PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL CONTRACTE MIXTE DE SERVEI I SUBMINISTRAMENT D'IMPLANTACIÓ DE L'EINA CCN-CERT "NGSIEM MONICA", EN EL MARC DEL PLA DE RECUPERACIÓ, TRANSFORMACIÓ I RESILIÈNCIA FINANÇATS PER LA UNIÓ EUROPEA AMB ELS FONS NEXT GENERATION EU.
TRAMITACIÓ ORDINÀRIA MITJANÇANT PROCEDIMENT OBERT SIMPLIFICAT AMB DIVERSOS CRITERIS D'ADJUDICACIÓ.

ANTECEDENTS

L'Ajuntament de Lleida necessita potenciar la recollida de logs i la seguretat TIC dels seus principals sistemes informàtics, comunicacions i de seguretat perimetral. Aquesta necessitat s'ha vist confirmada pel gran nombre d'atacs cibernètics que s'estan desenvolupant en l'àmbit de les administracions publiques.

Per tal de millorar els sistemes i processos d' informació cal implantar un "Gestor d'events de seguretat i informació de seguretat de nova generació" que correlacioni esdeveniments potencialment perillosos per a la seguretat dels sistemes d'informació. Aquesta eina NGSIEM MONICA permet la recol·lecció i emmagatzematge centralitzada de logs, serviria per evidenciar digitalment qualsevol incident de seguretat que es pogués produir i recolzant-se en un servei avançat de Ciberseguretat, que utilitzi aquesta eina, per respondre a qualsevol requeriment d'evidència o resposta a incident de seguretat TIC que es pogués produir a les instal·lacions.

Durant els últims anys s'han anat desenvolupant una sèrie d'eines per part del CCN-CERT per a la recol·lecció de logs, comunicació d'incidents i amenaces de seguretat. Aquestes eines han evolucionat per permetre la seva instal·lació en els diferents organismes de l'AGE que han de reportar incidents d'aquest tipus, amb l'objecte de permetre intercanvi automatitzat d'informació amb el CCN CERT pel que fa a la comunicació i actualització de l'estat d'incidents de seguretat.

El CCN CERT ofereix eines capdavanteres, sense cost de llicenciament i adaptades a les necessitats de les administracions públiques i amb presència en totes les categories d'interès: auditoria, detecció, anàlisi, vigilància i intercanvi.

Per últim, cal destacar que les eines del CCN CERT han estat desenvolupades amb el compliment normatiu en ment, i per tant serveixen d'excepcional ajut per a l'obligat compliment del que estableix el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat.

L'Ajuntament de Lleida ha realitzat una recerca d'eines SIEM al mercat, fent especial la recerca en les eines del CCN-CERT, que compleixin les següents capacitats i funcionalitats:

- Punt únic de control securitzat i emmagatzematge centralitzat de logs.
- Securització dels registres o logs per a generació d'evidències digitals.
- Detectar i resoldre amenaces en temps real mitjançant un motor de correlació.
- Prioritzar i investigar incidents rellevants mitjançant casos d'ús (playbooks) personalitzables.
- Analitzar el comportament de l'usuari (UEBA).
- Tractament i emmagatzematge il·limitat d'esdeveniments diaris (des de 5Gb a més d'1,5 Tb).
- Integració amb la resta d'ecosistema d'eines del Centre Criptològic Nacional, de valor per a la seguretat: SATINET, LUCIA, MICRO-CLAUDIA.
- Producte qualificat i de desenvolupament nacional, que harmonitzi amb les directrius de l'Estratègia Nacional de Seguretat i fomenti l'ús de plataformes europees i espanyoles.

El NGSIEM elegit per implantar a l'Ajuntament de Lleida és la solució NGSIEM MONICA del Centre Criptològic Nacional, posada a disposició de les Administracions Públicas sense cost de llicenciament, ja que compleix totes les característiques enumerades anteriorment i sobretot pel que fa al tractament dels logs.

OBJECTE DEL CONTRACTE

L'objecte del contracte és l'adquisició del servidor, tal i com es detalla en els plecs tècnics que acompanyen aquest informe, i contractació d'un servei per a la implantació d'un sistema de seguretat de la informació i gestió de la seguretat amb l'eina del CCN-CERT " NGSIEM MONICA", de manera que permeti a l'Ajuntament de Lleida la recol·lecció i emmagatzematge centralitzada de logs, gestionar eficaçment les alertes de les ciberamenaces de seguretat (detecció i gestió avançada d'amenaces, gestió eficaç de la resposta i anàlisi forense) que potencialment afectin els sistemes d'informació , i donar resposta ràpida a aquelles que arribin a materialitzar-se.
Aquest servei ha d'englobar un conjunt de mesures encaminades a millorar la seguretat de la informació, permetent disposar de capacitat de detecció, anàlisi i resposta davant incidents de seguretat que puguin succeir a les xarxes i sistemes d'informació.

