Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Digitalización e Inteligencia Artificial

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Plec de prescripcions tècniques particulars que regeix la contractació dels serveis per a transició post-quàntica

Índex

1 Introducció

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 *segons recull la memòria de l'Agència de Ciberseguretat de Catalunya de 2023, l'entitat ha tingut un paper rellevant en les tasques de resposta i coordinació per a la gestió d'incidents de seguretat durant el 2023, tant pel que fa a la Generalitat com en diferents entitats del territori català.* En aquest sentit, l'Agència 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 alt nivell d'activitat de gestió. Més concretament, el nombre de ciberatacs rebuts durant l'any 2023 va ser de més de 5.000 milions, en contraposició als 4.400 milions d'atacs del 2022. Pel que fa als incidents de seguretat, l'Agència en va gestionar prop de 2.670 durant el 2023, en comparació amb els 2.175 de l'exercici anterior.

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.

Aquest contracte està finançat per Fons Europeus. El programa RETECH constitueix un dels nous eixos transversals de l'Agenda España Digital 2026 promoguts pel Ministerio de Asuntos Económicos y Transformación Digital, i està alineat amb dues de les principals fites de l'Agenda, com són, liderar la transformació digital de manera inclusiva i sostenible i focalitzar els esforços de digitalització en

sectors econòmics clau. L'objectiu del Programa RETECH és impulsar xarxes territorials d'especialització tecnològica, articulant projectes regionals que s'orientin a la transformació i especialització digital, assegurant la coordinació, la col·laboració i la complementarietat.

Gràcies a aquest nou eix de l'Agenda España Digital 2026, es pretén liderar un canvi disruptiu, de manera inclusiva i sostenible, focalitzant els esforços de digitalització en sectors econòmics clau. En definitiva, la iniciativa RETECH permetrà impulsar els projectes tractors proposats per les Comunitats i Ciutats Autònomes, fomentant l'intercanvi de coneixement i multiplicant les oportunitats de cada regió, a través de xarxes d' impacte nacional que permetin maximitzar l'equilibri territorial i la cohesió social entre elles.

Per fer efectiva la iniciativa RETECH amb total transparència i igualtat d'oportunitats per a totes les Comunitats i Ciutats Autònomes interessades, el Ministerio de Asuntos Económicos i Transformación Digital, a través de la Secretaria d'Estado de Digitalización e Inteligencia Artificial, va llançar una invitació pública destinada al desenvolupament de propostes de cooperació per finançar iniciatives emblemàtiques d'especialització territorial tecnològica dins de les seves competències.

L'Agència de Ciberseguretat de Catalunya lidera una d'aquestes iniciatives, un projecte amb participació de València i Galícia per a impulsar un Centre de Competències i innovació en Ciberseguretat: CENTRO DE INNOVACIÓN Y COMPETENCIA EN CIENCIAS DE LA SALUD, TRANSPORTE INTELIGENTE, INDUSTRIA CONECTADA Y EXCELENCIA OPERATIVA, amb cada comunitat sent-ne un node. El Centre de Competències té els següents àmbits d'actuació:

- El desenvolupament de solucions i serveis de gran valor afegit en l'àmbit de la ciberseguretat.
- La formació i capacitació de persones amb talent especialitzades en l'àmbit de la ciberseguretat.
- El desenvolupament de certificacions per a l'etiqueta de ciberseguretat.
- L'increment del nivell de ciberseguretat a partir de la conscienciació i formació de la ciutadania.
- L'impuls de la indústria de ciberseguretat nacional amb vistes a l'aparició, el creixement i el desenvolupament de noves empreses en aquest sector.

Els eixos temàtics del node de Catalunya són la ciberseguretat a l'àmbit de la Salut i l'excel·lència operativa de la ciberseguretat.

Dins aquest darrer eix temàtic neix el Centre DemoTEC: Centre Demostrador de Tecnologies Emergents en Ciberseguretat. Un sub-programa dins el Centre de Competències i innovació en Ciberseguretat de Catalunya, explicitat en el conveni de RETECH signat amb INCIBE, vinculat a les tecnologies emergents i la ciberseguretat. Concretament:

- Computació quàntica
- Automatització intel·ligent: RPA, IA, analítica avançada i blockchain

El Centre DemoTEC persegueix estimular la generació i adopció de solucions vinculades a aquestes tecnologies, mitjançant la creació de solucions i els seus demostradors tant per a eines com per a serveis, que en validin la viabilitat tècnica i la satisfacció dels casos d'ús i permetin estimar la dimensió i viabilitat econòmica i organitzativa de la seva adopció a escala.

Aquest plec desplega una part del Centre DemoTEC vinculada a la computació quàntica, centrada en la transició de l'administració pública de Catalunya a la criptografia de seguretat quàntica, que anomenem transició post-quàntica.

Davant l'amenaça de l'aparició de computadors quàntics capaços de trencar el xifrat usat actualment (CRQC, de les sigles en anglès) i amb previsió que això pugui ocórrer en un període d'entre 10-30 anys vista, i davant la previsió d'atacs de "harvest now - decrypt later", urgeix desplegar una estratègia de criptografia quantum resistent.

Aquesta estratègia impulsada per l'Agència de Ciberseguretat està alineada amb els criteris i recomanacions formulats pel Centro Criptológico Nacional mitjançant el document "CCN-TEC 009 Recomendaciones para una transición postcuántica segura" publicat el desembre de 2022, i respon a la necessitat i urgència expressada en aquest document i aquí citada:

"El CCN sigue atentamente las publicaciones del NIST (National Institute of Standards and Technology) conducentes al establecimiento de nuevos estándares resistentes a la computación cuántica. En este sentido, el CCN, en colaboración con otros organismos internacionales, y especialmente europeos, lleva a cabo sus propias investigaciones sobre los algoritmos postcuánticos propuestos. Ya nadie pone en duda la amenaza que para la criptografía actual supone el desarrollo de los ordenadores cuánticos, por lo que para el CCN es de capital importancia que la comunidad criptográfica española, así como la industria, los organismos y las empresas, comience a prepararse, a la mayor brevedad posible, para evitar o, al menos, paliar, tal amenaza. Para ello es preciso ir adaptándose a los nuevos desarrollos y tener en consideración las propuestas que van superando los diferentes filtros de seguridad. Por este motivo, el CCN recomienda llevar a cabo las acciones necesarias para iniciar los procesos migratorios necesarios para implementar los algoritmos postcuánticos recomendados con el fin de paliar los aspectos adversos de la computación cuántica."

Més enllà del requeriment als fabricants que els productes suportin protocols i algorismes quantum resistents (PQC i QKD), aquesta estratègia requereix a les organitzacions un full de ruta per a la transició, a partir d'una diagnosi criptogràfica i un pla de migració.

La migració a PQC es pot entendre com un cas d'ús particular per al que es coneix com a criptoagilitat.

