Plec de prescripcions tècniques particulars que regeix la contractació relativa a serveis vinculats a l'execució d'auditories de certificació de la conformitat amb l'Esquema Nacional de Seguretat (ENS) a les Administracions Locals

Exp. COS.02.2025

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

Índex

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

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.

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.

El programa RETECH

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

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

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.

En aquesta línia, l'Agència participa d'aquesta iniciativa per reforçar la Ciberseguretat a Catalunya mitjançant el desplegament de projectes finançats que garanteixin l'aportació de valor i ajudin a millorar el nivell de Ciberseguretat de Catalunya i dels seus ciutadans.

Per assolir aquest objectiu, l'Agència es veu en la necessitat de licitar dues Oficines Tècniques per la gestió dels fons i per la gestió dels projectes, finançades amb fons RETECH , com a eina per assegurar que tots els projectes i iniciatives desplegats per l'Agència de Ciberseguretat assoleixin els objectius establerts i es garanteixi el compliment de tots els mecanismes de control i supervisió que siguin necessaris.

Aquest contracte està finançat per Fons Europeus.

2. Descripció dels serveis objecte de la contractació

2.1. Context dels serveis objecte de la licitació

El servei objecte de licitació en aquest plec està contextualitzat en els fons RETECH. El Projecte RETECH CCAA va ser avaluat i aprovat per la Comissió d'Avaluació de l'INCIBE el 7 de desembre de 2022. Posteriorment, el 18 de desembre de 2023, INCIBE i les comunitats autònomes de Catalunya (a través de l'Agència de l'Agència de Ciberseguretat de Catalunya), la Comunitat Valenciana (a través de la Direcció General de Tecnologies de la Informació i les Comunicacions de la Conselleria d'Hisenda, Economia i Administració Pública de la Generalitat Valenciana) i Galícia (a través de l'Agència per a la Modernització Tecnològica de Galícia, AMTEGA) van formalitzar un conveni de col·laboració per a l'execució del projecte.

En el cas de la Comunitat Autònoma de Catalunya l'Agència de Ciberseguretat és l'entitat responsable de la implementació del Projecte RETECH CCAA i de les actuacions derivades de l'Acord RETECH a Catalunya. Per tant, li correspon concretar els múltiples subprojectes i accions de ciberseguretat que promouran el desenvolupament tecnològic i incrementaran la confiança digital tant del govern autonòmic com dels ciutadans i empreses del territori català.

Concretament s'emmarca en el Component 15.I07

L'Agència de Ciberseguretat de Catalunya impulsa la gestió i execució de projectes finançats amb fons europeus en el marc del programa de RETECH, amb l'objectiu d'enfortir les capacitats de ciberseguretat del territori.

Un dels projectes contemplat en les actuacions previstes en el Pla Anual Operatiu (PAO) dels fons europeus Retech és de la protecció de les administracions locals.

Com a part de les activitats previstes en el projecte de protecció de les administracions locals, es troba l'adequació i certificació en l'Esquema Nacional de Seguretat de les administracions locals a Catalunya. La present licitació inclou només les activitats de certificació en l'Esquema Nacional de Seguretat, quedant separada i independent de qualsevol tasca d'adequació que es farà via un altre canal.

A data de 4 d'agost de 2023 es va certificar el reconeixement de l'Agència com Òrgan d'Auditoria Tècnica (OAT, en endavant) per part del Centre Criptològic Nacional (CCN, en endavant), permetent a l'Agència realitzar auditories de certificació de conformitat amb l'Esquema Nacional de Seguretat en l'Administració de la Generalitat de Catalunya i el seu sector públic, així com en les entitats i àmbits sota el seu àmbit competencial.

L'objecte d'aquest contracte és la prestació de serveis d'**auditories de certificació de la conformitat amb l'Esquema Nacional de Seguretat, sota la coordinació de l'Òrgan d'Auditoria Tècnica de l'Agència de Ciberseguretat de Catalunya, per a les administracions locals**.

2.2. Servei d'Auditories de certificació de la conformitat amb l'ENS

2.2.1. Objecte i abast del servei

L'objecte dels serveis és dur a terme auditories de certificació de la conformitat amb l'Esquema Nacional de Seguretat (ENS, en endavant) en les entitats del món local a Catalunya, emetent els certificats de conformitat de l'OAT de l'Agència de Ciberseguretat derivats, i vetllant per l'alineament dels processos segons el sistema de gestió de l'Òrgan d'Auditoria Tècnica de l'Agència i les guies i Instruccions Tècniques de Seguretat (ITS) del CCN.

