Contractació de subministrament de de llicències d'ús de certificats digitals SSL per l'Agència de Ciberseguretat de Catalunya

CO.03.2024

ÍNDEX

01 INTRODUCCIÓ

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència), té la necessitat de licitar un conjunt de solucions de suport per a l'execució de les funcions de seguretat TIC en virtut del "Acord del Govern pel qual s'aprova el contracte programa entre l'Administració de la Generalitat de Catalunya, mitjançant el Departament de Presidència, i la Fundació Centre de Seguretat de la Informació de Catalunya per als anys 2025-2028, de 9 de febrer de 2025."

L'Agència, amb aquest encàrrec del Govern, assumeix funcions i responsabilitats en l'àmbit de la ciberseguretat, esdevenint així una peça cabdal en l'estratègia de ciberseguretat del Govern de Catalunya.

Com a part d'aquesta estratègia, i en consonància amb les necessitats dels seus clients, l'Agència necessita dotar-se de les millors pràctiques, eines i proveïdors, per portar a terme els seus serveis, i entre ells, la gestió del cicle de vida dels certificats SSL de la Generalitat de Catalunya de poder donar resposta als requeriments i encàrrecs rebuts.

1.1 Agència de Ciberseguretat

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència), establerta sota el marc de la Llei 15/2017, del 25 de juliol, és l'entitat que lidera i coordina els esforços de la Generalitat de Catalunya en la protecció de la informació i les infraestructures del país davant les ciberamenaces. En un món digitalitzat i interconnectat, la seguretat de la informació s'ha convertit en una prioritat estratègica, i l'Agència subratlla el compromís de Catalunya amb la promoció d'un entorn digital segur i de confiança.

Amb un enfocament clar en la prevenció i detecció de ciberamenaces, la resposta efectiva davant incidents de ciberseguretat, la promoció de la cultura de ciberseguretat, i la col·laboració i coordinació amb diferents actors a nivell local i internacional, l'Agència opera dins de l'àmbit d'actuació definit per la llei, que marca les directrius d'actuació de l'Agència, les seves funcions, estructura orgànica i el règim de Governança.

L'Agència sota la direcció estratègica del Govern de la Generalitat de Catalunya, en coordinació amb les entitats del sector públic de l'Administració de la Generalitat de Catalunya, i col·laborant amb governs locals de Catalunya, sector privat i societat civil és l'encarregada d'establir i de liderar el servei públic de ciberseguretat i té com a objectiu garantir una Societat de la Informació segura i confiable per al conjunt de la ciutadania catalana i de la seva Administració Pública, amb la voluntat d'esdevenir un referent a nivell nacional i internacional en matèria de ciberseguretat.

Els avenços impulsats per l'Estratègia 2019-2022 han establert un sòlid punt de partida per a futures accions, incloent la consolidació de l'Agència de Ciberseguretat com a entitat de referència. Aquests avenços no només han millorat la capacitat de resposta davant incidents sinó que també han promogut una major consciència i formació en ciberseguretat entre la ciutadania i les organitzacions. La nova Estratègia 2023-2027, "Una Catalunya Cibersegura en una Europa Digital", s'orienta cap a reforçar la resiliència digital, protegir els serveis i infraestructures essencials, i assegurar que ciutadans i organitzacions es beneficiïn de tecnologies digitals de confiança.

En el marc de l'activitat gestionada per l'Agència de Ciberseguretat, cal destacar que aquesta gestiona més de 2.200 sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants. Aquest perímetre protegit provoca un nivell d'activitat de gestió de més de 4.424 milions de ciberatacs durant el 2022, una xifra 20 cops superiors a la del 2021.

D'aquests 4.424 milions de ciberatacs gestionats, 2.175 van esdevenir en un incident efectiu de seguretat gestionat per l'Agència de Ciberseguretat, el que representa una reducció del 22% respecte de l'any 2021.

