Signat electrònicament per Eva Guijarro
Provencio . Data: 21/02/2025 10:59:17 CET

Localret

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea NextGenerationEU

PLEC DE PRESCRIPCIONS TÈCNIQUES QUE REGULEN L'ACORD MARC DEL SUBMINISTRAMENT DE SOLUCIONS I SERVEIS GESTIONATS DE SEGURETAT TIC

ÍNDEX

1 Objecte de l'acord marc 5
2 Divisió en lots 5
2.1 Seguretat de la informació 7
3 Modalitat de contractació de les solucions i serveis gestionats de seguretat TIC 9
4 Lot 1: Solucions de seguretat TIC incloses al CPSTIC 9
4.1 Abast i requeriments 10
4.2 Assistència tècnica per al desplegament dels serveis de seguretat TIC 11
4.3 Suport tècnic 12
4.4 Organització del servei 13
4.5 Capacitació dels administradors 14
4.6 Agrupació de productes oferts 14
4.6.1 Grup 1: Bàsic 15
4.6.2 Grup 2: Mitjà 15
4.6.3 Grup 3: Avançat 16
4.6.4 Altres grups 16
4.6.5 Resum 18
5 Lot 2: Serveis d'auditoria tècnica de ciberseguretat 19
5.1 Descripció del servei 19
5.2 Pla d'execució: 20
5.3 Abast 22
5.4 Documentació a entregar 23
5.5 Organització del servei 25
6 Lot 3: Serveis de gestió de la ciberseguretat 26
6.1 Funcions a realitzar 27
6.1.1 Descobriment, anàlisis i interlocució en matèria de ciberseguretat 27
6.1.2 Gestió operativa de la ciberseguretat 28
6.1.3 Anàlisi i gestió d'incidents de ciberseguretat 30
6.2 Organització del servei 31
6.3 Gestió i execució del Pla de Seguretat 33
6.3.1 Gestió del Pla de Seguretat 34
6.3.2 Adequació normativa prevista en el Pla de Seguretat 34

6.3.3 Actuacions i projectes específics en el marc del Pla de Seguretat 35
6.4 Acords de Nivell de Servei (SLA)..... 37
7 Lot 4: Serveis de Centre d'Operacions de Seguretat (SOC) 38
7.1 Implantació del SOC..... 40
7.2 Funcions i capacitats del SOC 43
7.2.1 Disponibilitat del servei 43
7.2.2 Capacitats de prevenció 43
7.2.3 Capacitats de detecció..... 45
7.2.4 Capacitats de protecció 46
7.2.5 Capacitats de resposta a incidents..... 47
7.3 Plataforma de correlació d'esdeveniments de seguretat de la informació (SIEM) 48
7.4 Organització del servei 49
7.5 Acords de Nivell de Servei (SLA)..... 51
8 Lot 5: Serveis d'adequació a l'Esquema Nacional de Seguretat (ENS) 53
8.1 Pla d'adequació 53
8.1.1 Política de Seguretat i normativa interna 54
8.1.2 Identificació dels serveis presents i categorització dels sistemes de l'entitat contractant, amb la valoració de la informació tractada. 54
8.1.3 Anàlisi de riscos..... 55
8.1.4 Elaboració de la Declaració d'Aplicabilitat. 55
8.1.5 Pla de millora..... 56
8.2 Tasques relacionades amb la protecció de dades. 56
8.3 Governança de la seguretat. 57
8.4 Gestió del canvi i formació. 57
8.5 Acompanyament a l'obtenció de la conformitat. 58
8.6 Lliurables 58
8.7 Equip de treball 59
9 Lot 6: Serveis de formació i conscienciació en ciberseguretat ad-hoc 60
9.1 Nivells de formació 62
9.1.1 Nivell bàsic de formació 62
9.1.2 Nivell avançat de formació..... 64

9.2 Itineraris de perfils especialitzats de ciberseguretat 64
9.3 Altres seccions formatives complementàries 65
10 Lot 7: Serveis de CSIRT (Computer Security Incident Response Team) 66
10.1 Característiques del servei 66
10.2 Compliment Normatiu i Confidencialitat. 68
10.3 Modalitat de prestació del servei. 69
10.4 Organització del servei 71
11 Devolució del servei 73
12 Terminis i model de relació 73
13 Facturació 74
14 Despeses d'Impuls 75

ANNEX 10 – Descripció de les actuacions previstes en el model de ciberseguretat de l'Agència de Ciberseguretat de Catalunya.
ANNEX 11. CCN-STIC-105 CPSTIC – Catàleg de productes i serveis de seguretat de les tecnologies de la Informació i la comunicació.
ANNEX 12. CCN-STIC-140 – Taxonomia de referència per a productes i serveis de seguretat TIC.

1 OBJECTE DE L'ACORD MARC

L'acord marc té per objecte el subministrament, instal·lació i suport de productes i la prestació de serveis destinats a la seguretat TIC dels ens, organismes i entitats del sector públic local català.

L'objecte de l'acord marc es defineix segons les funcionalitats concretes que es pretenen satisfer.

L'acord marc pretén construir una oferta de productes i serveis amb capacitat suficient per donar resposta a les necessitats actuals i futures de la ciberseguretat dels ens locals, recolzant el desplegament de qualsevol pla de seguretat de la informació que requereixi tecnologia aprovada pel Centre Criptogràfic Nacional (CCN).

La finalitat de l'acord marc és que les entitats beneficiàries puguin assolir els objectius següents:

- Adquirir productes i serveis destinats a la millora de la seguretat de les seves infraestructures TIC.
- Implementar mecanismes de ciberseguretat que incorporin les funcionalitats necessàries per a obtenir un millor escenari de protecció davant de possibles atacs i incidents de seguretat TIC.
- Polititzar, monitoritzar i supervisar les aplicacions, les connexions i, si s'escau, les dades, que emprin la xarxa de l'ens local.
- Desenvolupar capacitat de resposta davant de ciberincidents en termes de recuperació de la informació i del bon funcionament dels sistemes informàtic en cas d'infecció.
- Adoptar les mesures necessàries per adaptar el funcionament de les estructures TIC a les necessitats inherents pròpies d'aquest acord marc.

Els beneficiaris potencials de l'acord marc són totes les entitats que, durant la vigència de l'acord marc, formin el Consorci Localret (https://www.localret.cat/qui-som/ens-adherits/), així com els seus ens dependents i aquells ens en què les entitats que formen el Consorci tenen una participació majoritària, prèvia la seva adhesió específica a l'acord marc.

2 DIVISIÓ EN LOTS

Atenent als diferents tipus de solucions i serveis de seguretat TIC que han de ser proveïts en el marc del present plec, els productes objecte de l'acord marc s'han agrupat en els lots següents:

- Lot 1: Solucions de seguretat TIC incloses al Catàleg de Productes i Serveis de Seguretat de las Tecnologies de la Informació i la Comunicació del CCN (CPSTIC) .

  Subministrament de productes, llicències o subscripcions de programari, instal·lacions i manteniments inclosos al CPSTIC relacionades amb la seguretat TIC. Addicionalment, han d'oferir serveis d'implantació.

Els següents lots conformen serveis gestionats de ciberseguretat que han de contemplar tots els elements necessaris per a la gestió, monitorització, administració i execució de totes les tasques necessàries a fi de cobrir la seva execució.

A continuació es detallen cadascun dels serveis que formen part de l'acord marc. Cada servei gestionat conforma un lot en si mateix. Aquests serveis gestionats contemplaran tots els elements necessaris per a la gestió, monitoratge i administració de totes les tasques necessàries a fi de cobrir la seva execució. Els requeriments i les seves descripcions seran d'obligat compliment per part de l'adjudicatari, sense menyscapte d'ampliar les funcionalitats i oferir millors prestacions que les descrites. De la mateixa manera, una empresa adjudicatària es podrà presentar a qualsevol dels serveis presents en aquests lots.

- Lot 2: Serveis d'auditoria tècnica de ciberseguretat.
  Engloba els requeriments per a la realització d'una auditoria tècnica a fi d'establir el grau de maduresa de l'entitat contractant en termes de seguretat TIC.

- Lot 3: Serveis de gestió de la ciberseguretat.
  Gestió dels serveis de ciberseguretat de manera integral pel licitador a fi de proveir de capacitats de ciberseguretat a l'ens públic contractant.

- Lot 4: Serveis de Centre d'Operacions de Seguretat (SOC).
  Servei SOC a proporcionar pel licitador així com de la seva operativa tant a nivell tècnic com organitzatiu.

- Lot 5: Servei d'adequació a l'Esquema Nacional de Seguretat (ENS).
  El servei inclou els treballs necessaris per a l'adequació de tots els sistemes d'informació de l'ens contractant a l'Esquema Nacional de Seguretat.

- Lot 6: Serveis de formació i conscienciació en ciberseguretat ad hoc.
  Servei encarregat de la generació d'activitats i continguts dissenyats per a educar i conscienciar usuaris i organitzacions sobre les millors pràctiques, amenaces i riscos relacionats amb la seguretat informàtica i així minimitzar el risc d'incidents.

- Lot 7: Serveis de CSIRT (Computer Security Incident Response Team).
  Servei de gestió i resposta a incidents de ciberseguretat, així com a l'anàlisi forense digital per a investigar i comprendre aquests incidents. Aquest servei té

com a objectiu minimitzar l'impacte dels incidents, restaurar les operacions normals i proporcionar informació crítica per a millorar les defenses de seguretat de les entitats contractants.

Les empreses licitadores hauran d'adjuntar a les seves propostes el detall de la plataforma o plataformes que ofereixin (especificacions tècniques, funcionalitats...), i dels diferents nivells de subscripció, si és el cas, per oferir els serveis dels lots 2 a 7.

Les empreses vetllaran perquè l'entitat obtingui el servei requerit amb el mínim cost, proposant els productes que millor s'adeqüin a les necessitats de l'ens, i hauran d'assessorar proactivament els clients per tal d'optimitzar l'adquisició de productes.

Els serveis de ciberseguretat descrits (lots 2 a 7) contemplen tots els elements i serveis necessaris pera la seva execució. Seran els contractes basats els que definiran l'abast del servei que requereixi cada ajuntament.

L'empresa adjudicatària assumirà el servei contractat de seguretat TIC durant la vigència dels contractes basats, responsabilitzant-se de la bona execució del servei contractat. Haurà de disposar dels recursos tècnics, humans i materials adequats per a la prestació del servei contractat garantint els temps de resposta i resolució d'incidències detallats a l'apartat d'Acords de Nivell de Servei (SLA).

2.1 Seguretat de la informació

Les empreses adjudicatàries de l'acord marc seran responsables de la seguretat dels sistemes d'informació utilitzats per a l'execució del contracte. Les empreses hauran de comptar, almenys, amb una política de seguretat aprovada i, en tot moment, actualitzada, que es posarà a disposició de l'òrgan de contractació, si aquest ho sol·licita. Considerant l'impacte que tindria un incident que afectés la seguretat de la informació o dels serveis, amb perjudici per a la disponibilitat, autenticitat, integritat, confidencialitat o traçabilitat, els sistemes d'informació en què es sustenten els serveis prestats per les empreses adjudicatàries de contractes basats, hauran de complir, com a mínim, els requisits establertes en el Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), per a la categoria que estableix aquest mateix plec per cada lot. No obstant, els òrgans de contractació dels contractes basats podran elevar la categoria de seguretat –a mitjana o alta segons el cas– dels sistemes d'informació exigibles per a l'execució del contracte.

El compliment d'aquests requisits s'acreditarà mitjançant la declaració de conformitat amb l'ENS, quan es tracti de sistemes de categoria bàsica, o la certificació de conformitat amb l'ENS, quan es tracti de sistemes de categoria mitja o alta, o la justificació de tenir implementades les mesures de tipus organitzatiu, operacional y de protecció previstes

en el Reial decret 311/2022, de 3 de maig, pel qual es regula l'ENS, que li permetin obtenir aquestes certificacions. Entre els sistemes d'informació coberts per la declaració o certificació de conformitat s'hauran de trobar, necessàriament, aquells que resultin necessaris per realitzar l'objecte del contracte.

En cas que l'empresa adjudicatària de l'acord marc no disposi de la declaració o certificació de conformitat, exigida en el moment de l'adjudicació, disposarà d'un termini de quatre mesos per, almenys, implementar les mesures de tipus organitzatiu, operacional i de protecció previstos en el Reial decret 311/2022, que li permetin obtenir la declaració i les certificacions de conformitat corresponents a la categoria exigida. Transcorregut aquest termini, l'empresa comunicarà a l'òrgan de contractació les mesures adoptades per garantir la seguretat dels sistemes d'informació utilitzats per a l'execució dels contractes.

Aquest termini de quatre mesos s'aplica a tots els lots amb serveis que requereixen certificació de l'ENS, per tal de garantir que totes les empreses adjudicatàries compleixin amb els requeriments de seguretat establerts.

Igualment, l'empresa adjudicatària d'un contracte basat en aquest acord marc haurà de complir, almenys, les següents obligacions:

- Persona de contacte. Comunicar al responsable del contracte el nom i les dades de contacte de la persona designada com a responsable de la seguretat de la informació.
- Cadena de subministrament. En cas que s'autoritzi la subcontractació d'actuacions que impliquin l'ús de sistemes d'informació, l'empresa adjudicatària traslladarà a les empreses subcontractistes qualsevol requisit de seguretat en relació amb l'execució del contracte, així com monitoritzarà el correcte compliment dels mateixos. En qualsevol cas, l'adjudicatària assumirà qualsevol responsabilitat en què incorrin els seus subcontractistes.
- Notificació i gestió d'incidents. L'empresa adjudicatària del contracte basat notificarà a l'entitat contractant qualsevol incident de seguretat que pugui redundar directament o indirectament en la seguretat dels sistemes d'informació. A més, disposarà de procediments de gestió d'incidents de seguretat, així com còpies de seguretat per garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals.
- Resolució de vulnerabilitats. L'empresa adjudicatària del contracte basat haurà de reparar tota vulnerabilitat que afecti als sistemes d'informació utilitzats durant l'execució del contracte.
- L'òrgan de contractació dels contractes basats en l'acord marc podrà verificar, en qualsevol moment, el compliment de les mesures de seguretat requerides.

3 MODALITAT DE CONTRACTACIÓ DE LES SOLUCIONS I SERVEIS GESTIONATS DE SEGURETAT TIC

Les solucions i serveis de seguretat TIC del present acord marc podran ser contractats en les diferents modalitats que ofereixi el fabricant o licitador, com per exemple:

- Adquisició de llicències perpètues i manteniments (amb pagament mensual o anual).
- Adquisició de maquinari amb servei d'instal·lació i registre d'alta de l'entitat contractant envers el fabricant.
- Mode de subscripció o pagament per ús (amb pagament mensual, anual o plurianual).
- Servei gestionat (amb pagament mensual o anual).

En els contractes basats es podrà establir un model de tarifació segons els paràmetres i característiques que el licitador consideri per respondre a les necessitats de l'ens contractant.

En cas que la solució contempli el pagament per ús, els paràmetres de pagament i els preus corresponents seran definits a la proposta del licitador del contracte basat.

En el cas dels serveis gestionats i monitoritzats es definirà un preu per servei segons els paràmetres establerts en el present plec i els requeriments concrets que defineixi el contracte basat.

4 LOT 1: SOLUCIONS DE SEGURETAT TIC INCLOSES AL CPSTIC

Les empreses adjudicatàries del lot 1 hauran de proveir les llicències o subscripcions de programari de seguretat TIC presents a les guies publicades al CPSTIC, oferint els serveis següents:

- Tasques de subministrament, instal·lació, configuració i suport tècnic als usuaris/operadors.
- Traspàs de llicències.
- Gestions amb el fabricant per tal de donar d'alta els equips i llicències així com per activar els serveis de suport i manteniment oferts pels fabricants.
- Subministrament de maquetes d'instal·lació i configuració necessàries durant el període de vigència del contracte.
- Suport tècnic als usuaris operadors durant el període de vigència del contracte.
- Es realitzarà un seguiment de la utilització dels diferents productes, ja sigui amb una eina de monitorització o en base als logs d'accés del servidor de llicències.

La solució presentada podrà estar formada per productes de diferents fabricants i es podrà proveir més d'una solució.

Es permetrà la creació de paquets (*bundles*) de productes sempre que el seu preu final sigui menor a la suma del preu d'adquisició per separat. En aquest cas el temps de durada de la subscripció del programari i servei de suport o manteniment serà pel conjunt i no pels elements per separat.

Les empreses han d'adjuntar a les seves ofertes el detall de la seva solució (fabricants dels diferents components, especificacions tècniques, funcionalitats...) i dels diferents nivells de subscripció.

Les empreses licitadores han d'adjuntar, igualment, el detall de productes i manteniment, i dels diferents nivells de subscripció.

Les empreses hauran d'oferir el servei de monitorització de les llicències contractades establint mètodes de seguiment de les renovacions de les mateixes, l'expiració de garanties i el suport dels productes contractats, sempre vetllant per l'ús correcte de les mateixes.

Addicionalment, les empreses poden oferir serveis d'assistència tècnica per al desplegament del servei de seguretat TIC, que podran ser facturats segons l'oferta presentada com a serveis d'implantació.

Per a la instal·lació i configuració dels productes, els licitadors hauran de seguir les instruccions, sempre que el producte disposi, de la guia de configuració aprovada i publicada a les guies del CCN dedicada a tal efecte.

Per tal de facilitar la tria de la solució, s'oferirà l'accés a una demostració de la solució proposada, un enllaç a una web explicativa o qualsevol altre mitjà que ho possibiliti.

4.1 Abast i requeriments

El primer lot comprèn el subministrament de productes, instal·lacions i manteniments qualificats pel CCN, que compleixen els requisits de seguretat exigits per l'ENS i que, per tant, es troben inclosos dins del CPSTIC, donades les garanties de seguretat contrastades de què disposen. S'entén que aquests productes i serveis poden ser físics o virtuals i de diferents fabricants.
S'adjunta el document com a annex núm. 11.

De la mateixa manera, també seran acceptats aquells productes que estiguin en procés de qualificació i que ja apareixen com a productes qualificats o aprovats pel CPSTIC.

Mitjançant l'adquisició d'aquests productes i tecnologies, les entitats beneficiàries de l'acord marc hauran de poder cobrir les necessitats relacionades amb la ciberseguretat als seus sistemes.

En la mateixa línia, els productes que responen a l'anterior taxonomia de referència es poden consultar i descarregar en format PDF i *xlsx* al "Catàleg de productes CPSTIC".

La classificació i descripció de les famílies de productes objecte d'aquest lot es troba a la "Guia de Seguretat de les TIC CCN-STIC 140", que té l'objectiu de descriure la taxonomia de referència per a productes i serveis de seguretat TIC.
S'adjunta el document com a annex 12.

Donada l'evolució tecnològica constant dels productes i tecnologies inclosos al llistat CPSTIC es preveu la seva actualització periòdica i conseqüentment l'actualització de productes i tecnologies del present lot. La incorporació de productes i fabricants nous al llistat CPSTIC permetrà que les empreses puguin oferir-los dintre del present acord marc.

Cada element es dimensionarà d'acord amb les necessitats de l'entitat que s'estabiliran al contracte basat. El programari, maquinari i servei de manteniment ofert pel licitador ha d'estar inclòs al CPSTIC.

El licitador facilitarà un llistat dels productes inclosos al CPSTIC que ofereix a la seva oferta segons el model de presentació d'oferta de l'annex 9. Aquests productes podran ser de diferents fabricants, igual que els del llistat CPSTIC.

Existeixen productes catalogats que incorporen components que no estan inclosos al llistat del CPSTIC. Un exemple d'aquesta casuística pot ser un tallafocs (qualificat) que inclogui WAF (*Web Application Firewall*) o *anti-spam* (no qualificats).

