Aprovat per decret d'alcaldia
de data 28 de desembre de 2023

En dono fe,
El Vicesecretari de l'Ajuntament de Lleida
en funcions de Secretari General

PLEC DE CONDICIONS TÈCNIQUES PARTICULARS QUE HA DE REGIR LA CONTRACTACIÓ DEL SERVEI PER LA GARANTIA I ACOMPANYAMENT DE L'EINA "NGSIEM MONICA" MITJANÇANT TRAMITACIÓ ANTICIPADA I PROCEDIMENT NEGOCIAT SENSE PUBLICITAT

1. Antecedents

L'Ajuntament de Lleida, l'any 2022, va contractar un servei de "Gestor d'events de seguretat i informació de seguretat de nova generació" (NGSIEM MONICA) per potenciar la recollida de logs i la seguretat TIC dels seus principals sistemes informàtics, comunicacions i de seguretat perimetral.

Aquesta necessitat es va confirmar pel gran nombre d'atacs cibernètics que s'estan desenvolupant en l'àmbit de les administracions publiques.

Durant l'últim any, aquesta eina no només ha permès la recol·lecció i emmagatzematge centralitzada de logs, servint per evidenciar digitalment qualsevol incident de seguretat que es pogués produir i recolzant-se en un servei avançat de Ciberseguretat, sinó que també s'han configurat i parametritzat totes les sondes.

A més, s'han realitzat les correlacions de registres i s'han configurat les diferents alertes possibles. Aquesta informació reflecteix el treball exhaustiu i meticulós realitzat durant l'any per garantir la seguretat i l'eficiència de l'eina.

Aquest projecte va implicar la configuració de 28 tipus diferents de dades per ingressar al SIEM i el desplegament d'agents de MONICA en aproximadament 1.100 ordinadors d'usuaris i 150 servidors. A més, es van incloure tots els esdeveniments dels serveis i servidors desplegats al AZURE, també s'ha inclòs tota l'activitat d'Office 365 per a uns 1.800 usuaris.

La renovació d'aquest servei és essencial per a l'Ajuntament de Lleida per continuar millorant els seus sistemes i processos d'informació, i per garantir la seguretat TIC dels seus principals sistemes informàtics, comunicacions i de seguretat perimetral.

2. Objecte del contracte

Aquest contracte té per objecte la renovació dels següents serveis i manteniments que l'Ajuntament de Lleida va contractar l'any 2022:

- **Renovació del manteniment MONICA NGSIEM i 28 monitors:** Aquest servei inclou el manteniment correctiu, evolutiu, preventiu, suport telefònic i suport tècnic remot de l'eina NGSIEM MONICA i els 28 tipus de monitors associats.

- **Renovació dels Serveis d'operació en 24x7:** Aquest servei inclou la notificació d'incidències 24x7, la contenció, l'anàlisi i la col·laboració en la recuperació dels sistemes enfront d'un incident, així com la notificació de les incidències al Centre Criptològic Nacional (CCN) mitjançant l'eina LUCIA.

- **Renovació del servei d'alerta primerenca:** Aquest servei permet detectar i respondre ràpidament a qualsevol amenaça o incident de seguretat.

- **Manteniment dels servidors implicats:** Durant la vigència d'aquest contracte, els dos servidors implicats en aquests serveis estaran sota un manteniment constant per garantir el seu correcte funcionament i la seguretat de les dades.

3. Requisits

En aquest punt es plantejant un seguit de requisits mínims que el proveïdor haurà de complir per:

A. <u>El manteniment de MONICA NGSIEM i 28 agents.</u>

- Actualitzacions: S'han d'incloure les actualitzacions del programari i del sistema operatiu del servidor.

- Configuració de fonts: En el supòsit que sigui requerit, es procedirà a l'actualització i configuració de les fonts que estan desplegades en un total de 1.100 equips i 65 servidors, afectant a 1.800 usuaris. Aquesta tasca es realitzarà amb la màxima diligència i eficiència per garantir la continuïtat del servei. Les fonts configurades actualment son:

    - **Sistemes operatius**: Windows Server (versions 2008, 2012, 2016, 2019 i 2022) tant en local com en Azure, així com Linux (Centos, Ubuntu, Debian).

    - **Bases de dades i servidors web**: MySql, Tomcat, Postgres, Apache, Plone, NGINX.

    - **Aplicacions i serveis**: Azure,Office365, Sql Managed Instance, Sophos UTM, Microsoft Defender.

    - **Dispositius de xarxa i seguretat**: Fortigate IDS/IPS, FortiAnalyzer, Finalitzadors VPN Fortigate, Finalitzadors VPN Cisco Meraki, Cisco Router/Switches.

    - **Altres**: MicroClaudia, SAT INET.

- Administració i operació: S'ha d'administrar i operar la configuració de LUCIA per a la gestió automatitzada de l'obertura d'incidències al CCN des de MONICA, així com la configuració de la plataforma NG SIEM MONICA.

- Manteniment i reconfiguració: Si fos necessari, s'ha de mantenir i reconfigurar tots els agents desplegats a l'organització que estan enviant events al NG SIEM MONICA, així com les regles de correlació i alertes que han estat configurades durant la fase d'implementació de l'eina.