Les xifres fan paleses la necessitat de dotar-se de noves eines i de seguir ampliant el perímetre d'actuació. En aquest sentit, i alineat amb la nova Estratègia, l'Agència ampliarà el seu perímetre d'actuació i per tant, incrementar el nivell de protecció, resiliència i prevenció de més àmbits.

1.2 Àmbits d'actuació

Es mostren a continuació els principals àmbits d'actuació de l'Agència:

- **Generalitat i el seu sector públic:** L'Agència desplega els seus serveis de Ciberseguretat als departaments i ens adscrits de la Generalitat. Els departaments, a través del personal d'àmbit del CTTI, tenen potestat per a la construcció d'aplicacions i desplegament de solucions. Els Responsables de Seguretat de la Informació són els encarregats de realitzar la Governança de la ciberseguretat de la Generalitat i el seu sector públic.

- **Centre de Telecomunicacions i Tecnologies de la Informació (CTTI):** El CTTI és l'empresa pública que integra tots els serveis informàtics i de telecomunicacions de la Generalitat de Catalunya, més enllà de proveir solucions transversals i adaptades als Departaments. Els seus objectius inclouen dissenyar, construir, coordinar i desplegar projectes tecnològics, fomentant i incorporant la innovació i la transformació digital.

- **Salut (sector públic / privat):** el sector salut, tant privat com públic, esdevé un àmbit molt rellevant d'actuació de l'Agència donada l'elevada criticitat dels serveis que presta i la sensibilitat/confidencialitat de la informació que tracta.

- **Universitats, Educació i Centres de Recerca**: l'entorn educatiu, format per Universitats, centres educatius i centres de recerca esdevé una de les prioritats de l'Agència a l'hora de desplegar el model de Ciberseguretat.

- **Món Local (Ajuntaments, diputacions, consells comarcals, Consorci AOC - Administració Oberta de Catalunya):** Ajuntaments, consells comarcals, diputacions i Consorci AOC presten serveis de molta rellevància a la ciutadania i, per tant, esdevenen un actor molt rellevant pel que fa al desplegament de model de Ciberseguretat de l'Agència.

- **Infraestructures crítiques**: les infraestructures crítiques esdevenen potencials objectius dels ciberatacants i, per tant, la protecció d'aquestes infraestructures (aigua, comunicacions, salut, ...) requereix de processos de coordinació i desplegament de mesures de Ciberseguretat essencials per evitar l'impacte sobre les mateixes.

1.2 Dades de context i abast

La Generalitat de Catalunya disposa actualment de llocs web, intranet i extranets per l'intercanvi i accés a informació de diferent tipologia (confidencial, estratègica, dades privades). La protecció d'aquesta informació esdevé una prioritat molt important i cal disposar dels mecanismes per garantir-la en tot moment.

Els certificats SSL (Secure Sockets Layer) són essencials per a la seguretat i l'autenticació dels llocs web. Hi ha diversos tipus de certificats SSL, cadascun amb funcionalitats i nivells de seguretat diferents:

- **SSL OV (Organisation Validated):** Aquest certificat requereix una validació de l'entitat o organització propietària del lloc web. La certificació OV confirma la identitat de l'empresa, la qual cosa ofereix una capa addicional de confiança als visitants del lloc web.

- **SSL EV (Extended Validation):** Aquests certificats SSL proporcionen el nivell més alt de validació i confiança. L'EV requereix una exhaustiva validació de l'empresa, incloent una revisió detallada del registre de l'empresa per assegurar-se que és una entitat legal. Els llocs web amb certificats EV mostren una barra d'adreça verda al navegador, indicant als usuaris que el lloc és altament fiable.

- **SSL MD (Multi-Domain):** Aquests certs permeten protegir diversos dominis amb un sol certificat SSL. També es coneixen com a certs de "subject alternative name" (SAN) o certs "Unified Communications" (UC). Amb un SSL MD, pots protegir múltiples dominis de primer nivell amb una sola instal·lació de certificat.