Aquest programa pretén generar serveis per a la transició post-quàntica de la Generalitat de Catalunya i el seu sector públic, per tal de facilitar aquest exercici de diagnosi i migració a PQC, mitjançant l'aixecament en un exercici one-shot d'un pla de migració a PQC i de l'estructura de serveis i sistemes que l'hauran de dur a terme en els propers anys.

Cal mencionar que, si bé l'Agència pren amb aquesta iniciativa una posició pionera en aquesta qüestió en l'àmbit de l'Administració Pública de Catalunya, tant la tipologia de la demanda, com l'oferta de serveis similars, existeixen actualment al mercat; amb els sectors defensa i bancaris liderant-ne la demanda, i empreses dels sectors de consultoria tecnològica estratègica i de seguretat i empreses i centres de base tecnològica amb especialitzacions en criptografia i/o tecnologia quàntica, amb coneixement específic de l'estat de l'art i l'ecosistema de solucions existent, liderant-ne l'oferta.

2 Descripció dels serveis objecte de la contractació

2.1 Lot 1: serveis

2.1.1 Objecte i abast dels serveis.

(i) Objecte i descripció

L'objecte del present contracte és la contractació de serveis de gestió sistemàtica de la transició a la criptografia de seguretat quàntica de la Generalitat de Catalunya, mitjançant l'aixecament en un exercici one-shot d'un pla de migració a la criptografia de seguretat quàntica i de l'estructura de serveis i sistemes que l'hauran de dur a terme en els propers anys.

Més concretament, el present contracte cobreix els serveis per al disseny, capacitació i demostració de la transició post-quàntica a la Generalitat de Catalunya:

- Dissenyar, capacitar i executar el servei de gestió i governança de la transició post-quàntica, per al disseny sistemàtic i alineat de plans d'acció de les entitats per a la transició post-quàntica i l'acompanyament d'aquestes en l'execució del pla. Executar el servei en un entorn/entitat rellevant per a l'Administració Pública de Catalunya (p.e. CTTI), començant per involucrar i conscienciar tots els actors necessaris i generant els òrgans de decisió adients.
- Dissenyar i redactar el full de ruta i el pla d'acció per a la transició post-quàntica, partint de la situació de l'entitat i del context tecnològic actuals.
- Elaborar la normativa per a la regulació de la transició post-quàntica a la Generalitat de Catalunya, d'acord al pla d'acció i les seves fases.
- Dissenyar, desplegar i executar (amb medis propis o integrat als mecanismes de vigilància tecnològics existents a les entitats adients) el servei de vigilància tecnològica i actualització contínua tant de l'amenaça i la vulnerabilitat vers aquesta, com de les capacitats, maduresa i viabilitat de les solucions disponibles.
- Dissenyar, desenvolupar o integrar solucions quan sigui necessari, desplegar i integrar en l'operativa de les entitats adients els mecanismes d'avaluació i anàlisi continu de la robustesa, vers la capacitat de computació quàntica, de les implementacions criptogràfiques presents a l'entitat, les quals caldrà tipificar i identificar prèviament (inventariat).
- Dissenyar, implementar i desplegar demostradors que resolguin múltiples casos d'ús de transició post-quàntica rellevants per al pla d'acció.
- Dissenyar i desplegar un entorn de proves per a la realització de proves de rendiment, seguretat, validació i auditoria de les solucions post-quàntiques.
- Dissenyar, capacitar i executar el servei de validació i auditoria de seguretat de solucions amb criptografia post-quàntica a desplegar a les entitats dins de les àmbits d'actuació de l'Agència de Ciberseguretat de Catalunya, i habilitar-ne legalment l'operació com a servei amb preu de venta al públic, executant-lo com a mínim per als demostradors desplegats.
- Dissenyar, desenvolupar, desplegar i integrar en l'operativa de les entitats adients, mitjançant la capacitació, el servei de proves de rendiment en relació a la criptoagilitat.
- Conscienciar, formar i difondre: Presentar un pla de conscienciació i formació, generar els continguts i executar-lo, alimentant la Ciberacademy amb contingut específic i cursos. Generar articles de difusió a mitjans i realitzar jornades de difusió.

Aquest programa pretén generar serveis per a la transició post-quàntica de la Generalitat de Catalunya i el seu sector públic, per tal de facilitar aquest exercici de diagnosi i migració a PQC,

mitjançant l'aixecament en un exercici one-shot d'un pla de migració a PQC i de l'estructura de serveis i sistemes que l'hauran de dur a terme en els propers anys.

En primer lloc, el programa persegueix una diagnosi mitjançant l'enteniment dels processos on intervé la criptografia i l'estructura organitzativa que els sosté, seguida d'una enumeració automàtica i contínua mitjançant eines, que culmini en una anàlisi de situació de l'entitat respecte de la criptografia i habiliti la revisió periòdica d'aquesta situació, mitjançant quadres de comandament amb els indicadors rellevants integrats als sistemes de gestió i seguiment de l'Agència de Ciberseguretat de Catalunya.

A partir d'aquesta diagnosi, el programa ha de generar l'escenari desitjat i un pla de migració que es recolzi en la incorporació de tecnologia específica. Caldrà generar un pla director de ciberseguretat, coordinadament amb els responsables adients, que planifiqui el desplegament de tecnologia específica, la substitució iterativa d'algorismes i sistemes criptogràfics tradicionals per alternatives que suportin PQC junt amb les proves, detecció de problemes de rendiment i retards i decisions al respecte. El seguiment d'aquest pla director caldrà també plasmar-lo a les eines de gestió i seguiment de l'Agència de Ciberseguretat de Catalunya, així com vetllar per a generar, actualitzar i transmetre els indicadors de seguiment rellevants, mitjançant quadres de comandament i indicadors que caldrà proposar, implementar, i integrar amb els sistemes de l'Agència.

Si bé aquest programa, amb l'abast temporal i pressupostari del que disposa, no pretén finalitzar la implementació del pla director, sí és imperatiu que demostri la viabilitat de la metodologia i del propi pla, així com el valor de la iniciativa, mitjançant múltiples demostradors funcionals en entorns d'abast reduït dins l'àmbit de la Generalitat de Catalunya o com a mínim demostradors en escenaris que emulin aquests entorns en laboratoris a desplegar a la Generalitat. S'entén per demostradors escenaris comparatius amb la solució pre-quàntica i una solució post-quàntica per a l'entorn, que permeten comparar-les a nivell d'arquitectura, processos i rendiment. Els demostradors hauran de ser rellevants per al pla de transició i satisfer els principals casos d'ús dels reptes prioritaris d'aquest pla. Sense que sigui una llista extensiva, els següents son possibles escenaris d'interès per a cobrir en demostradors: (1) la protecció de la navegació corporativa des d'una seu concreta, (2) la protecció de les connexions ciutadanes cap a una aplicació corporativa, (3) la protecció d'una VPN corporativa (en la identitat i el xifrat de la connexió), (4) el xifrat i signatura del correu corporatiu p.e. des d'una extensió del client de correu, (5) la protecció d'una cabina de backups, (6) la protecció de la informació dins bases de dades de l'àmbit, (7) la signatura del codi d'aplicacions corporatives, per exemple la signatura via git amb claus PQC, (8) el xifrat del tràfic de xarxa entre dos seus corporatives, (9) la protecció de les PKIs, amb la gestió integral de la vida dels certificats d'identitats i de dominis corporatius, (10) el desplegament de canvis a escala en les polítiques de xifrat dins l'organització (p.e. mitjançant l'AD), (11) la gestió de l'accés físic als edificis corporatius, (12) l'aprofitament de desplegaments de tecnologia QKD per a la satisfacció d'algun dels casos d'ús mencionats, mitjançant la integració de claus generades amb QKD en aquests escenaris.

