CONVENI DE COOPERACIÓ HORITZONTAL ENTRE LA SINDICATURA DE COMPTES DE CATALUNYA I L'AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA PER A L'ASSISTÈNCIA TÈCNICA I LA IMPLEMENTACIÓ DE MESURES DE CIBERSEGURETAT PER A LA CONSECUCIÓ CONJUNTA DE LES FUNCIONS PÚBLIQUES QUE TENEN ATRIBUÏDES

A Barcelona, a data de signatura electrònica.

REUNITS

D'una banda, la **Sindicatura de Comptes de Catalunya**, representada per l'Il·lustre senyor Miquel Salazar Canalda, síndic major de la Sindicatura de Comptes de Catalunya, en virtut de les facultats que li confereix l'article 29 de la Llei 18/2010, del 7 de juny, de la Sindicatura de Comptes de Catalunya, amb NIF S5800001I (en endavant, "**Sindicatura**").

De l'altra banda, la Sra. Laura Caballero Nadales, Directora General de l'**Agència de Ciberseguretat de Catalunya**, designada per acord del Govern de la Generalitat de Catalunya Acord GOV/1/2025, de 7 de gener, amb les competències que li són atribuïdes en virtut de la lletra l) de l'article 12.3 dels Estatuts de l'Agència, aprovats per Decret 223/2019 de 29 d'octubre, amb NIF Q0802270I (en endavant "**l'Agència**").

L'Agència i Sindicatura podran ser denominades conjuntament com les "**Parts**" i individual i indistintament, quan correspongui, com la "**Part**".

Ambdues Parts es reconeixen recíprocament competència per a subscriure el present "**Conveni**" i, de comú acord i reconeixent-se plena capacitat per aquest acte, a tal efecte

EXPOSEN

I. La Sindicatura exerceix la funció de fiscalització dels comptes de la Generalitat, els ens locals i la resta del sector públic de Catalunya, conforme als articles 80 i 81 de l'Estatut d'Autonomia de Catalunya. Entre les funcions establertes en l'article 2 de la Llei 18/2010, de 7 de juny, de la Sindicatura de Comptes ("**Llei 18/2010**"), destaca la revisió de la legalitat, l'eficàcia i l'eficiència de la gestió econòmica dels ens públics, així com la proposta d'innovacions per millorar la gestió pública.

A través d'aquestes funcions, la Sindicatura realitza un control exhaustiu sobre les activitats econòmiques i financeres del sector públic català. A més, des de la Sindicatura s'ha promogut la subscripció de convenis amb l'Administració de la Generalitat, el Tribunal de Comptes i altres administracions per unificar els retiments de comptes i dades que les diferents normes imposen. Aquest procés es realitza mitjançant eines electròniques que permeten una interconnexió de dades entre les entitats i la Sindicatura, amb accés recurrent a les dades per fer el bolcat de manera contínua.

II. Per dur a terme aquestes funcions, la Sindicatura necessita accedir de manera constant a una gran quantitat d'informació d'elevada sensibilitat i importància institucional. Aquesta informació inclou dades econòmiques i financeres, informes d'auditoria, documents vinculats a la gestió pública, dades personals de responsables d'entitats fiscalitzades i altres informacions que, per la seva naturalesa, han de ser tractades de manera confidencial.

L'article 4.3 de la Llei 18/2010 estableix l'obligació de col·laboració de les entitats fiscalitzades amb la Sindicatura i el deure de facilitar tota la informació i documentació requerida per a l'exercici de les seves funcions. Aquesta potestat es reforça amb el reconeixement de la condició d'autoritat al personal de la Sindicatura en l'exercici de les seves funcions de fiscalització, segons l'article 49 de la mateixa Llei, així com en les actuacions d'inspecció previstes a l'article 51.

L'accés a aquestes dades, així com la seva custòdia i preservació, és fonamental per complir amb les funcions legals de la Sindicatura i per garantir la transparència i la bona gestió dels fons públics.

III. La gestió d'aquesta informació crítica comporta riscos inherents derivats de l'exposició a ciberamenaces, com ara l'accés no autoritzat, el sabotatge de sistemes o l'ús maliciós de dades confidencials. Qualsevol incident en aquest àmbit podria comprometre la integritat de les actuacions fiscalitzadores, posar en risc el dret a la protecció de dades i afectar el bon funcionament i la confiança en les institucions públiques.

IV. Per mitigar aquests riscos i garantir un alt nivell de seguretat de la informació, la Sindicatura requereix l'assistència tècnica de l'Agència per implementar mesures de seguretat robustes i contínues per protegir les dades a les quals accedeix. Això inclou l'adopció de sistemes de xifratge, controls d'accés, vigilància dels sistemes d'informació i protocols per garantir que la informació no sigui lliurament accessible.

V. L'Agència és una entitat de dret públic de l'Administració de la Generalitat de Catalunya que actua amb plena autonomia orgànica i funcional, objectivitat i independència tècnica i professional, adscrita al Departament de la Presidència. Actua en compliment de la Llei 15/2017 de 25 de juliol de 2017, de l'Agencia de Ciberseguretat de Catalunya ("**Llei 15/2017**").

VI. L'Agència té com a objectiu garantir la ciberseguretat al territori de Catalunya, entenent aquesta com la seguretat de les xarxes de comunicacions electròniques i dels sistemes d'informació en els àmbits de la seva competència i respectant sempre les competències de l'Estat (article 2.4.a de la Llei 15/2017, interpretat conforme als paràmetres acotats per la Sentència del Tribunal Constitucional 142/2018, de 20 de desembre).

La Llei 15/2017 i els seus Estatuts, aprovats pel Decret 223/2019, de 29 d'octubre, atribueixen a l'Agència una sèrie de funcions clau, entre les quals destaca la prevenció, detecció i resposta davant incidents de ciberseguretat (article 6.2.a de la Llei 15/2017). Aquestes funcions impliquen l'adopció de mesures de seguretat davant les ciberamenaces que poden afectar les infraestructures tecnològiques, els sistemes d'informació, els serveis de les tecnologies de la informació i la comunicació, i la informació que aquests tracten.

L'Agència exerceix les seves funcions en el marc de la ciberseguretat del sector públic català, amb tasques com la planificació i gestió de la ciberseguretat a l'Administració de la Generalitat i el seu sector públic (article 6.2.b del Decret 223/2019), la detecció i resposta a incidents (article 6.2.a del Decret 223/2019), i l'anàlisi de riscos i gestió de la seguretat de les infraestructures tecnològiques (article 6.2.g del Decret 223/2019). A més, l'Agència té la responsabilitat d'exercir funcions com a equip de resposta a emergències (CERT), coordinar les actuacions en matèria de ciberseguretat amb altres organismes nacionals i internacionals, i vetllar per la continuïtat dels serveis i la protecció de les infraestructures de la Generalitat i altres entitats públiques (article 6.2.h del Decret 223/2019).

Per a la consecució d'aquests objectius, l'Agència pot subscriure qualsevol tipus de conveni (articles 1.4 i 8 del Decret 223/2019).

VII. D'aquest marc normatiu s'infereix que l'objectiu de l'Agència és cobrir tot el territori de Catalunya, incloent-hi totes les administracions públiques i el seu sector públic, exercint les competències assignades i respectant els límits establerts per la Sentència del Tribunal Constitucional 142/2018.

VIII. Tot i que la Llei 15/2017 no inclou expressament la Sindicatura dins de l'àmbit operatiu de l'Agència, des d'aquestes institucions es va promoure la seva incorporació en una proposta de modificació legislativa presentada a l'avantprojecte de llei de mesures 2024. Tot i que aquesta modificació no va prosperar a causa de la finalització de la legislatura, ambdues entitats han continuat col·laborant de manera informal, com ho demostren els incidents passats, incloent-hi l'assistència de l'Agència a la Sindicatura en un ciberatac sofert el novembre de 2023 i l'assessorament respecte a la publicació d'informes de control de ciberseguretat durant el 2024.

IX. La necessitat de formalitzar aquesta col·laboració neix de la importància que té la seguretat cibernètica en el context de la Sindicatura, que té accés a dades sensibles relacionades amb la gestió pública. L'Agència aporta a la Sindicatura l'expertesa tècnica i els recursos necessaris per implementar les mesures de seguretat més adequades per protegir aquesta informació davant de ciberamenaces. Així, es vetlla per garantir la seguretat, la confidencialitat i la integritat de les dades que la Sindicatura manega en el seu treball de fiscalització del sector públic català.