D'acord amb això, el contracte basat podrà incloure productes no inclosos en el CPSTIC (o no qualificat pel CPSTIC), que siguin complementaris o auxiliars, i sempre que el seu cost no superi el 20 per cent del valor total del contracte.

4.2 Assistència tècnica per al desplegament dels serveis de seguretat TIC

L'empresa adjudicatària d'un contracte basat en l'acord marc vetllarà per garantir les funcionalitats requerides i optimitzar el cost de la subscripció. També assegurarà que les entitats adquireixin una solució de seguretat que garanteixi el bon funcionament i les funcionalitats necessàries, proposant la subscripció més adequada a les seves necessitats i oferint un assessorament suficient i adequat.

Els projectes d'implantació seran requerits als contractes basats amb la definició i l'abast dels serveis demandats, i l'empresa licitadora haurà de presentar una oferta ajustada a aquests requeriments particulars.

En qualsevol cas, es seguiran les instruccions de la guia de configuració aprovada i publicada a les guies del CCN, sempre que el producte en disposi.

4.3 Suport tècnic

Suport bàsic

El suport bàsic estarà inclòs en el preu del contracte.

Els licitadors d'un contracte basat hauran d'oferir un suport bàsic que inclourà els aspectes següents:

a) Creació (i baixa) del client.
b) Registre i alta de la subscripció a nom de l'entitat.
c) Donar accés i suport a totes les actualitzacions i novetats sobre les aplicacions contractades que tinguin lloc durant el termini de vigència del contracte,
d) Suport en el procés de facturació.

En els casos que es requereixin tasques d'administració avançada, es podrà sol·licitar els serveis de recolzament a la implantació de noves funcionalitats que desenvolupi el fabricant o que per modificació de l'arquitectura dels ens siguin necessaris realitzar sobre l'entorn actual del fabricant. En línies generals es consideraran sota aquest epígraf totes aquelles tasques que no siguin considerades una incidència i suposi una modificació de la configuració i/o parametrització dels serveis.

Les empreses adjudicatàries de l'acord marc hauran de tenir un centre de suport on les entitats que adjudiquin un contracte basat puguin comunicar incidències, sol·licitar informació i resoldre dubtes. Les empreses adjudicatàries proporcionaran suport telefònic, almenys, entre les 9.00 h. i les 14.00 h. els dies laborables de dilluns a divendres, a més d'una adreça de correu electrònic on poder adreçar les consultes. El temps de resposta màxim des de la petició de l'entitat fins a la recepció de la resposta serà de 8 hores laborables. El temps de resposta podrà ser millorat per l'oferta del licitador.

Opcionalment, el licitador podrà oferir un espai on es registrin les comunicacions de les incidències o peticions de suport. Aquesta eina haurà de conservar l'històric de les incidències reportades per l'entitat i els temps de resposta per cadascuna d'elles amb el seu estat (oberta, resolta, tancada....).

Els contractes basats podran tenir com a requeriment el subministrament d'aquesta

eina de *ticketing*.

Suport del fabricant

El suport de fabricant estarà inclòs en el preu del contracte.

Les empreses adjudicatàries hauran de garantir el servei de suport del fabricant:

a) Resolució d'incidències en cas de fallida del servei, *bug* del producte i actualització per resolució de vulnerabilitats.
b) Accés al servei d'assistència del propi fabricant, per telèfon o mitjançant adreça de correu electrònic.
c) Accés a la base de coneixements del fabricant, si en disposa, per consulta i resolució de dubtes relacionats amb el producte.

Aquestes incidències seran gestionades pel contractista a petició de l'entitat, sense cap cost.

4.4 Organització del servei

Estructura organitzativa

Per part de l'entitat, s'establirà la figura del responsable del servei, que serà l'encarregat de dirigir i coordinar la relació amb l'adjudicatari.

Per part de l'adjudicatari, de la mateixa manera, s'establirà un responsable del servei, encarregat de coordinar i garantir el compliment dels requisits del servei, assignant els mitjans adequats per a la correcta prestació del servei.

Equip de treball

Els integrants de l'equip de treball es concretaran en cada contracte basat en funció del servei requerit.

El personal inclòs a la proposta de l'empresa licitadora del contracte basat haurà de reunir els requisits mínims establerts com a requeriment del contracte basat per a la categoria professional concreta i funció a desenvolupar i, a més, que els mateixos perfils coincideixin amb els presentats a la proposta efectuada per l'adjudicatari en la seva oferta del present acord marc .

Si durant l'execució del contracte sorgeix la necessitat de substitució d'algun membre de l'equip de treball, l'adjudicatària haurà de motivar la sol·licitud amb almenys dues setmanes d'antelació, i ser autoritzada, si s'escau, per l'entitat. Donat l'elevat impacte

que suposa la rotació de perfils, l'adjudicatari vetllarà perquè aquesta rotació sigui baixa una vegada aprovat l'equip de treball de cada contracte basat.

En general, si es produís la substitució d'un membre de l'equip de treball, hi haurà un procés de traspàs del coneixement o solapament entre el recurs sortint i els recursos que assumeixen les tasques exercides pel recurs sortint, de 10 dies hàbils mínim per assegurar el traspàs de coneixement intern.

Les empreses hauran de disposar, com a mínim, d'un equip de treball format pels següents perfils:

- Responsable del servei, les funcions del qual és garantir servei i gestionar la relació amb l'entitat.
- Un expert tècnic en seguretat. Les principals funcions seran les corresponents a la prestació del serveis d'assistència tècnica per al desplegament dels serveis de seguretat TIC i el suport tècnic del present lot.

Tots els perfils hauran de tenir com a mínim **3 anys** d'experiència en projectes similars.

4.5 Capacitació dels administradors

Les entitats podran sol·licitar la formació o plans de capacitació pels usuaris administradors de la plataforma de seguretat, lligats als serveis contractats. Aquests serveis hauran d'estar inclosos en el preu del producte o servei i no haurà de suposar un càrrec econòmic addicional per l'entitat.

L'ens podrà sol·licitar un pla de capacitació per a que el seu administrador pugui gestionar els dispositius, els punts de connexió i la seguretat de forma centralitzada des de la consola d'administració, segons els productes adquirits.

Aquesta formació tindrà una durada mínima de dues hores.

En cas de fer la formació telemàtica el licitador haurà de proveir els mitjans telemàtic per fer la formació i haurà d'incloure la presència del formador.

En cas de fer la formació presencial aquesta serà a la ubicació designada per l'entitat local.

4.6 Agrupació de productes oferts

Els productes que poden ser oferts per les empreses licitadores es classifiquen en tres grups diferenciats, segons el nivell d'exigència i complexitat de les demandes dels ens contractants.

Si les empreses licitadores són directament els fabricants d'una solució que pertany a una família específica, no estaran obligades a ajustar-se a les agrupacions descrites més endavant. Així, podran oferir la seva solució sense necessitat d'haver de proveir la resta de famílies del grup.

4.6.1 Grup 1: Bàsic

Les empreses adjudicatàries han de proporcionar productes de totes les categories i famílies que es descriuen a continuació:

Categoria	Família
Monitoratge de la seguretat	IDS, IPS y AntiDDoS
Protecció de les Comunicacions	Tallafocs
Protecció de les Comunicacions	Xarxes privades virtuals: IPSec
Protecció de les Comunicacions	Xarxes privades virtuals: SSL
Seguretat a l'explotació	Antivirus / EPP (Endpoint Protection Platform)
Seguretat a l'explotació	EDR (Endpoint Detection and Response)

Les empreses adjudicatàries que vulguin ser homologades en aquest grup han de poder oferir la totalitat dels productes presents a la taula anterior. A més, han de complir amb els següents requeriments:

- Nivell d'assistència: han d'oferir un servei d'assistència tècnica 8x5 (laborables de dilluns a divendres).
- Servei de reposició: opcionalment es pot oferir el servei de reposició temporal (en forma de préstec) en cas d'avaria d'un dispositiu.

4.6.2 Grup 2: Mitjà

Les empreses adjudicatàries han de proporcionar productes de totes les categories i famílies del Grup 1 (bàsic) i, com a mínim, 6 de les 10 famílies que es descriuen a continuació:

Categoria	Família
Conformitat i governança de la seguretat	Formació i conscienciació
Control d'accés	Control d'accés a la xarxa (NAC)
Control d'accés	Servidors d'autenticació
Protecció d'equips i serveis	Protecció de correu electrònic
Protecció de la informació i els suports de la informació	Hardware Security Module (HSM)
Protecció de les comunicacions	Dispositius de xarxa sense fils

Protecció de les comunicacions	Rúter
Protecció de les comunicacions	Proxy
Protecció de les comunicacions	Switch
Seguridad en l'explotació	Eines de gestió de xarxa

Les empreses adjudicatàries que vulguin ser homologades en aquesta categoria han de poder oferir, com a mínim, 6 de les 10 famílies de productes presents a la taula anterior a més de tots els presents al **Grup 1 (bàsic)**. Addicionalment, han de complir amb els següents requeriments:

- Nivell d'assistència: han d'oferir un servei d'assistència tècnica 8x7.
- Servei de reposició: ha d'oferir el servei de reposició temporal (en forma de préstec) en cas d'avaria d'un dispositiu.

4.6.3 Grup 3: Avançat

Les empreses adjudicatàries han de proporcionar productes de la següent família a més d'heretar les obligacions dels grups 1 i 2.

Categoria	Família
Seguretat en l'explotació	Sistemes de gestió d'incidències i informació de seguretat (SIEM)

Les empreses que vulguin ser homologades en aquesta categoria han de poder oferir la família d'aquesta categoria, com a mínim, 6 de les 10 famílies de productes presents a la taula de la categoria del Grup 2 (mitjà), a més de totes les present al Grup 1 (bàsic). Addicionalment, han de complir amb els següents requeriments:

- Nivell d'assistència: han d'oferir un servei d'assistència tècnica 24x7.
- Servei de reposició: ha d'oferir el servei de reposició temporal (en forma de préstec) en cas d'avaria d'un dispositiu.

4.6.4 Altres grups

Addicionalment, existeixen una sèrie de categories presents al CPSTIC que contenen famílies de productes acceptats i que poden complementar les solucions basades en els grups anteriorment exposats en aquest document.

En aquest sentit, les empreses licitadores podran complementar les solucions ofertes amb els elements presents en la llista que es mostra a continuació:

Categoria	Família
Comunicacions tàctiques segures	Solucions per a protecció de les comunicacions tàctiques
Comunicacions tàctiques segures	Plataformes i dispositius tàctics confiables
Conformitat i governança de la seguretat	Notificació i gestió de ciberincidents
Conformitat i governança de la seguretat	Governança i planificació de la seguretat
Conformitat i governança de la seguretat	Normativa de seguretat i conformitat
Conformitat i governança de la seguretat	Anàlisis i gestió de riscos
Control d'accés	Gestió d'identitats (IM)
Control d'accés	Gestió d'accés privilegiat (PAM)
Eines per al desenvolupament de productes de seguretat	-
Monitorització de la seguretat	Captura, monitorització i anàlisis de tràfic
Monitorització de la seguretat	Eines d'entorn controlat de proves (*sandbox*)
Altres eines	Altres eines
Protecció d'equips i serveis	Sistemas operatius
Protecció d'equips i serveis	Eines de videoidentificació
Protecció d'equips i serveis	Dispositius mòbils
Protecció d'equips i serveis	Sistemas de gestió de bases de dades (DBMS)
Protecció d'equips i serveis	Commutadores KVM
Protecció d'equips i serveis	Hiperconvergència
Protecció d'equips i serveis	Balancejadores de carga
Protecció de la informació i els suports de la informació	Emmagatzematge xifrat de dades
Protecció de la informació i els suports de la informació	Eines per a la signatura electrònica
Protecció de la informació i els suports de la informació	Xifrat i compartició segura de dades
Protecció de la informació i els suports de la informació	Eines d'esborrat segur
Protecció de la informació i els suports de la informació	Sistemas para prevenció de fugues de dades
Protecció de les comunicacions	Eines de missatgeria instantània (IM)

Protecció de les comunicacions	Eines de veu IP
Protecció de les comunicacions	passarel·les segures d'intercanvi de dades
Protecció de les comunicacions	Díodes de dades
Protecció de les comunicacions	Eines de videoconferència
Protecció de les comunicacions	Xifradores IP
Protecció de les comunicacions	Xarxes definides per software (SDN)
Protecció de les comunicacions	Xarxes privades virtuals: altres
Protecció de les comunicacions	Eines per a comunicacions mòbils segures
Seguridad en l'explotació	Dispositius per a la gestió de claus criptogràfiques
Seguridad en l'explotació	Eines de filtrat de navegació
Seguridad OT	Seguridad OT
TEMPEST	Servidor
TEMPEST	Armaris apantallats
TEMPEST	Perifèrics
TEMPEST	Monitors
TEMPEST	Impressores
TEMPEST	CPU

4.6.5 Resum

Grups	Obligacions
Grup 1: Bàsic Productes i serveis Grup Bàsic	• Oferir totes les famílies del Grup 1. • Nivell d'assistència: han d'oferir un servei d'assistència tècnica 8x5 (laborables de dilluns a divendres). • Servei de reposició: opcionalment es pot oferir el servei de reposició temporal (en forma de préstec) en cas d'avaria d'un dispositiu.

Grup 2: Mitjà (Grup 1: Bàsic + Grup 2: Mitjà)	• Oferir com a mínim 6 famílies del Grup 2 i totes les del Grup 1. • Nivell d'assistència: han d'oferir un servei d'assistència tècnica 8x7. • Servei de reposició: ha d'oferir el servei de reposició temporal (en forma de préstec) en cas d'avaria d'un dispositiu.
Grup 3: Avançat (Grup 1: Bàsic + Grup 2: Mitjà + Grup 3: Avançat)	• Oferir la família del Grup 3, 6 del Grup 2 i totes les del Grup 1. • Nivell d'assistència: han d'oferir un servei d'assistència tècnica 24x7 • Servei de reposició: ha d'oferir el servei de reposició temporal (en forma de préstec) en cas d'avaria d'un dispositiu.

5 LOT 2: SERVEIS D'AUDITORIA TÈCNICA DE CIBERSEGURETAT

El servei d'auditoria tècnica interna i supervisió en ciberseguretat haurà d'analitzar l'estat de l'entitat: detectar i informar de totes les possibles vulnerabilitats i riscos, incloent un anàlisi dels usuaris existents amb accés als sistemes i l'actualització del programari utilitzat, que puguin comprometre la integritat, confidencialitat i disponibilitat de la informació i dels sistemes informàtics de l'ens contractant que la contenen mitjançant la simulació d'intrusions reals i controlades. També inclourà la revisió del pla de seguretat que tingui l'entitat i l'exposició de les dades de caràcter personal.

La prestació del servei es durà a terme a les instal·lacions de l'empresa adjudicatària, sense menyscapte de desenvolupar-ho a les instal·lacions de l'ens contractant si les necessitats del servei així ho determinen.

Les empreses hauran de garantir que els seus sistemes d'informació que sustenten els serveis prestats en ser adjudicatàries de contractes basats del present lot apliquen les mesures de seguretat establertes al Reial decret 311/2022, de 3 de maig, pel qual es regula l'ENS. L'adjudicatari haurà de disposar d'un certificat d'acompliment de l'ENS de nivell MIG, i aportar el certificat corresponent i que figurar en la web del CNI (https://gobernanza.ccn-cert.cni.es/certificados).

5.1 Descripció del servei

El servei s'executarà d'acord amb la metodologia prevista en el Model de ciberseguretat de l'Agència de Ciberseguretat de Catalunya, per a la fase de diagnòstic i la revisió del pla de seguretat. Aquesta metodologia, disponible a l'annex 10, determina l'enfoc,

criteris i lliurables a tenir en compte durant l'execució dels test de penetració, l'avaluació de controls en el procés de consultoria i l'elaboració d'informes de diagnòstic.

En termes generals, el servei d'auditoria tècnica interna de ciberseguretat estarà vertebrat en l'anàlisi dels procediments relacionats amb la governança dels circuits de ciberseguretat, de l'equipament disponible a l'entitat en quant a programari i maquinari i en la simulació de diferents ciberatacs, amb una durada a establir amb l'ens contractant, en els quals els atacants tractaran d'accedir a actius o sistemes d'informació de l'ens públic, aprofitant febleses tant en l'àmbit tecnològic com en el físic i en el de l'enginyeria social.

En quant a l'anàlisi de la governança dels circuits relacionats amb ciberseguretat i l'anàlisi de l'equipament de l'entitat, l'auditoria haurà de complir, com a mínim, els següents punts:

- Identificació i inventariat dels actius presents als sistemes de l'ens.
- Identificació dels usuaris amb accés als actius i a les dades.
- Revisió del Pla de Seguretat (conjuntament amb les normatives, procediments principals i avaluació de riscos) per tal d'assegurar el seu estricte compliment posterior i actualització.
- Identificació de les mesures de seguretat tècniques, legals i organitzatives necessàries per a la protecció dels sistemes d'informació en tots els entorns existents a l'entitat.

En quant a la simulació d'atacs per a determinar el grau de robustesa dels sistemes de l'entitat contractant, el proveïdor dissenyarà i posarà en marxa un conjunt d'escenaris realistes que mostrin mètodes de ciberatacs dirigits als àmbits corresponents a l'ens contractant.

5.2 Pla d'execució:

El licitador, d'acord amb la metodologia indicada, haurà de seguir la següent estructura per a dur a terme el servei:

- Planificació:
  - Anàlisi de l'organització.
  - Aplicació de processos d'identificació i model d'amenaces.
  - Determinar l'abast final i els objectius.
  - Determinar els temps d'inici i final de la fase d'execució.
  - Establir els requeriments inicials per a les proves i interlocutors.
- Execució de l'auditoria:
  - Executar els supòsits per a aconseguir els objectius establerts prèviament.

    - Registrar les observacions de les àrees de revisió i la evidència dels objectius aconseguits.
- Presentació d'informes:
    - Presentació i informe: documentar les observacions en un informe de diagnòstic final juntament amb un resum-informe executiu.
    - Presentació dels resultats als responsables de les àrees revisades a fi de discutir les febleses trobades.
    - Documentar els problemes identificats per a cada observació, amb una valoració de la seva gravetat i les recomanacions adients.
- Remediació:
    - Proposar accions per a la remediació de les febleses indentificades basat en recomanacions, que haurà de ser consensuat amb els responsables de l'ens contractant.
    - Prioritzar les accions a prendre en funció de la seva criticitat.
- Suport post-auditoria:
    - Un cop acceptat l'informe d'auditoria, es prendran mesures per corregir les vulnerabilitats segons la seva rellevància. Després que l'entitat contractant executi les accions de remediació, caldrà confirmar que les vulnerabilitats s' han solucionat amb èxit.
    - L'adjudicatari verificarà que les correccions hagin estat realitzades i redactarà un Informe de Confirmació de Remediació. Si la solució implementada per l'entitat afectada no compleix amb els requisits per remeiar la vulnerabilitat especificada, l'adjudicatari proporcionarà noves recomanacions per a la correcta resolució de les vulnerabilitats detectades.
    - El suport post-auditoria haurà de comptar com a mínim amb reunions quinzenals amb l'entitat oferint les solucions per a la resolució dels problemes detectats. El suport tindrà una durada mínima de 2 mesos. Es valorarà l'ampliació d'aquest suport.
- Esborrat d'informació
    - En finalitzar el servei, l'adjudicatari haurà d'eliminar dels seus sistemes o arxius tots els codis font, certificats o altra informació que pertanyi a l'entitat contractant i que hagi rebut per a l'execució del seu treball.

Les empreses hauran de proposar, per a cada contracte basat, una planificació inicial dels serveis a proveir: termini, hores, pla de revisió, programes de proves a realitzar i el procediment de supervisió i seguiment del servei.