- **Certificats Wildcard:** Aquests certs SSL són útils quan vols protegir múltiples subdominis sota un domini principal. Un certificat Wildcard s'aplica a tots els subdominis d'un domini base, permetent xifrar la informació de manera segura en totes les pàgines web associades.

Els certificats codesign son certificats de signatura de codi generats per l'Agència a través d'un **dispositiu HSM en format USB**. Aquest dispositiu es **renova cada dos anys.**

En l'àmbit de la Generalitat de Catalunya, l'Agència té la funció de gestionar el cicle de vida dels certificats digitals SSL, des de la seva petició inicial fins que el certificat ha expirat o ha estat revocat, així com de donar tot el suport que se'n derivi per assegurar la seva correcta instal·lació i renovació. Actualment, aquesta gestió es desenvolupa des del servei d'Identitat Digital de l'Agència ubicat dins de l'Àrea d'Operacions.

En línia del creixement de l'abast del servei i que Google ha proposat una nova política que exigeix que el cicle de vida dels certificats digitals sigui de 90 dies. Un cop aquesta política s'apliqui, el servei haurà d'adaptar a aquestes noves directrius. Després de la seva implementació, **estimem que el nombre de Certificats que es gestionaran al llarg de l'any es multiplicaran per 4.**

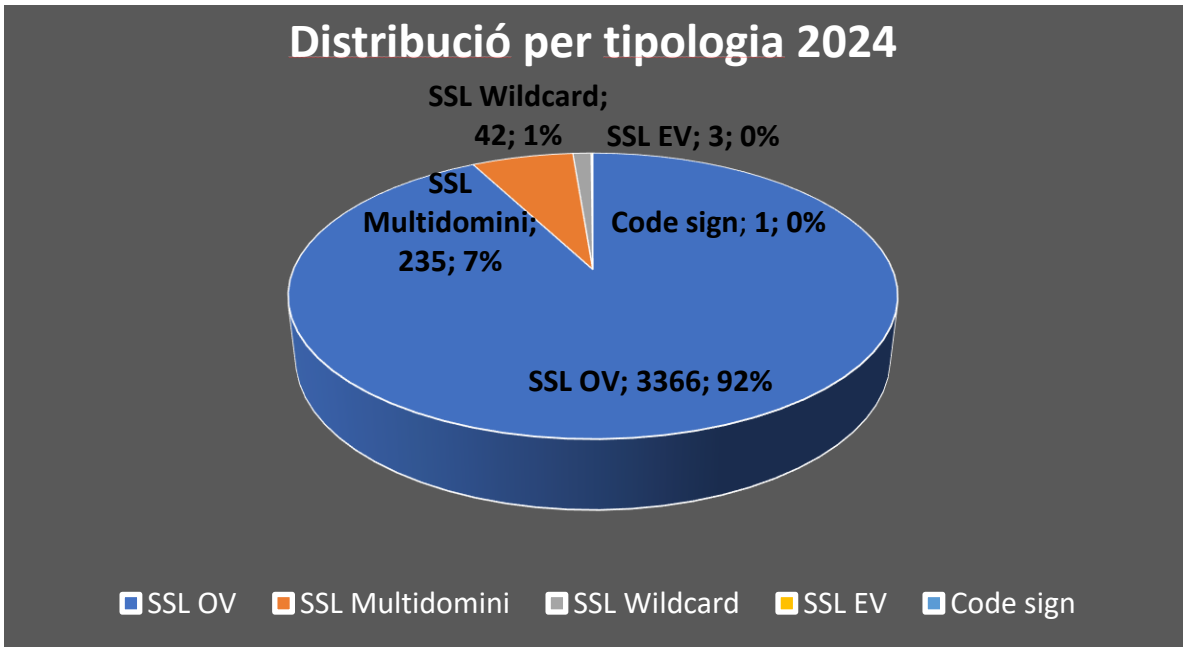
En base a l'historial de certificats gestionats i al volum de **creixement estimat dels últims anys, de prop d'un 30% anual**. Ens porten a fer la següent estimació:

	SSL OV	SSL Multidomini	SSL Wildcard	Codesign	SSL EV	
abr-24	380	22	7			409
maig-24	366	21	6			393
juny-24	333	27	3			363
jul-24	223	22	3		1	249
ag-24	491	37	9			537
set-24	598	50	6			654
oct-24	452	56	1			509
nov-24	321	33	3		2	359
des-24	409	30	3			442
gen-25	336	35	16			387
febr-25	308	28	7		2	345
març-25	412	25	8			445
abr-25	387	23	6			416
maig-25	386	31	3			420
juny-25	272	25	4		1	302
jul-25	557	37	9			603
ag-25	643	57	6			706
set-25	498	59	2			559
oct-25	364	36	3	1	2	406
	7736	654	105	1	8	8504

**Codesing: Renovació del dispositiu HSM*

L'Agència preveu que el volum de certificats que s'haurien de poder gestionar al llarg del 2025 és de **4.862** certificats (distribuïts en diferents tipologies).

A 25 de març de 2024 es disposava de la següent distribució per tipus de certificat, emesos principalment per les CA de Sectigo i Entrust que estan integrades via API amb les eines de l'Agència:



02 OBJECTE DEL SUBMINISTRAMENT

La finalitat d'aquesta licitació és garantir que durant el període de vigència establert, el proveïdor serà capaç de subministrar el nombre necessari de certificats sol·licitats pel servei de manera eficaç, demostrant capacitat per gestionar el volum de certificats requerits amb eficiència i fiabilitat, complint amb els requisits necessaris.

2.1 REQUERIMENTS TÈCNICS

A continuació es detallen els requeriments tècnics mínims que els licitadors hauran de complir en el marc d'aquesta licitació:

1) Serveis

- El licitador haurà d'oferir com a **mínim 3 Autoritats de Certificació arrel vàlides diferents** (CAs). Per a que les CAs siguin considerades vàlides, hauran de complir tots els requeriments tècnics indicats.

- L'Agència podrà determinar en cada moment de quina CA arrel vol adquirir cada certificat.

- De forma obligatòria, com **a mínim dues de les CAs arrel incloses en l'oferta del licitador hauran de tenir un certificat intermig** que permeti emetre certificats amb ECC o ECDSA (Certificats amb algoritme de Corba El·líptica)..

- És un requisit indispensable que **les CAs ofertes disposin d'un full de ruta d'adaptació per al Post Quantum i/o** s'hi estiguin adaptant, alineant-se amb les institucions nacionals o internacionals.

- El licitador **haurà d'oferir accés directe a les MPKIs de les CAs arrel ofertades** a determinar per l'Agència. Aquestes MPKIs permetran reduir els temps de provisió de certificats de les CAs root escollides facilitant:

    - l'inventari i descobriment de certificats
    - la gestió del cicle de vida dels certificats
    - l'automatització de la gestió i del desplegament dels certificats
    - la integració amb eines de tercers
    - segregació de rols
    - log d'activitat
    - descàrrega del certificat un cop emès en qualsevol moment del seu cicle de vida.

- L'adjudicatari s'haurà de **coordinar i relacionar de forma continua amb el servei d'Identitat Digital** de l'Agència, per assegurar un correcte desplegament de la solució aportada i garantir un subministrament adequat durant tota la durada del contracte.

- L'adjudicatari **haurà d'aportar a principis de cada més un report mensual amb l'historial i el cost dels certificats consumits** per cada tipus de CA, així com l'estat del dipòsit avançat conforme la previsió semestral de les necessitats.

- L'adjudicatari **assessorarà i donarà suport en l'automatització del desplegament de certificats** a l'Agència i al CTTI.