X. La Sindicatura i l'Agència formalitzen aquest conveni de cooperació dins del marc legal establert per la legislació de contractes i règim jurídic del sector públic. En concret, l'article 31 de la Llei 9/2017, de Contractes del Sector Públic ("**LCSP**"), permet a les entitats del sector públic cooperar entre elles mitjançant sistemes de cooperació horitzontal —sense relació de dependència—, mitjançant convenis que compleixin els requisits establerts en l'article 6 de la mateixa norma (i en l'article 12.4 de la Directiva 2014/24/UE). Aquests requisits són: (i) les entitats no han de tenir vocació de mercat; (ii) el conveni ha d'establir una cooperació amb l'objectiu comú de garantir la prestació dels serveis públics que els incumbeixen; i (iii) la cooperació ha de ser guiada exclusivament per consideracions d'interès públic.

En interpretació d'aquests requisits, la Sentència de 28 de maig de 2020 del Tribunal de Justícia de la Unió Europea (assumpte C-796/18) admet la cooperació entre entitats públiques quan aquesta impliqui activitats de suport a serveis públics que cadascun dels participants ha de prestar, fins i tot de manera individual, sempre que aquestes activitats contribueixin a la realització efectiva dels serveis públics. Així doncs, el TJUE accepta que les relacions entre entitats públiques poden presentar els elements essencials definitoris d'un contracte públic —això és, onerositat i un objecte comprensiu d'una prestació de serveis subministraments i obres— i no queden automàticament subjectes a la normativa de contractació pública.

Per la seva banda, la Junta Consultiva de Contractació Pública de Catalunya també ha interpretat aquesta qüestió a la llum de la normativa europea i els pronunciaments del TJUE (Informes 7/2020, de 17 de juny, 3/2019, de 13 de març i 6/2017, de 16 de maig). Així, en l' Informe 23/2024, de 25 de juliol, la Junta Consultiva afirma que "els convenis que estableixen una cooperació horitzontal entre entitats públiques tenen per objecte garantir la realització d'una missió de servei públic comuna a les entitats i resten exclosos de l'àmbit d'aplicació de la normativa sobre contractació pública malgrat presentar elements definitoris dels contractes públics". En aquests casos no hi haurà transferències financeres entre les parts, més enllà del reemborsament dels costos reals dels serveis, obres o subministraments.

XI. D'acord amb aquest marc normatiu, el present conveni s'inscriu plenament en una cooperació horitzontal activa entre les dues institucions. L'Agència aportarà el suport tècnic necessari per garantir que els sistemes d'informació de la Sindicatura estiguin protegits davant de ciberamenaces, mantenint la confidencialitat, integritat i disponibilitat de les dades gestionades per la Sindicatura. Així, la Sindicatura podrà continuar exercint les seves funcions de fiscalització amb les garanties de seguretat requerides, assegurant que la informació sensible que maneja estigui protegida, permetent la seva anàlisi i difusió de manera segura i en compliment amb les normatives aplicables.

Ambdues parts manifesten la seva voluntat de col·laborar a l'empara dels articles 47 a 53 de la Llei 40/2015 de Regim Jurídic del Sector Públic ("**Llei 40/2015**"), de la Llei 26/2010, del 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya i dels articles 6.2 i 31 de la LCSP, atesa la naturalesa jurídica pública d'ambdós entitats i el caràcter no contractual de la relació que es pretén materialitzar, amb subjecció als següents

PACTES

PRIMER.- OBJECTE

1.1. L'objecte del present Conveni és establir el marc de cooperació que ha de permetre millorar la seguretat cibernètica de la Sindicatura, en particular, mitjançant la col·laboració de l'Agència, que aportarà el suport tècnic necessari per garantir la protecció dels sistemes d'informació de la Sindicatura davant de ciberamenaces.

1.2. La formalització d'aquest Conveni té com a objectiu contribuir a l'execució de les polítiques públiques en matèria de seguretat cibernètica, en concret, per tal de garantir que la Sindicatura pugui exercir les seves funcions amb les

garanties de seguretat requerides, especialment, pel que fa a la protecció de les dades confidencials i la integritat dels seus informes en el marc del control del sector públic català.

SEGON.- COMPROMISOS I OBLIGACIONS DE LES PARTS

Per a l'assoliment dels objectius perseguits amb el present Conveni, les Parts es comprometen conjuntament a assumir els següents compromisos:

2.1 Compromisos de l'Agència de Ciberseguretat de Catalunya:

(i) Ajudar a la Sindicatura en la millora contínua de les seves capacitats de prevenció, protecció, detecció i resposta davant incidents de seguretat. En aquest sentit, **es col·laborarà en l'establiment o actualització d'un programa de seguretat de la Sindicatura**, donant suport en la definició de iniciatives, polítiques internes, procediments i controls per garantir la protecció de les dades i sistemes. L'Agència orienta aquest suport en base a cinc eixos fonamentals: sistemes d'informació crítics, persones, cultura, governança i infraestructures transversals.

(ii) En la línia de l'estipulat en el punt anterior, també es contempla la col·laboració en el desplegament del model de ciberseguretat definit per l'ACC (com a pas previ a una integració adequada amb la pròpia ACC) , assessorant tècnicament i proporcionant els suports necessaris per identificar les prioritats d'actuació i establir les mesures que resultin més adequades d'acord amb el nivell de risc i la criticitat de les dades gestionades per la institució.

(iii) Assistència en la **Resposta a ciberincidents i assistència tècnica** davant d'amenaces, atacs o vulnerabilitats que puguin afectar la Sindicatura. Aquest suport inclourà accions d'identificació, contenció, recuperació i recomanacions de millora per reduir riscos futurs.

(iv) Organitzar activitats de sensibilització i formació realitzades directament per l'Agència, per tal de contribuir a la millora de la cultura de ciberseguretat a la Sindicatura, amb la finalitat de reforçar la seguretat dels seus sistemes i la capacitat de resposta davant incidents.

En l'execució d'aquestes actuacions de difusió i formació, ambdues Parts podran acordar actuacions concretes i detallades per donar cobertura a les necessitats plantejades. L'execució d'aquests plans de difusió i formació es podran dur a terme en col·laboració amb altres administracions o organismes públics per tal de maximitzar el seu impacte així com facilitar la seva organització.

2.2 Compromisos de la Sindicatura de Comptes de Catalunya:

(i) Utilitzar les eines, plataformes, solucions, materials, informació i altres elements que hagi posat a disposició l'Agència per a l'exercici de les funcions pròpies de la Sindicatura, d'acord amb els nivells establerts de disponibilitat, configuració dels sistemes i usos establerts.

(ii) Proporcionar els mitjans tècnics i humans necessaris per a desplegar les prestacions de ciberseguretat en els serveis de la Sindicatura, organitzant les tasques, reunions o plans de desplegament que siguin necessaris per a implementar les solucions acordades amb l'Agència.

(iii) Comunicar a l'Agència qualsevol incident de ciberseguretat que tingui un impacte en els sistemes de la Sindicatura, a través del sistema de resposta a incidents de ciberseguretat (CERT), per tal de garantir el suport tècnic i la correcta recuperació dels sistemes afectats.

(iv) Facilitar a l'Agència tota la informació necessària per poder accedir a les prestacions acordades, incloent les dades i documents que l'Agència necessiti per desenvolupar les accions de seguretat, garantint que aquestes dades siguin exactes, completes i adequades per a l'ús en l'àmbit de la ciberseguretat.

(v) Difondre, en col·laboració amb l'Agència, els materials, informes i campanyes de sensibilització i formació sobre ciberseguretat entre el personal de la Sindicatura per assegurar la millor comprensió i aplicació de les mesures de seguretat establertes.

(vi) Participar activament en la promoció de la seguretat cibernètica a la Sindicatura, implementant les campanyes de seguretat que es considerin necessàries i treballant amb l'Agència en la creació d'una cultura de ciberseguretat robusta a tots els nivells de l'organització.

2.3 En cas que es produeixi una incidència o bretxa de seguretat derivada de les actuacions tècniques objecte d'aquest Conveni que pugui afectar la informació o els sistemes de la Sindicatura, les Parts cooperaran de manera immediata per identificar-ne les causes, corregir-ne els efectes i restablir la normalitat en el funcionament dels sistemes afectats.