Els requisits generals d' aquest servei per a la implantació d' un sistema de seguretat de la informació i gestió de seguretat estan detallats en el plec tècnic que acompanya aquest informe.

ABAST DE DESPLEGAMENT I OPERACIÓ

Són objecte d'aquest contracte els treballs necessaris per a la instal·lació i parametrització de l'eina NGSIEM MONICA, així com l'administració i operació posterior de la infraestructura instal·lada. El

personal de l'equip tècnic de l'Ajuntament de Lleida tindrà accés igualment a l'operació de la plataforma.

L'explotació haurà de permetre mantenir un equilibri entre la detecció d'alertes de seguretat i l'esforç precís per solucionar-les i documentar-les.

En general, haurà de ser possible i dur-se a terme:

- Recollir, analitzar i presentar informació de :
  - Servidors físics i virtuals amb sistema operatiu Windows i Linux
  - Servidors virtuals i serveis desplegats al cloud Azure
  - Avisos i logs generats des d'Azure i Office 365
  - Equips de seguretat i de Proxy del fabricant SOPHOS
  - Equips de seguretat del fabricant FORTINET i CISCO
  - Ordinadors i estacions de lloc de treball
  - Sondes SATINET i MICRO-CLAUDIA
  - Utilització dels logs generats del producte NESSUS
  - Integració amb LUCIA

- Facilitats d'identificació d'accessos (logs).
- Detecció de vulnerabilitats i comprovació de compliment de polítiques de seguretat.
- Capacitat d'incloure informació de NDR i EDR.
- Possibilitat d'inclusió del context de l'activitat de la xarxa, el context dels usuaris/actius, registres d'aplicacions i reducció d'incidents en alertes reals.
- Traçabilitat d'informació de la infraestructura objecte de l'abast.
- Detecció, anàlisi, gestió i contenció/remei d'incidents de seguretat.

També haurà de ser possible configurar diferents panells d'informació, casos d'ús personalitzats i models d'informes en formats explotables externament. En cas que es produeixi un incident de seguretat, l'adjudicatari haurà de lliurar un informe relatiu a aquest incident incloent-hi les traces de detecció del mateix i les mesures que s'han de prendre per contenir o mitigar.

En el cicle de vida de la prestació dels serveis contractats distingim dos fases:

- **FASE 1 D'IMPLANTACIÓ – Disseny, preparació i posada a punt del servei amb els nous elements**
  Instal·lació, parametrització i formació de l'eina NGSIEM MONICA.

- **FASE 2 DE GARANTIA I ACOMPANYAMENT – Transició i transformació inicial**
  - 2.1 Prestació dels serveis avançats de Gestió d'Incidents de Seguretat sobre l' eina NG SIEM MONICA.
  - 2.2 Serveis de suport en modalitat 8x5 de NGSIEM NG MONICA.

FASE 1 - SERVEIS D' INSTAL·LACIÓ DE L'EINA NGSIEM MONICA

El Proveïdor posarà en marxa els següents serveis durant aquesta fase:

Instal·lació del servidor dedicat

El proveïdor subministrarà i instal·larà el servidor dimensionat a les necessitats de l'Ajuntament de Lleida per poder garantir la correcta gestió de tots els logs.

L'adjudicatari proveirà la infraestructura de maquinari en format appliance físic i programari necessària per suportar l'eina NGSIEM MONICA. L'equip o equips subministrats han d'estar certificats pel fabricant del NGSIEM MONICA. En tractar-se d'una eina integrada i compacta, els requisits mínims a aportar per a la instal·lació en aquesta fase inicial d'implantació seran:

- Servidor en format rack 19'
- Doble font d'alimentació
- Ram 128gb
- Cpu 24 x 2,4 mhz
- Storage :
    - 2Tb RAID1
    - 32Tb RAID5

Activitats

En aquesta fase del servei s'emmarquen les següents activitats per part de l'adjudicatari :

- Disseny de l'arquitectura de l'eina NGSIEM MONICA a instal·lar definitivament, incloent requisits maquinari en base a logs monitoritzats.
- Definició dels requeriments tècnics sobre els quals s'instal·larà l'eina NGSIEM MONICA.
- Preparació, documentació i desplegament de l'eina NGSIEM MONICA en format físic dins del CPD principal.
- Desplegament de l'eina integrada NGSIEM MONICA
- Integració de les fonts acordades en l'arrencada del projecte en l'eina NGSIEM MONICA i que tindran un abast mínim de **28 fonts** diferents .
- Definició de quadre de comandaments de les fonts d'informació integrades.