L'entitat contractant estarà al dia sobre les proves realitzades en cada moment, a més de facilitar l'establiment de la cooperació per a la facilitació d'informació necessària per a dur a terme les proves. Les àrees concretes subjectes a l'auditoria tècnica en ciberseguretat, en termes de personal, no han de rebre informació sobre les proves realitzades i els seus resultats fins a l'acabament d'aquestes, a fi d'elevar la complexitat i l'efectivitat dels intents d'intrusió.

S'establirà un pla de reunions de seguiment on l'adjudicatari haurà de presentar un informe de seguiment amb els treballs realitzats i la planificació prevista.

5.3 Abast

Per a dur a terme les tasques d'auditoria tècnica es farà un treball de camp en les instal·lacions municipals que constitueixin el centre de treball que es basarà en els següents punts:

- Visitar i supervisar el sistema d'informació de l'entitat.
- Assignar responsables d'auditoria interna de protecció de dades i ciberseguretat.
- Mantenir entrevistes amb els responsables o bé amb les persones designades de les entitats.
- Recollir evidències per part de la comissió o responsable de seguretat.
- Revisió de la documentació de la gestió de la seguretat de la informació.
- Definició de registres i indicadors, i realització pràctica dels mateixos.

En quant a la determinació de la robustesa dels sistemes davant atacs, els vectors d'atac hauran d'emprar els àmbits digital, físic i social per detectar vulnerabilitats tan tècniques com humanes. Les tècniques d'intrusió específiques hauran de ser proposades per l'adjudicatari i ser emprades segons els escenaris i vectors possibles per a cada cas. Es podran contemplar els següents:

- Intrusió física:
  - Anàlisis perimetral de seguretat.
  - Identificació d'accessos alternatius.
  - Anàlisis de xarxes sense fils.
  - Control remot de CCTV (si s'escau).
- Intrusió digital:
  - Anàlisis de sistemes perimetrals.
  - Anàlisis de servidors públics i actius presents a la xarxa.
  - Intrusió i control de dominis interns.
  - Obtenció d'informació crítica.
  - Infraestructura Wi-Fi.
  - Simulació d'atacs avançats:
    Incorporació de tècniques d'atac moderns, com ransomware simulation, per avaluar la capacitat de resposta de l'entitat davant d'amenaces complexes i avançades.
    Simular atacs de moviment lateral i persistència dins de la xarxa per detectar febleses en la capacitat de contenció i resposta.
  - Anàlisi de l'entorn Cloud:
    Si l'entitat utilitza serveis al núvol (AWS, Azure, Microsoft 365, Google Cloud, etc.), es realitzarà una revisió detallada de les configuracions,

exposició i mesures de seguretat per garantir que no existeixen vulnerabilitats derivades d'aquest entorn.
    - Auditoria de les polítiques de recuperació i continuïtat:
      Revisió dels plans de recuperació davant desastres (DRP) i continuïtat del negoci (BCP) per assegurar que poden mitigar adequadament els efectes d'un ciberatac o desastre.
    - Anàlisi de l'eficàcia de les alertes i monitoratge:
      Es durà a terme, en cas que l'entitat en tingui, una avaluació dels sistemes de monitoratge i resposta a incidents (SIEM/SOAR) per verificar que aquests detecten i responen amb eficiència davant d'incidents crítics de seguretat.
    - Indicadors d'exposició a Internet:
      Anàlisi detallada de l'exposició pública dels sistemes i actius de l'entitat, incloent open ports, configuracions DNS, i possibles filtracions d'informació a repositoris públics (com GitHub o altres plataformes).

- Enginyeria social:
    - Desplegament de dispositius esquer (*Media dropping*).
    - Enviament de malware controlat a un conjunt d'equips reduït.
    - *Phising, Vishing,...*
    - Suplantació d'identitats (*spoofing*).

En tot cas, les proves executades no han de suposar una interrupció o degradació de la operativa de l'ens contractant, ni es realitzaran fora de l'horari marcat per l'entitat amb objecte de no comprometre la operativa i tenir capacitat de recuperar el funcionament dels serveis si resulta necessari. Tanmateix, aquestes proves han de permetre revertir qualsevol modificació i recuperar l'estat original dels sistemes o les dades.

De la mateixa manera, l'empresa adjudicatària ha d'informar a l'ens contractant de les proves que siguin susceptibles d'afectar els sistemes o les dades a fi d'aprovar la seva execució.

5.4 Documentació a entregar

L'empresa adjudicatària haurà de deixar constància dels treballs realitzats en els següents informes, que seran presentats a les reunions amb l'adjudicatari:

- Informe tècnic:
    - Adequació de les mesures i controls existents.
    - Descripció de les proves realitzades.
    - Abast de les proves.
    - Mesures de protecció identificades.
    - Detall de la intrusió.
    - Llistat de troballes, vulnerabilitats, debilitats o riscos obtinguts.
    - Mètode per a reproduir les vulnerabilitats detectades.

Per a la puntuació i classificació de les vulnerabilitats obtingudes, s'utilitzarà el sistema de puntuació i mètriques Sistema de Puntuació de Vulnerabilitats Comunes o *Common Vulnerability Scoring System* (CVSS, per les sigles en anglès) CVSS 3.1. Tanmateix cadascuna d'aquestes vulnerabilitats disposarà d'una fitxa amb una descripció completa, el seu risc associat, els sistemes afectats i un seguit de recomanacions per a la seva solució.

Complementàriament al sistema de puntuació i mètriques CVSS per cada vulnerabilitat obtinguda es reforçarà amb l'anàlisi de factors addicionals per a una gestió més efectiva:

- Impacte organitzatiu: Es valorarà com les vulnerabilitats poden afectar els processos crítics i la continuïtat operativa, identificant ajustos necessaris per minimitzar els riscos associats.
- Esforç de remediació: Cada vulnerabilitat es categoritzarà en baixa, mitjana o alta segons la complexitat de la solució requerida, detallant breument les accions necessàries per abordar-la.
- Impacte econòmic i de recursos: Es calcularà el cost material, el temps necessari i els recursos implicats per implementar les solucions, prioritzant les accions en funció del risc i l'anàlisi cost-benefici.

Si es troben vulnerabilitats crítiques o d'alt risc de fuga d'informació durant les auditories, s'emetrà una alerta al responsable del servei auditat. Aquesta alerta inclourà un informe amb la descripció de la vulnerabilitat, el tipus d'impacte i una solució o mesura temporal per mitigar-la si no hi ha una solució disponible.

- Informe final:
  - Descripció del treball realitzat.
  - Conclusions i recomanacions amb les dades, fets i observacions sobre les que es basen.
  - Revisió del Pla de Seguretat.
  - Identificació de les accions i projectes a realitzar que permetin reduir les febleses i riscos identificats a l'ens contractant.
  - Classificació d'actius segons l'ENS. L'informe inclourà una revisió de la classificació dels actius de l'entitat, seguint els principis de confidencialitat, integritat i disponibilitat de l'ENS, per tal de garantir que cada actiu té el nivell de protecció adequat.
- Formació:
  - Addicionalment es valorarà que l'adjudicatari ofereixi un pla de conscienciació i formació adaptat a l'entitat i el resultat obtingut de l'auditoria tècnica.

Tots els informes i les dades que en aquests puguin aparèixer, que hagin estat generats com a conseqüència de la prestació del servei constitueixen informació confidencial i es mantindran sota custòdia de l'ens contractant.

L'empresa adjudicatària es comprometrà a guardar absoluta confidencialitat sobre totes les dades i coneixements que es derivin de l'execució del servei d'auditoria interna de ciberseguretat i les dades manegades.

Tots els documents generats seran confidencials i no podran ser total ni parcialment reproduïts en cap mitjà, o lliurats a terceres persones sense l'expressa autorització de l'ens contractant per escrit.

5.5 Organització del servei

Estructura organitzativa

Per part de l'entitat, s'establirà la figura del Responsable del Servei, que serà l'encarregat de dirigir i coordinar la relació amb l'adjudicatari.

Per part de l'adjudicatari, de la mateixa manera, s'establirà un Responsable del Servei, encarregat de coordinar i garantir el compliment dels requisits del servei, assignant els mitjans adequats per a la correcta prestació del servei.

Equip de treball

Els integrants de l'equip de treball es concretaran en cada contracte basat en funció del servei requerit.

El personal inclòs a la proposta del licitador del contracte basat haurà de reunir els requisits mínims establerts com a requeriment del contracte basat per a la categoria professional concreta i funció a desenvolupar i, a més, que els mateixos perfils coincideixin amb els presentats a la proposta efectuada per l'adjudicatari en la seva oferta del present acord marc .

Si durant l'execució del contracte sorgeix la necessitat de substitució d'algun membre de l'equip de treball, l'adjudicatari haurà de motivar la sol·licitud amb almenys dues setmanes d'antelació, i ser autoritzada, si s'escau, per l'entitat. Donat l'elevat impacte que suposa la rotació de perfils, l'adjudicatari vetllarà perquè aquesta rotació sigui baixa una vegada aprovat l'equip de treball de cada contracte basat.

En general, si es produís la substitució d'un membre de l'equip de treball, hi haurà un procés de traspàs del coneixement o solapament entre el recurs sortint i els recursos que assumeixen les tasques exercides pel recurs sortint, de 10 dies hàbils mínim per assegurar el traspàs de coneixement intern.

Les empreses hauran de disposar, com a mínim, d'un equip de treball format pels següents perfils:

- Responsable del servei, les funcions del qual és garantir servei i gestionar la relació amb l'entitat.
- Un expert tècnics en Seguretat. Les principals funcions seran les corresponents a la prestació del serveis.

Tots els perfils hauran de tenir com a mínim **3 anys** d'experiència en projectes similars.

6 LOT 3: SERVEIS DE GESTIÓ DE LA CIBERSEGURETAT

El servei de gestió de la ciberseguretat englobarà totes les actuacions relacionades amb la ciberseguretat i, per tant, contemplarà tots els elements i serveis necessaris per a la implantació, administració i manteniment de la ciberseguretat de l'entitat.

Un cop implementat l'ecosistema que regula la ciberseguretat de l'ens local, el proveïdor serà el responsable de gestionar tots els treballs de configuració, manteniment, monitoratge, prevenció d'incidents i d'actuació davant atacs en el caire de la ciberseguretat, segons la política establerta per l'entitat.

De la mateixa manera, l'empresa adjudicatària assumirà els treballs necessaris per a la recuperació del bon funcionament de tots els sistemes informàtics així com el programari i les dades afectades per un incident de seguretat amb la finalitat de recuperar el normal funcionament de l'entitat en el menor temps possible.

El proveïdor escollit assumirà el servei encarregat de la ciberseguretat durant la vigència dels contractes basats, responsabilitzant-se de la gestió de les incidències relacionades amb el sistema. Haurà de disposar dels recursos tècnics, humans i materials adequats per a la prestació del servei contractat garantint els temps de resposta i resolució d'incidències detallats a l'apartat corresponent als acords de nivell de servei.

En el cas que l'ens contractant requereixi incorporar noves solucions o programari, aquest programari i/o maquinari haurà d'estar inclòs al catàleg CPSTIC, tal i com s'estableix al lot 1 d'aquest mateix plec.

En el supòsit de que l'entitat contractant ja disposi d'un programari en funcionament, l'empresa adjudicatària del servei haurà de poder acreditar que posseeix experiència amb aquest programari i un equip tècnic humà amb els coneixements necessaris per a operar amb la plataforma establerta.

En qualsevol cas, l'empresa adjudicatària del servei d'operació de la ciberseguretat haurà de poder acreditar que opera amb un programari reconegut i homologat al catàleg CPSTIC i que està capacitada a tal efecte.

L'empresa adjudicatària haurà de garantir que els seus sistemes d'informació que sustenten els serveis prestats en ser adjudicatàries de contractes basats del present lot apliquen les mesures de seguretat establertes al Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS). L'adjudicatari haurà de disposar d'un certificat d'acompliment de l'Esquema Nacional de Seguretat de nivell MIG, i aportar el certificat corresponent i que figurar en la web del CNI (https://gobernanza.ccn-cert.cni.es/certificados).

6.1 Funcions a realitzar

Els serveis oferts estaran inclosos en els següents punts que es detallen a continuació i que les entitats podran sol·licitar totalment o parcialment en els contractes basats:

6.1.1 Descobriment, anàlisis i interlocució en matèria de ciberseguretat

S'inclouen en aquest apartat tots els serveis orientats a realitzar un descobriment i diagnòstic inicial dels actius, serveis i nivell de compliment de l'entitat que permetin planificar i executar auditories i avaluacions tècniques de seguretat, de controls normatius i de compliment legal:

- Configuració, monitorització i millora/ampliació dels actius relacionats amb la seguretat d'operacions.
- Descobriment, identificació, catalogació i manteniment de l'inventari dels actius, dispositius, comunicacions, serveis i sistemes d'informació de l'entitat, per obtenir una visió completa i detallada dels recursos, serveis i infraestructures TIC i de seguretat. Aquesta informació haurà de permetre facilitar les auditories tècniques i avaluacions en ciberseguretat, planificar estratègies de seguretat més eficients, respondre de manera més efectiva a incidents de seguretat, i afavorir el compliment dels requisits de compliment i auditoria. La catalogació seguirà les directrius i classificacions establertes a l'Esquema Nacional de Seguretat (ENS)
- Execució o suport en l'execució de proves i anàlisis tècniques de seguretat portades a terme per l'Agència de Ciberseguretat de Catalunya, personal intern o altres actors (SOC operatiu que es defineix al lot 4).
- Execució o suport en l'execució de revisions i avaluacions de controls tècnics i de compliment normatiu portats a terme per l'Agència de Ciberseguretat de Catalunya, personal intern o extern de l'entitat.

- Interlocució tècnica en matèria de ciberseguretat amb els proveïdors, entitats públiques o privades que estiguin executant o proveint serveis de ciberseguretat i procediments d'auditoria.
- Treballs necessaris per a la realització d'un diagnòstic preliminar del nivell d'adequació dels sistemes d'informació a l'Esquema Nacional de Seguretat, que permeti identificar el correcte compliment dels aspectes tant generals com específics de l'ENS tals com, el nivell de categorització dels sistemes d'informació i declaració d'aplicabilitat, el nivell de compliment de les mesures del marc organitzatiu, operacional i de protecció, i la disponibilitat i qualitat de tota la documentació associada al seu compliment.
- Treballs necessaris per a la realització d'un diagnòstic preliminar del nivell de compliment de l'entitat en matèria de protecció de dades d'acord amb allò establert per la normativa vigent.
- Capacitat per descriure els requeriments i característiques tècniques de les eines i serveis en ciberseguretat que l'ens local requereixi adquirir mitjançant els procediments de contractació i licitació que es determinin.
- Actualització i seguiment del pla d'adequació i monitorització de la implantació de les mesures definides al pla.

6.1.2 Gestió operativa de la ciberseguretat

En aquest apartat es descriuen el conjunt d'actuacions i serveis destinats a oferir el suport necessari perquè les eines i serveis de protecció de l'ens local estiguin integrats en el SOC corresponent, bé sigui el SOC Operatiu de l'entitat o el de l'Agència de Ciberseguretat que es referencia al Lot 4:

- El servei per part de l'empresa adjudicatària s'haurà d'encarregar de la gestió de les operacions de seguretat diàries, en la mesura d'aglutinar en un mateix punt tant les alertes emeses -en cas d'existir- pel servei de monitorització de la seguretat descrit més endavant en aquest document (SOC) com aquelles provinents de les sondes SAT-INET, organismes CERT o un altre tipus de sondes que estiguin presents a l'entitat.
- Monitoritzar en temps real tots els dispositius que l'ens contractant defineixi com a crítics.
- Mantenir degudament actualitzats a les darreres versions els programaris i el firmware del maquinari vinculats al perímetre de seguretat de l'entitat.
- El servei de ciberseguretat contractat haurà de garantir que el sistema de còpies de seguretat funcioni de manera òptima, assegurant que totes les còpies es realitzin correctament i que incloguin tots els elements crítics configurats de manera adequada. A més, s'hauran de dur a terme proves periòdiques de restauració, que permetin verificar la integritat i fiabilitat de les còpies, garantint així la capacitat de recuperació de les dades en cas d'incident.

- Instal·lació, configuració, manteniment i millora/ampliació de les eines, programaris i serveis de ciberseguretat vinculats al perímetre de seguretat de l'entitat necessaris per protegir la informació i els seus sistemes i equips informàtics:
  - En el cas que l'ens contractant no disposi del programari necessari o desitgi operar amb el programari de l'empresa adjudicatària, aquesta haurà d'implantar el programari i/o maquinari pertinent.
  - En el supòsit de que l'entitat contractant ja disposi d'un programari en funcionament, aquest haurà de ser integrat per l'empresa adjudicatària del servei i el seu equip tècnic humà seva haurà de portar a terme l'operació i manteniment.
- Assumir els treballs necessaris per a la integració i monitorització, en el SOC corresponent de les alertes generades per les eines, programaris i serveis de ciberseguretat descrits anteriorment.
- Notificar les amenaces i incidents identificats, al SOC corresponent, i als interlocutors que formin part del procés d'escalat i presa de decisions, per a la seva avaluació i tractament.
- Amb les indicacions i recolzament del SOC corresponent, realitzar les tasques necessàries per:
  - Detectar amenaces i riscos tals com la identificació de comportaments anòmals, dispositius i usuaris compromesos, i descobriment de potencials escletxes de ciberseguretat, entre d'altres.
  - Classificar i prioritzar les alertes de seguretat que es puguin detectar en l'àmbit.
  - Realitzar les tasques necessàries per preservar els logs de l'entitat segons les polítiques acordades i la normativa vigent.
- Assumir la gestió de les incidències relacionades amb els programaris, serveis i equipaments de ciberseguretat desplegats a l'entitat, disposant dels recursos tècnics, humans i materials adequats per atendre les incidències relacionades amb aquests, tot garantint els temps de resposta i resolució d'incidències detallats a l'apartat d'Acords de Nivell de Servei (SLA).
- Recollida d'evidències en cas d'incident de seguretat.
- Adoptar mesures de contenció per als incidents de seguretat, o donar indicacions precises perquè aquestes siguin implementades pel personal de l'àrea TIC de l'entitat, segons els protocols establerts, així com verificar-ne l'eficàcia.
- Estudi d'impacte d'incidents, actius afectats i nivell de compromís dels serveis.
- Proposició del pla de mitigació i remediació o adopció del pla proposat pel SOC Operatiu o de referència de l'entitat. Coordinació amb l'entitat sobre l'execució dels plans de mitigació i remediació iniciats fins a la finalització.

6.1.3 Anàlisi i gestió d'incidents de ciberseguretat

En aquest apartat es descriuen el conjunt d'actuacions i serveis destinats a habilitar les capacitats de resposta en incidents de seguretat de l'ens local, amb el suport i supervisió del SOC corresponent:

- Assumir, seguint les estratègies de resposta del SOC corresponent, i sota la seva direcció i supervisió, els treballs necessaris derivats de la materialització d'un incident de seguretat, amb l'objectiu d'assolir el restabliment i el bon funcionament de tots els sistemes informàtics i de les dades, per tal de recuperar la normal activitat de l'entitat en el menor temps possible.
- Desenvolupar polítiques i procediments de resposta i recuperació davant esdeveniments de destrucció d'informació o interrupció del funcionament del sistema informàtic de l'ens contractant.
- Capacitat per a la recollida i preservació segura d'evidències relatives a l'incident de seguretat, sota la direcció i supervisió del SOC corresponent, garantint en tot moment el manteniment de la cadena de custòdia per assegurar la seva validesa i integritat en possibles processos d'investigació o legals.
- Coordinar amb l'entitat i els actors que corresponguin, l'execució dels plans de mitigació i remediació acordats fins a la finalització de l'incident de seguretat, sota la direcció i supervisió del SOC corresponent.
- En l'execució d'aquests treballs i en cas d'incidents greus de ciberseguretat, l'adjudicatari haurà d'oferir una disponibilitat i capacitat de treball en format 24x7 fins que el SOC corresponent ho determini en el marc de l'estratègia de resposta. A tal efecte haurà de poder participar en els diferents comitès i sales de crisi que es convoquin durant l'episodi.
- Suport en l'avaluació de l'impacte, i en la classificació i priorització dels incidents de seguretat.
- Establir i mantenir procediments per investigar i documentar els incidents de seguretat.
- Investigació d'esdeveniments de seguretat per a notificar les amenaces i incidents identificats, al SOC corresponent, i als interlocutors que formin part del procés d'escalat i presa de decisions, per a la seva avaluació i tractament.
- Registrar i preservar la informació relativa als esdeveniments associats als incidents i dur a terme l'anàlisi forense de l'incident de seguretat.
- Realització d'anàlisi forense per determinar les causes i les responsabilitats de l'incident, amb el suport del SOC corresponent
- Realització d'avaluacions i revisions un cop superat l'incident, per analitzar i desenvolupar un pla d'acció que permeti corregir les deficiències identificades durant l'incident de ciberseguretat.
- Suport tècnic a les accions comunicatives que pugui requerir l'entitat, en el marc del govern i la comunicació d'un incident de ciberseguretat.