2.3.1 La Sindicatura es compromet a comunicar a l'autoritat de control competent qualsevol incidència o bretxa de seguretat que produeixi una violació de la seguretat de les dades personals en els termes i terminis establerts per l'article 33 del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27

d'abril de 2016 ("**RGPD**") i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals ("**LOPD**"). Si escau, també haurà de notificar-ho als interessats afectats, conforme a l'article 34 del mateix Reglament.

A aquests efectes, l'Agència, en el marc del present Conveni, prestarà a la Sindicatura el suport tècnic, documental i institucional necessari per a l'anàlisi de la bretxa, la identificació de riscos per als drets i llibertats dels afectats i l'elaboració de la documentació de suport tècnic que sigui necessària per a la tramitació de les notificacions esmentades. A més, l'Agència col·laborarà en la defensa de la Sindicatura davant de possibles procediments administratius o reclamacions de responsabilitat vinculades a la bretxa de seguretat, acreditant la traçabilitat de la incidència i les mesures correctores adoptades.

TERCER.- COMPROMISOS DE CONTINGUT ECONÒMIC

3.1 Inexistència de compromisos econòmics generals: Les Parts acorden que la col·laboració establerta en aquest Conveni no implicarà una transferència directa de fons entre elles amb caràcter periòdic, exceptuant-se els casos on es requereixin reemborsaments per costos derivats de les prestacions, serveis o recursos específics que s'hagin de proporcionar d'acord amb allò previst en el present Pacte. Tots els costos generals derivats de la col·laboració seran assumits per cada part en funció dels seus propis recursos, d'acord amb els pressupostos anuals corresponents.
3.2 Reemborsament de costos per accions concretes: Es preveu amb caràcter general el reemborsament dels costos derivats de les actuacions concretes que pugui dur a terme l'Agència en l'àmbit de les seves funcions.

El present Conveni no constitueix una prestació de serveis a efectes de l'Impost sobre el Valor Afegit (IVA), motiu pel qual l'aportació realitzada, en el seu cas, no restarà gravada pel referit tribut.

3.2.1 **Tipologies d'actuacions**: L'Agència posarà a disposició de la Sindicatura el portfoli d'actuacions de ciberseguretat d'acord amb el model de governança establert i amb les necessitats de seguretat identificades. Les actuacions en matèria de ciberseguretat que es divideixen en dues categories:

(i) Governança i desplegament del model de ciberseguretat.
(ii) Actuacions específiques en ciberseguretat.

L'anterior de conformitat amb l'Annex I i II al present Conveni.

3.2.2 **compensació**:

L'Agència comunicarà a la Sindicatura els costos derivats de les actuacions sol·licitades. **Els costos detallats per a cada actuació seran acordats mitjançant Addenda**, les quals establiran tant actuacions a escometre com la compensació econòmica corresponent.

3.3 Condicions de reemborsament: El reemborsament de costos es realitzarà d'acord amb les condicions establertes en el present Conveni i amb la presentació de la documentació justificativa corresponent.

3.4 Contribució per activitats conjuntes: En el cas d'organitzar activitats conjuntes (formació, sensibilització, esdeveniments, etc.), les Parts acordaran prèviament la distribució dels costos associats. Si alguna de les Parts assumeix totalment els costos d'una activitat, la Part beneficiària podrà abonar una quantitat acordada per la seva participació, segons el criteri que es fixi en cada cas.

3.5 Previsió anual dels compromisos econòmics: Les Parts acordaran, en el marc de la reunió anual de la Comissió de Seguiment, la previsió dels compromisos econòmics derivats de l'execució del present conveni per a l'exercici següent. Aquesta previsió haurà de tenir en compte les actuacions programades, les prioritats de col·laboració i els recursos disponibles, i podrà donar lloc, si escau, a l'aprovació d'una addenda per concretar-ne l'abast i els imports corresponents.

QUART.- VIGÈNCIA

4.1 El present Conveni tindrà una vigència de quatre (4) anys a comptar des de la data de la seva signatura.

4.2 La vigència inicial del Conveni podrà ser prorrogada, de forma expressa i per escrit, pels períodes que convinguin les Parts, sempre que considerin que la col·laboració continua sent necessària i eficaç per als objectius establerts. En tot cas, les pròrrogues, sumades, no podran excedir un nou període de quatre (4) anys addicionals.

4.3 Per fer efectiva la pròrroga del Conveni, qualsevol de les Parts signants podrà comunicar a l'altra la seva voluntat de prorrogar o no el Conveni amb una antelació mínima de tres mesos abans de la fi de la durada inicial del Conveni o de qualsevol de les seves pròrrogues. En cas de no acordar la pròrroga en el temps i forma establerts, el Conveni es considerarà finalitzat a l'expiració del període inicial o prorrogat, segons correspongui.

CINQUÈ.- MECANISMES DE SEGUIMENT, VIGILÀNCIA I CONTROL DE L'EXECUCIÓ DEL CONVENI

5.1 Comissió de Seguiment: Es constitueix una Comissió de Seguiment amb l'objectiu de vetllar pel compliment dels compromisos establerts en aquest Conveni. La Comissió estarà formada per un màxim de 3 representants de cadascuna de les Parts i en formaran part, en tot cas, la persona que ostenti la Direcció de l'Agència i un representant de la Secretaria General de la Sindicatura.

5.1.1 La Comissió serà responsable de dur a terme un seguiment exhaustiu de l'execució del Conveni, mitjançant la revisió de documentació, informes i altres evidències relacionades amb les accions de seguretat implementades. Igualment, valorarà l'efectivitat de les mesures adoptades, identificarà possibles àrees de millora i podrà proposar ajustos en les actuacions a desenvolupar.

5.1.2 La Comissió es reunirà sempre que ho sol·liciti alguna de les Parts i, com a mínim, un cop l'any, amb la finalitat d'avaluar l'estat de la col·laboració, el grau d'assoliment dels objectius i la resolució d'incidències que puguin haver sorgit.

5.1.3 A les reunions hi assistiran els responsables designats per les Parts, que analitzaran conjuntament els resultats obtinguts i acordaran, si escau, les accions correctores pertinents. A la reunió anual es durà a terme, igualment, el retiment de comptes sobre els compromisos tècnics i econòmics assumits.

5.2 Informes de seguiment: L'Agència remetrà a la Sindicatura informes de seguiment amb la periodicitat que determini la Comissió, amb informació sobre l'evolució de les actuacions implementades, les incidències detectades i les mesures adoptades. Els informes es lliuraran dins del termini màxim de trenta dies a comptar de la finalització de cada període acordat.

5.3 Resolució de discrepàncies: En cas que es detectin discrepàncies o problemes en l'execució o interpretació del Conveni, les Parts acordaran conjuntament mesures correctives i establiran un termini per a la seva implementació. Si les discrepàncies persisteixen, es farà ús de la mediació o altres mecanismes que les Parts considerin adients per resoldre qualsevol disputa.

SISÈ.- MODIFICACIÓ I DESENVOLUPAMENT

6.1 Aquest Conveni podrà ser modificat de mutu acord per les Parts, que caldrà recollir per escrit justificant les circumstàncies que aconsellen la modificació i assegurant que es manté l'objecte i finalitat del mateix.
6.2 Les modificacions s'hauran de formalitzar mitjançant addendes signades per les Parts, que passaran a formar part integrant del Conveni.

6.3 Les Parts podran desenvolupar aspectes tècnics o operatius del Conveni mitjançant protocols d'actuació, sempre que aquests no contradiguin el contingut del present Conveni ni en modifiquin la seva naturalesa jurídica.

6.4 En cas que durant la vigència del Conveni s'aprovi una modificació normativa que inclogui expressament la Sindicatura en l'àmbit subjectiu d'actuació de l'Agència, les Parts es comprometen a modificar aquest Conveni per tal d'adaptar-lo al nou marc legal**.** Aquesta modificació es produirà en la següent sessió de la Comissió de Seguiment que es celebri amb posterioritat a l'entrada en vigor de la norma.

SETÈ.- INCOMPLIMENT DELS COMPROMISOS ASSUMITS

7.1 En cas d'incompliment per alguna de les Parts de qualsevol dels compromisos assumits en aquest Conveni, la Part afectada ho posarà en coneixement de la Comissió de Seguiment, que requerirà formalment a la Part incomplidora la seva esmena en un termini màxim de trenta (30) dies naturals des de la recepció del requeriment.