2) Certificats

- Les CAs arrel ofertades permetran generar certificats que suportin **els algorismes de xifratge RSA, ECC o ECDSA i DSA.**

- És imprescindible que, com a mínim, **l'algorisme de hash de signatura** de tots els certificats disponibles sigui **SHA256 i la llargada de la clau pública de fins a 2048 bits.**

- És indispensable que cada CA root ofertada ofereixi els següents tipus de certificats:

    - **OV SSL**
    - **EV SSL (Extended Validation)**
    - **Wildcard SSL OV**
    - **Multi-Domain SSL OV**
    - **Code signing Certificate (Inclós en un HSM)**

    En cas que el licitador no compleixi aquests requeriments, la CA no serà avaluada dins la oferta.

- Addicionalment, s'exigeix que almenys alguna de les CAs arrels permeti **proveir certificats de seu electrònica qualificats eIDAS** i **certificats de signatura de codi**, sense ser imprescindible que sigui la mateixa CA.

- Els certificats oferts han de ser reconeguts pels principals navegadors de l'actualitat, tant des de Windows/MAC OS, com des de dispositius mòbils, tant Apple com Android. Concretament, les CAs root ofertades hauran d'estar a les llistes de confiança de:

    - **List of available trusted root certificates in iOS.**
    - **List of all root certificates that Firefox trusts for SSL/TLS.**
    - **Chrome root program**
    - **Microsoft trusted root certificate list**

- Els certificats hauran de portar una garantia mínima associada de 25.000 €.

- En cas que el període màxim de vigència dels certificats es veiés reduït per les directrius del mercat, la reducció del preu de les diferents tipologies serà proporcional al decrement en el termini de la vida útil dels certificats.

3) Qualitat

- El licitador haurà d'aportar una garantia de devolució de certificats dins els 30 dies posteriors a la seva emissió sense cost ni penalització per l'entitat.

- Aportar evidències de certificacions ISO27001, ISO22301 o mesures equivalents vinculades a la prestació dels serveis de certificació.

- Disposar d'un gestor dedicat al servei per atendre a l'Agència durant l'horari laboral d'aquesta (de 9 a 19h).

- Disposar d'un servei de suport 24x7 per atendre tot tipus de peticions i incidències que puguin sorgir durant la prestació del servei. Aquest suport podrà ser telefònic, per xat, per correu o per qualsevol altre canal que ho agilitzi. En cas d'elevar la petició a urgent o crítica, serà requisit disposar d'interlocució directa que faciliti una ràpida gestió del problema. Per incidències crítiques, es demana un temps de resposta inferior a 2 hores i un temps de resolució inferior a 1 hora.

- Disposar d'una base de dades de coneixement en tot allò relacionat amb els serveis de certificació (compatibilitats, canvis legislatius, etc).

NOTA IMPORTANT: El licitador que hagi presentat la oferta presumiblement més avantatjosa, d'acord amb el model d'oferta econòmica i l'excel corresponent, quan se li requereixi la documentació acreditativa de la seva capacitat i solvència haurà de presentar una memòria descriptiva dels certificats ofertats d'acord amb l'article 6 dels plecs administratius de la licitació.

Aquesta memòria haurà de demostrar clarament que els certificats reuneixen els requisits descrits en els presents plecs tècnics.

Control de Gestió

L'empresa adjudicatària de la present licitació, i en especial el cap de servei, haurà de col·laborar amb el responsable de la planificació pressupostària i el control de gestió de l'Agència per tal:

- De complir amb el model de seguiment econòmic i planificació en termes de capacitat i execució de tasques.
- D'ajustar-se als procediments de facturació que determini l'Agència.
- De conformar les factures en relació amb el reportat de serveis efectuat i acceptat per l'Agència, d'acord amb els procediments establerts.
- D'exercir la gestió del contracte amb capacitats de forecast.
- Realitzar el reporting en les eines proporcionades per l'Agència amb els següents conceptes.
- Fitxer mestre de persones.
- Fitxer mestre de projectes i activitats.
- Estimació de recursos per projecte.
- Seguiment dels riscos.
- Seguiment del consum de recursos.
- Imputació de temps i activitats.
- Assignació de tasques a persones.
- Memòria d'activitat del contracte.
- Facturació i Conformació de factures.