En la mesura del possible la detecció i resposta d'incidències han d'estar automatitzades per reduir el temps de resposta davant les amenaces.

El registre, el control i el seguiment de l'activitat es durà a terme, si en disposa, utilitzant l'eina interna de gestió (*ticketing*) de l'adjudicatari, així com les eines de notificació de ciberincidents que s'estableixi per part de les autoritats nacionals (del CCN-CERT o de l'Agència de Ciberseguretat de Catalunya).

L'entitat determinarà els canals de comunicació amb el proveïdor que serà a tot cas a través de telèfon, adreça de correu electrònic i/o de l'eina interna de gestió de incidències de l'entitat en mode no automatitzat.

També haurà de recollir aquelles alertes emeses pel CAU (Centre Atenció Usuaris) o altres fonts internes en el cas que aquestes no hagin estat identificades per la eina de monitorització de l'empresa adjudicatària.

L'adjudicatari, a petició de l'ens, impartirà formació als tècnics de l'entitat que siguin designats, sobre les eines i metodologies implantades al projecte. La mateixa es realitzarà de forma telemàtica i tindrà un caràcter bàsic incloent l'ús de l'aplicació, la configuració i la instal·lació dels sistemes desplegats.

6.2 Organització del servei

Estructura organitzativa

Per part de l'entitat, s'establirà la figura del Responsable del Servei, que serà l'encarregat de dirigir i coordinar la relació amb l'adjudicatari.

Per part de l'adjudicatari, de la mateixa manera, s'establirà un Responsable del Servei, encarregat de coordinar i garantir el compliment dels requisits del servei, assignant els mitjans adequats per a la correcta prestació del servei.

Equip de treball

Els integrants de l'equip de treball es concretaran en cada contracte basat en funció del servei requerit.

El personal inclòs a la proposta del licitador del contracte basat haurà de reunir els requisits mínims establerts com a requeriment del contracte basat per a la categoria professional concreta i funció a desenvolupar i, a més, que els mateixos perfils coincideixin amb els presentats a la proposta efectuada per l'adjudicatari en la seva oferta del present acord marc .

Si durant l'execució del contracte sorgeix la necessitat de substitució d'algun membre de l'equip de treball, l'adjudicatari haurà de motivar la sol·licitud amb almenys dues setmanes d'antelació, i ser autoritzada, si s'escau, per l'entitat. Donat l'elevat impacte que suposa la rotació de perfils l'adjudicatari vetllarà perquè aquesta rotació sigui baixa una vegada aprovat l'equip de treball de cada contracte basat.

En general, si es produís la substitució d'un membre de l'equip de treball, hi haurà un procés de traspàs del coneixement o solapament entre el recurs sortint i els recursos que assumeixen les tasques exercides pel recurs sortint, de 10 dies hàbils mínim per assegurar el traspàs de coneixement intern.

Les empreses hauran de disposar, com a mínim, d'un equip de treball format pels següents perfils:

- Consultor de Govern de Seguretat, les funcions del qual estaran relacionades amb el servei de Governança de la Ciberseguretat, que engloba la gestió de l'Oficina Tècnica de Seguretat.
- Un expert tècnic en Seguretat. Les principals funcions seran les corresponents a la prestació dels següents serveis:
    - La instal·lació, configuració i manteniment d'eines que donin suport al servei de seguretat d'operacions de ciberseguretat.
    - Servei de Gestió d'Incidents de Seguretat de la Informació, mitjançant la detecció, contenció, anàlisi, resposta i recuperació a esdeveniments de ciberseguretat.
    - Interlocució, si existeix, amb el Centre d'Operacions de Seguretat (SOC) i el CERT.

  Tots els perfils hauran de tenir com a mínim 3 anys d'experiència en projectes similars.

Seguiment del servei

A les reunions de seguiment participaran, almenys, el Responsable del Servei de l'entitat i de l'adjudicatari.

Durant les fases inicials de posada en marxa i de devolució del servei es duran a terme reunions de seguiment amb periodicitat mensual. En aquestes reunions, es portarà un seguiment de la planificació i tasques realitzades, així com una anàlisi de riscos per part de l'adjudicatari.

Durant la fase de prestació del servei s'estableix una periodicitat semestral per a les reunions de seguiment, encara que l'entitat podrà sol·licitar reunions extraordinàries per l'existència de circumstàncies que ho facin necessari.

L'adjudicatari lliurarà un informe mensual d'activitat (que alhora servirà per a donar conformitat a les factures) que reculli:

- Avanç en el compliment de l'objecte del contracte.
- Incidents de seguretat que cal destacar.
- Riscos existents i previstos.
- Altres aspectes rellevants en matèria de seguretat de la informació detectats i que hagin de ser coneguts per l'entitat.

En cas que, per qüestions relacionades amb la prestació del servei, fos necessari el desplaçament del personal de l'equip tècnic a qualsevol ubicació, aquest desplaçament aniria a càrrec de l'adjudicatari, sense que suposi un cost addicional.

Les reunions de seguiment es duran a terme a les instal·lacions de l'entitat o en línia si l'entitat hi està d'acord.

Horari del servei

El servei es prestarà per l'equip de treball especialitzat amb disponibilitat diària de 8 hores, de dilluns a divendres (model 8x5), amb un servei de resolució d'incidències amb horari 24x7 (24 hores, de dilluns a diumenge) per proveir d'un servei d'operacions de seguretat gestionada a l'entitat.

6.3 Gestió i execució del Pla de Seguretat

La gestió del servei d'operació ha d'englobar, per part de l'empresa adjudicatària, la gestió de la Oficina Tècnica de Seguretat de l'ens local, el manteniment del marc normatiu i de procediments de seguretat a més de l'anàlisi i la presentació de resultats de manera recurrent i programada o sota petició explícita. Aquesta gestió haurà d'assegurar el compliment de les mesures de seguretat establertes a l'ENS.

Amb l'objectiu d'executar el Pla de Seguretat, s'hauran d'oferir serveis i funcions orientades a l'execució de les mesures i accions identificades en el Pla, i al seu seguiment i actualització.

El servei ofert pel licitador haurà d'incloure les prestacions dividides en els següents àmbits:

6.3.1 Gestió del Pla de Seguretat

- Implementació, seguiment i Gestió del Pla de Seguretat impulsant totes aquelles accions generals i específiques per assolir la seva consecució.
- Revisió i avaluació del Pla de Seguretat per entendre i valorar dintre del context de l'entitat, els riscos identificats i mesures compensatòries proposades.
- Avaluació dels riscos i de les mesures proposades per a determinar la seva viabilitat, impacte, i priorització 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.
- Elaboració de 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.
- Mesura, interpretació i seguiment d'indicadors i mètriques de seguretat, i l'agrupació dels mateixos en la confecció de Quadres de Comandament.
- Suport a la direcció de l'entitat en la convocatòria del Comitè de Seguretat de la Informació i preparació de la documentació per al desenvolupament de les sessions.
- Assessorament tècnic i jurídic de primer nivell en matèria de ciberseguretat i compliment normatiu, amb la possibilitat d'elevar qüestions complexes a altres entitats o autoritats amb un alt nivell de coneixement i competència en la matèria.
- Suport en les accions de comunicació que es derivin de la gestió del Pla de Seguretat.
- Atenció i resposta a consultes tècniques i jurídiques en matèria de seguretat de la informació.

6.3.2 Adequació normativa prevista en el Pla de Seguretat

La implementació de les mesures i actuacions previstes en el Pla de Seguretat comporten progressivament a l'adequació normativa de l'entitat a l'Esquema Nacional de Seguretat.

L'operativa d'adequació normativa es fonamenta en la implementació del Pla de Seguretat i en el desplegament de les capacitats i recursos necessaris per governar el compliment normatiu de l'entitat, amb l'objectiu d'assolir de manera satisfactòria els futurs processos de certificació dels serveis escollits a tal fi per l'entitat. A tal efecte, les principals tasques a desenvolupar seran les següents:

- Donar suport actiu i constant, en el desplegament del model de ciberseguretat, durant les diferents fases, respecte a les diferents activitats i tasques relacionades amb el compliment i l'adequació normativa.
- Impulsar i governar la implantació de les iniciatives i projectes, associats al compliment normatiu, definits en el Pla de Seguretat.
- Identificar i establir, conjuntament amb la direcció de l'entitat, l'objectiu d'implantació de les normatives, legislacions i estàndards de bones pràctiques a implantar en l'entitat, així com el serveis susceptibles de passar els futurs processos de certificació.
- Realitzar avaluacions periòdiques de l'estat d'implantació dels requeriments normatius de l'entitat, tant des del punt generalista, a nivell d'entitat, com específic, dels serveis que es volen adequar, i posteriorment certificar, per tal d'identificar les mancances respecte al compliment, que cal adreçar.
- En referencia a les avaluacions periòdiques realitzades, definir les iniciatives i projectes que caldria abordar, de manera coordinada i consensuada amb l'estratègia del Pla de Seguretat, i impulsar la seva implantació.
- Coordinar la generació de les evidencies necessàries, vetllar pel seu manteniment actualitzat, i realitzar l'operativa per fer la seva entrega a l'Agencia de Ciberseguretat de Catalunya o a l'entitat certificadora corresponent quan es requereixi durant el procés de certificació.
- Portar a terme els treballs necessaris, per a elaborar, adaptar i mantenir la documentació i procediments relacionats amb el marc organitzatiu, normatiu i de compliment de l'ENS seguint, quan estiguin disponibles, les indicacions, guies i models de referència que l'entitat local pugui facilitar.
- Col·laborar i realitzar els treballs necessaris de suport en el procés d'auditoria externa i certificació en l'ENS.
- Dur a terme les tasques necessàries associades al govern i manteniment de la certificació.

6.3.3 Actuacions i projectes específics en el marc del Pla de Seguretat

La implementació del Pla de Seguretat pot suposar l'execució i governança de projectes, tant de ràpida execució, com d'actuacions més complexes que requereixin d'una anàlisi i planificació per a la seva consecució. A tal efecte l'adjudicatari haurà de proveir dels recursos, capacitats i coneixement tècnic necessaris per portar-los a terme. A títol orientatiu, els projectes podran abastar les següents tipologies sense descartar-ne d'altres d'homòlogues en l'àmbit de la ciberseguretat:

- Projectes de transformació per esmenar l'obsolescència tecnològica dels entorns, sistemes d'informació i lloc de treball de l'entitat.
- Projectes de gestió vulnerabilitats i millora de configuracions, tals com la protecció de serveis configurats per defecte, l'aplicació de pegats de seguretat, mitigació de vulnerabilitats associades a solucions pròpies o de tercers, i la realització d'escanejos de seguretat interns i gestió de vulnerabilitats.
- Projectes d'adquisició i desplegament d'eines de seguretat i perimetrals, projectes de gestió centralitzada de logs i millora de les configuracions de les eines de seguretat.
- Projectes d'elaboració de polítiques i procediments vinculats al compliment i al cos normatiu de l'entitat.
- Projectes per implementar una gestió d'usuaris i control d'accés, tals com les restriccions d'accés a serveis i actius de l'entitat, gestió de les baixes dels usuaris inactius, desplegament de solucions de MFA (factor d'autenticació múltiple), implementació de polítiques de mínims privilegis, configuracions segures de les solucions d'accés remot, i implementació de millores de la seguretat i detecció d'atacs als directoris actius.
- Projectes de securització de la xarxa, tals com la millora de la seguretat dels protocols i serveis de la xarxa, segmentació segura, securització de xarxes Wifi i configuració adequada de les solucions NAC.
- Projectes de millora en la protecció i securització dels equips de treball i dispositius mòbils.
- Projectes en l'àmbit de la criptografia i relatius a la implementació de certificats reconeguts i segurs, i de configuració segura de la signatura electrònica.
- Projectes orientats a la millora de la gestió i protecció de les còpies de seguretat.
- Projectes d'anàlisi de riscos dels sistemes utilitzant l'eina PILAR o una altra en cas que el Supervisor de Seguretat de les Tecnologies de la Informació i les Comunicacions (SSTIC) així ho determinés. Aquesta anàlisi de riscos ha de ser completa, de manera que permeti validar el conjunt de mesures de seguretat implantada, detectar la necessitat de mesures addicionals i justificar-ne l'ús de mesures de protecció alternatives.
- Projecte d'elaboració del pla de contingència i continuïtat de negoci. Es portarà a cap un pla de continuïtat dels serveis i de la infraestructura de suport als sistemes d'informació i telecomunicacions davant de possibles contingències.

Les entitats podran sol·licitar la totalitat de les prestacions o una part d'elles.

6.4 Acords de Nivell de Servei (SLA)

Els SLA dels contractes basats podran ser especificats al propi contracte, o establir com a genèrics els que es descriuen en aquest apartat. Tanmateix, als contractes basats s'establiran els mitjans amb els que es faran les comunicacions (com per exemple correu electrònic, trucades telefòniques, eina de tiqueting, etc..).

Totes les comunicacions relacionades amb els serveis o amb el corresponent acord de nivell de servei s'hauran de realitzar per les àrees o departaments de l'entitat contractant.

Obligatòriament, l'entitat adjudicatària disposarà d'un registre operatiu de les peticions o notificacions realitzades per l'entitat contractant, emprant, en el seu cas, l'eina senyalada a tal efecte al contracte basat. A tots els efectes aquest registre haurà de ser també el registre d'incidències i peticions, i haurà de complir les premisses establertes a la normativa de protecció de dades.

Les incidències i les peticions de servei mantindran un flux amb el comunicant, procedint al seu tancament quan s'hagués comunicat al mateix i no es consideri cap acció addicional.

Serà d'obligatòria inclusió al registre:

- Hora d'inici de la incidència i hora de finalització (incloent l'hora en la que es produeix la incidència, l'hora de notificació i l'hora de finalització de la resolució).
- Hora de comunicació d'inici i hora de comunicació de finalització.
- Temps de resolució.
- Conclusions i millora.

En aquest sentit es tindran en compte els punts requerits per la normativa aplicable, per a la identificació, gestió i registre d'incidències, que puguin afectar al servei , que seran acordats amb la entitat contractant.

Davant les incidències produïdes i comunicades correctament, l'entitat adjudicatària disposarà d'un temps de resposta per a la resolució de les mateixes, així com les penalitats derivades del seu incompliment, que estaran definits al corresponent acord basat segons la criticitat:

- Alta: incidències que suposen una aturada dels sistemes d'informació de l'entitat o que generen un impacte reputacional significatiu.
- Mitjana: incidències que afecten al funcionament de més d'un 5% dels empleats de l'entitat.
- Baixa: incidències que generen un funcionament incorrecte, però permet continuar treballant als empleats de l'entitat.

Nivell de criticitat	Temps de resposta	Temps de resolució
Alta	60 minuts	4 hores
Mitjana	4 hores	48 hores
Baixa	48 hores	5 dies

En quant a les proves necessàries després d'un incident, i en el seu cas, després d'acordar-ho amb l'entitat contractant, es programaran generant el menor impacte possible en la operativitat del servei. Totes les parades tècniques del servei seran en horaris prèviament acordats amb l'entitat contractant.

S'ha de tenir en compte que el temps de resolució és el temps transcorregut entre la detecció de la incidència pel sistema de monitoratge o comunicació de la incidència a l'empresa contractista pel canal previst i la resolució documentada de la incidència per part de l'empresa contractista.

Els temps de resposta i de resolució d'incidències no es podran veure afectats per augments esporàdics del nombre d'incidències.

7 LOT 4: SERVEIS DE CENTRE D'OPERACIONS DE SEGURETAT (SOC)

Aquest lot del present acord marc té per objecte la contractació d'un SOC operatiu per a l'entitat contractant. El SOC haurà de proporcionar serveis de monitoratge, detecció, prevenció i resposta a incidents de seguretat, sota la supervisió, directrius, suport i acompanyament de l'Agència de Ciberseguretat de Catalunya (en endavant, Agència).

De la mateixa manera, el SOC implantat haurà de formar part de la Xarxa Nacional de Centres d'Operacions de Seguretat i compartir informació amb aquesta, que integrarà el Centre d'Operacions de Ciberseguretat de l'Administració General del Estat i els de les altres administracions públiques d'àmbit nacional.

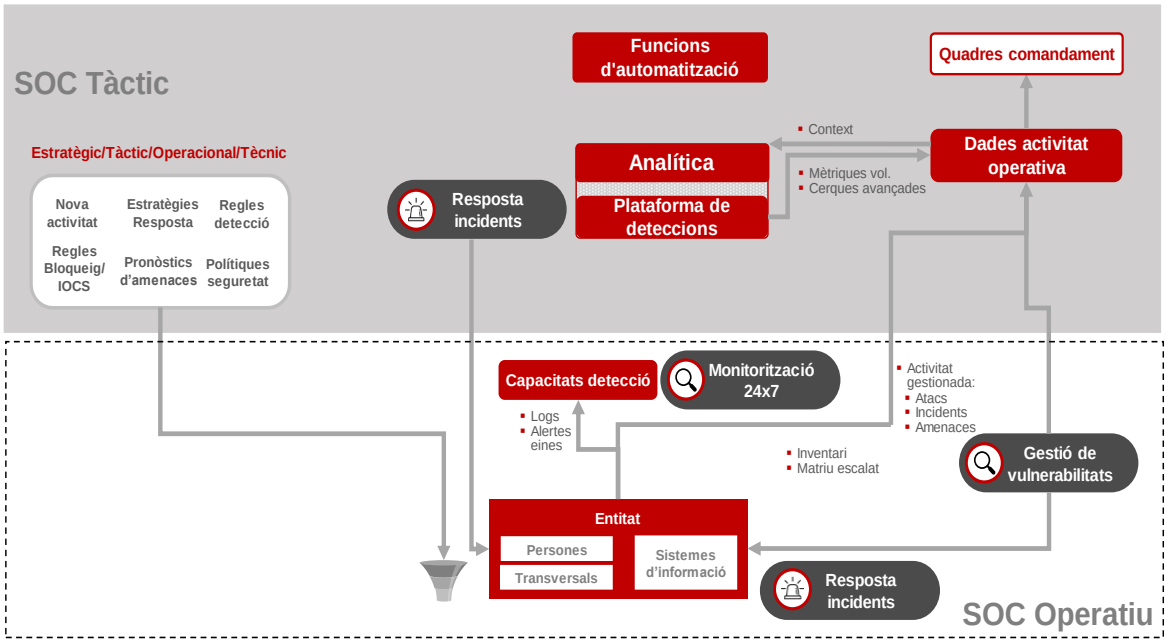
L'Agència és l'entitat que coordina la protecció i seguretat de la informació i les infraestructures de Catalunya davant les ciberamenaces, i la resposta efectiva davant dels mateixos, sempre sota l'empara de la col·laboració i coordinació amb diferents actors a nivell local, nacional i internacional.