7.2 Si transcorregut aquest termini l'incompliment persisteix i no s'ha arribat a cap acord en el si de la Comissió de Seguiment, la Part afectada podrà notificar formalment a l'altra Part la seva decisió de resoldre el Conveni.

7.3 La resolució anticipada per aquesta causa haurà de ser comunicada de manera fefaent a l'altra Part, i implicarà la finalització de les obligacions pendents, sense perjudici del seguiment de les mesures que calgui per garantir la protecció de la informació o la finalització ordenada de les activitats en curs.

VUITÈ.- RESPONSABILITAT

8.1 Cada Part serà responsable de les actuacions que dugui a terme en el marc del present Conveni, d'acord amb les funcions i compromisos assumits. L'Agència, com a entitat especialitzada en matèria de ciberseguretat, prestarà el suport tècnic acordat amb la diligència exigible, d'acord amb els estàndards tècnics aplicables en cada cas.

8.2 La Sindicatura continuarà sent responsable del contingut i la custòdia de la informació que tracta en l'exercici de les seves funcions, incloent-hi aquells supòsits en què, tot i comptar amb l'assistència de l'Agència, es produeixi una incidència que afecti aquesta informació. No obstant això, les Parts es comprometen a actuar amb la màxima diligència per prevenir i mitigar qualsevol risc en aquest àmbit, dins del marc de col·laboració establert pel present Conveni.

8.3 L'Agència no serà responsable dels danys derivats de la informació o instruccions incorrectes, incompletes o inexactes facilitades per la Sindicatura, ni tampoc dels danys derivats de l'incompliment per part de la Sindicatura de les recomanacions o mesures proposades per l'Agència en el marc d'aquesta col·laboració.

8.4 En cap cas no s'exigirà cap tipus d'indemnització entre les Parts derivada de l'execució del present Conveni, atesa la naturalesa institucional de la col·laboració i el caràcter no contractual de la relació. Tanmateix, la Comissió de Seguiment establerta al Pacte CINQUÈ serà l'encarregada de valorar qualsevol incidència rellevant i proposar les mesures correctores que calguin.

NOVÈ.- EXTINCIÓ I EFECTES

9.1 El present Conveni s'extingeix pel compliment de les actuacions que en constitueixen l'objecte o per resolució anticipada per alguna de les causes establertes a continuació.

9.2 Són causes de resolució del Conveni:

a) El transcurs del termini de vigència del Conveni sense que s'hagi acordat una pròrroga.
b) El mutu acord exprés i per escrit de les Parts.
c) L'incompliment dels compromisos assumits per alguna de les Parts. En aquest cas, la Part complidora podrà requerir per escrit a l'altra que compleixi en els termes previstos en el Pacte Setè.
d) L'existència d'una causa d'impossibilitat sobrevinguda, legal o material, que impedeixi el compliment de les obligacions assumides.
e) Qualsevol altra causa prevista en el present Conveni o en la normativa d'aplicació.

9.3 La finalització del Conveni donarà lloc a la seva liquidació, amb l'objectiu de determinar les obligacions i compromisos pendents d'execució, així com el tancament tècnic i administratiu de les actuacions desenvolupades en el seu marc.

9.4 L'extinció del Conveni, per qualsevol causa diferent a l'incompliment d'alguna de les Parts, no donarà lloc al reintegrament de les quantitats percebudes, sempre que aquestes s'hagin destinat a l'execució de les actuacions compromeses en el marc d'aquest Conveni.

9.5 Sense perjudici del previst als apartats anteriors, si en el moment d'extingir-se el Conveni hi haguessin actuacions en curs d'execució, aquestes continuaran executant-se fins a la seva completa finalització, d'acord amb el que estableixin els pactes econòmics i tècnics previs.

DESÈ.- CONFIDENCIALITAT

10.1 Les Parts es comprometen a mantenir el caràcter confidencial de tota la informació, documentació, dades i coneixements als quals tinguin accés en el marc de l'execució del present Conveni i que no tinguin caràcter públic, amb independència del seu format o suport.
10.2 Aquesta obligació de confidencialitat afecta, entre d'altres, la informació sobre mesures de ciberseguretat, vulnerabilitats detectades, resultats d'anàlisis o auditories, metodologies, procediments interns, així com qualsevol altra informació facilitada per l'altra Part en el marc de les actuacions derivades del Conveni.

10.3 Les Parts adoptaran les mesures tècniques i organitzatives necessàries per preservar la confidencialitat de la informació i evitar-ne l'alteració, la pèrdua, el tractament o l'accés no autoritzats.

10.4 Només podrà accedir a la informació confidencial el personal pròpiament autoritzat per cada Part, que haurà de conèixer i complir les obligacions derivades d'aquest Pacte. En cap cas la informació confidencial podrà ser divulgada a tercers sense el consentiment previ i exprés de la Part que l'ha facilitat, excepte en cas d'obligació legal o requeriment judicial o administratiu.

10.5 Les obligacions de confidencialitat s'entenen sense perjudici del compliment de les obligacions de transparència i publicitat que corresponguin a cadascuna de les Parts d'acord amb la normativa vigent en matèria de transparència i accés a la informació pública.

10.6 L'obligació de confidencialitat continuarà vigent un cop extingit el Conveni, mentre la informació conservi aquest caràcter, i com a mínim durant un termini de cinc (5) anys des de la data de finalització.

ONZÈ.- PROTECCIÓ DE DADES

11.1 Les Parts es comprometen a complir, en tot moment, la normativa vigent en matèria de protecció de dades de caràcter personal, en especial el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

11.2 En cas que l'execució de les actuacions derivades del present Conveni requerís l'intercanvi o accés a dades personals, les Parts determinaran de manera expressa i per escrit el règim de responsabilitat de cada Part, atenent a les funcions respectives conforme el Reglament (UE) 2016/679.

11.3 En tot cas, les Parts adoptaran les mesures tècniques i organitzatives apropiades per garantir un nivell de seguretat adequat al risc, i vetllaran pel respecte dels drets de les persones interessades, especialment en relació amb el deure d'informació, l'accés i la rectificació de les dades, la limitació del tractament, la portabilitat i la supressió.

11.4 Les obligacions en matèria de protecció de dades de caràcter personal continuaran vigents un cop extingit el Conveni, mentre sigui necessari per garantir el compliment dels principis i obligacions derivats de la normativa aplicable.

DOTZÈ.- RÈGIM JURÍDIC I RESOLUCIÓ DE CONFLICTES

12.1 El present Conveni té caràcter administratiu i queda subjecte a les previsions dels articles 47 i següents de la Llei 40/2015, la Llei 26/2010 i la resta de normes de dret administratiu que resultin d'aplicació i supletòriament pel dret civil.

12.2 El Conveni queda exclòs de l'àmbit d'aplicació de la LCSP, d'acord amb l'article 6 de la mateixa, per tractar-se d'un instrument de cooperació interadministrativa que fomenta la col·laboració entre dues entitats del sector públic per a l'execució de funcions públiques pròpies de les entitats participants, en l'àmbit de la ciberseguretat i la fiscalització del sector públic de Catalunya. Sense perjudici d'aquesta exclusió, els principis de la LCSP podran aplicar-se de manera supletòria per a resoldre dubtes interpretatius o llacunes que puguin sorgir durant l'execució del Conveni.

12.3 Les Parts es comprometen a resoldre, de manera amistosa, qualsevol desacord que pugui sorgir en la interpretació i compliment del present Conveni preferentment per la Comissió de seguiment. En cas de no ser possible un acord en aquest àmbit, les qüestions litigioses que puguin sorgir seran resoltes, si escau, per la jurisdicció contenciosa administrativa, amb submissió expressa als òrgans jurisdiccionals de la ciutat de Barcelona, amb renúncia expressa del seu propi fur.

TRETZÈ.- PUBLICITAT I TRANSPARÈNCIA

De conformitat amb l'article 14 de la Llei 19/2014, de 29 de desembre, de transparència, accés a la informació i bon govern, el present conveni es publicarà en el Registre de Convenis de Col·laboració i Cooperació de la Generalitat, el qual s'integra en el Portal de Transparència.