L'adjudicatari proporcionarà la seva total col·laboració per a la realització d'auditories i la verificació del compliment dels compromisos. Aquestes auditories, realitzades en qualsevol de les instal·lacions involucrades en la prestació del servei, podran ser portades a terme per personal de l'Agència o sol·licitades a tercers. No serà necessari fer una notificació prèvia per a la realització de tasques d'auditoria que no requereixin la col·laboració activa per part del personal de l'adjudicatari. En el cas en què sigui necessària aquesta col·laboració, l'Agència farà una notificació amb dues setmanes d'antelació.

Contingència

El contractista haurà de proveir un pla de contingència, en cas de desastre de les instal·lacions principals, en unes instal·lacions alternatives (centre de gestió secundari) propietat del licitador, que inclouran:

- Estacions de treball amb el programari adequat per realitzar les tasques descrites.
- Comunicacions d'accés a les aplicacions informàtiques.
- Telefonia fixa a les instal·lacions del servei.
- Accés a Internet a través de la xarxa d'àrea local.
- Espai suficient per allotjar en condicions de treball òptimes:
    - El personal necessari de l'adjudicatari per realitzar el servei.
    - Personal de l'Agència, o de terceres parts determinades per aquest, per a la correcta gestió del servei.
- Pla i execució de proves per validar la solució de contingència implementada, amb la periodicitat que l'Agència determini.
- Les instal·lacions i equipament haurà de ser suficient per garantir la continuïtat dels serveis de l'Agència durant l'existència de la causa que doni lloc a la contingència.

Seguretat

En matèria de seguretat de la informació, l'empresa adjudicatària té les següents obligacions:

3.11.1. Deure de confidencialitat

Tot el seu personal de l'empresa licitadora així com les CAs ofertades han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels servei contractat. Aquesta obligació de confidencialitat

s'haurà de mantenir durant 10 anys, o el que s'especifiqui en la licitació, des de que es va tenir coneixement de la informació, excepte en relació a les dades personals a les que accedeixin respecte a les que caldrà mantenir el deure de confidencialitat de manera indefinida, subsistint inclús quan es finalitzi la relació contractual, segons estableix la Llei Orgànica 3/2018.
L'empresa licitadora ha de comunicar aquesta obligació de confidencialitat al seu personal ja sigui intern com extern, que estigui involucrat en l'execució del contracte i les CAs ofertades i ha de controlar el seu compliment.
L'empresa licitadora ha de posar en coneixement de l'Agència, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de la informació.

3.11.2. Dades de caràcter personal

En relació amb el tractament de dades de caràcter personal, l'empresa adjudicatària de la present licitació donarà compliment com a encarregat de tractament del que estableix el Reglament General de Protecció de Dades.