Una de les funcions principals de l'Agència és exercir com a SOC Tàctic dins del model d'integració i govern operatiu dels diferents SOC's Operatius, definint l'estratègia de prevenció, detecció, protecció i resposta davant amenaces, que aquests han de tenir com a referència per a adaptar les seves pròpies.

L'estructura funcional del model d'Integració i Govern Operatiu pretén satisfer els quatre eixos fonamentals de la seguretat de la informació enfront d'amenaces i incidents de seguretat (detecció, prevenció, protecció i resposta) en un model d'Integració amb responsabilitat i operació distribuïda, a on:

- **El SOC Tàctic** té les competències de definir l'estratègia de prevenció, detecció, protecció i resposta davant amenaces i acompanyar als SOCs Operatius en la seva adaptació. Per tal de facilitar aquesta adaptació, el SOC Tàctic proposarà regles de correlació per detectar les principals amenaces a l'entitat, polítiques de seguretat a desplegar, contramesures a desplegar a les eines de detecció/protecció de l'entitat sobre amenaces actives, i estratègies de resposta davant incidents i informació d'intel·ligència operativa. Igualment liderarà la resposta a incidents complexos segons s'estableix a l'Esquema Nacional de Seguretat (ENS).
- **El SOC Operatiu** té la responsabilitat de dotar de visibilitat al SOC Tàctic respecte a l'activitat gestionada de l'entitat, i el grau d'exposició a l'amenaça de forma que doti a l'Agència de disposar del coneixement de l'entorn i el context necessari per fer front a les amenaces, atacs i incidents, fent més productiva i operativa l'estratègia definida per l'entitat. Per això és imprescindible la coordinació operativa amb el SOC Tàctic amb un seguiment periòdic d'acord al que s'estableixi al model d'integració del SOC Operatiu de l'entitat.

El següent esquema mostra a grans trets el model de Govern Operatiu de relació entre el SOC Tàctic i els SOC's Operatius:



Les funcions, a mode d'exemple no limitatiu, que hauran d'executar els SOC's Operatius en termes d'integració operativa són:

- Adaptació de l'estratègia definida pel SOC Tàctic, mitjançant la definició i aplicació dels procediments i instruccions operatives internes que apliquin a l'entitat en cada cas, així com la seva actualització continua, d'acord als processos de millora continua que es puguin esdevenir durant el servei.
- Coordinació operativa amb el SOC Tàctic amb seguiment periòdic segons el que s'estableix al model d'integració del SOC Operatiu de l'entitat, aportant en qualsevol cas informació actualitzada que permeti per tal d'assegurar la visibilitat de l'activitat gestionada i el grau d'exposició des del SOC Tàctic.

7.1 Implantació del SOC

L'entitat adjudicatària s'encarregarà d'implantar el SOC així com de la seva operativa tant a nivell tècnic com organitzatiu.

Durant la fase embrionària del projecte d'implantació del SOC, l'entitat adjudicatària realitzarà un estudi preliminar per part d'un tècnic propi in situ, a fi d'establir les següents fites:

- Coneixement de la infraestructura tecnològica de l'entitat pública per a la implantació del SOC i totes les eines que l'han de constituir.
- Identificació dels processos, procediments i polítiques d'operació per a una correcta adequació del SOC a l'entitat pública.
- Definició de l'estratègia d'implantació de les eines necessàries.

En el moment de la detecció d'un incident a través del servei de monitorització, o bé aquest sigui comunicat per algun dels canals establerts, el SOC procedirà a la gestió completa de l'incident realitzant, almenys, les activitats següents:

- Registrar, classificar, valorar, prioritzar i escalar els incidents de seguretat que siguin detectats a través del servei de monitorització, que siguin comunicats pel personal de seguretat o TIC de l'entitat.
- Emetre les alertes oportunes davant d'esdeveniments de seguretat, tant internes com a tercers (autoritats nacionals i/o altres organitzacions).
- Realitzar la notificació i documentació dels incidents de seguretat segons la Guia nacional de notificació i gestió de ciberincidents i els protocols establerts conjuntament amb l'entitat.

El cicle de vida de l'incident es gestionarà segons els procediments i l'estratègia definida pel SOC Tàctic.

Addicionalment l'adjudicatari haurà de mantenir actualitzats i provats els procediments de resposta davant d'incidents.

Per a l'atenció al servei de Gestió d'Incidents de Seguretat l'adjudicatari haurà de comptar almenys amb un Punt Únic de Contacte a l'interval de servei ofert per l'atenció a incidències, consultes, peticions i gestió de notificacions.

El responsable del contracte designat per l'entitat contractant controlarà l'acompliment dels terminis acordats així com la qualitat de la instal·lació i la seva adequació als requeriments tècnics.

L'empresa adjudicatària destinarà una persona com a responsable únic durant tot el procés d'implantació i més endavant durant tota la vigència del contracte. En cas de canvi de la persona responsable del contracte, es comunicarà per escrit al responsable designat per l'ens.

Tot el maquinari i programari necessari pel projecte, que haurà d'estar homologat al catàleg del CPSTIC, serà a compte de l'adjudicatari i haurà d'estar correctament dimensionat amb la infraestructura de l'ens públic per poder oferir el servei amb garanties durant la durada del contracte, incloent les actualitzacions i/o ampliacions oportunes.

L'adjudicatari haurà de tenir en compte l'existència d'un entorn d'alta disponibilitat en cas d'existència de màquines virtuals a l'entitat. Si es dona el cas, tot allò necessari (maquinari, programari i llicències) per a aquests recursos serà proporcionat per l'empresa adjudicatària.

Les tasques de llicenciament, implantació, integració, configuració, automatització i proves hauran de ser realitzades per l'adjudicatari íntegrament, incloent totes les tasques a realitzar envers l'equipament de l'entitat pública que siguin requerides, i estaran basades en l'estudi d'implantació prèviament generat.

L'adjudicatari configurarà i desplegarà a través de la infraestructura de l'entitat totes aquelles instal·lacions i/o actualitzacions susceptibles de ser automatitzades. Aquestes tasques hauran de ser desenvolupades, sempre que sigui possible, de forma presencial a les dependències de l'entitat pública.

Les eines a implantar i desplegar que ha d'incloure l'oferta del licitador son les següents, sense menyscapte d'ampliar el catàleg segons les necessitats de l'ens públic:

- **Plataforma de correlació d'esdeveniments de seguretat de la informació (d'ara en endavant SIEM):**
  L'empresa adjudicatària oferirà la implantació i desplegament d'una plataforma dedicada a la recol·lecció i anàlisi de dades a temps real de les alertes generades

pels components que conformen els diferents sistemes d'informació de l'entitat. Aquesta plataforma haurà d'estar qualificada al catàleg CPSTIC.

Es recolliran i es centralitzaran els registres i *logs* que continguin informació i esdeveniments relacionats amb la seguretat de l'entitat, detectant incidents i generant les alertes pertinents.

El període de retenció dels *logs* serà acordat amb l'entitat, i sempre serà més gran de trenta (30) dies per a l'operació d'esdeveniments i incidents i de sis (6) mesos per l'arxivat.

- **Eina d'intercanvis**
  L'adjudicatari del contracte oferirà la implantació i desplegament, en mode federat, l'eina pertinent a fi de permetre l'intercanvi automàtic i fluid dels ciberincidents amb la Plataforma Nacional de Notificació i Seguiment de ciberincidents.

- **Sistema d'Alerta Primerenca d'internet (SAT INET)**
  L'empresa adjudicatària del servei oferirà la implantació i desplegament del SAT-INET desenvolupat pel CCN-CERT mitjançant la instal·lació d'una sonda a la xarxa de l'entitat pública contractant.

- **Eina MicroCLAUDIA**
  L'empresa contractant oferirà la instal·lació de l'agent lleuger MicroCLAUDIA a la infraestructura de l'entitat contractant amb la finalitat de descarregar i executar les vacunes que el CCN-CERT hagi desenvolupat.

- **Sistema de detecció d'atacs avançats**
  L'empresa contractant haurà d'oferir la implantació de les eines del CCN-CERT Carmen i Clàudia d'anàlisi i gestió d'incidents per a identificar el compromís de la xarxa per amenaces persistents avançades (APT).

L'adjudicatari també s'encarregarà de la instal·lació i/o automatització de la instal·lació dels diferents agents a l'equipament de l'entitat objecte de monitorització i de les actualitzacions necessàries que requereixi l'entitat contractant en el seu contracte basat. Aquests equipaments i/o programaris hauran d'estar inclosos al catàleg de productes del CPSTIC.

La implantació i desplegament d'aquestes eines es realitzarà a les mateixes condicions que la resta de l'equipament a implantar sense intervenció del personal municipal.

A la fase final de la implantació del servei de SOC, l'adjudicatari farà una avaluació de la seguretat de l'entitat amb les pertinents proves que consideri oportunes i s'aplicaran les metodologies, procediments i activitats previstes al model de servei.

7.2 Funcions i capacitats del SOC

Els següents apartats descriuen les funcions i capacitats principals requerides al SOC Operatiu en les àrees de prevenció, detecció, protecció i resposta dins del model de Govern exposat anteriorment.

Aquestes funcions s'hauran d'anar adaptant per a garantir l'òptima execució del contracte. En tot cas, aquestes tasques no eximeixen en cap cas de la realització d'altres tasques addicionals necessàries per a garantir la ciberseguretat de l'entitat contractant.

En tots els casos, romandrà com a base l'adaptació de l'estratègia definida pel SOC Tàctic per a cada matèria, mitjançant la definició de procediments i instruccions operatives internes i adaptació d'eines que apliquin a l'entitat, per tal de garantir una òptima gestió, assegurant la visibilitat gestionada i el grau d'exposició des del SOC Tàctic.

7.2.1 Disponibilitat del servei

Atenent a la naturalesa del servei de SOC, es pot requerir que la seva prestació es dugui a terme en un horari 24x7 365 dies a l'any.

En aquests casos s'indicarà aquesta necessitat en la contractació basada. Addicionalment, s'informa que els serveis inclosos en aquest Acord Marc poden implicar la necessitat de dur a terme guàrdies i feines fora d'horari. En aquest sentit:

- Es considera guàrdia la disponibilitat per atenció telefònica i actuació presencial en horari no laboral en el cas d'actuacions especials o que la importància de la incidència ho requereix.
- A petició expressa de l'entitat, es podria demanar la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

7.2.2 Capacitats de prevenció

La prevenció té com a objectiu analitzar i aplicar mesures que permetin anticipar-se a la possible materialització de les amenaces als actius, mitigant o eliminant el risc i l'impacte a l'entitat. Per això esdevé un factor clau conèixer l'estat dels actius en matèria de seguretat, les vulnerabilitats i les amenaces que els poden afectar, i actuar de forma preventiva.

Dins del model d'integració i de Govern Operatiu, s'haurà de preveure que el SOC Tàctic (SOC/CET de l'Agència), elaborarà pronòstics d'amenaces i alertes primerenques, i executarà tasques relacionades amb el servei de vigilància/monitorització digital (fuites d'informació, credencials, suplantació d'identitat, etc.), així com exercicis d'exposició a l'amenaça, o proves tècniques d'intrusió sobre els sistemes crítics.

En aquest context, el SOC Operatiu implantat haurà d'executar les següents funcions:

- Inventari i classificació en base a la criticitat dels actius objecte de monitorització i gestió en aspectes relatius a la seguretat, per tal de poder fer un correcte diagnòstic de la seguretat i una gestió preventiva dels mateixos. El SOC Operatiu facilitarà aquests informes actualitzats al SOC Tàctic.
- Anàlisi i gestió de vulnerabilitats dels actius i sistemes de l'entitat, execucions d'escanejos de vulnerabilitats i classificació mitjançant *scoring* CVE, CVSS 3.1, etc. aplicant les implantacions i desplegament de contramesures als actius sota la seva responsabilitat, que permetin evitar o minimitzar l'impacte de les vulnerabilitats esmentades.

  El SOC Operatiu es coordinarà amb el SOC Tàctic, informant dels resultats obtinguts, identificant especialment els casos complexos i participant en el procés de gestió dels casos, inclosos el seguiment i el suport en la gestió d'aquests.
- Anàlisi de la superfície d'exposició externa de l'entitat, revisant de forma activa les configuracions, infraestructures, i actius de l'entitat exposats a Internet, per tal d'identificar des de la perspectiva d'un atacant extern, vulnerabilitats i debilitats que puguin ser explotades, poder prioritzar-les, gestionar-les i mitigar-les. Dins d'aquesta funció es contemplen, escanejos de vulnerabilitats, auditories tècniques i proves d'intrusió necessàries, com poden ser *pentests*, anàlisi de codi font, tests de *phishing*, entre d'altres; els qual generen resultats i diagnòstic de seguretat, que seran compartits amb el SOC Tàctic de l'Agència. Igualment proposaran proves de concepte i plans d'acció per mitigar els aspectes identificats, realitzant el seguiment de les accions correctives.
- Determinació del grau d'exposició d'amenaça de l'entitat segons sol·licitud del SOC Tàctic dels organismes competents, aportant informació actualitzada respecte a actius de l'entitat, informació rellevant del darrer anàlisi de seguretat, indicadors de compromís rellevants per l'amenaça i la seva evolució, i informes de grau d'exposició, de forma que es pugui mantenir el relat de l'entitat respecte a l'amenaça.
- Donar visibilitat de l'activitat gestionada als organismes competents amb seguiment periòdic segons el que s'estableix al model d'integració del SOC Operatiu de l'entitat, aportant en qualsevol cas inventaris actualitzats dels actius de l'entitat, informes d'activitat gestionada amb exportacions de les eines que s'integraran en un repositori del SOC Tàctic de l'Agència, i quadres de comandament accessibles. Igualment es reportaran indicadors i informes que permetin evidenciar l'eficàcia dels plans de desplegament i contramesures relatives a la prevenció d'amenaces. Es podran sol·licitar igualment informes detallats o executius segons el tipus d'amenaça.

- Mantenir i evolucionar les eines i els procediments que siguin objecte del seu àmbit de responsabilitat i que necessaris per dur a terme aquestes tasques.

7.2.3 Capacitats de detecció

La detecció d'amenaces té com a objectiu identificar ciberamenaces i permetre aplicar mesures de mitigació i contenció abans que aquestes que causin un dany significatiu a l'entitat. En aquest sentit, les operacions del SOC/CERT de l'Agència giren al voltant del concepte de "perímetres de ciberseguretat" que, mitjançant un conjunt d'activitats i tecnologies desplegades i gestionades, ajuden a millorar la ciberseguretat dels sistemes d'informació, les infraestructures transversals i les persones.

En el marc de la integració del model, el SOC Tàctic haurà d'identificar a alt nivell els casos d'ús per a la detecció d'amenaces en base als marcs de referència com ara MITTRE ATT&CK, elaborarà regles de detecció per a noves amenaces i propostes per a missions de ThreatHunting, i proporcionarà indicadors d'intel·ligència operativa a fi de poder fer una gestió de la seguretat efectiva.

En aquest context, el SOC Operatiu implantat haurà d'executar les següents funcions:

- Detecció d'activitat relacionada amb ciberamenaces basant-se en una monitorització i detecció automàtica 24x7 d'activitat relacionada amb ciberamenaces, mitjançant eines de correlació tipus SIEM/XDR. Serà responsabilitat del SOC Operatiu el correcte manteniment, configuració i actualització d'aquestes eines i les seves fonts integrades per permetre identificar potencials amenaces, atacs o incidents de seguretat sobre els actius dins del seu àmbit de responsabilitat.
- Implementació de regles de detecció d'amenaces o casos d'ús en les eines de correlació tipus SIEM/XDR, indicades pel SOC Tàctic i que siguin d'aplicació a l'entitat, així com aquelles que, d'acord a l'anàlisi d'informació de l'activitat i context disponible, el SOC Operatiu consideri adients per permetre identificar potencials amenaces, atacs o incidents de seguretat sobre els actius dins del seu àmbit de responsabilitat.
- Monitorització d'indicadors de compromís sobre les eines de ciberseguretat per a la cerca continua d'activitat relacionada amb les amenaces.
- Anàlisi i gestió priorització de les alertes de detecció d'amenaces, aplicant les implantacions i desplegament de contramesures a les eines perimetrals i actius sota la seva responsabilitat, que permetin evitar o minimitzar l'impacte de les amenaces esmentades.
- Execució de les missions de ThreatHunting sobre la entitat a la que es dona servei, en base als indicadors d'intel·ligència d'amenaces, així com aquelles que,

d'acord a l'anàlisi d'informació de l'activitat i context disponible, el SOC Operatiu consideri adients per detectar possibles exposicions a les amenaces i actuar de forma preventiva sobre els actius dins del seu àmbit de responsabilitat.

- Elaboració i monitorització de quadres d'activitat en temps real i accessibles de forma que permetin disposar d'informació en temps real del grau d'exposició de l'amenaça, evolució dels indicadors de compromís, actius afectats i grau d'adaptació dels plans d'actuació i contramesures, de cara a que el SOC Tàctic pugui mantenir el relat de l'entitat respecte a les amenaces.
- Donar visibilitat de l'activitat gestionada al organismes competents amb seguiment periòdic, aportant en qualsevol cas informes d'activitat gestionada i quadres de comandaments, accessibles. Per això el SOC Operatiu haurà de ser capaç de recopilar, inventariar, registrar i documentar les evidències d'amenaces gestionades, i extreure indicadors que permetin al SOC Tàctic tenir un relat de l'entitat respecte a amenaces. Igualment es reportaran indicadors i informes que permetin evidenciar l'eficàcia dels plans de desplegament i contramesures relatives a la detecció d'amenaces. Es podran sol·licitar igualment informes detallats o executius segons el tipus d'amenaça.
- Mantenir i evolucionar les eines i els procediments que siguin objecte del seu àmbit de responsabilitat i que necessaris per dur a terme aquestes tasques.

7.2.4 Capacitats de protecció

La protecció té com a objectiu donar resposta a aquells esdeveniments significatius que suposin o puguin suposar un potencial incident de seguretat. Això inclou: aplicació o sol·licitud d'aplicació de contramesures, així com la participació en tot el procés de gestió dels casos, inclosos el seguiment i el suport en comitès de crisi quan sigui necessari.

Dins del model d'integració i de Govern Operatiu, cal tenir en compte que el SOC Tàctic prescriurà les polítiques de detecció/protecció a desplegar sobre les eines de Ciberseguretat (mitjançant llibres blancs o guies de configuració), així com accions de protecció enfront a nous atacs i amenaces.
En aquest context, el SOC Operatiu implantat haurà d'executar les següents funcions:

- Operació de les eines de ciberseguretat de l'entitat, configurant-les per a que funcionin segons les polítiques de detecció/protecció prescrites, i administrant-les gestionant tot el seu cicle de vida (manteniment i posta a punt, optimitzacions, actualitzacions, llicenciament, etc.)
- Aplicació de contramesures sobre les eines de ciberseguretat, per evitar o reduir l'impacte sobre els actius de l'entitat, l'escalat de casos complexos a altres grups resolutoris, així com la participació en tot el procés de gestió dels casos, inclosos el seguiment i el suport corresponent.

- Desplegament d'indicadors de compromís sobre les eines de protecció/detecció per la cerca continua d'activitat relacionada amb les amenaces.
- Automatització de les tasques més concurrents, de forma que es doni una ràpida resposta d'execució i evitant errors degut a l'acció humana.
- Donar visibilitat de l'activitat gestionada al SOC Tàctic amb seguiment periòdic segons el que s'estableix al model d'integració del SOC Operatiu de l'entitat, aportant en qualsevol cas informes d'activitat gestionada i quadres de comandament, accessibles, que permetin monitorar el desplegament de les fonts d'intel·ligència. Per això el SOC Operatiu haurà de ser d'accedit en mode auditoria i via API a la configuració de les eines gestionades.
- Mantenir i evolucionar les eines i els procediments que siguin objecte del seu àmbit de responsabilitat i necessaris per dur a terme aquestes tasques.