* *

I en prova de conformitat, les Parts signen electrònicament el present Conveni, a un sol efecte, en el lloc i la data indicats.

Miquel Salazar Canalda
Sindicatura de Comptes de Catalunya

Laura Caballero Nadales
Agència de Ciberseguretat de Catalunya

ANNEX I – DESCRIPCIÓ DE LES ACTUACIONS PREVISTES EN EL MODEL DE CIBERSEGURETAT DE L'AGÈNCIA

Es descriuen a continuació les accions a implementar en cada fase del desplegament del model, detallant les tasques que corresponen tant a l'Agència de Ciberseguretat de Catalunya (en endavant, l'Agència) com a l'entitat on es farà efectiu el desplegament.

1.1. Fase preliminar

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

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

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

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

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

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

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

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

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

1.2. Fase 1 - Diagnòstic

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

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

1. **Anàlisi de l'arquitectura de seguretat:** consultoria de l'estat de ciberseguretat de l'entitat realitzada mitjançant entrevistes i recollida d'informació, basada en una matriu de controls de ciberseguretat que es considerin necessaris per a poder reduir el grau d'exposició a les principals ciberamenaces de l'àmbit. L'anàlisi inclourà, entre d'altres, controls relatius a la seguretat de la xarxa, dels sistemes d'informació, dels llocs de treball, la gestió d'identitats i els accessos, la continuïtat dels serveis, etc.

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

3. **Anàlisi del compliment inicial de l'Esquema Nacional de Seguretat**: d'entrada el Model inclourà l'anàlisi del Perfil de Compliment Específic de Requisits Fonamentals de Seguretat (PCE RFS). En funció del tipus d'entitat i del seu grau de maduresa es podran aplicar altres categories de l'ENS o perfils de compliment. L'avaluació d'aquest estat de compliment inicial es portarà a terme a partir de la resposta del formulari preliminar per al desplegament del Model i les visites presencials i entrevistes per part de l'equip de projecte de l'Agència.

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

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

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

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

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

1.3. Fase 2 - Pla de seguretat

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

Si s'escau, en aquesta fase, s'elaboraran també els plans de protecció requerits per la normativa de protecció d'infraestructures crítiques o serveis essencials.

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

- Elaboració del Pla de seguretat que inclourà els següents continguts:
    - Estat de ciberseguretat de l'entitat
    - Grau de compliment de l'ENS d'acord amb el perfil de compliment específic o, en el seu defecte, amb la categoria de l'ENS que s'hagi determinat que apliqui a l'entitat .

- Detall de les anàlisis tècniques i d'arquitectura de la infraestructura tecnològica.
- Relació i detall dels projectes, en base a les proves i diagnòstics realitzats durant la fase anterior, identificant com a prioritàries aquelles accions més rellevants i urgents a abordar per reduir les febleses i fer front a les principals amenaces. Els projectes identificaran el seu impacte tant en relació a la protecció enfront les ciberamenaces aplicables a l'entitat (d'acord amb les funcions de ciberseguretat incloses en el perímetre de seguretat definit per l'Agència amb aquest propòsit), com en relació amb el compliment de l'ENS.
- S'introduirà una estimació a alt nivell del cost de les iniciatives en base a ordres de magnitud obtinguts al llarg del desplegament del Model a diferents àmbits per part de l'Agència obtinguts a partir de la tipologia d'entitat, les seves volumetries de sistemes d'informació i persones i la complexitat i localització dels seus sistemes d'informació, entre d'altres aspectes que es puguin analitzar. Aquesta estimació inicial tindrà com a objectiu donar visibilitat de les necessitats pressupostaries i de les capacitats associades a la implementació del pla que haurà d'executar l'entitat, quedant fora de l'abast del desplegament del Model.

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

<u>Correspon a l'entitat l'execució de les següents accions:</u>

- Implementació, seguiment i governança del Pla de seguretat impulsant totes aquelles accions generals i específiques per a assolir la seva consecució (dotació pressupostària, dotació de capacitats i recursos, etc.).
- Revisió i avaluació del Pla de seguretat, amb l'objectiu d'entendre la viabilitat, impacte, i priorització de les mesures previstes davant dels òrgans de decisió de l'entitat.
- Implementació de les mesures proposades al pla, coordinant-se amb els actors pertinents, i executant un seguiment de la seva execució fins a la seva finalització.
- Execució de projectes o plans d'acció específics per a la implementació de mesures d'elevada complexitat
- Actualització i documentació del Pla de seguretat per a la seva traçabilitat, auditoria i millora continua.
- Presentació i seguiment del Pla de seguretat a la Direcció i/o al Comitè de Seguretat de l'entitat, per a disposar del suport necessari per a l'execució de les actuacions previstes i consecució dels objectius del pla.

1.4. Fase 3 - Integració operativa

Durant aquesta fase es desplegaran els processos i serveis necessaris per a la integració de l'entitat amb l'Agència.

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

- Definició i entrega a l'entitat del model de relació i protocols de resposta davant d'incidents
- Configuració i entrada en funcionament del serveis de detecció d'amenaça i intel·ligència operativa, que han de permetre a l'entitat disposar informació proactiva d'amenaces i la monitorització digital.
- Desplegament de capacitats de prevenció a través de les anàlisis d'exposició a l'amenaça sobre els actius publicats .
- Desplegament de capacitats de resposta mitjançant les matrius d'escalat i els protocols de gestió d'incidents establerts.
- Desplegament de les capacitats de detecció a través de la integració de les fonts dels principals actius de seguretat de l'entitat en el SOC de l'Agència o SOC Operatiu.
- En el cas que l'entitat disposi d'un SOC Operatiu, moltes de les capacitats i serveis descrits en els anteriors punts es desplegaran i portaran a terme mitjançant el model d'integració i govern operatiu dels diferents SOC Operatius a través el SOC Tàctic de l'Agència, i que es troben descrits en l'annex III. Des del SOC Tàctic de l'Agència es definiran les estratègies prevenció, detecció, protecció i resposta davant ciberamenaces, que el SOC Operatiu de l'entitat haurà de tenir com a referència per a adaptar les seves pròpies.

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

- Aprovació a l'entitat del model de relació i protocols establerts amb l'Agència.
- Facilitar la informació i portar a terme les accions necessàries per habilitar a l'entitat, les capacitats d'identificació d'amenaces, prevenció i resposta a incidents, d'acord amb els serveis activats per part de l'Agència.
- Portar a terme les tasques necessàries per habilitar el manteniment i integració de les fonts dels principals actius de seguretat identificats, assegurant la seva incorporació al SOC de l'Agència per a la seva monitorització.
- Iniciar el desplegament i mantenir les capacitats de protecció a l'entitat, d'acord amb el que es determini en el pla de seguretat, i amb l'objectiu de disposar d'un perímetre de protecció adequat pels sistemes d'informació, lloc de treball i les persones.
- En el cas que l'entitat disposi d'un SOC Operatiu, aquesta tindrà la responsabilitat de garantir que el SOC Operatiu doti de visibilitat al SOC Tàctic respecte a l'activitat gestionada de l'entitat i del grau d'exposició a l'amenaça, aportant a l'Agència el 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. En aquest sentit l'entitat local garantirà la coordinació operativa amb el SOC Tàctic, a través d'un seguiment periòdic segons el que s'estableixi al model d'integració i govern del SOC Operatiu de l'entitat.

1.5. Fase 4 - Protecció

La fase 4 del Model, és una etapa recurrent que preveu l'execució de funcions i serveis orientats a oferir una protecció continua i unes capacitats per a governar el desplegament del Model i fer seguiment del Pla de seguretat. En aquest sentit les actualitzacions i noves iteracions de les fases del model s'invocaran des d'aquesta fase d'operació continua.

Correspon a l'Agència l'execució de les següents accions, que inclouran el desplegament de funcions i serveis recurrents de l'Agència:

- **Serveis d'Operacions de Ciberseguretat de l'Agència** (en endavant, SOC de l'Agència)**:** servei 24x7 de monitorització de l'estat de seguretat de l'entitat i resposta a incidents, mitjançant el desplegament de capacitats d'intel·ligència operativa, detecció, prevenció i resposta, un cop integrades les eines tecnològiques de seguretat de l'entitat. En el cas que l'entitat disposi d'un SOC Operatiu aquest servei es facilitarà tal i com està previst en el model d'integració i govern dels SOC Operatius, a través del SOC Tàctic de l'Agència.

