ANNEX 10 – DESCRIPCIÓ DE LES ACTUACIONS PREVISTES EN EL MODEL DE CIBERSEGURETAT DE L'AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA (ACC)

El Model Integral de Ciberseguretat de l'Agència de Ciberseguretat de Catalunya (en endavant, el Model), té com a objectiu protegir a les entitats de les amenaces en ciberseguretat dirigides contra el sector de les administracions locals i abordar les actuacions necessàries per a protegir i prevenir dels ciberincidents que puguin impactar contra les entitats.

A tal efecte, el Model preveu l'execució de les següents fases per al seu desplegament:

- **Fase I - Diagnòstic:** identificació del grau actual d'exposició a les principals ciberamenaces que apliquen a l'àmbit de les administracions locals.
- **Fase II** - **Pla de seguretat:** determinació del pla de seguretat de cada entitat per tal de ser més resilient i reduir l'exposició a les amenaces més significatives, amb una orientació a assolir el compliment normatiu en l'Esquema Nacional de Seguretat i, quan correspongui, en altres normatives sectorials o específiques que siguin d'aplicació.
- **Fase III - Integració operativa:** desplegament, a partir de les capacitats de protecció desplegades per les entitats, de les capacitats de prevenció, detecció i resposta, i dels processos i serveis associats a la integració amb l'Agència de Ciberseguretat de Catalunya.
- **Fase IV - Protecció:** activació i operació del serveis de monitorització i resposta 24x7 de l'Agència, i dels serveis i oficines necessàries per a la governança, comunicació, formació i evolució en la ciberseguretat.
- **Fase V - Certificació:** procés de certificació mitjançant les auditories de la conformitat en l'Esquema Nacional de Seguretat.

Es descriuen a continuació les accions corresponents a les **Fases I i II de Diagnòstic i de Pla de Seguretat** respectivament, com a **metodologia de referència a utilitzar pel Lot 2 - Servei d'Auditoria de la Ciberseguretat del present Acord Marc**. L'abast dels serveis que haurà d'oferir el licitador vindran especificats en cada contracte basat.

1. Fase preliminar

S'inclou en aquesta fase aquelles accions prèvies necessàries per a desplegar el Model Integral de Ciberseguretat (en endavant, el Model) de l'Agència.

Correspon a l'adjudicatari l'execució de les següents accions:

1. **Identificació de l'abast del desplegament**. Anàlisi previ de l'entitat amb l'objectiu de concretar l'abast del desplegament i detectar particularitats específiques de l'àmbit que requereixin d'una especial atenció o orientació concreta.

2. **Identificació i revisió de les amenaces** que afecten a l'àmbit objecte del desplegament del model, en base a les alertes existents, informació d'intel·ligència operativa i tendències per a aquest àmbit.

3. **Qüestionari preliminar** amb l'objectiu de disposar d'un context suficient de l'entitat per a poder abordar les següents fases d'implementació del Model. En aquest qüestionari es recollirà la següent informació:

    - Contactes i matrius d'escalat davant d'incidents
    - Adreçaments de xarxa
    - Dominis públics
    - Xarxes socials
    - Arquitectura de xarxa
    - Gestió d'identitats, control d'accés i autoritzacions
    - Elements de seguretat transversal
    - Sistemes d'Informació
    - Lloc de treball
    - Serveis de correu electrònic
    - Directori Actiu

4. **Activació de serveis universals**: mitjançant la informació recollida a través del qüestionari preliminar, s'habilitaran d'una manera àgil determinats serveis i procediments (monitorització digital, alertes primerenques, procediments de gestió d'incidents, etc.) per a atendre i gestionar adequadament les ciberamenaces i els ciberincidents de l'entitat mentre s'implementen les successives fases el Model. Aquests serveis seran proveïts pel SOC Operatiu o de referència de l'entitat.

Correspon a l'ens contractant l'execució de les següents accions:

1. *Informar sobre el context de l'entitat i requeriments específics ja siguin tècnics o legals, que suposin una especial atenció a tenir en compte durant el desplegament del Model, i puguin incidir sobre el catàleg de ciberamenaces als quals està subjecte l'entitat.*
2. *Facilitar la informació sol·licitada en el qüestionari preliminar, perquè l'adjudicatari pugui planificar i executar les següents fases del desplegament.*
3. *Esdevenir l'interlocutor amb els serveis de l'entitat, proveïdors i serveis de tecnologia i ciberseguretat que estiguin operant en l'entitat.*
4. *Incorporar els serveis i procediments establerts en aquesta fase preliminar, per a gestionar les ciberamenaces i ciberincidents que puguin succeir mentre es despleguen les successives fases del Model.*

2. Fase 1 - Diagnòstic

En aquesta fase s'identificarà el grau actual d'exposició a les principals ciberamenaces que apliquin a l'àmbit de desplegament del model.

Correspon a l'adjudicatari l'execució de les següents accions:

1. **Anàlisi de l'arquitectura de seguretat:** consultoria de l'estat de ciberseguretat de l'entitat realitzada mitjançant entrevistes i recollida d'informació, basada en una matriu de controls de ciberseguretat que es

considerin necessaris per a poder reduir el grau d'exposició a les principals ciberamenaces de l'àmbit. L'anàlisi inclourà, entre d'altres, controls relatius a la seguretat de la xarxa, dels sistemes d'informació, dels llocs de treball, la gestió d'identitats i els accessos, la continuïtat dels serveis, etc.