(ii) Objectius del servei

L'Agència de Ciberseguretat de Catalunya persegueix amb aquest servei l'objectiu de:

- Capacitar l'Agència i la resta d'entitats involucrades en l'execució sistemàtica dels serveis relacionats amb la transició post-quàntica que els siguin propis d'acord a les seves funcions i identificar la possible necessitat d'assignació de noves funcions.
- Inventari criptogràfic: Identificar on s'usen algorismes vulnerables a l'escenari d'aparició de computadors quàntics universals criptogràficament rellevants,
- Incorporar l'amenaça quàntica a l'avaluació contínua de la ciberseguretat: Desplegar eines de monitoratge, avaluació i anàlisi continu de la vulnerabilitat criptogràfica i integrar-les als procediments d'avaluació de la ciberseguretat (risc, exposició a l'amenaça, criticitat de la vulnerabilitat, etc.) i proposta i priorització d'actuacions.
- Planificar la transició post-quàntica: Elaborar un full de ruta, plà de transició detallat que determini i dimensioni les actuacions i guiï les inversions per a fer efectiva i completar la transició post-quàntica.
- Habilitar el desplegament del pla mitjançant l'elaboració de la normativa específica adient.
- Demostrar la viabilitat tecnològica i mesurar el dimensionament d'infraestructura i econòmic i l'impacte organitzatiu de la transició, mitjançant desplegar demostradors per a diferents casos d'ús rellevants per al pla d'acció.
- Habilitar la revisió contínua del pla: Planificar la revisió del pla i desplegar els mecanismes de seguiment junt amb la vigilància tecnològica adient per a alimentar-la.
- Capacitar l'Agència i la resta d'entitats involucrades en la realització de proves de rendiment de les diferents solucions i configuracions, i en el dimensionament de la infraestructura necessària per a suportar la transició a partir de les proves amb els demostradors i les seves conclusions.
- Transversalitzar el projecte i la transició: Conscienciar les parts involucrades al projecte i generar i dinamitzar els òrgans de governança del projecte incorporant als actors necessaris. Presentar un pla de conscienciació i formació, generar els continguts i executar-lo, alimentant la Ciberacademy amb contingut específic i cursos. Difondre mitjançant generar articles de difusió a mitjans i realitzant jornades de difusió del projecte.

(iii) Activitats i funcionalitats que s'esperen del servei

Les activitats previstes del servei comprenen les següents tipologies:

- Governança, gestió i planificació estratègica de caire tecnològic
- Coordinació d'actors i gestió de projectes d'envergadura a tots els nivells
- Consultoria especialitzada en ciberseguretat i criptografia post-quàntica
- Disseny, implantació i execució de serveis operatius en relació a la ciberseguretat post-quàntica:
  - Inventariat, diagnosi, avaluació i anàlisi contínua per a la transició criptogràfica
  - Prescripció: full de ruta i pla d'acció detallat complementant el pla director de seguretat
- Desenvolupament, integració i desplegament d'eines d'inventariat criptogràfic i d'avaluació i anàlisi continues de la vulnerabilitat criptogràfica i la criptoagilitat.
- Prototipatge, disseny, desenvolupament i desplegament de demostradors.
- Avaluació de la viabilitat de les solucions demostrades.
- Execució de proves de rendiment i comparatives.
- Elaboració i redacció de normativa.
- Conscienciació, formació i difusió.

S'avaluarà la proposta d'activitats concretes oferta pel licitador com un dels criteris d'adjudicació de la licitació.

(iv) Productes del servei

El servei haurà de produir com a mínim els següents lliurables:

Governança de la transició:

- Servei de governança de la transició post-quàntica. Disseny del servei amb perfils, dimensionament i elements de cost, procediments, metodologies i eines per a la gestió i governança de la transició post-quàntica, és a dir, per al disseny sistemàtic i alineat de plans d'acció de les entitats per a la transició post-quàntica i l'acompanyament d'aquestes en l'execució del pla.
- Procés estructurat i replicable a les diferents entitats de l'Administració Pública de Catalunya per a la transició a la criptografia post-quàntica.
- Execució del servei per a generar i executar el projecte demostrador, en una entitat rellevant per a l'Administració Pública de Catalunya, preferiblement el CTTI. Conclusions de l'execució del servei vers el seu disseny i dimensionament i capacitat d'execució.
- Òrgans de governs de la transició post-quàntica a l'Administració pública de Catalunya, als diferents nivells de decisió necessaris. Relació d'òrgans, amb les seves funcions, entitats rols i persones integrants. Execució de les sessions de governança i actes de les mateixes.
- Full de ruta per a la transició post-quàntica de l'Administració Pública de Catalunya.

Projecte demostrador:

- Projecte demostrador de la transició post-quàntica de l'Administració Pública de Catalunya.
- Pla de projecte amb actors involucrats, rols i dedicacions, calendari de fites i tasques. Gestió del projecte i dels riscos de la seva execució, seguiment i control de l'execució.
- Execució del projecte amb els recursos del plec, tot coordinant els actors involucrats i sota la direcció de l'agència i els òrgans de govern generats al respecte.
- Informes de seguiment periòdic del projecte i actes de les reunions.
- Informe de tancament del projecte, amb conclusions i recomanacions de continuïtat.
- Resultat d'execució dels serveis objecte del plec a l'entitat objecte del projecte.
- Pla d'acció detallat de la transició post-quàntica a una entitat rellevant de a l'Administració Pública de Catalunya (entitat objecte del projecte demostrador), preferiblement el CTTI.

Identificació i inventari criptogràfic:

- Servei d'inventariat criptogràfic: Disseny del servei amb perfils, dimensionament i elements de cost, procediments, metodologies i eines per a l'inventariat de la criptografia present a les entitats. Execució del servei per a l'entitat objecte del projecte demostrador. Conclusions de l'execució del servei vers el seu disseny i dimensionament i capacitat d'execució.
- Eines per a l'inventariat criptogràfic
- Desplegament de les eines d'inventariat a l'entitat objecte del projecte demostrador.
- Integració de les eines d'inventariat a l'operativa d'avaluació de ciberseguretat de l'Agència de Ciberseguretat de Catalunya.
- Inventari criptogràfic de l'entitat objecte del projecte demostrador, comprenent l'enteniment dels processos on intervé la criptografia i l'estructura organitzativa que els sosté, seguida d'una enumeració automàtica i contínua dels elements tècnics que l'habiliten i configuren.
- Quadres de comandament associats a l'inventari criptogràfic (resultat de la tasca) i el seu assoliment (progrés de la tasca).