- **Oficina de Governança i Compliment:** oferirà acompanyament periòdic a les entitats i seguiment de les accions dels plans d'acció per a fer seguiment de l'evolució de l'entitat cap l'assoliment dels objectius fixats en el Pla de seguretat, així com resoldre vulnerabilitats i reduir l'exposició a l'amenaça. Amb un seguiment amb periodicitat mensual, es posarà a disposició de l'entitat quadres de comandament amb les mètriques i indicadors necessaris per a facilitar aquesta funció. També podrà oferir acompanyament a l'entitat en l'execució de les tasques prèvies i auditoria interna en relació a la preparació a la certificació de l'Esquema Nacional de Seguretat.

- **Oficina de Comunicació i Cultura de Ciberseguretat:** oferirà continguts i estratègies perquè l'entitat pugu**i** capacitar i conscienciar la totalitat de la seva plantilla, amb nivells i objectius de formació adaptats als perfils i necessitats corresponents. En aquest sentit l'oficina oferirà el suport en l'activitat formativa d'acord amb els següents tres nivells:

    - **Nivell bàsic de formació**, adreçat a tots els empleats públics de l'entitat.
    - **Nivell avançat de formació,** 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 coneixement si habilitats.
    - **Itineraris de perfils especialitzats de ciberseguretat**, desenvolupats a través de la Ciberacadèmia de l'Agència de Ciberseguretat, amb diferents itineraris formatius adreçats específicament als tècnics del món local que volen aprofundir i ampliar coneixements, en habilitats i competències.

- **Oficina Tècnica de Ciberseguretat:** oficina dotada amb tècnics especialistes en ciberseguretat que tindran com a objectiu oferir una prescripció, orientació experta i recomanacions sobre arquitectures de seguretat, guies i bones pràctiques a implementar en el disseny i evolució d'aplicacions i sistemes d'informació.

- **Servei continu de càlcul de la superfície d'exposició davant de ciberamenaces.** Servei recurrent de pentesting i de realització d'anàlisis d'exposició a l'amenaça per a una actualització periòdica del coneixement de l'exposició davant d'amenaces a l'entitat.

- **Simulacres d'incidents.** Sessions preparatòries amb les entitats perquè coneguin com es gestiona una cibercrisi i avaluar la capacitat de gestió enfront un ciberincident i el seu grau de preparació a través d'exercicis teòrics i pràctics, sense afectació en els entorns de les entitats.

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

- **En relació als serveis proporcionats pel SOC de l'Agència i pel servei continu de càlcul de la superfície d'exposició davant d'amenaces:**

  - Notificar les amenaces i incidents identificats al SOC de l'Agència o SOC Operatiu, i als interlocutors que formin part del procés d'escalat i presa de decisions, per a la seva avaluació i tractament.
  - Donar resposta a les alertes reportades pel SOC de l'Agència o SOC Operatiu.
  - Adoptar l'estratègia, accions, protocols i procediments previstos pel SOC de l'Agència o SOC Operatiu com a resposta a un incident de seguretat.
  - Disposar de capacitats tècniques per a dur a terme les accions necessàries (desplegament de polítiques, pegats, configuracions, instal·lació de programaris, adquisició d'evidències, restauració de còpies de seguretat, etc.) per a fer front als ciberincidents.
  - Implementar les accions prescrites des del SOC de l'Agència o SOC Operatiu de l'entitat, destinades a millorar la protecció i operació de la seguretat i relatives a la gestió del perímetre de seguretat, la prevenció d'amenaces, la protecció davant de ciberatacs i la identificació, anàlisi i gestió de vulnerabilitats.
  - Suport en l'execució de proves i anàlisis tècniques, facilitant la informació, mitjans, condicions, accés i usuaris necessaris per a portar-les a terme en el marc temporal pactat inicialment.

- **En relació a la Governança i Compliment:**

  - Assumir la gestió i govern del Pla de seguretat de l'entitat per a garantir l'existència de recursos tècnics i les capacitats necessàries en l'àmbit directiu i/o del Comitè de Seguretat.
  - Dur a terme les tasques necessàries per a permetre la implementació de les diferents fases del Model.

- Impulsar el compliment normatiu de l'entitat amb l'objectiu d'assolir, en la següent fase, la certificació de compliment en l'ENS i de qualsevol altra normativa sectorial o específica que els sigui d'aplicació.
- Executar i participar en els processos d'adequació, desplegar dels projectes, actuacions i mesures de seguretat necessàries, per a complir amb el marc normatiu i legal de ciberseguretat aplicable a l'entitat.
- Portar a terme, per a les categories que sigui necessari, les tasques prèvies per a verificar l'adequació a l'ENS com a pas previ per a la seva certificació.
- Portar a terme els treballs necessaris, per a elaborar, adaptar i mantenir la documentació i procediments relacionats amb el marc organitzatiu, normatiu i operatiu en referència al compliment de l'ENS seguint, quan estiguin disponibles, les indicacions, guies i models de referència a disposició de l'entitat.
- Visibilitzar l'estat de situació i avançament del Pla de seguretat a la direcció i/o al Comitè de Seguretat mitjançant, entre d'altres eines i informació, els indicadors i quadres de comandaments que es posin a disposició.

- **En relació a l'Oficina Tècnica en Ciberseguretat:**

  - Realitzar les accions necessàries per vetllar per la seguretat durant el cicle de vida de les aplicacions, adquisició de productes i en la gestió de proveïdors, com a elements clau per assolir un alt nivell de protecció i complir amb els estàndards i normatives vigents.

- **En relació a la Comunicació i Cultura de Ciberseguretat:**

  - Promoure i executar iniciatives formatives d'acord amb els diferents nivells proposats i amb el suport de l'oficina de formació prevista en el Model.
  - Adaptar els continguts, organització i disseny de les activitats formatives a la realitat organitzativa i funcional de l'entitat.
  - Cercar els recursos i suport organitzatiu necessaris per dur a terme les accions formatives previstes.

1.6. Fase 5 - Certificació en l'ENS

En aquesta fase del Model es preveu la certificació de l'Esquema Nacional de Seguretat mitjançant la realització d'auditories de conformitat. La certificació es podria dur a terme des de l'Òrgan d'Auditoria Tècnica (OAT) de l'Agència com a entitat reconeguda pel Centro Criptológico Nacional (CCN), prèvia conformitat de les parts.

Com s'ha comentat en apartats anteriors, el Model ofereix per defecte la certificació en el Perfil de Compliment de Requisits Fonamentals de Seguretat (PCE RFS) que inclou els requisits mínims que una entitat hauria d'abordar. El PCE RFS va dirigit a aquelles entitats amb dificultats per abordar el procés

d'adequació de l'ENS o, a aquelles on es determina que l'aplicació de les mesures del PCE RFS són suficients tenint en compte la postura de seguretat adoptada.

En funció de l'àmbit i de la maduresa de les entitats, es preveu que les re-certificacions previstes cada dos anys, estiguin enfocades a perfils de compliment específic o categories de l'ENS superiors, si escau.
L'enfocament de les re-certificacions es basa en un procés de millora contínua del compliment impulsat per les entitats.

Inicialment l'abast previst de la certificació correspondrà als serveis identificats al perfil de compliment específic o a la categoria determinada.

Correspon a l'Agència l'execució de les següents accions, en funció de la categoria o del perfil de compliment específic a certificar:

- **Certificació en els PCE:** L'OAT de l'Agència realitzarà les auditories de certificació dels diferents PCE en tot el seu cicle de vida amb la revisió d'evidències recollides en les fases anteriors del model, i d'acord al procés i a la metodologia µCeENS establerts pel CCN per als PCE. Com a resultat, l'OAT de l'Agència emetrà el certificat de conformitat de compliment de l'ENS, en cas de resultar satisfactòria l'auditoria.

- **Certificacions en les diferents categories de l'ENS:** un cop l'entitat estigui adequada, mitjançant la consecució de les accions identificades en el Pla de seguretat i amb la implementació per part de l'entitat de totes les mesures necessàries de l'ENS, i superat el procés d'auditoria interna, l'OAT de l'Agència executarà el procés d'auditoria mitjançant l'ús d'eines i la realització de les corresponents sessions a l'entitat. A tal efecte es podran utilitzar les eines previstes pel CCN-CERT en la preparació i execució d'aquests processos d'auditoria.