7.2.5 Capacitats de resposta a incidents

La resposta a incidents té com a objectiu fer front als incidents de seguretat, tant de manera proactiva com reactiva. Addicionalment ha de garantir la gestió correcta de les evidències i la validesa jurídica, així com proveir el coneixement i els plans d'actuació necessaris per reduir de manera efectiva i eficient l'impacte de les ciberamenaces dins dels àmbits d'actuació.

Dins del model d'integració i de Govern Operatiu, cal tenir en compte que el SOC Tàctic definirà les estratègies de resposta per a incidents de Ciberseguretat, i establirà el model de relació i matriu de responsabilitats dels equips de resposta, liderant la resposta davant d'incidents crítics i donant suport al SOC Operatiu en incidents no crítics

En aquest context, el SOC Operatiu implantat haurà d'executar les següents funcions:

- Resposta davant d'incidents no crítics, en temps i en forma, minimitzant l'impacte, assegurant-ne l'erradicació i garantint que no es puguin tornar a repetir de la mateixa manera. Per això s'encarregarà de la gestió de l'incident, així com de proveir el relat necessari respecte a la investigació per a la presa de decisions en el context d'un incident.
- Cerca proactiva d'amenaces (Threat Hunting), per detectar possibles incidents no detectats pels sistemes de detecció desplegats, però que poden ser visibles via la detecció d'anomalies o correlació avançada d'esdeveniments, o executant els anàlisis forense posteriors. Així, cerca proactiva d'amenaces proporcionaria informació a l'anàlisi forense per a enfocar la investigació, mentre que el segon aportaria proves al Threat Hunting per a confirmar les amenaces identificades.
- Coordinació amb el SOC Tàctic per a la resposta davant incidents crítics, executant un primer anàlisi de l'afectació, proveint el context necessari que ajudi

a la presa de decisions del SOC Tàctic als diferents comitès. Per això haurà de recopilar, analitzar les evidències seguint un procés que garanteixi la integritat d'aquestes i de la seva cadena de custòdia garantint-ne la validesa davant un possible procés judicial, així com aplicar les mesures de contenció inicials establertes o aquelles indicades des del SOC Tàctic com a proposta de contenció, erradicació i/o recuperació.

- Donar visibilitat de l'activitat gestionada al SOC Tàctic amb seguiment periòdic segons el que s'estableix al model d'integració del SOC Operatiu de l'entitat, aportant en qualsevol cas informes d'activitat gestionada i quadres de comandament, accessibles. Per això el SOC Operatiu haurà de ser capaç de recopilar, inventariar, registrar i documentar les evidències i incidents gestionats i investigacions realitzades, i extreure indicadors que permetin al SOC Tàctic tenir un relat de l'entitat respecte a incidents. Igualment es reportaran indicadors i informes que permetin evidenciar l'eficàcia de plans de millora o erradicació relatius a la resposta a incidents.
- Mantenir i evolucionar les eines i els procediments que siguin objecte del seu àmbit de responsabilitat i que necessaris per dur a terme aquestes tasques.

7.3 Plataforma de correlació d'esdeveniments de seguretat de la informació (SIEM)

En el cas que l'ens contractant no disposi o desitgi operar amb el sistema de gestió d'esdeveniments d'informació de l'empresa adjudicatària, aquesta haurà d'implantar un SIEM que estigui reconegut al catàleg CPSTIC, tal i com s'estableix al lot 1 d'aquest mateix plec.

En el supòsit de que l'entitat contractant ja disposi d'un SIEM, l'empresa adjudicatària del servei haurà de poder acreditar que posseeix experiència amb el programari i un equip tècnic humà amb els coneixements necessaris per a operar amb la plataforma establerta.

En qualsevol cas, l'empresa adjudicatària del servei de monitorització de la seguretat haurà de poder acreditar que opera amb un programari reconegut i homologat al catàleg CPSTIC i que està capacitada a tal efecte.

El servei ha de permetre el monitoratge i la correlació d'esdeveniments de seguretat, integrant les fonts de dades que generin tots els dispositius i sistemes de xarxa oferts així com els sistemes preexistents en l'ens contractant, a fi de detectar anomalies de seguretat i generar alertes que permetin l'adequada classificació del nivell d'amenaça de qualsevol dels incidents de seguretat detectats. El sistema haurà de suportar la creació de tiquets en el sistema de *helpdesk* de l'ens contractant, si s'escau, per a aquelles activitats que hagin de ser ateses pel personal d'aquest.

El licitador detallarà l'arquitectura de components del sistema SIEM proposat, incloent tots els elements de recol·lecció, agregació i processament d'esdeveniments, així com la ubicació dels mateixos (en les instal·lacions de l'ens públic contractant, en les infraestructures del propi licitador o altres a aquest efecte).

El licitador indicarà les mètriques de llicenciament que siguin aplicables al sistema SIEM ofert, justificant adequadament el seu dimensionament per a les fonts de dades dels sistemes que formin part de la seva oferta, així com de les fonts dels sistemes preexistents en l'ens contractant, durant tota la durada del contracte.

Es valoraran les automatitzacions i correlacions a implantar en el SIEM, per la qual cosa, per a la seva correcta valoració, s'hauran de detallar els casos d'ús a implantar en la proposta. També es valorarà la inclusió d'elements que facilitin la integració amb les eines de l'ecosistema del Centre Criptològic Nacional i l'enviament de trànsit de xarxa de manera selectiva a aquestes.

L'adjudicatari proporcionarà, com a mínim cada tres mesos, els registres d'activitat complets dels sistemes oferts en format interoperable.

7.4 Organització del servei

Estructura organitzativa

Per part de l'entitat, s'establirà la figura del Responsable del Servei, que serà l'encarregat de dirigir i coordinar la relació amb l'adjudicatari.

Per part de l'adjudicatari, de la mateixa manera, s'establirà un Responsable del Servei, encarregat de coordinar i garantir el compliment dels requisits del servei, assignant els mitjans adequats per a la correcta prestació del servei.

Equip de treball

Els integrants de l'equip de treball es concretaran en cada contracte basat en funció del servei requerit.

El personal inclòs a la proposta del licitador del contracte basat haurà de reunir els requisits mínims establerts com a requeriment del contracte basat per a la categoria professional concreta i funció a desenvolupar i, a més, que els mateixos perfils coincideixin amb els presentats a la proposta efectuada per l'adjudicatari en la seva oferta del present acord marc .

Si durant l'execució del contracte sorgeix la necessitat de substitució d'algun membre de l'equip de treball, l'adjudicatari haurà de motivar la sol·licitud amb almenys dues setmanes d'antelació, i ser autoritzada, si s'escau, per l'entitat. Donat l'elevat impacte que suposa la rotació de perfils l'adjudicatari vetllarà perquè aquesta rotació sigui baixa una vegada aprovat l'equip de treball de cada contracte basat.

En general, si es produís la substitució d'un membre de l'equip de treball, hi haurà un procés de traspàs del coneixement o solapament entre el recurs sortint i els recursos que assumeixen les tasques exercides pel recurs sortint, de 10 dies hàbils mínim per assegurar el traspàs de coneixement intern.

Les empreses hauran de disposar, com a mínim, d'un equip de treball format pels següents perfils:

- Responsable del servei, les funcions del qual és garantir servei i gestionar la relació amb l'entitat.
- Un expert tècnic en Seguretat. Les principals funcions seran les corresponents a la prestació del serveis SOC:
    - Gestió de vulnerabilitats.
    - Monitoratge i operació de la seguretat
    - Gestió d'incidents.
    - Generació de noves regles, automatització i integració de desplegaments adhoc.
- Un expert en el desplegament de les eines SIEM proposades a l'oferta presentada.

Tots els perfils hauran de tenir com a mínim **3 anys** d'experiència en projectes similars.

Seguiment del servei

A les reunions de seguiment participaran, almenys, el Responsable del Servei de l'entitat i de l'adjudicatari.

Durant les fases inicials de posada en marxa i de devolució del servei es duran a terme reunions de seguiment amb periodicitat mensual. En aquestes reunions, es portarà un seguiment de la planificació i tasques realitzades, així com una anàlisi de riscos per part de l'adjudicatari.

Durant la fase de prestació del servei s'estableix una periodicitat semestral per a les reunions de seguiment, encara que l'entitat podrà sol·licitar reunions extraordinàries per l'existència de circumstàncies que ho facin necessari.

L'adjudicatari lliurarà un informe mensual d'activitat (que alhora servirà per a donar conformitat a les factures) que reculli:

- Avanç en el compliment de l'objecte del contracte.
- Incidents de seguretat que cal destacar.
- Riscos existents i previstos.
- Altres aspectes rellevants en matèria de seguretat de la informació detectats i que hagin de ser coneguts per l'entitat.

En cas que, per qüestions relacionades amb la prestació del servei, fos necessari el desplaçament del personal de l'equip tècnic a qualsevol ubicació, aquest desplaçament aniria a càrrec de l'adjudicatari, sense que suposi un cost addicional.

Les reunions de seguiment es duran a terme a les instal·lacions de l'entitat o en línia si l'entitat hi està d'acord.

7.5 Acords de Nivell de Servei (SLA)

Les penalitats i els SLA dels contractes basats podran ser especificats al propi contracte, o establir com a genèrics els que es descriuen en aquest apartat:

Mètrica	Objectiu	Descripció
Temps de detecció	< 5 minuts	Temps en el que el SOC ha de detectar un incident de seguretat.
Temps de resposta	< 30 minuts	Temps des de que es detecta l'incident de seguretat fins que el SOC respon l'incident.
Temps de resolució d'incidències no crítiques	24h	Temps des de que es detecta l'incident de seguretat fins que es resol la incidència no crítica.
Comunicació d'incidents	30 minuts	El temps màxim en el qual el SOC ha de comunicar incidents crític a la direcció de l'organització.

Els valors indicats a la taula es podran personalitzar segons les necessitats i recursos de l'ens contractant.

Els SLA's es revisaran i s'actualitzaran regularment per a garantir que continuïn sent efectius a mesura que canvien les amenaces i les necessitats de seguretat de l'ens contractant.

Totes les comunicacions relacionades amb els serveis o amb el corresponent acord de nivell de servei s'hauran de realitzar per les àrees o departaments de l'entitat contractant.

Tanmateix, als contractes basats s'establiran els mitjans mitjançant els quals es faran les comunicacions (com per exemple correu electrònic, eina de tiqueting, trucades telefòniques, etc..).

Obligatòriament, l'entitat adjudicatària disposarà d'un registre operatiu de les peticions o notificacions realitzades per l'entitat contractant, emprant, en el seu cas, l'eina senyalada a tal efecte a contracte basat. A tots els efectes aquest registre haurà de ser també el registre d'incidències i peticions, i haurà de complir les premisses establertes a la normativa de protecció de dades.

Les incidències i les peticions de servei mantindran un flux amb el comunicant, procedint al seu tancament quan s'hagués comunicat al mateix i no es consideri cap acció addicional.

Serà d'obligatòria inclusió al registre:

- Hora d'inici de la incidència i hora de finalització (incloent l'hora en la que es produeix la incidència, l'hora de notificació i l'hora de finalització de la resolució).
- Hora de comunicació d'inici i hora de comunicació de finalització.
- Conclusions i millora.

En aquest sentit es tindran en compte els punts requerits per la normativa aplicable, per a la identificació, gestió i registre d'incidències, que puguin afectar al servei , que seran acordats amb la entitat contractant.

Anualment, es remetran aquests valors en un informe a l'entitat contractant.

Els temps de resposta i de resolució d'incidències no es podran veure afectats per augments esporàdics del nombre d'incidències.

8 LOT 5: SERVEIS D'ADEQUACIÓ A L'ESQUEMA NACIONAL DE SEGURETAT (ENS)

L'adequació a l'Esquema Nacional de Seguretat, és un procés que es podrà culminar a través de l'execució i seguiment del Pla de Seguretat generat en el lot 2 del present Acord Marc. No obstant això per aquelles entitats que requereixin un procés d'adequació específic a l'ENS es preveu aquest servei que tindrà com a objectiu la confecció dels treballs necessaris per a la realització d'una consultoria a l'organització per a l'adequació dels seus sistemes d'informació a l'Esquema Nacional de Seguretat, establint la política de seguretat en la utilització dels mitjans electrònics així com els principis bàsics i els requisits mínims que permetin una protecció adequada de la informació en l'àmbit de l'administració electrònica.

Aquells sistemes que tractin fitxers, ja siguin o no automatitzats, que continguin dades de caràcter personal, també s'analitzaran des dels punts de vista de l'actual normativa en matèria de protecció de dades amb caràcter personal.

En tot cas, l'objectiu final del servei d'adequació a l'ENS és preparar adequadament els sistemes, el tractament de les dades i l'organització de l'ens contractant per a la certificació per part de l'Agència de Ciberseguretat de Catalunya o per altres entitats de certificació acreditats aquest llistat.

Objectius i abast

El procés d'implantació de l'ENS començarà amb l'elaboració del Pla d'Adequació, que serà la base pel procés de gestió continuada de la seguretat de l'entitat contractant mitjançant la designació de rols, la constitució d'òrgans de seguretat, a més de l'adquisició dels compromisos de seguretat i d'implantació, que es veuran reflectits a la Política de Seguretat de la Informació i el Pla d'Adequació, respectivament.

L'empresa adjudicatària haurà de garantir que els seus sistemes d'informació que sustenten els serveis prestats en ser adjudicatàries de contractes basats del present lot apliquen les mesures de seguretat establertes al Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS). L'adjudicatari haurà de disposar d'un certificat d'acompliment de l'Esquema Nacional de Seguretat de nivell MIG, i aportar el certificat corresponent i que figurar en la web del CNI (https://gobernanza.ccn-cert.cni.es/certificados).

8.1 Pla d'adequació

El Pla d'Adequació serà el punt inicial pel procés d'implantació de l'ENS i estarà composat per les següents actuacions:

- Elaboració de la Política de Seguretat i la normativa corresponent.
- Identificació dels serveis presents i categorització dels sistemes de l'entitat contractant, amb la valoració de la informació tractada.

- Realització d'un anàlisi de riscos.
- Elaboració de la Declaració d'Aplicabilitat.
- Desenvolupament d'un Pla de Millora de la seguretat a partir de les deficiències que s'hagin detectat.

El Pla d'adequació identificarà tant les persones i òrgans responsables involucrats en la futura implantació com en la definició de les mesures de seguretat a implantar, conjuntament amb les seves fites i els recursos necessaris per a dur-les a terme.

8.1.1 Política de Seguretat i normativa interna

La Política de Seguretat es sublimarà en un document d'alt nivell, mitjançant el qual, l'entitat definirà el seu compromís al respecte de la seguretat de la informació i els serveis que pugui prestar. En aquesta política es descriuran els mecanismes implementats per a una gestió continuada de la seguretat així com els seus responsables. Aquests continguts, sense menyscapte de ser ampliats, seran els següents:

- Compromís de compliment de la totalitat del Real Decret de l'ENS (principis bàsics i requeriments mínims).
- Marc legal i regulatori.
- Indicadors de compliment de la normativa de protecció de dades.
- Rols de seguretat i funcions designades. Com a mínim seran els següents:
    - Responsable de la Informació, i Responsables dels Serveis per a tots aquells sistemes que siguin operats directament per l'entitat contractant.
    - Responsable de Seguretat i Responsable de Sistema, estructura del comitè de seguretat i les seves funcions o, segons el cas, l'estructura simplificada que preveu el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad (PCE-RES).
- Detall dels mecanismes implementats per a la resolució dels conflictes entre els diferent rols assignats.
- Indicació sobre com es desenvoluparà, les revisions previstes tot indicant la periodicitat de les mateixes.

La Normativa Interna serà un compendi de normes de caràcter intern que s'hauran definir i instaurar de cara al comportament dels usuaris dels sistemes presents a l'entitat contractant.

8.1.2 Identificació dels serveis presents i categorització dels sistemes de l'entitat contractant, amb la valoració de la informació tractada.

L'empresa adjudicatària haurà de categoritzar els sistemes d'informació de l'ens contractant i realitzar una declaració d'aplicabilitat d'acord amb la categorització realitzada. Qualsevol canvi que es realitzi en la categorització dels sistemes s'haurà de reflectir en la declaració d'aplicabilitat, així com en el pla de millora de la seguretat.

Amb aquesta identificació es procedirà a identificar la informació tractada i la seva tipologia, així com els serveis prestats per l'entitat contractant i es procedirà a la seva valoració tal i com estableixen els principis de l'Annex I de l'Esquema Nacional de Seguretat.

En cas d'adherir-se a un perfil de compliment específic, l'adequació es realitzarà mitjançant microCeENS, i es seguirà la metodologia i plataforma prevista a tal efecte.

8.1.3 Anàlisi de riscos

L'empresa adjudicatària farà les tasques necessàries per a assegurar que es compleixen les mesures del marc operacional segons el definit en l'article 14 i Annex II de l'ENS per a la categoria establerta pel sistema.

En base a això, l'anàlisi de riscos es desenvoluparà sota la metodologia MAGERIT – metodologia d'anàlisi i gestió de riscos el·laborada pel "*Consejo Superior de Administración Electrónica*"-, determinant els riscos que comporten els sistemes d'informació involucrats. Les eines a utilitzar seran les previstes sota aquesta metodologia: PILAR sota qualsevol de les seves versions, a més de la plataforma INÉS en cas de ser online.

En base als riscos, es desenvoluparan un seguit de tasques tècniques i mesures de protecció per part de l'empresa adjudicatària per a assegurar que es compleixen les mesures de protecció segons el definit en la declaració d'aplicabilitat. A títol indicatiu i no exhaustiu, s'assenyalen les tasques requerides en aquest àmbit de treball:

- Implantar un registre de e/s d'equipament.
- Realitzar l'etiquetatge de suports.
- Fer tasques de conscienciació i formació.
- Assegurar la inclusió i compliment dels requisits de seguretat en els aplicatius a desenvolupar.
- Verificar ús correcte dels certificats digitals.
- Determinar i revisar els perfils de seguretat a implantar en cada tipus de component dels sistemes d'informació.

En cas d'adherir-se a un perfil de compliment específic, l'adequació es realitzarà mitjançant microCeENS, i es seguirà la metodologia i plataforma prevista a tal efecte.

8.1.4 Elaboració de la Declaració d'Aplicabilitat.

En resposta al resultat de l'anàlisi de riscos, l'empresa a contractar haurà d'elaborar una relació de les mesures recollides a l'ENS que són d'aplicació als sistemes de l'entitat contractant.

Per a tal qüestió, es recorrerà a tot allò detallat a l'Annex II de l'ENS, havent de justificar la no aplicació de totes aquelles mesures que no puguin ser aplicades degut a la casuística de l'entitat.

La Declaració d'aplicabilitat s'haurà de reflectir en un document aprovat pel Responsable de Seguretat designat i estarà basat en el perfil de categoria o perfil de compliment específic que correspongui

En cas d'adherir-se a un perfil de compliment específic, l'adequació es realitzarà mitjançant microCeENS, i es seguirà la metodologia i plataforma prevista a tal efecte.

8.1.5 Pla de millora

L'empresa adjudicatària farà tasques d'anàlisis i consultoria que permetin verificar el correcte compliment dels aspectes tant generals com específics de l'ENS, es detectaran les deficiències que tingui el sistema i es realitzarà la proposta de millores que es veuran reflectides en un pla d'acció. A títol indicatiu i no exhaustiu, s'assenyalen les tasques requerides en aquest àmbit de treball:

- Realitzar l'anàlisi de vulnerabilitats de webs i aplicacions.
- Realitzar proves d'intrusió en sistemes.
- Hacking ètic.
- Assessoria en contractació i desplegament de components de seguretat (*web application firewall*, antivirus de passarel·la, antivirus de servidors, sistema de gestió d'incidents de seguretat, sistemes de xifratge de suports, sistemes de seguretat física, etc.).
- Millora contínua. Es faran tasques sistemàtiques orientades a la millora contínua de l'adaptació a l'ENS.