Avaluació i anàlisi contínua:

- Diagnosi mitjançant l'enteniment dels processos on intervé la criptografia i l'estructura organitzativa que els sosté, seguida d'una enumeració automàtica i contínua mitjançant eines, que culmini en una anàlisi de situació de l'entitat respecte de la criptografia i habiliti la revisió periòdica d'aquesta situació, mitjançant quadres de comandament amb els indicadors rellevants integrats als sistemes de gestió i seguiment de l'Agència de Ciberseguretat de Catalunya.
- Servei d'avaluació i anàlisi contínua de la robustesa vers la capacitat de computació quàntica, de les implementacions criptogràfiques presents a les entitats. Disseny del servei amb perfils, dimensionament i elements de cost, procediments, metodologies i eines (incloent qüestionaris, frameworks o controls, etc.) per a l'avaluació i anàlisi contínua de la robustesa criptogràfica de l'entitat. Execució del servei per a l'entitat objecte del projecte demostrador. Conclusions de l'execució del servei vers el seu disseny, dimensionament i capacitat d'execució.
- Desplegament de les eines d'avaluació i anàlisi contínua de la robustesa criptogràfica a l'entitat objecte del projecte demostrador, per a l'avaluació contínua de la criptografia present a l'entitat.
- Integració de les eines d'avaluació i anàlisi contínua a l'operativa d'avaluació de la ciberseguretat de l'Agència de Ciberseguretat de Catalunya.
- Evolutius o eines de nova creació per a l'avaluació i anàlisi contínua de la robustesa de la criptografia en ús.
- Avaluació de la robustesa de la criptografia en ús a l'entitat objecte del projecte demostrador, cobrint un percentatge superior al 80% del seu inventari criptogràfic objectiu.
- Quadres de comandament associats a la diagnosi i anàlisi contínua, i el seu assoliment.

Vigilància tecnologia i actualització contínua:

- Servei de vigilància tecnològica PQC i quàntica. Disseny del servei amb entitats i rols, perfils, dimensionament i elements de cost, procediments, metodologies i eines per a vigilància tecnològica i actualització contínua tant de l'amenaça i la vulnerabilitat vers aquesta, com de les capacitats, maduresa i viabilitat de les solucions disponibles. Execució del servei per a generar informes.. Conclusions de l'execució del servei vers el seu disseny, dimensionament i capacitat d'execució.
- Informe de vigilància tecnològica i actualització contínua PQC i quàntica. Per a alimentar el full de ruta amb un punt de partida, així com alimentar el pla d'acció de l'entitat objecte del projecte demostrador. Que estimi el termini d'aparició d'ordinadors quàntics universals criptogràficament rellevants, que identifiqui les novetats rellevants en a l'àmbit (estandardització, desenvolupament tecnològic de les solucions disponibles, adopció PQC en productes rellevants, etc.), i mesuri l'amenaça i la vulnerabilitat vers aquesta, com les capacitats, maduresa i viabilitat de les solucions disponibles.

Planificació estratègica: Full de ruta i pla d'acció:

- Servei de generació del full de ruta i dels plans d'acció per a la transició. Disseny del servei amb perfils, dimensionament i elements de cost, procediments, metodologies i eines per a oferir el servei a les entitats de l'Administració Pública de Catalunya. Execució del servei per a generar un full de ruta global i un pla d'acció per a l'entitat objecte del projecte demostrador.

Conclusions de l'execució del servei vers el seu disseny i dimensionament i capacitat d'execució
- Full de ruta per a la transició post-quàntica de l'Administració Pública de Catalunya
- Pla d'acció detallat de la transició post-quàntica a una entitat rellevant de l'Administració Pública de Catalunya, complementant el pla director de seguretat de l'entitat amb la vessant relativa a la transició post-quàntica. Aquest pla d'acció ha d'incloure la planificació de les activitats en les diferents vessants del pla (transició tecnològica amb proves, dimensionament i implantació; normativa; formació i conscienciació i gestió del canvi, etc.), acompanyades d'una planificació econòmica, però també aportant criteris de priorització. Caldrà que es recolzi en els resultats de l'execució de la identificació i anàlisi criptogràfica, l'avaluació i anàlisi contínua, i els demostradors, i generi projeccions a partir d'aquests resultats, els àmbits no coberts durant el projecte demostrador i el dimensionament dels serveis generats en l'execució del plec.
- Quadres de comandament associats a l'assoliment del full de ruta i del pla d'acció.

Normativa:

- Normativa compatible amb el marc regulatori de la ciberseguretat de la Generalitat de Catalunya, per al desplegament del pla d'acció per a la transició post-quàntica, d'acord a les seves fases i marc temporal. S'inclouen, entre altres, normes internes, guies de prescripció de requeriments tècnics a incorporar per a la contractació de solucions TIC (p.e. requerir suport PQC o suport a criptografia híbrida), etc.
  El mínim requerit es:
  - 1) les clàusules de la primera fase d'adopció de PQC en la contractació de noves aplicacions i solucions TIC,
  - 2) normativa de transició a la primera fase d'adopció de PQC per a les aplicacions, solucions i serveis existents

Demostració i mesura de viabilitat:

- Servei de demostració i mesura de viabilitat. Disseny del servei amb perfils, dimensionament i elements de cost, procediments, metodologies, eines i infraestructura. Execució del servei per a identificar i prioritzar els casos d'ús rellevants a demostrar per al pla d'acció de l'entitat, generar demostradors per a aquests casos d'ús i mesurar la viabilitat tecnològica, econòmica i organitzativa d'aplicabilitat d'aquests demostradors.
- Casos d'ús de demostració prioritzats.
- 5-10 demostradors tecnològics i de viabilitat per a casos d'ús prioritaris per al pla d'acció de l'entitat, desenvolupats, desplegats i mesurats. Repetibles i executables [i aprovisionables] sota demanda per a la demostració.
- Informe de conclusions de satisfacció del cas d'ús i de viabilitat per a cada demostrador.

Proves de rendiment i dimensionament d'arquitectura:

- Servei de proves. Disseny del servei amb entitats i rols, perfils, dimensionament i elements de cost, procediments, metodologies i eines. Execució del servei sobre els demostradors generats per a l'avaluació del rendiment comparat a les solucions pre-quàntiques i l'elaboració de conclusions vers el dimensionament de l'arquitectura que les suporta necessari per a suportar la transició.
- Entorn de proves on desplegar les solucions i els demostradors, i realitzar les proves de rendiment.