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

- Oferir tota la col·laboració necessària per abordar el procés d'auditoria de certificació.
- Garantir la disponibilitat de les evidències necessàries per al procés d'auditoria.
- Garantir un bon ús del certificat de l'auditoria i del distintiu associat.
- Tenir el compromís per mantenir i evolucionar el compliment de l'ENS, si escau, en les futures re-certificacions i dur a terme les accions necessàries.
- Dur a terme les tasques necessàries associades al govern i manteniment de la certificació.
- Quan es realitzin auditories de conformitat amb l'ENS de categoria mitjana o alta, la Sindicatura haurà de comprometre's a subscriure

amb l'OAT els següents dos acords que consten en l'Annex III del present Conveni:

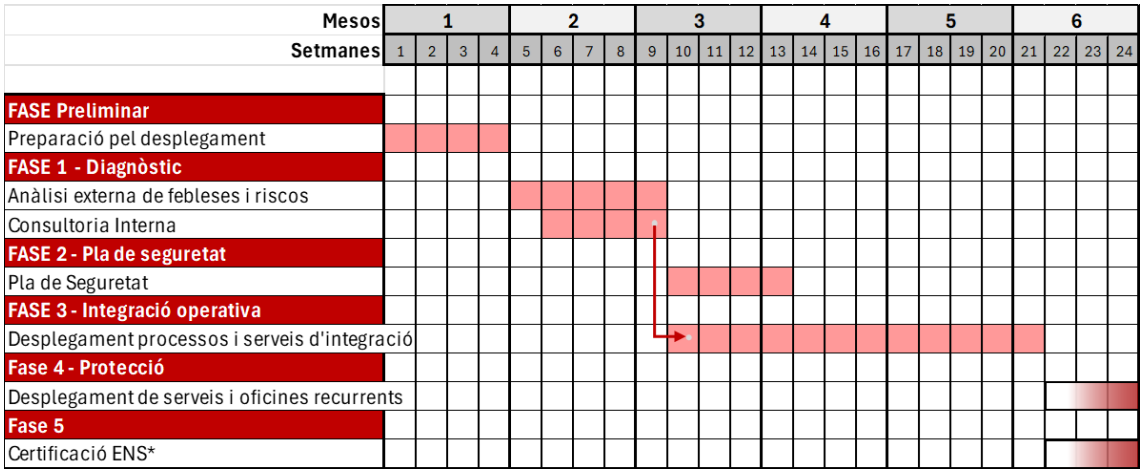
- Acord de drets i obligacions de qui es certifica de l'ENS.
- Acord d'ús de marques de certificació.

***

ANNEX II - PLANIFICACIÓ TEMPORAL EN EL DESPLEGAMENT DEL MODEL.

Pel desplegament del model de ciberseguretat, de manera orientativa es preveu en mitjana, el següent calendari temporal per a cadascuna de les fases previstes en el model.

Aquesta planificació de referència, s'adequarà durant la fase preliminar d'acord amb les dimensions i capacitats de l'entitat.



(*) El calendari de certificació en l'ENS, dependrà de l'entitat, d'acord amb l'execució que porti a terme de les accions previstes en el Pla de Seguretat.

***

ANNEX III - MODEL D'ACORD DE DRETS I OBLIGACIONS DE QUI ES CERTIFICA EN L'ENS I D'ÚS DE MARQUES DE CERTIFICACIÓ

ACORD D'ÚS DE MARQUES DE CERTIFICACIÓ (SEGELLS I CERTIFICATS)

ACORD ENTRE L'AUDITAT CERTIFICAT, O EN PROCÉS, I L'OAT

Les organitzacions, o les seves àrees o unitats, que estiguin certificats de la conformitat d'algun dels seus sistemes d'informació respecte a les disposicions de l'Esquema Nacional de Seguretat (en endavant, ENS), gaudiran d'una sèrie de drets, alhora que estaran subjectes a una sèrie d'obligacions d'ús de les marques de certificació, que es detallen en aquest document.

En conseqüència, [NOM I COGNOMS] amb DNI [NIF], en qualitat de [POSICIÓ en l'Organització auditada] de [NOM de l'Organització Auditada] reconeix que té capacitat prou per subscriure aquest acord.

DETALL DE L'ACORD D'ÚS DE MARQUES DE CERTIFICACIÓ

ÚS DE LES MARQUES DE CERTIFICACIÓ

Aquest Acord es refereix a les marques de certificació de l'ENS, en base a segells oficials, el model base dels quals és propietat del Centre Criptològic Nacional (CCN), així com certificats de conformitat, el model dels quals és propietat de l'OAT, seguint continguts mínims i directrius del CCN.

Les marques de certificació atorgades per l'OAT a l'organització, àrea o unitat que certifica algun dels seus sistemes d'informació per a les finalitats d'aquest document, estarà alineada amb la Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat (ITS) de conformitat amb l'Esquema Nacional de Seguretat i amb qualsevol Resolució posterior que la reemplaci o modifiqui.

Així mateix, es concretarà en base a annexos de la Guia CCN-CERT IC-01/19 sobre criteris generals d'auditoria i certificació de l'ENS, o qualsevol altra guia CCN-STIC que es consideri.

L'ús de la Marca de Certificació únicament està autoritzat en les condicions fixades en el present document, comprometent-se a respectar-lo les organitzacions, àrees o unitats amb algun sistema d'informació certificat de conformitat amb les disposicions de l'ENS. Porta aparellat la llicència d'ús de la marca, en els termes previstos, en qualitat d'organització que ha obtingut la certificació per a algun dels seus sistemes d'informació. L'ús d'aquesta marca (certificat o segell de certificació) per un període renovable,

habitualment de dos anys, es limita estrictament a l'organització, àrea o unitat que el seu(s) sistema(s) d'informació ha(n) estat certificat(s) satisfactòriament respecte a les disposicions de l'ENS per l'OAT en qualitat d'organisme de certificació, no havent estat retirats o suspesos els certificats per l'OAT.

La Marca de Certificació mostrada a l'annex I és un exemple dels tres segells de certificació disponibles en funció de la categoria del sistema: BÀSICA, MITJANA o ALTA. A més, l'organisme de certificació expendrà a l'organització client el sistema d'informació de la qual ha estat certificat, un certificat de conformitat amb les disposicions de l'ENS per a la categoria i abast acordats. L'OAT es reserva el dret de reemplaçar el segell de certificació mostrada a l'annex I, o el Certificat de Conformitat amb l'ENS, de l'altra en qualsevol moment, de comú acord amb el CCN, encara que sempre s'advertirà les organitzacions, àrees o unitats titulars del certificat de l'esmentada circumstància, igual que de qualsevol altre canvi que es produeixi en l'Esquema de certificació, sempre alineat amb les ITS o guies corresponents editades pel CCN.

Únicament poden utilitzar la marca de certificació (segell i certificat de conformitat) les organitzacions, àrees o unitats el sistema d'informació de les quals hagi estat certificat satisfactòriament per un OAT reconegut pel CCN, per una Entitat de Certificació (EC) acreditada per ENAC, o directament pel CCN en casos especials.

L'autorització del dret d'ús de la marca de certificació (segell i certificat de conformitat) s'obté amb la consecució i posteriors renovacions de la Certificació de Conformitat amb les disposicions de l'ENS. No substituirà en cap cas la garantia ni la responsabilitat sobre els serveis suportats pel sistema d'informació certificat que, d'acord amb la llei, correspon al llicenciatari de la marca de certificació.

COMPROMISOS DEL LLICENCIATARI

L'organització, àrea o unitat amb llicència d'ús de la marca de certificació, en qualitat d'organització certificada, adquireix els compromisos següents:

I. Complir amb tots els requisits que pugui estipular l'Esquema de certificació de l'ENS amb relació a l'ús de les marques de conformitat i a la informació relacionada amb els serveis suportats pel sistema d'informació certificat.

II. Mantenir els sistemes d'informació en l'àmbit de la certificació de conformitat amb l'ENS, per als quals s'ha concedit el dret d'ús de la marca de certificació, conforme a les disposicions de l'Esquema Nacional de Seguretat.

III. Acceptar les decisions preses respecte a l'aplicació del present Esquema de certificació, segons les condicions establertes en cada cas.

IV. Facilitar a l'equip auditor tots els mitjans necessaris per realitzar les verificacions que implica l'aplicació del present Esquema de certificació.