2. **Anàlisi tècnica de febleses i riscos de ciberseguretat:** execució d'un conjunt d'activitats i proves tècniques sobre la infraestructura tecnològica responsabilitat de l'entitat, orientades a identificar el grau d'exposició a les ciberamenaces aplicables, utilitzant metodologies reconegudes i simulant la forma d'actuar dels ciberatacants. Sempre que sigui possible, en aquestes proves s'utilitzaran el mateix tipus de tècniques i eines que fan servir els ciberatacants per accedir i explotar vulnerabilitats de la infraestructura tecnològica d'una entitat. L'abast i duració de les proves dependrà del context d'amenaces i la complexitat tecnològica de l'entitat.

3. **Anàlisi del compliment inicial de l'Esquema Nacional de Seguretat**: d'entrada el Model inclourà l'anàlisi del Perfil de Compliment Específic de Requisits Essencials de Seguretat (PCE RES). En funció del tipus d'entitat i del seu grau de maduresa es podran aplicar altres categories de l'ENS o perfils de compliment. L'avaluació d'aquest estat de compliment inicial es portarà a terme mitjançant qüestionaris, visites presencials i entrevistes per part de l'equip de projecte de l'adjudicatari.

4. **Elaboració i presentació de l'informe de diagnòstic**: entrega a l'entitat d'un primer informe de diagnòstic amb els resultats de les diferents anàlisis tècniques, d'avaluació de controls i de compliment normatiu. L'informe incorpora un annex amb el detall de les metodologies, resultats de les anàlisis tècniques, dels controls de ciberseguretat, de les vulnerabilitats identificades, de les tècniques MITRE provades i del resultat del diagnòstic d'acord al compliment de l'ENS.

Correspon a l'entitat l'execució de les següents accions:

1. *Suport en l'execució de les avaluacions de controls, facilitant la informació i documentació necessària que permeti donar resposta tant als controls tècnics com de compliment normatiu plantejats, aportant el detall necessari per a la seva correcta validació i interpretació en el marc temporal definit per a l'avaluació. A tal efecte caldrà designar els interlocutors, planificar temporalment les entrevistes, assignant el temps i els espais necessaris perquè les sessions d'avaluació es puguin dur a terme amb la qualitat i terminis previstos en aquesta fase.*

2. *Suport en l'execució de proves i anàlisis tècniques, facilitant la informació, mitjans, condicions, accés i usuaris necessaris per portar-les a terme en el marc temporal pactat inicialment.*

3. *Analitzar l'informe de diagnòstic presentat per l'adjudicatari com a lliurable d'aquesta fase, per a conèixer i validar els aspectes de millora detectats i procedir a la mitigació de les febleses més crítiques informades.*

3. Fase 2 - Pla de seguretat

En aquesta fase s'elaborarà i es posarà a disposició de l'entitat el Pla de seguretat que permetrà augmentar la protecció i la resiliència de l'entitat davant les ciberamenaces. El pla està composat pel conjunt de projectes derivats del diagnòstic de seguretat realitzat durant la fase anterior, així com per les accions necessàries per conduir a l'entitat a l'adequació i certificació en el compliment de l'ENS.

Correspon a l'adjudicatari l'execució de les següents accions:

- **Elaboració del Pla de seguretat** que inclourà els següents continguts:
    - Estat de ciberseguretat de l'entitat
    - Grau de compliment de l'ENS d'acord amb el perfil de compliment específic o, en el seu defecte, amb la categoria de l'ENS que s'hagi determinat que apliqui a l'entitat .
    - Detall de les anàlisis tècniques i d'arquitectura de la infraestructura tecnològica.
    - Relació i detall dels projectes, en base a les proves i diagnòstics realitzats durant la fase anterior, identificant com a prioritàries aquelles accions més rellevants i urgents a abordar per reduir les febleses i fer front a les principals amenaces. Els projectes identificaran el seu impacte tant en relació a la protecció enfront les ciberamenaces aplicables a l'entitat, com en relació amb el compliment de l'ENS.
    - S'introduirà una estimació a alt nivell del cost de les iniciatives en base a la tipologia d'entitat, les seves volumetries de sistemes d'informació i persones, i la complexitat i localització dels seus sistemes d'informació, entre d'altres aspectes que es puguin analitzar. Aquesta estimació inicial tindrà com a objectiu donar visibilitat de les necessitats pressupostaries i de les capacitats associades a la implementació del pla que haurà d'executar l'entitat, quedant fora de l'abast del desplegament del Model.

- **Presentació del Pla de seguretat**, amb una explicació complerta i detallada, per tal de garantir la comprensió dels resultats, dels projectes associats i de les implicacions en la seva execució.

Correspon a l'entitat l'execució de les següents accions:

- *Implementació, seguiment i governança del Pla de seguretat impulsant totes aquelles accions generals i específiques per a assolir la seva consecució (dotació pressupostària, dotació de capacitats i recursos, etc.).*
- *Revisió i avaluació del Pla de seguretat, amb l'objectiu d'entendre la viabilitat, impacte, i priorització de les mesures previstes davant dels òrgans de decisió de l'entitat.*
- *Implementació de les mesures proposades al pla, coordinant-se amb els actors pertinents, i executant un seguiment de la seva execució fins a la seva finalització.*

- *Execució de projectes o plans d'acció específics per a la implementació de mesures d'elevada complexitat*
- *Actualització i documentació del Pla de seguretat per a la seva traçabilitat, auditoria i millora continua.*
- *Presentació i seguiment del Pla de seguretat a la Direcció i/o al Comitè de Seguretat de l'entitat, per a disposar del suport necessari per a l'execució de les actuacions previstes i consecució dels objectius del pla.*