Els requeriments que estableix el CCN per a un OAT, es troben recollits a la guia "CCN-STIC-122 Procediment de reconeixement d'entitats de certificació de l'ENS del sector públic i requisits de l'OAT". L'Agència té l'obligació de donar compliment a aquesta guia per mantenir-se reconeguda com a OAT, i es troba sotmesa a revisions periòdiques per part del CCN per verificar aquest fet.

Per tal de donar compliment a la guia CCN-STIC-122, l'Agència ha desplegat un sistema de gestió basat en la "ISO/IEC 17065:2012 Avaluació de conformitat – Requisits per a organismes que certifiquen productes, processos i serveis". Aquest sistema de gestió ajuda a disposar d'uns processos coherents, i garantir la imparcialitat i competència de l'OAT. Així mateix, els processos definits per dur a terme les auditories de certificació es basen en la guia de seguretat "CCN-STIC CCN-CERT IC-01/19 – ENS. Criterios Generales de Auditoría y Certificación", que serveix de referència i estableix els criteris generals per a auditoria i certificació dels sistemes d'informació de l'àmbit d'aplicació de l'ENS, dirigit a entitats de certificació i OAT, de conformitat amb allò assenyalat a l'article 31 del Reial Decret 311/2022, de 3 de maig, sobre auditoria de seguretat, i en allò disposat a la seva normativa de desenvolupament o complementària, singularment, les Instruccions Tècniques de Seguretat i les Guies CCN-STIC que resultin d'aplicació.

L'abast del servei inclou aproximadament 22 auditories de certificació de conformitat amb l'ENS a entitats del món local, amb una estimació inicial d'1 auditoria de certificació de conformitat de categoria Alta, 4 auditories de certificació de conformitat de categoria Mitjana, 2 auditories de certificació de conformitat de categoria Bàsica i 15 auditories de certificació de conformitat al Perfil de Compliment Específic de Requisits Essencials de Seguretat (o equivalent). Aquesta repartició és una estimació inicial, però cal tenir present que pot veure's alterada en funció de les necessitats reals de les entitats i el seu nivell de maduresa.

2.2.2. Objectius del servei

El servei sol·licitat en aquest contracte vol assolir els següents objectius, que es llisten a continuació:

- Executar auditories de certificació de la conformitat amb l'ENS en sistemes d'informació de les entitats del món local seguint els processos de l'Òrgan d'Auditoria Tècnica de l'Agència de Ciberseguretat, així com les guies i Instruccions Tècniques de Seguretat (ITS) del CCN, en tot el seu cicle de vida: suport en la planificació i preparació prèvia a l'auditoria, pla d'auditoria, auditoria en sí (revisió d'evidències *in-situ*), valoració dels incompliments, informe de resultats, valoració dels PAC (Plans d'Accions Correctives) i recomanació per certificació, entre d'altres.
- Assegurar l'exactitud, coherència i completesa dels resultats de l'auditoria i realitzar una comunicació clara i transparent a l'auditat.
- Gestionar i custodiar adequadament la documentació de l'auditoria als repositoris de l'Agència.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

- Garantir l'absència de conflictes d'interès.

2.2.3. Activitats que s'esperen del servei

Les activitats i funcions que s'esperen del servei són:

- Executar auditories de certificació de conformitat amb l'ENS sol·licitades per les entitats de l'administració local un cop estiguin adequades a l'ENS, seguint els criteris generals d'auditoria i certificació CCN-CERT IC-01/19, la guia d'auditories de compliment CCN-STIC-802 i els procediments de l'OAT. Les diferents auditories sol·licitades poden ser, de Perfils de Compliment Específics, o auditories d'ENS estàndard de categoria Bàsica, Mitjana o Alta.
- Gestionar adequadament les peticions sol·licitades i donar suport al Responsable tècnic de l'OAT per calcular les jornades d'auditoria i planificar-la.
- Gestionar adequadament l'eina AMPARO en les auditories de perfils de compliment específic. AMPARO és una eina desenvolupada pel CCN per a la governança de la ciberseguretat d'ús exclusiu per a entitats de certificació i OAT, que incorpora funcionalitats per facilitar els processos d'auditoria, la conformitat del sistema i la gestió de la certificació de conformitat.
- Preparar el pla d'auditoria en les auditories ENS de categoria Bàsica, Mitjana o Alta.
- Documentar totes les notes d'auditoria per donar evidència de les mesures auditades i l'exactitud de l'auditoria de cara a una possible revisió per part del Responsable Tècnic de l'OAT o el CCN.
- Redactar de forma clara i entenedora, les observacions i no conformitats identificades.
- Realitzar les reunions i visites presencials que pertoquin per verificar la conformitat de les mesures.
- Reportar l'avenç de l'auditoria, riscos i problemes detectats al Responsable de Servei d'Auditoria de l'Agència de forma coordinada, així com la proposta de millores detectades durant el procés.
- Elaborar l'informe de resultats de l'auditoria seguint les plantilles de l'Agència.
- Sol·licitar i validar, en cas de ser necessari, un Pla d'Accions Correctives (PAC) en relació a les troballes identificades durant l'auditoria.
- Reportar de forma coordinada al Responsable Tècnic de l'OAT les conclusions de l'auditoria, i la recomanació de certificar o no el sistema auditat. El Responsable Tècnic de l'OAT serà l'encarregat d'escalar la recomanació al Comitè de Certificació de l'Agència, qui comunicarà finalment la decisió de certificar a l'auditor cap.
- Donar suport als responsables de l'Agència en la creació del certificat de conformitat en l'ENS amb les plantilles de l'Agència.
- Comunicar a l'entitat la publicació del certificat al Portal de Governança del CCN.
- Gestionar, tractar i emmagatzemar adequadament totes les evidències i documentació recopilada durant l'auditoria a les eines que disposi l'Agència.