- Informe de resultat de les proves de rendiment i dimensionament, per a cada demostrador. Amb mesures nominals i comparatives del rendiment i conclusions vers el dimensionament de l'arquitectura que les suporta necessari per a suportar la transició.
- Pla de formació, generar els continguts i executar-lo, per a formar als equips dedicats a aquest tipus de proves per a habilitar-los en l'execució d'aquestes proves i incorporar casuístiques, característiques, indicadors i elements propis de la transició post-quàntica.

Conscienciació, formació i difusió:

- Pla de conscienciació, alineat amb la Ciberacademy, dissenyat per a exposar la problemàtica als diferents agents clau per a la transformació i per a que cadascun entengui el seu rol i els terminis de la transformació.
- Contingut didàctic de conscienciació.
- Sessions de conscienciació, amb els agents i perfils clau. Contingut i informe d'execució i resultats de les sessions.
- Informe d'execució del pla de conscienciació, amb resultats i conclusions.

- Pla de formació, alineat amb la Ciberacademy, dissenyat per a capacitar els diferents agents clau en l'exercici del seu rol per a dur a terme la transformació.
- Continguts formatius.
- Cursos formatius per als diferents agents i perfils clau. Contingut, execució i informe d'execució dels cursos.
- Informe d'execució del pla de formació, amb resultats i conclusions.

- Pla de difusió del projecte, alineat i en col·laboració del servei de Comunicació de l'Agència.
- Articles de difusió a mitjans.
- Jornades de difusió i informe d'impacte comunicatiu.

(iv) Abast del servei

L'abast mínim del servei és conforma segons les indicacions següents:

- Governança de la transició:
  - 1 entitat rellevant de l'Administració pública de Catalunya, preferiblement el CTTI.
- Projecte demostrador:
  - 1 projecte demostrador
- Identificació i inventari criptogràfic i Avaluació i anàlisi contínua:
  - Mostra representativa dels sistemes d'informació crítics i de les tecnologies que els suporten. No menor de 40 sistemes d'informació.
  - Mostra representativa de la infraestructura de xarxa amb funció de concentradors d'activitat criptogràfica. No menor de 5 elements, entre concentradors VPN, balancejadors, *proxies* de navegació i sistemes de protecció del correu i la navegació.
  - Mostra representativa de la gestió de la identitat digital corporativa i dels casos d'ús d'aquesta identitat. Contemplant la gestió del cicle de vida de la identitat i no menys de 2 casos d'ús d'aquesta identitat.
  - Mostra representativa de la infraestructura cloud de l'entitat. Contemplant com a mínim un proveïdor cloud i algun dels *tenants* de l'entitat en aquest.

  - Mostra representativa de les tècniques actualment viables d'identificació i inventari criptogràfic i Avaluació i anàlisi contínua. Contemplant identificació en xarxa i en host, en producció/ús i en codi, sempre que siguin d'utilitat en la satisfacció dels punts anteriors d'aquest mateix apartat.
- Planificació estratègica: Full de ruta i pla d'acció:
  - Donant cobertura mínim al 80% dels elements contemplats en la Identificació i inventari criptogràfic i l'Avaluació i anàlisi contínua.
  - Contemplant tots els demostradors i incorporant els aprenentatges, resultats i projeccions derivades dels mateixos (projeccions de viabilitat, costos, temporalitat, dimensionament d'arquitectura i serveis, etc.)
- Normativa
  - El mínim requerit es:
    - 1) redacció de les clàusules tipus per inserir en els plecs de contractació de l'entitat, per a la primera fase d'adopció de PQC en la contractació de noves aplicacions i solucions TIC,
    - 2) redacció d'una norma de transició a la primera fase d'adopció de PQC per a les aplicacions, solucions i serveis existents, donant cobertura mínim al 80% dels elements contemplats en la Identificació i inventari criptogràfic i l'Avaluació i anàlisi contínua.
- Demostració i mesura de viabilitat:
  - Mínim 5 demostradors tecnològics i de viabilitat per a casos d'ús prioritaris per al pla d'acció de l'entitat, desenvolupats, desplegats i mesurats. Repetibles i executables [i aprovisionables] sota demanda per a la demostració.
- Proves de rendiment i dimensionament d'arquitectura:
  - Per a tots els demostradors tecnològics desplegats,
  - Així com per a la mesura de l'impacte en aplicacions i infraestructura, de la Identificació i inventari criptogràfic i Avaluació i anàlisi contínua.
- Conscienciació, formació i difusió:
  - La necessària per a involucrar als actors necessaris per al projecte i garantir l'exercici dels rols assignats amb continuïtat en el temps. Amb mínim un curs per tipologia d'actor.
  - Mínim una jornada de difusió a les acaballes del projecte.

2.1.2 Característiques del servei.

De tot el que s'ha exposat prèviament s'han de tenir en compte els següents elements per a la prestació de l'objecte del contracte:

- Estratègia d'execució amb detall de la segmentació de l'abast i la seva priorització i la metodologia i mecanismes tecnològics per a l'avaluació. Interessa un enfoc a resultats que garanteixi completar cicles d'identificació-avaluació-planificació-demostració-viabilitat, i parteixi del coneixement del licitador de què funciona en cada segment.

- Propostes de millores en el servei que tinguin com objectiu augmentar el nivell de cobertura (abast) del pla d'acció vers els elements TIC de l'entitat. Mantenint l'orientació del projecte cap a l'avaluació i demostració de viabilitat, i per tant, cap a nous casos d'ús i no tant cap a la completesa del desplegament. P.e. a priori interessa més contemplar 10 aplicacions significatives en un balancejador i una VPN corporativa, que no totes les aplicacions del balancejador.

3 Condicions d'execució del servei

3.1 Horaris

El servei s'haurà de prestar d'acord amb els horaris de prestació dels serveis de l'Agència, 8x5 en horari de dies laborables. Es considera horari de dies laborables els dies que siguin laborables al centre de treball de l'Hospitalet de Llobregat amb prestació de 9:00h a 18:00h.

A petició expressa de l'Agència, es podria demanar la realització d'algunes tasques fora de l'horari de dies laborables per tal de garantir el correcte desenvolupament del servei.

Si durant l'execució del contracte l'Agència o l'adjudicatari detecten la necessitat de modificar l'horari del servei o equip descrit en aquest plec, l'Agència i l'adjudicatari consensuaran de forma conjunta la modificació, essent l'Agència qui finalment designi l'horari de prestació que s'adeqüi a les necessitats pròpies i que no perjudiqui de forma excessiva a l'adjudicatari.

3.2 Localització física.

Inicialment, els equips prestataris dels serveis estaran ubicats físicament a les oficines de l'adjudicatari o en alguna altra que ambdues parts acordin, atenent sempre a la seguretat de la informació gestionada pel servei. Tot i això, l'Agència considera que l'adjudicatari, en coordinació amb la Direcció de l'àrea de l'Agència, podria arribar a prestar/executar fins al 50% de les tasques/projectes/serveis amb recursos ubicats a les instal·lacions de l'Agència de Ciberseguretat a l'Hospitalet de Llobregat.