El Pla de Millora haurà de mostrar quines deficiències millora en cada actuació, amb el seu termini d'execució i les dates d'inici i fi, i el cost aproximat que suposarà.

En cas d'adherir-se a un perfil de compliment específic, l'adequació es realitzarà mitjançant microCeENS, i es seguirà la metodologia i plataforma prevista a tal efecte.

8.2 Tasques relacionades amb la protecció de dades.

L'empresa adjudicatària realitzarà les tasques de suport necessàries per l'adaptació de l'ens contractant al RGDP i la normativa derivada. A tel efecte, s'haurà de donar compliment als requeriments previstos en el propi ENS en el seu Annex II, segons la guia CCN-STIC 808. Amb caràcter indicatiu i no exhaustiu es realitzaran les següents tasques:

- Anàlisi situació actual. L'empresa adjudicatària realitzarà una anàlisi de la situació actual respecte als requisits marcats en matèria de protecció de dades.
- Full de ruta. L'empresa adjudicatària establirà les deficiències entre la situació actual i la situació requerida per a adaptar-se a la normativa de protecció de dades i realitzarà el full de ruta amb les accions necessàries per a adaptar-se.

- Execució de tasques d'adaptació. L'empresa adjudicatària farà les tasques necessàries per a adaptar-se als requisits definits en matèria de protecció de dades.
- Col·laboració amb el Delegat de Protecció de Dades de l'ens contractant. L'empresa adjudicatària assumirà l'assessorament sobre les funcions del subdelegat de protecció de dades de l'ens contractant, si s'escau, segons la normativa vigent.
- Millora contínua. Es faran les tasques necessàries per a establir un cicle de millora contínua en matèria de protecció de dades.

8.3 Governança de la seguretat.

L'empresa adjudicatària farà les tasques necessàries per a poder realitzar una governança eficient de la seguretat i adaptació al RGPD, així com el compliment i gestió de la informació requerida per les aplicacions actuals i futures que el CCN-CERT posa a la disposició de les administracions públiques. Amb caràcter indicatiu i no exhaustiu es faran les següents tasques:

- Emplenar la informació requerida en l'informe anual de seguretat per l'aplicació INES o qualsevol que la substitueixi.
- Realitzar la gestió d'incidents. Incloent la gestió a través de l'aplicació LUCIA o la corresponent de l'Agència de Ciberseguretat de Catalunya.
- Revisar i mantenir actualitzat el sistema d'indicadors.
- Mantenir i actualitzar el pla d'adequació

8.4 Gestió del canvi i formació.

L'empresa adjudicatària realitzarà la gestió del canvi i formació necessària en temes de seguretat i protecció de dades. La formació serà, com a mínim, la requerida per la normativa d'aplicació. S'inclou formació específica en l'àmbit de l'ENS i la protecció de dades.

- Es faran les tasques necessàries de difusió i formació a tots els usuaris de l'ens contractant en temes de seguretat i protecció de dades. L'empresa adjudicatària aportarà un Pla de Comunicació i un Pla de Formació, en aquest sentit, que inclourà com a mínim les accions plantejades a continuació, i que serà aprovat prèviament pel Responsable del Contracte.
- Es realitzarà formació al personal designat per l'entitat contractant durant 15 dies hàbils presencials, almenys, cada any del contracte, tant en temes de seguretat com en protecció de dades.

8.5 Acompanyament a l'obtenció de la conformitat.

L'empresa adjudicatària acompanyarà a l'entitat contractant en el procés d'obtenció de la certificació de conformitat amb l'ENS. Amb caràcter indicatiu i no exhaustiu es faran les següents tasques:

- Pre-auditoria. L'empresa adjudicatària haurà de realitzar una auditoria prèvia interna que permeti analitzar el grau d'implantació i prepari l'entitat per a l'auditoria d'obtenció de la conformitat. A partir del resultat de la mateixa s'establiran les tasques a realitzar per a resoldre les no conformitats detectades i els punts de millora.
- Suport al procés d'auditoria. L'empresa adjudicatària haurà de donar el suport necessari en el procés d'auditoria per a assegurar que aquesta es pugui realitzar en les millors condicions, ajudarà en les gestions amb l'empresa certificadora i acompanyarà presencialment en el procés d'auditoria externa.
- No conformitats. Una vegada realitzada la pre-auditoria i l'auditoria de conformitat, s'analitzarà i establirà el pla de treball per a resoldre les no conformitats detectades, així com els punts de millora o altres aspectes que es considerin en aquests processos. Aquest pla de treball s'haurà de dur a terme per part de l'empresa adjudicatària.

Pel seguiment del servei es nomenaran els interlocutors necessaris a nivell d'àrees funcionals que l'entitat contractant cregui oportunes a fi de poder participar en les reunions adjacents al projecte i que portaran a un informe final amb anàlisi de les no-conformitats respecte el model de seguretat proposat per l'ENS.

L'ens públic rebrà un pla de formació i sensibilització, generat per l'adjudicatari, per al personal implicat en els procediments afectats per l'ENS, donant èmfasi a la formació impartida al personal tècnic que gestionarà la seguretat informàtica i que vetllarà pel seu seguiment i compliment.

En tot cas, aquests treballs representen una especificació de la "**Guia CCN-STIC 806 – Pla d'adequació a l'ENS"**.

8.6 Lliurables

Com a resultats dels treballs realitzats, l'empresa adjudicatària haurà de lliurar a l'ens contractant com a mínim els següents lliurables, durant l'execució del contracte.

Tasques relacionades amb l'ENS

- Documentació generada en les tasques d'ENS.
- Plans d'adequació i informes de seguiment.
- Informes de tasques realitzades.

Tasques relacionades amb la protecció de dades

- Documentació generada en les tasques de protecció de dades.
- Plans d'adequació i informes de seguiment.
- Informes de tasques realitzades.

Governança de la seguretat

- Documentació generada en les tasques de governança.

Gestió del canvi i formació

- Pla de formació detallat. Independentment del pla de formació proposat en la proposta tècnica, el pla de formació final s'haurà de consensuar i aprovar per part de l'ens contractant.
- Pla de comunicació detallat, amb les accions de comunicació i difusió a realitzar.
- Informes de les accions de comunicació i formació realitzades (sessions, assistents, contingut, incidències, enquesta de satisfacció...).
- Documentació utilitzada per a realitzar les accions de comunicació i formació.

Acompanyament a l'obtenció de la conformitat

- Pre-auditoria.
- Plans de resolució de no conformitats i punts de millora.
- Documentació de seguiment dels plans de resolució.

La documentació generada durant l'execució del contracte és de propietat exclusiva de l'ens contractant sense que l'adjudicatari pugui conservar-la, ni obtenir còpia de la mateixa o facilitar-la a tercers sense l'expressa autorització de l'ens públic, que la donaria si és el cas prèvia petició formal del contractista amb expressió de la fi. La documentació es lliurarà en format editable i en format pdf.

A la presentació dels resultats s'intentarà diferenciar clarament els àmbits de l'Esquema Nacional de Seguretat i del compliment de normativa en matèria de protecció de dades de caràcter personal.

8.7 Equip de treball

L'empresa de consultoria adjudicatària aportarà el personal que sigui necessari per al millor compliment de l'objecte del contracte. Aquest personal comptarà amb les competències, coneixements i qualificacions necessaris segons la vigent, i posterior si n'hi hagués, normativa sobre aquest tema; i la seva designació haurà de ser aprovada pel Responsable del Contracte, qui al llarg del desenvolupament del mateix podrà sol·licitar el seu relleu o substitució.

El personal de l'empresa adjudicatària que desenvolupi el servei objecte d'aquesta contractació actuarà, juntament amb els recursos humans designats per l'entitat, en cadascuna de les fases que esdevinguin necessàries.

Els licitadors hauran de descriure en les seves ofertes l'equip de treball proposat per a la prestació del servei, basant-se en els perfils detallats en aquest apartat. En general, hauran de presentar:

- Perfils que formen part de l'equip de treball.
- Funcions específiques de cadascun dels perfils dins de l'equip.
- Currículum dels perfils proposats, així com dedicacions i funcions d'aquests.
- Si és el cas, còpies de les certificacions sol·licitades.

Els perfils que realitzin els serveis detallats en el present plec, hauran d'adequar-se als proposats per l'adjudicatari. Aquests perfils seran els següents:

Cap de projecte:

- Direcció, seguiment i control del projecte.
- Generació de la documentació de control.
- Revisió de la documentació generada per l'equip de treball.
- Coordinar i organitzar les relacions de l'equip de treball amb els responsables de l'entitat en forma de reunions periòdiques de seguiment.

Un consultor expert en adequació a l'ENS:

- Direcció i execució de les tasques tècniques i operatives.
- Documentació tècnica.
- Seguiment i correcció dels plans d'acció.
- Propostes de millora contínua.
- Direcció de la governança de seguretat.
- Coordinació amb el DPD de l'entitat contractant.

Tots els perfils hauran de tenir com a mínim 3 anys d'experiència en projectes similars.

La falsedat en el nivell de coneixements tècnics dels perfils que s'incorporin, deduïda del contrast entre la informació especificada en l'oferta i els coneixements reals demostrats en l'execució dels treballs, implicarà la substitució del recurs per un altre en un termini no superior a 15 dies laborables.

A més, en el cas que sigui necessari realitzar una substitució d'un recurs, les empreses es comprometen a reemplaçar aquest recurs per un altre d'igual perfil en un termini no superior a 15 dies laborables.

9 LOT 6: SERVEIS DE FORMACIÓ I CONSCIENCIACIÓ EN CIBERSEGURETAT AD-HOC

Per tal d'impulsar una cultura de ciberseguretat, les entitats locals tenen la necessitat de disposar i executar un pla de formació on s'identifiquin les necessitats de les habilitats i coneixements en ciberseguretat per a cada lloc de treball.

L'empresa adjudicatària, definirà les accions formatives necessàries per la capacitació i conscienciació per la totalitat de la plantilla de l'administració pública que permeti dissenyar i desplegar les fases d'actuació del Pla de conscienciació i formació usant diferents nivells de continguts prèviament definits, amb una personalització i adaptació sobre continguts existents.

Les activitats pràctiques de conscienciació han de poder incloure la realització de campanyes simulades d'estafes digital utilitzant els mitjans disponibles (correu electrònic, Intranet, SMS..).

L'objectiu dels aprenentatges de la formació ha de ser capacitar les persones treballadores a utilitzar les eines de ciberseguretat que els permet garantir la confidencialitat de la informació que utilitzen durant la seva activitat professional (amb especial èmfasi en el treball a distància), així com conèixer en detall els protocols i metodologies que l'ens local ha adoptat per a garantir la seguretat i la privacitat de la informació.

En aquest sentit, la formació en Ciberseguretat ha de tenir com a objectius d'alt nivell l'assoliment, per part de l'alumnat, de les següents capacitats, sense menyscapte d'ampliar l'abast del coneixement impartit a voluntat de l'ens contractant:

- Autoprotegir-se en l'ús de les xarxes.
- Protegir-se del *malware*.
- Protegir-se del *phishing* i els enganys d'Internet.
- Millorar la seguretat de les eines ofimàtiques i missatgeria.
- Evitar el *hacking* dels sistemes d'informació.

El pla de formació s'ha d'adreçar a persones treballadores que vulguin protegir documents confidencials i conèixer en detall els sistemes i metodologies a seguir per garantir la seguretat i la privacitat de la informació.

En aquesta línia, s'han de presentar les mesures de seguretat TIC que hi ha configurades a l'organització (eines i dispositius) a més d'indicar com es garanteix la protecció de les dades de l'ens local i les persones usuàries dels serveis informàtic del municipi.

El contingut s'ha de treballar mitjançant lectures, vídeos, exercicis i qüestionaris els protocols a seguir per millorar les pràctiques en ciberseguretat i ha de donar suport mitjançant serveis de transcripció per a persones sordes.

L'adjudicatari proporcionarà material de formació i conscienciació, i s'encarregarà de la seva actualització.

9.1 Nivells de formació

L'empresa adjudicatària definirà les accions formatives necessàries per la capacitació i conscienciació de la totalitat de la plantilla de l'ens contractant utilitzant diferents nivells de contingut prèviament definits, amb una personalització i adaptació sobre els continguts que es descriuran a continuació.

9.1.1 Nivell bàsic de formació

Els continguts de formació i conscienciació considerats de nivell bàsic en ciberseguretat que s'adrecen a tots els empleats públics precisen d'una identificació/validació contínua de l'Agència de Ciberseguretat i s'estructuren en uns mòduls (del conegut com Curs de Ciberseguretat i Protecció de Dades en el lloc de treball) i que com a referència es disposen de la següent estructura de continguts:

1. El lloc de treball

   - Coneixement i presa de consciència del hàbits i accions quotidianes que poden afectar la seguretat de la informació.
   - Conscienciació de les bones pràctiques en l'ús de comptes personals i el tracte de les credencials d'accés.
   - Foment de l'ús del bloqueig de l'estació de treball.
   - Coneixement dels diferents nivells de confidencialitat de la informació.
   - Coneixement dels punts principals de la política de seguretat de la informació
   - Coneixement de bones pràctiques per atenció ciutadana per mitjans digitals.

2. Contextos de seguretat

   - Conscienciar sobre el rol actiu dels treballadors per afavorir la seguretat als equipaments públics.
   - Conèixer mesures de protecció en el marc del treball a distància: ús de VPN o xarxes wi-fi.
   - Conèixer eines autoritzades per a videoconferències.
   - Conèixer bones pràctiques amb eines d'e-administració: per exemple, IdCat.

3. Prevenció de riscos

   - Conèixer les principals tècniques de ciberatacs referides a les principals amenaces en el món local: malware-ransomware, phishing...
   - Aprendre a identificar les peculiaritats de cada eina d'atac en el context d'eines d'ofimàtica/ missatgeria usat.
   - Conèixer els protocols d'organització i tècnics en cas de ser víctimes d'un atac exitós.

- Conèixer les principals mesures per fer front als principals ciberincidents i eines que asseguren l'accés a les aplicacions.

4. Tractament de dades personals

- Conèixer el concepte de dades confidencials en el marc de l'Administració pública.
- Conèixer les bases i el marc normatiu de la LOPDGDD.
- Conèixer les tipologies de dades i les mesures de protecció associades.
- Conèixer com aplica l'Esquema Nacional de Seguretat (ENS) i els perfils de compliment previstos al món local.
- Conèixer les principals formes de xifrat de la informació.

5. Evitar pèrdues de dades i complir les normes:

- Ser conscient de la importància de notificar els incidents de seguretat i analitzar alguns casos.
- Ser conscient de la destrucció de la informació obsoleta i conèixer el millor sistema per fer-ho.
- Conèixer mesures de seguretat basades en les còpies de seguretat i ser conscients de la importància.
- Conèixer riscos de les memòries USB externes i els dispositius mòbils.

Es recomana la modalitat formativa en un entorn virtual d'aprenentatge propi o d'un tercer (Diputacions o Consells comarcals que disposin del curs).

Aquesta formació ha de comportar les següents accions formatives que l'empresa adjudicatària hauria de proposar, associades de cara a l'aprofitament i consolidació dels coneixements impartits:

- Dinamització del curs, amb dedicacions temporals de fins a 5 hores
- Tallers de sensibilització basats amb dossiers didàctics sobre els continguts bàsics
- Difusió i comunicació de píndoles (infogràfiques) referents a aquest contingut estructurat, per acompanyar el contingut autoformatiu, en intranets, correu corporatiu...
- Desenvolupament d'exercicis d'habilitat
- Exercicis pràctics on es simulin casos d'ús de les situacions exposades en el curs
- Qüestionari/quiz/test que permeti detectar aprofitament, comprensió i avaluació del contingut desenvolupat al curs

9.1.2 Nivell avançat de formació

Els continguts de formació i conscienciació considerats de nivell avançat en ciberseguretat estaran adreçats a empleats públics que han de desenvolupar capacitats tècniques o legals en relació a la matèria a fi de comptar amb un ventall més ampli de coneixements i habilitats.

En els darrers anys, l'Àrea de Cultura de Ciberseguretat de l'Agència, conjuntament amb entitats municipalistes i les Diputacions, han desplegat un catàleg de cursos de ciberseguretat d'aquest nivell que poden servir de base per la reutilització per a què l'empresa adjudicatària hagi de fer una adaptació mínima però que no representi un redisseny significatiu del contingut.

Aquestes capacitats s'adaptaran en cursos que tinguin una dedicació mínima de 5 hores i podran estar estructurats en els següents temes:

- Model d'anàlisi de riscos de ciberseguretat de la protecció de dades.
- Anàlisi i gestió de riscos de sistemes d'informació.
- Aproximació al µCeENS (adequació per a l'obtenció de la Certificació de Conformitat).
- Seguretat en entorn Cloud.
- Hàcking ètic: eines d'auditoria i OWASP.
- Resposta a incidents.
- Bastionat de xarxes i sistemes.
- Gestió de les vulnerabilitats.
- Seguretat en les aplicacions web.

Es recomana la modalitat formativa mixt, presencial i en entorn virtual d'aprenentatge propi o d'un tercer. I també que combini contingut teòric dels conceptes que es desenvolupen i pràctic amb ús d'eines o casos d'ús que apliquen al món local. En aquest sentit és exigible una avaluació final que permeti documentar l'aprofitament i aplicabilitat en les entitats del món local on provenen els usuaris/es sol·licitants del curs.

L'empresa adjudicatària haurà de fer propostes de nous continguts de cursos però requereix una validació de l'Agència de Ciberseguretat per a poder ser també compartida en el catàleg de cursos de ciberseguretat disponibles pel món local.

9.2 Itineraris de perfils especialitzats de ciberseguretat

L'empresa adjudicatària ha d'oferir una proposta de cara a col·laborar/participar en l'activitat que desenvolupa la Ciberacadèmia de l'Agència de Ciberseguretat, per desplegar diferents itineraris formatius que s'adrecen específicament als tècnics del món local que volen aprofundir i ampliar coneixements, en habilitats i competències, requerit per exemple per una promoció interna.

Els perfils d'itineraris previstos a desenvolupar cursos es troben descrits al document "European Cybersecurity Skills Framework (ECSF)" de "*The European Union Agency for cybersecurity" (ENISA)*.

Els continguts formatius organitzats van des de fonaments de ciberseguretat fins a un desenvolupament operatiu d'eines específiques. Aquests itineraris tindran cursos en diferents nivells que permeten:

- N1: Conversar /iniciació.
  - Es disposa del coneixement general sobre la competència i les seves implicacions en la seguretat podent realitzar tasques senzilles relacionades.
- N2: Fer / Creació i execució d'accions.
  - Té coneixement suficient sobre processos concrets i com la competència s'implementa en els sistemes, és capaç d'executar les tasques pròpies del lloc de treball i a més segueix metodologies i processos de treball
- N3: Modificar / Participació en els canvis.

Disposa de coneixements avançats sobre la majoria de processos de l'abast de la competència, configuracions i integracions amb la resta de sistemes relacionats. Treball autònom.

- N4: Liderar / Presa de decisions.
  - El coneixement profund de la competència també a nivell teòric i de bones pràctiques, dissenya nous processos segurs des de la seva concepció, modifica metodologies existents i estableix noves polítiques i estratègies en el seu camp.

En aquest sentit, es requeriran formadors que puguin desenvolupar els cursos en sessions teòriques (síncrones/asíncrones en streaming), en la definició d'activitats ad hoc o en el desenvolupament o correcció de pràctiques pels alumnes, en entorns presencials o en espai virtual.