- Aplicació d' intel·ligència mitjançant casos d'ús, personalització i desenvolupament de nous casos d'ús.
- En finalitzar la fase d'instal·lació i implantació, s'haurà de proporcionar al personal de l'equip tècnic de l'Ajuntament de Lleida accés a la consola de gestió de l'eina NGSIEM MONICA amb rol d'operació i la formació necessària sobre les eines de treball.

Instal·lació del servei de monitorització

Implantació del servei de monitorització d'esdeveniments de seguretat mitjançant l'eina del Centre Criptològic Nacional NGSIEM MONICA.

A més, al realitzar el desplegament de MONICA, es desplegaran les següents eines:

- Eines de gestió d'incidències i inventariat, monitorització i quadre de comandament del servei: sistema de diferents eines amb tots els elements centralitzats en un mateix quadre de comandament, facilitant el control del servei i la gestió d'aquest.
- Alerta primerenca: permet descobrir de forma ràpida i senzilla les vulnerabilitats que afecten als seus sistemes. A partir de l'inventari d'equipament de l'Ajuntament de Lleida, es notifica i proporciona el remei per la solució de vulnerabilitat.

Configuració en MONICA de les següents fonts de dades:

- Windows Server 2008 on premise
- Windows Server 2012 on premise
- Windows Server 2016 on premise
- Windows Server 2019 on premise
- Windows Server 2022 on premise
- Windows Server 2016 Azure
- Windows Server 2019 Azure
- Linux Centos
- Linux Ubuntu
- Linux Debian
- MySql
- Tomcat
- Postgres
- Apache
- Plone
- NGINX
- Office365
- Sql Managed Instance

- Sophos UTM
- Microsoft Defender
- Fortigate IDS/IPS
- FortiAnalyzer
- Finalitzadors VPN Fortigate
- Finalitzadors VPN Cisco Meraki
- Cisco Router/Switches
- MicroClaudia
- SAT INET
- Equips i Servidors Windows:
- 1100 equips
- 65 servidores
- Usuaris: 1800 usuaris

Instal·lació del servei LUCIA

Les tasques associades a aquest punt seran les d'instal·lació, implantació i administració de l'eina LUCIA.

Per la instal·lació de LUCIA es necessitarà:

- Instal·lar la màquina virtual de LUCIA
- Configuració de xarxa per la màquina
- Configurar un nombre de domini per la màquina, és a dir, la URL del servei LUCIA
- Configurar comptes de correo per la recepció de correus.
- Configurar un servidor SMTP per a l'enviament de correus.

Documentació a lliurar en aquesta fase

La documentació lliurada per l'adjudicatari servirà com a punt de partida per a la fase d'instal·lació i haurà d'incloure:

- Pla detallat de posada en marxa i configuració, incloent estimació de temps per a cadascuna de les tasques. Procés d'instal·lació, que inclogui tots els elements que són necessaris per disposar de l'equipament i les eines totalment operatives .
- Identificació de parts involucrades en el desplegament i dependències entre elles: necessitats d'infraestructura maquinari, connectivitat de xarxa, adreçament IP necessari.
- Pla de configuració el sistema.
- Proposta d'integració amb sistemes externs.
- Proposta de polítiques generals de configuració.
- Proposta de definició d'alertes i incidents.
- Arquitectura del sistema desplegat. Diagrames físics i lògics.

FASE 2 - GARANTIA I ACOMPANYAMENT

L'objectiu d'aquesta fase és afinar el mecanisme de prestació dels nous serveis i de col·laboració entre Ajuntament de Lleida i el proveïdor. Per a la qual cosa, es realitzaran les mesures dels indicadors, s'emetran els informes corresponents amb la periodicitat acordada i s'aplicaran les metodologies, procediments i activitats previstes en el model del servei.