Addicionalment a l'execució pròpiament dita de l'auditoria, s'espera:

- Garantir els temps, la coherència i les formes en la realització de les tasques i resultats de cadascuna de les auditories.
- Mantenir una comunicació efectiva tant amb l'OAT com amb l'entitat auditada, assegurant-se que es transmeti la informació adequada en cada etapa del procés.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

- Aportar millores al procés d'auditoria identificades per l'equip auditor durant el transcurs de la mateixa, en base a la seva experiència i coneixement, que permeti evolucionar i fer més eficient les futures auditories de conformitat en l'ENS.
- Garantir que els integrants de l'equip auditor no hagin participat o dut a terme responsabilitats prèvies en el sistema d'informació auditat, o no hagin donat cap tipus d'assessorament o consultoria, per a aquest sistema, almenys en els dos últims anys.
- Garantir que els integrants de l'equip auditor han signat abans de començar l'auditoria un acord de confidencialitat amb l'OAT.
- Garantir la imparcialitat dels equips en la realització de les auditories de certificació.

2.2.4. Lliurables del servei

El model de prestació del servei haurà de contemplar la definició, els continguts i la periodicitat dels lliurables del servei. Entre els lliurables se'n poden considerar alguns de recurrents, tant de la pròpia gestió i seguiment del servei, d'altres operatius, i d'altres sota demanda.

Durant la prestació de servei l'empresa adjudicatària ha de generar i entregar de forma enunciativa i no limitativa els següents lliurables:

Document	Descripció	Periodicitat
Report d'estat	Report de l'avenç de les auditories, així com riscos i problemes detectats, amb el seu pla de mitigació o resolució.	Mensual
Pla d'Auditoria	Pla d'auditoria amb la distribució de les mesures de seguretat a revisar, les diferents sessions a realitzar i els interlocutors que participaran en cadascuna d'elles.	Per auditoria
Notes de l'auditoria	Actes/notes de les troballes i aspectes identificats a les diferents entrevistes realitzades.	Per auditoria
Evidències	Evidències recopilades i emmagatzemades al Sharepoint intern de l'OAT.	Per auditoria
Document de treball de l'execució de l'auditoria	Document de treball de l'OAT amb totes les revisions i anotacions de l'auditoria en base a la guia CCN-STIC 808.	Per auditoria
Resum de troballes	Resum de troballes que serà presentat en la reunió de tancament de l'auditoria.	Per auditoria
Informe de resultats	Informe de resultats de l'auditoria.	Per auditoria
Informe d'acceptació del Pla d'Accions Correctives	Informe d'acceptació del Pla d'Accions Correctives de l'entitat, si escau.	Per auditoria
Informe de recomanació de l'auditor	Informe de recomanació de l'auditor en cap de certificar o no l'entitat en base als resultats.	Per auditoria
Seguiment contractual	Documents acordats amb l'Agència per al seguiment contractual del servei contractat.	Periodicitat definida
Mètriques del servei	Alimentar i mantenir disponibles els indicadors d'activitat i de seguiment definits per l'Agència.	Periodicitat definida
Altres lliurables	Altres lliurables que es puguin derivar de les auditories i de l'activitat del servei.	Sota petició

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

2.2.5. Característiques del servei

De tot el que s'ha exposat prèviament es pot observar com s'han de tenir en compte els següents elements essencials:

Requisits

- Les activitats es duran a terme seguint les directrius, metodologies, eines i formats establerts per l'Òrgan d'Auditoria Tècnica de l'Agència.
- L'equip humà proposat haurà de complir amb les capacitats i coneixements necessaris, així com amb els requeriments de confidencialitat i imparcialitat que té com a requeriment l'OAT mitjançant la signatura dels acords necessaris.
- La direcció i supervisió dels equips de treball, així com el control de la qualitat de l'activitat desenvolupada i dels productes resultants formaran part intrínseca de les funcions del servei.

