar apoio ao/á analista destinado ao proxecto
- Acordo de nivel de servizo (SLA): os licitantes deberán incluír unha proposta de tempos obxectivo para analizar, investigar e notificar as alertas, distinguindo entre alertas severas e non severas. Tamén incluirán a cantidade de alertas diarias que, en medio, se poderán analizar. Esta proposta valorarase conforme ao criterio B.2

5 Requisitos do equipo de traballo

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

5.1.1 Xefe/a de proxecto

Destinarase ao servizo un/unha 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 o mestrado en áreas de Enxeñaría de Telecomunicación ou Enxeñaría Informática ou título universitario equiparable.
- 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 funcións serán as seguintes:
  - Actuar de interlocutor, por parte do adxudicatario, coa dirección técnica.
  - Coordinar aos membros do 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 si procede, en caso de desviacións significativas.
  - Presentar ao CIXUG informes trimestrais de cumprimento do SLA ofertado.

- Realizar un 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, redactar as actas e remitilas á dirección do proxecto no prazo de 48 horas.

5.1.2 Analista de ciberseguridade

Destinarase aos servizo un **analista de ciberseguridade** que deberá 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 grado superior no ámbito da Informática e Comunicacións ou título universitario equiparable.
- 5 anos de experiencia como analista de seguridade ou en traballos técnicos ou de consultaría en ciberseguridade.
- Experiencia contrastable en proxectos do mesmo ámbito.
- Deberá contar con, polo menos, unha das seguintes certificacións:
  - Splunk Core Certified Power User
  - Splunk Cloud Certified Admin
  - Splunk Enterprise Certified Architect
  - Splunk Certified Cybersecurity Defense Analyst

Calquera cambio que o adxudicatario realice no persoal destinado ao proxecto deberá contar coa autorización expresa da dirección técnica e en ningún caso poderá modificar a acreditación aportada na solvencia técnica. A dita petición de cambio deberá ser notificada 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.

6 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 del 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.

6.1.1 Persoa de contacto

O adxudicatario deberá informar ao CIXUG, trala sinatura do contrato, da persoa

de contacto para a seguridade da información tratada e do servicio prestado, segundo os termos indicados no artigo 13 do Real Decreto 311/2022.

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 o cumprimento dos requisitos de seguridade do servizo ou solución implicados no contrato, realizar as comunicacións relativas á 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.

6.1.2 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 cós equipos de resposta de incidentes e análise forense.

6.1.3 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 “Requisitos do servizo” deste prego.

7 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 dito punto.

- ÍNDICE
- RESUMEN EXECUTIVO: Breve descrición das características principais do servizo ofertado.
- DESCRICIÓN DO SERVIZO OFERTADO
  - Proposta metodolóxica para cumprir os obxectivos indicados neste prego.
  - Perfís destinados ao proxecto: titulación y experiencia.
  - Proposta de SLA.

8 Control da calidade dos traballos

A dirección do proxecto do CIXUG levará a cabo un control da calidade dos traballos realizados e poderá rexeitar aqueles que non cumpran as condicións mínimas, todo elo con independencia das penalizacións ou dunha posible resolución contractual contempladas no PCAP.

As condicións mínimas de calidade serán:

- Que os traballos se realicen conforme á metodoloxía ofertada.
- Que se respecte o SLA ofertado.
- Que se respecte a planificación dos traballos.
- Que se realicen as reunións de seguimento e se entreguen as actas correspondentes no prazo marcado.

9 Universidades participantes

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

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

10 Duración do contrato, Prazo de execución

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

11 Actualizacións

Ao longo da duración do contrato e durante o proceso de sinatura, 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 as actuais, sen que elo supoña maior coste para o CIXUG.

12 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 ás 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.

Santiago de Compostela á data da sinatura electrónica.

Firmado digitalmente por LOPEZ DIAZ ANTONIO - 76565571C
Fecha: 2024.07.31 14:37:17 +02'00'

D. Antonio López Díaz
Presidente