Addicionalment, s'ha de contemplar la possibilitat que part d'aquests serveis requereixin del desplaçament dels professionals a les instal·lacions dels clients de l'Agència que poden estar ubicades a qualsevol part del territori de Catalunya.

Al llarg del contracte es podria requerir un canvi en la ubicació dels professionals, d'acord amb les necessitats dels serveis i l'organització d'equips de treball. En cap cas la ubicació dels professionals suposarà un increment dels costos vinculats a la prestació de

3.3 Equip de treball

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos de l'adjudicatari del contracte amb la qualificació necessària i adequada per a la prestació del servei.

Els mitjans personals necessaris per a la prestació dels serveis han de ser els adequats per realitzar amb garantia les tasques definides i han de mostrar les habilitats necessàries per tal d'integrar-se en un equip d'alt rendiment, entre les quals es podrien determinar a efectes enunciatius les següents:

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.

- Habilitat per identificar, analitzar i resoldre problemes.
- Capacitat de treball sota pressió.
- Coneixement de català, castellà i d'anglès, parlat i escrit.
- Ampli coneixement legal, tecnològic i de negoci de seguretat informàtica i de l'entorn de l'administració pública.
- Altres necessaris per al bon desenvolupament dels serveis.

El licitador proposarà un equip de treball (descrivint-ne els perfils, dedicació, pla de treball, etc.) per a l'execució dels serveis sol·licitats en el present plec, d'acord amb les condicions i paràmetres esmentats en els apartats d'aquest plec.

No es preveu la possibilitat de transferència del personal intern de l'Agència o dels seus clients.

L'adjudicatari disposarà d'una figura que assumirà les tasques de **cap de projecte.** A aquest efecte, ha de assumir les següents responsabilitats:

- Actuar com a punt de contacte únic en relació amb la gestió ordinària dels serveis amb poder de decisió sobre els principals elements del contracte.
- Consolidar i aportar a l'Agència les informacions objectives i subjectives que permetin a la Direcció la presa de decisions operatives i estratègiques relacionades amb el contracte i els serveis que se suporten.
- Garantir que l'Agència rebi els informes de gestió acordats i realitzar el seguiment econòmic i d'activitat amb els interlocutors de l'Agència.
- Garantir la transparència en el control de gestió per tal d'agilitzar el procés de seguiment i facturació.
- Coordinar i fer el seguiment de l'activitat.
- Planificar l'activitat i mantenir la informació dels plans de capacitat.
- Assegurar una bona col·laboració entre els diferents agents implicats en la prestació de serveis als clients de l'Agència.
- Coordinar l'equip del projecte, inclòsos els actors de l'Agència i de les altres entitats involucrades.

Si bé es considera necessària la implicació de múltiples perfils especialitzats per a la prestació del servei a fi de garantir l'èxit del projecte, la composició de l'equip es deixa a càrrec del licitador.

Els licitadors hauran d'incloure en la seva proposta l'organigrama i esquemes d'equips per tal de donar resposta a les necessitats expressades en aquest plec.

Per raons d'operativitat, de coneixement de les tasques a realitzar i de sensibilitat de la informació amb la que es treballa, cal garantir al màxim la continuïtat de l'equip que donen servei a l'Agència.

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest plec és de **17.000 hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals pels perfils indicats:

Perfil	Hores anuals mínimes estimades
Cap de projecte	**1.400 hores**

Els requisits anteriors s'han d'entendre com a mínims aproximats, podent els licitadors ampliar-los i millorar-los a les seves ofertes.

3.3.1 Perfils

Els requeriments mínims dels perfils professionals que poden composar l'equip són els següents:

Perfil	Experiència mínima
• Cap de projecte	5 anys
- Desenvolupador sènior/a - Integrador sènior/a - Consultor sènior/A - Formador/a sènior - IT Management - Tester seguretat i rendiment - Criptògraf/a	3 anys

En el marc de l'objecte del contracte s'haurà de realitzar el suport a la redacció de clàusules contractuals relacionades amb el projecte (apartat 2.1.1. (IV) del present plec)

S'entén que aquests perfils es corresponen amb els rols que, des de l'Agència, s'identifiquen per la prestació d'aquest servei, deixant a la banda dels licitadors la proposta de desplegament, composició de l'equip, adequació de perfils i dedicació global dels mateixos.

3.4 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present apartat o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies laborables a partir de la recepció de la comunicació per part de l'adjudicatari o bé la notificació de l'Agència a l'empresa adjudicatària del contracte. L'adjudicatari haurà de presentar en un termini màxim de 10 dies laborables a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució. Si l'objecte del contracte ho requereix, aquest aspecte es podrà concretar en aquest.

3.5 Control de rotació

L'estabilitat dels recursos del servei amb coneixement i compromís és molt important per a la correcta prestació del servei.

L'empresa adjudicatària del contracte podrà fer canvis en l'equip de treball durant l'execució del contracte, però ho haurà de notificar per escrit a l'Agència amb una antelació mínima de 14 dies naturals, justificant el canvi i informant del perfil i característiques de la persona que s'incorpora. L'Agència comprovarà que la persona a incorporar compleix amb les condicions curriculars del component de l'equip que substitueixi.

L'empresa assumirà la selecció de les persones de nova incorporació, la coexistència en el servei del personal sortint i l'entrant sense cost per l'Agència, assegurant el correcte traspàs de coneixement en els següents 15 dies i duent a terme els controls necessaris per garantir-lo entenent, per tant, la no facturació d'aquests dies d'adaptació i traspàs. Sens perjudici que si s'escau es puguin aplicar els ANS corresponents per rotació excessiva.

En cap cas la substitució de personal suposarà un cost addicional, havent-se de garantir que el servei no es vegi afectat per aquest canvi. Si l'objecte del contracte ho requereix, aquest aspecte es podrà concretar en el contracte.

3.6 Eines i equipament per a la prestació de serveis.

Les principals eines requerides (gestió d'esdeveniments, alertes, sistema de registre, anàlisi de codi, web i infraestructura...) per la prestació del servei seran proporcionades per l'Agència. El licitador haurà de fer servir aquestes eines, no podent extreure informació fora de l'àmbit d'actuació per la seva manipulació o explotació sense autorització prèvia de l'Agència.

Quan l'adjudicatari es trobi en les instal·lacions de l'Agència, proveirà a les persones que prestin els serveis:

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l'Agència.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides l'Agència.
- Telefonia fixa a les instal·lacions del servei.
- Telefonia mòbil per donar cobertura als serveis de guàrdia.
- Accés a Internet a través de la xarxa d'àrea local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.

L'Agència no proveirà:

- Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina ni tampoc ordinadors portàtils amb el programari habitual de l'Agència.
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'Agència.
- Accés a Internet via GPRS, UMTS.
- Cap altre recurs no especificat explícitament.

En conseqüència, els adjudicataris hauran de:

- Subministrar tots elements de maquinari, programari i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments de l'objecte del contracte. Aquests elements seran *d'ús exclusiu* pels serveis prestats a l'Agència i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.
- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat Corporativa de l'Agència.
- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip de Mitjans Tècnics de l'Agència.