9.3 Altres seccions formatives complementàries

L'empresa adjudicatària realitzarà proposta d'activitats pràctiques de conscienciació i complementàries als nivells i itineraris descrits amb anterioritat, que es vincularan al propi Pla de conscienciació i formació previst, com ara:

- Campanyes simulades d'estafes digital utilitzant els mitjans disponibles per l'ens local.

- Esquemes de gamificació o sensibilització per a les persones que desenvolupen funcions directives del món local.
- Elements comunicatius que involucren la participació de la ciutadania com a usuaris actius per la millora en ciberseguretat dels serveis prestats per l'ens local.

Aquestes activitats també requeriran la inscripció i registre en un catàleg d'activitats compatibles.

10 LOT 7: SERVEIS DE CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM)

El present lot de l'acord marc té per objecte la contractació d'un servei de CSIRT (*Computer Security Incident Response Team*) que tindrà com a missió la gestió i resposta a incidents de ciberseguretat, així com a l'anàlisi forense digital per a investigar i comprendre aquests incidents. Aquest servei té com a objectiu minimitzar l'impacte dels incidents, restaurar les operacions normals i proporcionar informació crítica per a millorar les defenses de seguretat de les entitats contractants.

El servei de CSIRT haurà de coordinar-se amb les capacitats de resposta en incidents del SOC que doni suport a l'entitat, bé sigui el SOC Operatiu de la mateixa entitat o el de l'Agència de Ciberseguretat.

Amb el funcionament d'aquest servei, els objectius a complir a nivell organitzatiu són els següents:

- Reducció de l'Impacte dels Incidents: Una resposta ràpida i efectiva, des del minut zero, minimitza el mal causat pels incidents de seguretat.
- Millora de la Seguretat: L'anàlisi forense proporciona informació crítica per a enfortir les defenses i prevenir futurs atacs.
- Compliment Normatiu: Assegura que l'organització compleixi amb les normatives i regulacions de protecció de dades.
- Recuperació Ràpida: Dota a l'ens contractant de procediments dedicats ben definits que permeten una ràpida restauració de la operativa normal.

10.1 Característiques del servei

El servei de CSIRT ofert per l'empresa contractada haurà de tenir, sense menyscapte d'ampliar el catàleg, les següents característiques:

- Preparació (aquesta fase es preveu en cas de contractar el servei abans de patir un incident de ciberseguretat)
  - Identificació i documentació de la informació de context de la entitat, potencialment necessària durant la gestió d'un incident.

  - Avaluació de la entitat i la seva infraestructura, des del punt de vista de la gestió d'un incident, per tal de mesurar i millorar les capacitats de resposta disponibles.
  - Manteniment de les matrius d'escalat rellevants en cas d'incident.
  - Elaborar un procediment de resposta a incident segons l'ENS establint el protocol de comunicació en cas d'incident (equip de resposta).
  - Capacitat d'integració del servei en un Pla de Continuïtat de Negoci basat en l'ENS.
- Monitoratge i Detecció (aquesta fase es preveu en cas de contractar el servei abans de patir un incident de ciberseguretat)
  - En cas el cas que sigui necessari, desplegament puntual d'eines de detecció, resposta i amb capacitat forense, tipus EDR, per guanyar visibilitat i capacitat de detecció i resposta a amenaces durant l'incident.
- Resposta a Incidents
  - Disponibilitat d'un Equip de Resposta a Incidents (IRT) especialitzat 24/7.
  - Determinació de la gravetat dels incidents.
  - Desenvolupament i implementació d'un Pla de Resposta a Incidents.
  - Procediments i actuació per a la contenció d'amenaces tan bon punt sigui adequat i evitar així la propagació de l'incident aïllant els sistemes compromesos i/o bloquejant accessos no autoritzats.
  - Mesures per a l'erradicació d'amenaces identificades a fi de netejar els sistemes afectats i assegurar la seva integritat.
  - Capacitat de coordinació amb altres equips i parts interessades durant incidents.
  - Recerca activa d'atacants dintre dels sistemes de l'ens contractant.
- Anàlisi Forense Digital
  - Recol·lecció d'evidències: Es recopilaran evidències digitals de tots els sistemes pels que sigui necessari de manera meticulosa per a assegurar la seva integritat i validesa legal.
  - Anàlisi forense: Utilitzant eines avançades, s'analitzarà l'evidència recopilada per a determinar l'origen, la metodologia i l'impacte de l'atac. Aquesta anàlisi inclou la identificació de vulnerabilitats explotades i la reconstrucció de la cronologia de l'incident.
  - Elaboració d'informes forenses detallats i comprensibles.
- Mitigació i recuperació
  - Procediments per a la restauració de sistemes: Es duran a terme procediments per a restaurar els sistemes afectats al seu estat operatiu normal de manera segura. Això inclou la reinstal·lació de sistemes, l'aplicació

de pegats i l'actualització de configuracions de seguretat que siguin necessaris.
    - Assegurament de la continuïtat del negoci durant i després d'un incident.
    - Implementació de solucions per a prevenir la recurrència d'incidents, que poden incloure la millora de configuracions i l'aplicació de solucions tecnològiques addicionals.
- Revisió post-incident i millora contínua
    - Avaluació post-incident: Es realitza una avaluació detallada del maneig de l'incident per a identificar lliçons apreses i àrees de millora. Això inclou la revisió de l'efectivitat de la resposta i la identificació de qualsevol bretxa en els procediments de seguretat.
    - Creació d'informes: Els investigadors hauran d'elaborar un informe on es detalli l'event de seguretat tractat, i si s'escau, la identificació dels atacants. En aquests lliurables s'entregaran també les recomanacions de cara a l'actualització de polítiques i procediments.
    - Assessoria legal en temes relacionats amb la ciberseguretat, gestió de la conformitat amb lleis i regulacions, suport en la preparació d'informes i evidències per a procediments legals.
    - Avaluació i gestió de riscos de seguretat, assegurament del compliment amb normatives i estàndards de seguretat.
    - Desenvolupament i execució de plans de recuperació de desastres, assegurament de la continuïtat del negoci durant i després d'un incident.

10.2 Compliment Normatiu i Confidencialitat.

El servei de CSIRT proposat per part del l'empresa haurà de proporcionar protecció legal en base al compliment de les normatives legals i estàndards. En base a aquest precepte, haurà de complir amb les següents normatives i estàndards:

- Normativa de Protecció de Dades Personals (GDPR)
- Compliance Corporatiu: Totes les operacions realitzades al servei de CSIRT hauran d'estar alineades amb les polítiques de seguretat, confidencialitat i privacitat de l'ens contractant.
- L'empresa adjudicatària haurà de garantir que els seus sistemes d'informació que sustenten els serveis prestats en ser adjudicatàries de contractes basats del present lot apliquen les mesures de seguretat establertes al Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS). L'adjudicatari haurà de disposar d'un certificat d'acompliment de l'Esquema Nacional de Seguretat de nivell MIG, i aportar el certificat corresponent i que figurar en la web del CNI (https://gobernanza.ccn-cert.cni.es/certificados).

10.3 Modalitat de prestació del servei.

L'adjudicació del servei CSIRT es formalitzarà mitjançant un **contracte de serveis per subscripció** que cobreixi totes les necessitats de preparació, monitoratge, resposta a incidents, anàlisi forense i recuperació post-incident. Aquest contracte, establert a llarg termini (anual o plurianual), garantirà la cobertura dels serveis CSIRT per a l'entitat contractant, assegurant la disponibilitat 24x7 del servei i una resposta immediata davant qualsevol incident de ciberseguretat. Aquest model resulta especialment adequat per a entitats amb requisits elevats de seguretat i necessitat de resposta àgil.

L'adjudicatari haurà d'oferir la contractació del servei amb la modalitat de pagament de serveis per subscripció segons les necessitats específiques de l'entitat:

> Un contracte de subscripció anual o plurianual que haurà de cobrir tots els serveis de preparació, monitoratge, resposta a incidents, anàlisi forense i recuperació post-incident. Aquest tipus de contracte garantirà la disponibilitat contínua del servei i oferirà al CSIRT un coneixement en profunditat de l'entitat, millorant la qualitat i rapidesa de la resposta.

Les empreses licitadores d'aquest servei CSIRT hauran d'oferir un catàleg de tarifes segons la mida de l'entitat i el nivell dels incidents que es cobreixen. Aquest catàleg, consta de dos nivells d'incidència i es segmenta segons el nombre de treballadors de l'entitat.

Catàleg de tarifes proposat

El catàleg es basa en una estructura que combina:

- **Volum de l'entitat contractant** segons el nombre de treballadors:
  - Menys de 15 treballadors.
  - Entre 15 i 50 treballadors.
  - Entre 50 i 100 treballadors.
  - Entre 100 i 500 treballadors.
  - Més 500 treballadors.
- **Nivell de complexitat de l'incident** gestionat:
  - Nivell 1: Incidents lleus i moderats

    Aquest nivell inclou incidents que afecten serveis no crítics però que poden tenir impacte operatiu significatiu, amb potencial d'escalar. Inclou, per exemple, infeccions per malware en estacions de treball o anomalies de seguretat en xarxes internes que impacten a un petit nombre de dispositius o usuaris. Inclou problemes com intents de phishing detectats i atacs de baixa complexitat que no han compromès sistemes.

  - Nivell 2: Incidents crítics

Aquest nivell inclou els incidents de nivell 1 i també els incidents amb afectació greu per a la infraestructura crítica o que comprometen dades sensibles o operacions essencials o que generen un impacte reputacional significatiu. Inclou atacs de ransomware, robatori de dades, accés no autoritzat a sistemes o denegacions de servei o sabotatge digital que impedeixen la continuïtat operativa.

Tarifes de subscripció

A continuació es proposen diferents tarifes ajustades a les dimensions del municipi, garantint un model escalable i adequat a les necessitats específiques de cada entitat que les empreses licitadores hauran d'oferir:

Nivell d'incidència	Tipus d'entitat	Tarifa proposada (€/any)
Nivell 1: Incidents lleus i moderats	< 15 treballadors	
	15 – 50 treballadors	
	50 – 100 treballadors	
	100 – 500 treballadors	
	> 500 treballadors	
Nivell 2: Incidents crítics	< 15 treballadors	
	15 – 50 treballadors	
	50 – 100 treballadors	
	100 – 500 treballadors	
	> 500 treballadors	

Servei addicional de consultoria post-incident i millora contínua

Addicionalment a les tarifes de subscripció s'oferirà un preu de servei de consultoria post incident. Aquest servei complementari es podrà requerir fora de la cobertura bàsica de resposta a incidents contractada com a subscripció:

Aquest servei addicional es centra en l'avaluació i millora dels processos de seguretat després de la resolució d'un incident per evitar que incidents similars es repeteixin. Inclou l'anàlisi del maneig global de l'incident per identificar àrees de millora, l'avaluació de l'eficàcia de la resposta, la rapidesa de la detecció i la capacitat de recuperació, i es proposen millores per augmentar la seguretat i evitar possibles futurs incidents.

El preu del servei de consultoria serà per sessió de revisió post-incident (amb una durada màxima de 4 hores/sessió).

10.4 Organització del servei

Estructura organitzativa

Per part de l'entitat, s'establirà la figura del Responsable del Servei, que serà l'encarregat de supervisar i coordinar l'actuació i la relació amb l'empresa que desenvolupa el servei.

Per part de l'adjudicatari, de la mateixa manera, s'establirà un Responsable del Servei, que serà el Director de Seguretat de la Informació (CISO) encarregat de la supervisió i coordinació, a més de garantir el compliment dels requisits, assignant els mitjans adequats per a la correcta prestació del servei.

Equip de treball

L'equip de CSIRT haurà d'estar compost per professionals altament qualificats i especialitzats per a gestionar eficaçment els incidents de ciberseguretat i dur a terme anàlisi forenses digitals.

La combinació de diverses especialitzacions permetrà una resposta integral i coordinada, assegurant la protecció dels actius digitals de l'organització contractant i la ràpida recuperació dels incidents de seguretat.

El licitador haurà d'incloure a la seva proposta els perfils següents:

- Gerent de Resposta a Incidents
  - Coordinació i lideratge de l'equip de resposta a incidents, i desenvolupament del pla de resposta a incidents.
- Un analista Forense Digital
  - Recol·lecció i preservació d'evidències digitals, realització d'anàlisi forense detallat i documentació de les troballes.

Tots els perfils hauran de tenir com a mínim 3 anys d'experiència en projectes similars.

Seguiment del servei

Un cop s'ha activat el servei per la detecció d'un incident de ciberseguretat, s'ha de fer un seguiment detallat, coordinat i transparent entre l'empresa que realitza el servei i l'entitat contractant, i ha d'arribar fins a la resolució de l'incident i implementació de mesures preventives.

En cas que, per qüestions relacionades amb la prestació del servei, fos necessari el desplaçament del personal de l'equip tècnic a qualsevol ubicació, aquest desplaçament aniria a càrrec de l'adjudicatari, sense que suposi un cost addicional.

En aquestes reunions es realitzarà un seguiment diari durant l'incident per a mantenir l'entitat contractant degudament informada del progrés de la investigació, les mesures preses i els passos a seguir. Els participants d'aquestes reunions seran, entre d'altres *stakeholders* rellevants, entre el CISO de l'empresa que realitza el servei i el CISO o responsable de l'entitat.

Les comunicacions podran ser efectuades per trucada telefònica, videoconferència, correus electrònics o presencials, sent en aquest últim supòsit possible que les reunions es duguin a terme a les instal·lacions de l'entitat si aquesta hi està d'acord i així ho demana.

El seguiment de l'execució del servei de CSIRT seguirà els següents passos a partir de la notificació inicial de l'incident:

- **Identificació i investigació**
  - Valorar les alertes i esdeveniments obtinguts a partir de la monitorització disponible o del SOC corresponent, per determinar l'existència d'un incident de seguretat.
  - Col·laboració coordinada amb d'altres CERTs o equips de ciberseguretat potencialment involucrats.
- **Contenció**
  - Aïllar sistemes compromesos per a prevenir la propagació de l'atac.
  - Utilitzar solucions temporals per a mitigar l'impacte immediat.
  - Coordinar amb altres equips d'IT o d'altres equips CERTs involucrats en la gestió de l'incident per a aplicar mesures de contenció.
- **Erradicació**
  - Realitzar una anàlisi exhaustiva per a trobar la causa arrel.
  - Eliminar tot rastre de l'amenaça de l'entorn.
  - Aplicar pegats i actualitzacions per a tancar les vulnerabilitats explotades.
- **Anàlisi forense i preservació d'evidències**
  - Recol·lecció i preservació d'evidències garantint en tot moment el manteniment de la cadena de custòdia per assegurar la seva validesa i integritat en possibles processos d'investigació o legals.
  - Anàlisi de logs, fitxers i sistemes compromesos.
  - Identificació de vectors d'atac i actors d'amenaça.
- **Recuperació**
  - Restaurar sistemes i dades a partir de còpies de seguretat segures.
  - Revisar i validar la integritat dels sistemes abans de posar-los en producció.
  - Implementar monitoratge continu per a assegurar que no hi hagi reinfeccions.
- **Lliçons apreses**
  - Realitzar una sessió de revisió post-incident amb tots els involucrats (*post-mortem*).

  - Documentar totes les etapes de l'incident i les accions preses.
  - Actualitzar el pla de resposta a incidents basat en els aprenentatges.
- **Report i compliment**
  - Generar informes detallats per a l'alta direcció i parts interessades.
  - Assegurar que totes les accions compleixen amb les regulacions aplicables.
  - Preparar comunicats públics si és necessari.

Horari del servei

El servei es prestarà per l'equip de treball especialitzat amb disponibilitat 24x7 (24 hores, de dilluns a diumenge) per proveir a l'entitat de resposta immediata a qualsevol incident detectat.

11 DEVOLUCIÓ DEL SERVEI

Segons el servei contractat i a determinació del contracte basat, en el cas que sigui d'aplicació la devolució del servei, sis (6) mesos abans de la seva finalització, l'empresa contractista haurà de presentar el pla de devolució del servei en qüestió que inclogui els mecanismes necessaris per tal de traspassar tota la informació relacionada amb el servei prestat.

La devolució del servei no tindrà un cost addicional per l'entitat i garantirà el traspàs del servei al nou adjudicatari. La durada màxima de la migració serà 1 mes des de la finalització del contracte.

La finalització del contracte exigirà també l'eliminació segura de tota la informació que s'hagi utilitzat per a l'execució del contracte.

Amb l'objectiu d'evitar que l'empresa contractista que estigui donant el servei pugui fer un ús indegut de la seva posició dominant, durant el procés de relleu per canvi de prestador del servei haurà de facilitar tota la informació tant tècnica com administrativa requerida per l'entitat contractant. Així mateix, l'empresa contractista no podrà dificultar el procés de canvi ni degradar els SLA pactats.

12 TERMINIS I MODEL DE RELACIÓ

Les empreses adjudicatàries de l'acord marc hauran de designar, durant els 15 primers dies de l'acord marc, els seus interlocutors:

- Un interlocutor únic per mantenir directament la interlocució amb el Consorci Localret. Tindrà les responsabilitats següents:

  - Vetllar pel compliment dels compromisos contractuals adquirits.
  - Seguiment i resolució de les incidències.
  - Enviament d'informes periòdics.

- Un centre de suport per a les entitats beneficiàries de l'acord marc:
  - Suport telefònic amb horari mínim de 9.00 h. a 14.00 h. en el lot 1 i de 9.00 h. a 18.00 h. en la resta de lots, a excepció d'aquells que han de tenir servei 24h (lots 3, 4 i 7).
  - Suport mitjançant una adreça de correu electrònic.
  - Eina de ticketing per comunicar incidències online si l'empresa l'ofereix.

En els contractes basats, l'empresa adjudicatària designarà una persona responsable que actuarà com a persona de contacte amb l'ajuntament o entitat, i serà la persona encarregada de planificar, gestionar i coordinar tot el procés d'adquisició i manteniment de les llicències o del servei gestionat de còpies.

Atenent a la naturalesa d'alguns dels serveis inclosos en aquest acord marc, es pot requerir que la seva prestació es dugui a terme en un horari 24x7 365 dies a l'any. En aquests casos, l'ampliació de l'horari quedarà indicat al posterior contracte basat.

Addicionalment, s'informa que els serveis inclosos en aquest acord marc poden implicar la necessitat de dur a terme guàrdies i feines fora d'horari. En aquest sentit:

- Es considera guàrdia la disponibilitat per atenció telefònica i actuació presencial en horari no laboral en el cas d'actuacions especials o que la importància de la incidència ho requereix.
- A petició expressa de l'entitat contractant, es podria demanar la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

Donat que els períodes de finalització dels contractes dels ajuntaments són diferents per a cadascun d'ells, caldrà gestionar la renovació dels serveis de llicenciament i manteniment dintre dels terminis imposats pel fabricant i sempre abans de la finalització del període de llicenciament.

13 FACTURACIÓ

La facturació serà en format digital e-FACT. El contractista haurà de facilitar la facturació electrònica a cada entitat i la plataforma a utilitzar serà FACe o e-FACTh o les que indiqui la normativa vigent. També es podrà entregar en format paper si les entitats així ho demanessin i sense cap cost addicional. A aquesta factura s'haurà d'annexar el document de detall que es correspongui amb l'import facturat. En cas de no annexar-se

el document de detall, les entitats podran retornar la factura per manca d'informació pel seu pagament.

14 DESPESES D'IMPULS

La clàusula CINQUANTENA del plec de clàusules administratives particulars (PCAP) estableix les despeses d'impuls, seguiment i coordinació dels contractes basats en el present acord marc que aniran a càrrec dels adjudicataris.

Eva Guijarro
Cap de l'Àrea de Transformació Digital i Tecnologies