- Gestió de panells: S'ha de mantenir, configurar i crear possibles nous panells de gestió i pki existents.

- Servei de recepció i registre d'incidències: Aquest servei ha d'estar disponible les 24 hores del dia, tots els dies de la setmana, per garantir una resposta ràpida i eficient a qualsevol incidència que pugui sorgir.

- Servei d'atenció tècnica telefònica i suport remot: Necessitem suport tècnic telefònic i remot de dilluns a divendres, en horari laboral, excepte dies festius.

- Revisió semestral preventiva de la plataforma: Aquest servei consisteix en analitzar les polítiques, els actius protegits i desprotegits, les amenaces detectades i altres aspectes de la plataforma. El servei ha de notificar-nos tots els errors o situacions anòmales que es detectin.

- Informes de resultats de les revisions preventives: Aquest servei consisteix en l'emissió d'informes que incloguin les recomanacions per millorar la seguretat i el rendiment de la plataforma.

- Reunions de seguiment amb l'Ajuntament de Lleida: Aquest servei consisteix en mantenir reunions periòdiques amb l'Ajuntament de Lleida per avaluar el pla de manteniment i resoldre qualsevol dubte o incidència.

B. <u>A la contractació del servei de SOC a l'Ajuntament</u>

Aquest servei serà suportat pel personal adscrit al CiberSOC de l'adjudicatari. Els serveis de gestió de la seguretat desenvolupats pel CiberSOC inclouran les següents funcions:

- Servei de detecció i resposta (Nivell 1 d'operació en modalitat 24x7):
    - Monitoratge d'esdeveniments de seguretat mitjançant la plataforma MONICA.
    - Correlació i anàlisi d'esdeveniments.
    - Operació i notificació d'alertes.
    - Coordinació de respostes a incògnites.

- Gestió d'esdeveniments i incidents de seguretat.

- Resposta davant incidents, que inclou la notificació dels incidents detectats, conforme als procediments establerts, així com la gestió del cicle complet dels mateixos, coordinant, de forma alineada i sota la supervisió de l'equip tècnic de l'Ajuntament de Lleida, les actuacions necessàries sobre els sistemes/xarxes entre els grups que els administren. A més, comptarem amb el suport necessari per solucionar qualsevol incidència detectada.

- Notificació d'incidències al CCN mitjançant LUCIA.

- Les alertes es definiran de la següent manera:

Nivell	**Escalat CCN**	**Atenció**	**Notificació**
Baix	no	24 hores	48 Hores
Mig	no	8 hores	24 hores
Alt	Sota demanda	4 hores	8 hores
Crític	Sota demanda	30 minuts	4 hores

- Informe d'incident: L'adjudicatari es compromet a lliurar en un termini inferior a 4 hores posterior a un incident crític un informe on inclogui la descripció de l'incident, afectació (objecte o servei afectat, temps total, temps d'inici i fi d'incidència), antecedents, causa arrel de l'incident, solució i accions realitzades.

- Informe mensual d'incidents: L'adjudicatari lliurarà informes incloent el resum mensual d'incidents.

- Durant la durada del contracte, el proveïdor del servei documentarà cada alerta aportant documentació i protocols a seguir per a la seva resolució.

- Reunions periòdiques de seguiment i coordinació del servei: Es proposa una reunió mínima mensual per al comitè de seguiment del servei. Aquestes reunions ens permetran coordinar-nos eficaçment i assegurar que el servei es desenvolupa segons les nostres expectatives.

C. La renovació del servei d'alerta primerenca

El servei que s 'ha de proporcionar consisteix en la notificació anticipada de la publicació de noves vulnerabilitats i actualitzacions de seguretat relatives a les tecnologies monitoritzades a través de l'eina NGSIEM MONICA.

És important destacar que aquesta plataforma està dissenyada per ser no intrusiva i no realitza escanejos continus en la infraestructura de l'Ajuntament de Lleida. Això garanteix que l'operativitat dels sistemes de l'Ajuntament no es veurà afectada mentre es manté una vigilància constant sobre les possibles amenaces de seguretat.

D. El manteniment dels servidors implicats

El manteniment del servidor ha d'incloure la reposició de peces i la mà d'obra per al servidor del fabricant Supermicro model SYS-5029P-WTR, que actualment té una garantia fins a novembre del 2025.

El adjudicatari proporcionarà tots els materials, equipament, eines, transport, mà d'obra i supervisió necessaris per a la reposició de peces i la mà d'obra del servidor.

A més, aquest contracte també cobrirà les targetes addicionals que vam instal·lar, específicament 2 unitats de la targeta de xarxa **PCIE 10Gb per Intel X520-DA2 2P SFP+**[12] i el **transceptor Ethernet de 10 Gb**[12].

Aquest manteniment cobrirà tots els serveis necessaris per a mantenir el servidor en condicions òptimes de funcionament durant la durada del contracte.

Lleida, en la data de la signatura electrònica

Xavi Pinyol Esteban
Responsable Coordinador d'Informàtica i Tecnologia

Carles Giné Sabaté
Cap de Sistemes d'Informació i Ciberseguretat