L'Agència es troba en un procés de revisió i millora contínua que pot implicar la realització de canvis importants en el referent a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei.

Per aquest motiu és imprescindible que l'adjudicatari tingui presents les següents consideracions en el referent a les eines de gestió durant l'execució del contracte.

- L'Agència decidirà la utilització de qualsevol tecnologia nova o evolució de les existents, relacionades amb la prestació del servei.
- L'Agència decidirà la forma d'implantar qualsevol d'aquests nous sistemes, planificar els projectes corresponents i el seu calendari, així com la transició des dels sistemes existents cap als nous.
- Els adjudicataris es comprometen a assumir i adaptar-se a aquestes noves tecnologies i sistemes per donar el servei de suport, així com participar activament en el procés de transició, formant i preparant el seu personal en aquestes noves tecnologies i sistemes implantats sense cost addicional per l'Agència.

3.7 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions com a Centre d'Innovació i Competència en Ciberseguretat (CIC4Cyber) i, especialment, l'impuls de la transformació fonamentada en el coneixement col·laboratiu, la coordinació de l'ecosistema de ciberseguretat i la voluntat per la innovació continua, es requereix que l'empresa adjudicatària registri tot el coneixement que disposi i es generi en la contractació que derivi d'acord amb les directrius del CIC4Cyber.

A tal efecte, l'adjudicatària haurà de mantenir aquest coneixement actualitzat i accessible per a l'organització, havent de proporcionar una descripció detallada del coneixement que es disposi i es generi al servei ofert, i tenint, per part de l'organització, accés a aquest coneixement en qualsevol moment.

Addicionalment a l'anterior, cal tenir en compte que el plec descriu requeriments de formació, conscienciació i difusió en relació a la gestió del coneixement relatiu al projecte, que també cal honorar.

3.8 Seguretat Corporativa

Un cop adjudicat el contracte, tant l'empresa adjudicatària com el personal de l'empresa adjudicatària s'haurà de sotmetre a les polítiques i regulacions internes que estableix l'àrea de Seguretat Corporativa en matèria de seguretat de la informació, com a mínim i no limitant-se a:

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per Seguretat Corporativa, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- Facilitar l'accés en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de l'Agència (sigui o no per l'exercici de la seva funció).
- Acceptar les normes i polítiques que estableix l'àrea de Seguretat Corporativa tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.
- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'àrea de Mitjans Tècnics per fer el desplegament de polítiques i controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.
- Els equips, així com la informació resident dels mateixos serà sempre custodiada per l'Agència.
- Garantir l'estabilitat dels equips (reduint al mínim la rotació de personal).
- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (ENS, LOPDGDD, GDPR, LSSI, etc.).

A la finalització del contracte, l'adjudicatari del contracte quedarà obligat al lliurament o destrucció en cas de ser sol·licitada, de qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

3.9 Control de Gestió

L'empresa adjudicatària del contracte, 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.

3.10 Documentació.

L'Agència és el propietari de tota la documentació elaborada pels adjudicataris referent al servei prestat pels adjudicataris i el seu personal i subcontractats que destini a l'execució dels serveis. L'adjudicatari s'encarregarà de disposar de totes les autoritzacions i permisos necessaris per tal de poder donar compliment a aquesta previsió, essent responsabilitat de l'adjudicatari qualsevol pagament o reclamació relativa a aquesta manca d'autoritzacions.

Els responsable de servei de l'Agència serà els responsable de la validació i aprovació dels documents elaborats pel personal de l'adjudicatari. En cas que la qualitat dels documents sigui molt baixa o de manera recurrent i/o perllongada en el temps de prestació dels serveis no assoleixi els nivells requerits s'aplicaran les penalitzacions establertes en la present contractació.

L'adjudicatari haurà de mantenir la documentació actualitzada en el sistema de gestió documental que l'Agència proporcioni per tal efecte

3.11 Formació

El personal de l'empresa adjudicatària del contracte realitzarà, si s'escau, formació continuada per tal de garantir l'actualització dels seus coneixements així com l'adquisició de nou coneixement que pugui ser de valor pels serveis de l'Agència.

L'adjudicatari haurà de reservar un 1% del temps del personal per tasques de formació i certificació (en matèries relacionades amb l'activitat del contracte) i aquest temps no serà facturat a l'Agència, valorant-se la disposició d'un pla de formació per al personal de l'adjudicatari destinat a l'Agència. Aquest pla es coordinarà amb les activitats i accions de formació pròpies de l'Agència.

Addicionalment a l'anterior, cal tenir en compte que el plec descriu requeriments de formació, conscienciació i difusió en relació a la gestió del coneixement relatiu al projecte, que també cal honorar. Aquests van destinats, en primer lloc a les persones clau de les entitats involucrades en el projecte amb l'objectiu de garantir-ne l'execució i, en segon lloc, a altres entitats amb l'objectiu de posar en valor el projecte demostrador per a facilitar la transició post-quàntica a altres entitats.

3.12 Contingència

Els licitadors hauran 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 de l'adjudicatari, 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 i
    - 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.

3.13 Metodologia, estàndards i lliurables

L'organització del treball i execució del servei s'haurà d'adequar a les metodologies, estàndards i lliurables establerts per l'Agència vigents en el moment de l'execució del servei objecte del contracte.

3.14 Seguretat

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

3.11.1. Deure de confidencialitat

Tot el personal de l'empresa adjudicatària així com els possibles subcontractistes han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat s'haurà de mantenir durant 10 anys, o el que s'especifiqui en el contracte, 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 ha de comunicar aquesta obligació de confidencialitat al seu personal ja sigui intern com extern, que estigui involucrat en l'execució del contracte i possibles subcontractistes i ha de controlar el seu compliment.

L'empresa adjudicatària 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 del contracte 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 del contracte 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 del contracte 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 del contracte el lliurament de la documentació acreditativa de la conformitat amb l'ENS. L'empresa adjudicatària del contracte 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 del contracte 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 del contracte haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

3.11.4. Capacitat tècnica

Per a poder executar el contracte i oferir garanties de la seva capacitat tècnica, l'empresa adjudicatària del contracte haurà de presentar compromís exprés d'adscripció al contracte dels mitjans personals que s'especifiquin als plecs, complint amb els requeriments definits de formació, i acreditar la disposició efectiva dels mateixos.

L'empresa adjudicatària del contracte 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. Adquisició de productes/eines i productes o serveis de seguretat

Tant en el cas que es desenvolupin productes/eines, es facin integracions amb altres eines o s'adquireixin eines de mercat o qualsevol component de sistemes d'informació (hardware, software, etc.), aquests hauran de ser compatibles amb l'arquitectura de seguretat de l'Agència i complir amb els requeriments de seguretat que estableixi el marc legal i el marc normatiu intern, sotmetre's a proves tècniques de seguretat i aplicar les correccions necessàries prèviament a la posada en producció del producte/solució/eina. Caldrà incorporar el producte/eina dins el procés de desenvolupament segur de l'Agència de Ciberseguretat des de la fase de disseny fins a la posada en producció.