V. Utilitzar la marca de certificació únicament en la forma establerta en el present document i exclusivament en relació amb el seu abast de certificació.

VI. Procedir a realitzar la sol·licitud d'una auditoria complementària davant qualsevol modificació que es desitgi fer a l'abast i categoria dels sistemes respecte als quals se li hagi concedit el dret d'ús de la marca de certificació.

VII. Abstenir-se de fer ús de la marca de certificació quan hi hagi risc de confusió amb activitats, productes, processos, serveis, sistemes d'informació o parts de l'organització que no gaudeixin del dret d'ús d'aquesta marca de certificació.

VIII. Informar a l'OAT de canvis en l'organització que puguin afectar els sistemes d'informació en l'àmbit de l'Esquema Nacional de Seguretat, a l'abast, o a la categoria de la certificació.

CONDICIONS D'APLICACIÓ

L'ús de la Marca de Certificació ha de complir les condicions següents:

I. El Certificat de Conformitat haurà d'aparèixer sempre complet, d'acord amb el literal, i no és possible suprimir conceptes, logotips, o retallar-ne parts. Ha de quedar clara l'organització que obté la certificació del seu sistema d'informació, així com l'OAT que la concedeix, així com especialment la seva vigència, el seu abast, la seva categoria, la seva data d'emissió i la seva validesa.

II. Si l'organització, àrea o unitat el sistema d'informació de la qual està certificat, ha de lliurar a un tercer una còpia del Certificat de Conformitat o de qualsevol altre document de certificació, aquest haurà de ser una còpia fidedigna del mateix que el reprodueixi en la seva totalitat, no podent esmenar-se o suprimir-se part del contingut a proporcionar.

III. No estarà autoritzada la utilització de marques de conformitat per part d'organitzacions sense sistemes d'informació certificats, amb independència que existeixi certa relació o dependència amb alguna altra organització que sí que en disposi.

IV. Si es produeix, o es requereix, un canvi que afecti parcialment o totalment la identitat legal que ha obtingut la certificació, s'ha d'exposar el cas al Comitè de Certificació de l'OAT que l'estudiarà i decidirà la forma d'abordar-lo. En determinats casos es pot requerir elevar una consulta al CCN amb el resultat de transferir directament el certificat a la nova entitat legal, o bé iniciar un nou procés de certificació.

V. Les organitzacions, àrees o unitats amb el seu sistema d'informació en procés de certificació no podran incloure en les seves comunicacions la marca de certificació amb l'ENS fins a la finalització del procés i els hagi estat facilitat per l'OAT el corresponent Certificat de Conformitat amb l'ENS, que quedarà registrat amb la seva referència identificativa exclusiva.

VI. El segell que es mostri correspondrà clarament a la categoria dels sistemes certificats (BÀSICA, MITJANA o ALTA) en funció del tipus d'auditoria realitzat en el procés de certificació, venint aquesta així mateix reflectida en el Certificat de Conformitat amb l'ENS expedit per l'OAT.

VII. En material de papereria únicament es podrà usar la marca de certificació si està clarament associada a l'organització (tal com apareix en el seu certificat) i al sistema d'informació certificat, no podent arribar a interpretar-se que podria abastar altres sistemes d'informació que no ho estan.

VIII. En material promocional de qualsevol índole (anuncis de premsa, TV, Internet, etc., únicament es podrà usar la marca de certificació si està clarament associada a l'organització certificada (tal com apareix en el seu certificat) i al

sistema d'informació certificat, no podent arribar a interpretar-se que podria abastar altres sistemes d'informació que no ho estan.

IX. L'ús conjunt d'altres Marques de Certificació juntament amb la de certificació de la conformitat amb l'ENS, haurà de ser analitzat cas a cas. Per a això l'organització sol·licitant comunicarà per escrit a l'OAT la seva intenció de fer aquesta utilització conjunta de marques. El Comitè de Certificació si estima que no entra en contradicció amb les normes aquí descrites, informarà en el seu cas al CCN, traslladant la decisió d'aquest a la unitat o organització certificada.

X. Els Segells de conformitat amb l'ENS s'han de reproduir literalment, complets, triant el model associat a la categoria del sistema, no estant permès emprar únicament el logo genèric de l'ENS que consta en el seu interior per denotar que l'organització està certificada, ja que s'interpreta com un ús incomplet i il·lícit.

XI. Quan els Segells de conformitat s'ubiquin en una pàgina web, portal o Seu Electrònica, si es punxa sobre el mateix ha de visualitzar el Certificat de Conformitat complet.

XII. Segons es determina a l'article 38.2 del RD 311/2022, els subjectes responsables dels sistemes d'informació certificats de conformitat amb l'ENS, donaran publicitat als corresponents portals d'internet o seus electròniques a les certificacions de conformitat amb l'ENS, atenent el que disposa la ITS de Conformitat i la guia CCN-CERT IC-01/19.

XIII. Quan excepcionalment en un mateix document s'incloguin serveis, tant emparats com no emparades per la certificació, s'assenyalaran les activitats no emparades mitjançant un asterisc o similar, incloent amb el mateix tipus de lletra que l'usat en el cos del document, en un lloc visible i proper a la marca, de forma que es perceben en un únic cop de vista, la següent llegenda "*els [serveis, productes o sistemes segons procedeixi] marcats no estan emparats per la Certificació de conformitat amb l'Esquema Nacional de Seguretat*". En aquests casos, l'organització, àrea o unitat certificada sotmetrà a la consideració de l'OAT els documents on pensa col·locar la marca, indicant el lloc de la seva ubicació i els serveis que seran relacionats.

XIV. L'organització certificada no podrà fer ús de la marca un cop finalitzat el període de validesa del certificat sense la seva renovació, o després de l'entrada en vigor d'una suspensió temporal, retirada o renúncia del dret d'ús

VIGILÀNCIA DE L'ÚS DE MARQUES DE CERTIFICACIÓ PER L'OAT

Durant tot el període de validesa de la marca de certificació, que per a l'ENS s'estableix inicialment en dos anys, l'OAT ha de realitzar totes les verificacions considerades necessàries respecte al seu bon ús, o encarregar la seva realització a un tercer. És habitual que aquestes es duguin a terme cada 6 mesos.

En cas d'ús indegut de la marca de certificació, l'organisme de certificació a través del seu Comitè de Certificació pot advertir inicialment, podent arribar a suspendre o retirar immediatament la certificació i el dret a utilitzar la marca de certificació.

L'Organització, àrea o unitat certificada pot apel·lar la decisió del Comitè de Certificació al Comitè d'Imparcialitat, si ha estat constituït per l'OAT, o el que és més habitual, al CCN.

RENÚNCIA VOLUNTÀRIA A L'ÚS DE LA MARCA DE CERTIFICACIÓ

L'organització, àrea o unitat certificada pot renunciar o suspendre per un període de temps l'ús de la marca de certificació. Notificarà per escrit a l'OAT i realitzarà tots els canvis necessaris respecte als seus possibles mitjans de comunicació. Davant d'aquestes circumstàncies l'OAT l'informarà respecte als termes i condicions per a la terminació temporal o definitiva de l'ús de la marca de certificació.

ACCEPTACIÓ

En prova d'acceptació, es signa aquest acord en [Població], el DD de MES d'AAAA, que tindrà els seus efectes jurídics en el moment en què l'organització, àrea o unitat que l'ha subscrit certifiqui el seu sistema d'informació conforme a les disposicions de l'ENS i actuï en qualitat d'organització, àrea o unitat certificada per l'Agència de Ciberseguretat de Catalunya.

Directora de l'Agència de Ciberseguretat de Catalunya

El representant de l'AUDITAT

ANNEX I. REPRODUCCIÓ DELS SEGELLS OFICIALS DE CERTIFICACIÓ

El disseny dels segells de certificats, estarà al que disposa l'última versió publicada de la guia tècnica CCN-STIC-809, juntament amb els seus annexos, i la Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat (ITS) de conformitat amb l'Esquema Nacional de Seguretat, i modificacions posteriors.

Es reprodueixen a continuació els segells proporcionats pel CCN, que així mateix poden descarregar-se del portal de l'ENS:

Certificación. Categoría Básica (RD 311/2022)

Certificación. Categoría Media (RD 311/2022)

Certificación. Categoría Alta (RD 311/2022)