3.11.3. Compliment del marc legal de ciberseguretat i del marc normatiu intern

L'empresa adjudicatària de la present licitació haurà de complir amb tots els requeriments que siguin d'aplicació d'acord amb el marc legal en matèria de ciberseguretat i amb el marc normatiu intern que siguin aplicables.
En relació al marc legal en matèria de ciberseguretat, i, en concret, al compliment de l'Esquema Nacional de Seguretat (ENS), l'empresa adjudicatària de la present licitació haurà d'assegurar la conformitat dels sistemes d'informació que sustentin la prestació de serveis o de les solucions que pugui proveir amb l'ENS durant tot el termini d'execució del contracte i, si escau, haurà d'estendre aquesta exigència a la cadena de subministrament. L'Agència de Ciberseguretat podrà requerir a l'empresa adjudicatària de la present licitació el lliurament de la documentació acreditativa de la conformitat amb l'ENS. L'empresa adjudicatària del contracte basat haurà de designar, segons estableix l'ENS, un punt de contacte per a la seguretat (POC) que canalitzarà i supervisarà el compliment dels requisits de seguretat de la informació i la gestió dels incidents que es puguin produir durant l'execució del contracte.
A més de l'ENS i la normativa i guies tècniques que el desenvolupen, l'empresa adjudicatària de la present licitació haurà de conèixer i aplicar el marc normatiu intern, que inclourà el Marc Normatiu de Seguretat la Informació de la Generalitat de Catalunya i la normativa pròpia, les directrius o instruccions de l'Agència de Ciberseguretat. Especialment haurà de complir amb la Política de seguretat aplicable i la normativa relativa a l'ús de les tecnologies de la informació i la comunicació, aprovada per Instrucció de la Secretaria d'Administració i Funció Pública i que es pot consultar al lloc web d'aquesta Secretaria. Si escau, l'empresa adjudicatària de la present licitació haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

3.11.4. Capacitat tècnica

L'empresa adjudicatària de la present licitació ha de garantir que tot el personal sigui conscienciat, rebi formació i informació sobre els seus deures, obligacions i responsabilitats en matèria de seguretat derivats de la legislació, del marc normatiu intern i dels procediments i directrius aplicables, recordant les possibles mesures disciplinàries aplicables i el seu deure de confidencialitat respecte a la informació a la que tingui accés.
.

3.11.5. Verificació del compliment i auditoria

L'Agència es reserva el dret a verificar i auditar, amb mitjans propis o de tercers, el compliment de les mesures de seguretat requerides en base al marc legal de ciberseguretat i al marc intern per als sistemes d'informació emprats per a l'execució del contracte, en el moment i amb la periodicitat que s'estimi convenient. L'Agència podrà requerir el seguiment dels plans d'acció derivats d'aquestes verificacions i auditories. L'empresa adjudicatària de la present licitació haurà de disposar dels recursos adients per a dur terme l'execució de les tasques que li corresponguin en relació a aquest model de compliment, donant resposta en els terminis marcats per l'Agència de Ciberseguretat. Si escau, la gestió del compliment es realitzarà amb les eines que determini l'Agència de Ciberseguretat.

3.11.6. Incidents de seguretat

L'empresa licitadora haurà de notificar a l'Agència de Ciberseguretat qualsevol incident de seguretat que pugui redundar, directament o indirectament, en la seguretat dels sistemes d'informació, en els terminis i per les vies que determini o els procediments establerts. L'empresa adjudicatària de la present licitació haurà d'aportar tota la informació necessària per a la seva gestió i notificació als organismes competents per part de l'Agència de Ciberseguretat.
En cas que sigui necessari, l'empresa adjudicatària de la present licitació haurà de col·laborar amb qualsevol de les tasques que siguin requerides per part de l'Agència de Ciberseguretat per a la identificació, contenció, erradicació, recuperació i recopilació de les evidències dels incidents de seguretat.

3.12. Assegurament i control de la qualitat i la millora contínua

L'empresa licitadora ha de vetllar per l'excel·lència i millora contínua dels processos, components tècnics i serveis sota el seu abast.
Per tal de garantir que s'aborda la qualitat i la millora, l'adjudicatari haurà d'elaborar, mantenir i executar un "Pla de Qualitat i Millora Contínua" que inclogui, entre d'altres:

- Anàlisi i avaluació de les dades obtingudes de la mesura del servei, tant de producció i activitat com de gestió de l'incidental i operació.
- Accions per l'assegurament i control de la qualitat (revisions, proves, etc.), amb major rigor, intensitat i profunditat segons la criticitat del projecte/servei/component.
- Accions per reduir el nombre d'incidències, problemes freqüents i el suport.
- Accions preventives per la mitigació de riscos, tenint en compte la seva probabilitat i el seu impacte.
- Accions per maximitzar l'eficiència i la sostenibilitat del servei.

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

Generalitat de Catalunya