L'empresa adjudicatària del contracte haurà de garantir que disposa dels perfils amb la capacitació i la formació necessària per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició. A més, haurà de proporcionar formació i capacitació per al personal que designi l'Agència per tal que aquest personal adquireixi els coneixements necessaris per tal de poder operar, gestionar i mantenir els productes, eines o components objecte d'adquisició.

En cas que es contractin productes de seguretat o serveis de seguretat de les tecnologies de la informació i la comunicació que vagin a ser emprats en els sistemes d'informació de l'Agència, segons estableix l'ENS, hauran de tenir certificada la funcionalitat de seguretat relacionada amb el seu objecte d'adquisició. Els productes o serveis de seguretat hauran de constar al Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del Centre Criptològic Nacional o bé complir amb els criteris que estableixi l'Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centre Criptològic Nacional o, en el seu defecte, acreditar que el producte o servei disposa de requeriments equivalents.

3.11.6. Interconnexions

Segons preveu l'ENS, en el cas que sigui necessari realitzar interconnexions entre sistemes de l'empresa adjudicatària del contracte i l'Agència o amb d'altres entitats:

- No es podran dur a terme, tret que prèviament hagin estat autoritzades expressament per l'Agència.
- En cas que s'autoritzi una interconnexió, l'empresa adjudicatària del contracte haurà de garantir que es documentin com a mínim les característiques de la interfície, els requisits de seguretat i protecció de dades i la naturalesa de la informació intercanviada. Aquesta documentació l'haurà de facilitar a l'Agència.
- L'empresa adjudicatària del contracte haurà de participar en els mecanismes de coordinació que estableixi l'Agència i seguir els procediments establerts per aquest fi, per a poder atribuir i exercir de manera efectiva, les responsabilitats en relació a cada sistema interconnectat.

3.11.7. 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 del contracte 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.

3.11.8. Incidents de seguretat

El POC 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 del contracte 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 del contracte 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.

3.11.9. Accés a la informació

L'empresa adjudicatària del contracte haurà de garantir l'accés del personal autoritzat de l'Agència de Ciberseguretat a la informació de seguretat (procediments, registre d'incidents, traces, etc.) per a poder desenvolupar l'objecte del contracte.

Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. L'Agència de Ciberseguretat i l'empresa establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.

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

L'empresa 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.
- Plans de millora del servei orientats a millorar el compliment dels objectius del servei i del negoci.
- 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 per millorar la qualitat percebuda i la satisfacció dels usuaris.
- Accions preventives per la mitigació de riscos, tenint en compte la seva probabilitat i el seu impacte.
- Accions dirigides a millorar la gestió del coneixement i incrementar la usabilitat dels serveis.
- Accions per maximitzar l'eficiència i la sostenibilitat del servei.

3.13. Seguiment del servei

Les empreses adjudicatària haurà de presentar un informe de seguiment de cada contracte d'acord amb els indicadors de compliment i altra informació rellevant pel seguiment del servei. Aquests informes s'avaluaran als comitès operatius i es formalitzaran i s'elevaran els seus resultats a la resta de comitès.

L'informe de seguiment haurà de tenir, com a mínim:

- Un informe de gestió dels serveis desenvolupats per a cada, amb indicació de les activitats realitzades i les previstes realitzar, les volumetries globals d'activitat i els indicadors de compliment especificats als. Acords de Nivell de Servei (ANS) de cada contracte.
- Un informe de dedicació del contracte a les diferents funcions requerides, per tal de poder avaluar la distribució dels esforços.

- Un informe d'accions de millora de l'activitat del propi contracte, on es detallaran les accions de millora proposades amb informació rellevant per a la seva gestió (per exemple, el benefici previst obtenir, el termini d'implantació, etc.). Per cada millora implantada s'establirà, sempre que sigui possible, un indicador que s'afegirà a l'informe de gestió dels serveis. La periodicitat de l'informe de seguiment serà mensual, quant al seguiment de les activitats i la implantació de les millores. La presentació de les propostes de millora es farà amb la periodicitat indicada en cada contracte o el que es determini per part del responsable del contracte de l'Agència de Ciberseguretat.

Pel control i seguiment del servei s'utilitzaran dades, mètriques i informes (en endavant informació) que serviran de suport als òrgans de gestió establerts i que són, en el seu conjunt, el mecanisme de seguiment i avaluació del servei. Aquesta informació es pot fer extensible a altres Unitats, Àrees, Direccions de l'Agència o tractar-se d'anàlisi puntual.

L'empresa adjudicatària del contracte és la responsable de generar i lliurar la informació que es determini en els diferents àmbits del servei, la qual ha de permetre a l'Agència governar, controlar i gestionar els serveis prestats objecte del contracte, tant des d'una òptica individual, com transversal i global.

La periodicitat, dates límit de lliurament, canals de transmissió, format exacte i contingut detallat de la informació a elaborar en tots els àmbits del servei, seran definits per l'Agència. L'Agència podrà sol·licitar, durant la vigència del contracte, ampliacions i canvis en el contingut, periodicitat, canals i format de la informació per ajustar-se a les necessitats de seguiment dels serveis.

L'empresa es compromet a automatitzar tot el possible els processos de generació i transmissió de la informació, arribant a la màxima integració possible.

L'empresa es compromet a proporcionar informació veraç i contrastada, i haurà de disposar dels mecanismes necessaris per garantir-ho. L'Agència podrà dur a terme les auditories que consideri necessàries per a la seva verificació, obligant-se l'empresa a participar-hi de manera activa i diligent sense cap cost afegit per a l'Agència.

L'Agència podrà sol·licitar informació de forma immediata i l'empresa hi donarà resposta ràpida fora de la planificació establerta.

3.14. Integració amb altres equips

L'adjudicatari del contracte haurà de portar a terme les activitats d'integració amb la resta d'equips operatius que conformen l'Agència, tant amb personal intern com amb personal d'altres empreses contractistes.

Aquesta integració s'haurà de portar a terme tant a nivell de la operativa diària (per garantir l'execució dels processos de la cadena de valor de l'Agència) com a nivell tàctic i operatiu.

Tot i això, els models de relació han de garantir els següents punts:

- Participació de l'adjudicatari en els processos que l'afectin.
- Compartició d'informació sobre fets puntuals (incidències, alertes, vulnerabilitats, etc.), ja sigui amb l'Agència com directament amb altres proveïdors.
- Compartició d'informació sobre fets agregats (tendències, patrons) i sobre afectacions col·lectives als diferents clients de l'Agència.
- Eliminació de les sitges organitzatives.

- Creació d'un fons comú de coneixement sobre la seguretat de la informació.
- Creació de bucles de retroalimentació que facilitin una resposta àgil davant de qualsevol nova situació en matèria de seguretat.