En aquesta fase, el proveïdor dedicarà un Coordinador Tècnic, expert en transició de serveis TIC i certificat en ITIL. Aquesta persona liderarà aquesta fase i serà l'encarregada de, mitjançant els workshops que corresponguin amb les diferents responsables i coordinadors del serveis actuals de l'Ajuntament de Lleida, adquirir el real coneixement del servei actual, analitzar la documentació actual, proposar ajustaments en els models de relació, operació i gestió del servei, realitzar la revisió i fixació de procediments.

Durant aquesta fase es porten a terme les següents tasques:

- Establiment dels Comitès de govern, control i seguiment del servei
- Revisió dels procediments operatius
- Revisió i ajustaments de les definicions i valors dels ANS. S'implantaran els mecanismes per efectuar la seva mesura
- Organització detallada de la documentació i el sistema de gestió del coneixement
- Pla de documentació
- Documentació de l'activitat del servei

En aquesta fase el proveïdor s'encarregarà de l'operació conjunta amb l'Ajuntament de Lleida, gestió i seguiment de les diferents alertes que generi el sistema MOINCA i la seva correlació amb LUCIA.

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

La finalitat d'aquesta fase es "knowledge transfer", durant aquest període l'Ajuntament de Lledia haurà d'adquirir els coneixements necessaris per poder gestionar el SOC.

FASE 2.1 - SERVEI DE GESTIÓ D' INCIDENTS DE SEGURETAT

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

1. 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

2. Gestió d'esdeveniments i incidents de seguretat:

Resposta davant incidents, englobant la notificació dels incidents detectats, conforme als procediments establerts, així com la gestió del cicle complet dels mateixos, coordinant, de forma alineada i baix la supervisió de l'equip tècnic de l'Ajuntament de Lleida, les actuacions necessàries sobre els sistemes/xarxes entre els grups que els administren.

3. Servei de prevenció i Alerta Primerenca:

Aquest servei consisteix en la notificació primerenca de la publicació de noves vulnerabilitats i actualitzacions de seguretat sobre les tecnologies monitoritzades en l'eina NGSIEM MONICA. Aquesta plataforma no ha de ser intrusiva ni realitzar escanejos continus en la infraestructura de L'ajuntament de Lleida.

Documentació a lliurar en aquesta fase

Almenys contemplarà els següents lliuraments:

- Protocols d'actuació davant alertes de seguretat : Del funcionament habitual del sistema de gestió centralitzada de la seguretat s'extrauran informacions conseqüència del monitoratge i de la correlació d'esdeveniments. A partir de l'experiència aportada per l'adjudicatari es definirà una classificació de severitats per a les alertes de seguretat, així com els protocols d'actuació associats per a cadascuna d'elles.

- Les alertes se 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 .

FASE 2.2 - SUPORT EINA NGSIEM MONICA 8X5

El servei de suport de l'eina NGSIEM MONICA inclourà:

- Actualitzacions del programari i sistema operatiu del appliance.
- Subministrament i substitució de qualsevol part del appliance.
- Administració i operació de la configuració de la plataforma NG SIEM MONICA.
- Recepció d' incidències 8x5.

La implantació de l'eina NGSIEM MONICA (FASE 1) i la posada en marxa del servei de gestió d'amenaces de seguretat (FASE 2), englobant els aspectes inicials de reconeixement o posada en context de les persones que l'integren amb l'àmbit tecnològic i organitzatiu de l'Ajuntament de Lleida, la formalització del procés de gestió d'incidents de seguretat, tindran començament com a màxim en cinc (5) dies després de la formalització del contracte, amb una reunió de llançament del servei, i tindrà una duració màxima de quatre (4) setmanes des de l'esmentada formalització del contracte.

FORMACIÓ

L'adjudicatari haurà d'incloure en la seva proposta 1 sessió de capacitació d'almenys **cinc (5) hores**. La formació ha d'incloure :

- Arquitectura del sistema desplegat. Funcionalitats dels seus components.
- Administració bàsica de la plataforma.
- Administració i gestió de casos d' ús.
- Administració i gestió de recol·lecció de dades.
- Gestió d'alerta primerenca.

Les sessions de capacitació seran realitzades a les instal·lacions de l'Ajuntament de Lleida, i si les condicions de Salut Pública no ho aconsellessin, mitjançant videoconferència .

Aquesta formació es prestarà a la finalització de la fase d'instal·lació, com a finalització d'aquesta etapa, abans de començar la fase de Gestió d'Incidents de Seguretat, llevat de modificacions aprovades juntament amb el responsable de l'Ajuntament de Lleida.

FIRMADO

Lleida, a la data de la signatura electrònica

Tècnic Planificació Implementació de Sistemes