Planificació

- L'OAT de l'Agència mantindrà el programa d'auditories amb les entitats que han sol·licitat la certificació. Es farà saber al licitador les dates en que les entitats estaran en disposició de certificar-se amb temps suficient com per poder planificar la seva execució.
- La periodicitat de les reunions de punt de control i l'entrega de lliurables serà acordada prèviament amb l'Agència.

Volumetria

El nombre d'entitats a auditar serà d'aproximadament 22 segons s'especifica a la memòria justificativa. Tant el nombre d'auditories com la distribució entre els diferents tipus d'auditoria és estimat i en qualsevol cas es podran fer auditories fins a la finalització del pressupost base de licitació. Tipus d'auditoria	Total
Perfil de Compliment Específic de Requisits Essencials de Seguretat	15
Categoria Bàsica	2
Categoria Mitjana	4
Categoria Alta	1
Total	**22**

Cal recordar que l'estimació és inicial i pot variar, tant el nombre total d'entitats candidates com la distribució de les mateixes en funció de les necessitats i la situació de cadascuna, sempre i quan tingui cabuda dins de l'import total del contracte.

El càlcul dels esforços de cada auditoria s'estableix en funció de la guia "*CCN-STIC CCN-CERT IC-01/19 – ENS. Criterios Generales de Auditoría y Certificación*". Per tant, cada auditoria s'avaluarà de forma independent per fer l'estimació d'esforços adient un cop conegut el context de la mateixa.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

3. Condicions d'execució del servei

3.1. Horaris

Les auditories de certificació es realitzaran d'acord a la planificació amb l'Agència i l'entitat auditada dins de l'horari laboral de prestació dels serveis de l'Agència especificat. 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 l'execució de les auditories requereixin del desplaçament dels professionals a les instal·lacions de les entitats auditades 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 dels serveis.

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.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

- 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.

En cap cas es preveu la possibilitat de transferència del personal intern de l'Agència o dels seus usuaris.

L'adjudicatari disposarà d'una figura que assumirà les tasques de **Cap de Servei**. A aquest efecte, ha d'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 la bona col·laboració entre els diferents agents implicats en la prestació de serveis als clients de l'Agència.

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 dona servei a l'Agència.

3.3.1. Perfils

A continuació, es detallen els perfils professionals que des de l'Agència s'identifiquen com a necessaris per la prestació dels serveis. Addicionalment, per a cada perfil es llisten els requisits mínims així com les funcions que han de complir les persones que assumeixin aquests rols.

Perfil	Requisits	Funcions
Cap de servei	• Graduat/da universitari/a (anteriorment diplomatures o llicenciatures). • Cal que acrediti un mínim de 5 anys d'experiència professional en l'àmbit de projectes similars a l'objecte del contracte.	• Responsable del servei, gestionant la capacitat de l'equip auditor proposat i la seva disponibilitat, competència i imparcialitat. • Efectua el seguiment global del servei, planifica i coordina les diferents accions. • Revisa el desenvolupament de les auditories en les que estigui treballant l'equip, així com el compliment de fites i calendaris previstos en cada cas. • Participa en les reunions dels comitès de seguiment del servei i d'altres comitès que determini l'Agència.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Perfil	Requisits	Funcions
		• Dona suport en la resolució de conflictes i incidències operatives. • Detecta oportunitats de millora en el servei i les escala a l'Agència amb el seu pla d'acció. • Garanteix la qualitat dels lliurables fets per l'equip del servei (Quality Assurance) • Gestiona els riscos operatius del servei.
Auditor Expert en l'ENS	• Formació en auditories de sistemes d'informació, a través de certificacions reconegudes a nivell nacional o internacional, o cursos, seminaris o activitats formatives reglades o impartides per entitats reconegudes, de qualitat i número d'hores formatives suficients que permetin evidenciar la suficiència dels coneixements adquirits. • Experiència verificable, d'almenys 4 anys, en la realització regular d'auditories, avaluacions o inspeccions de seguretat en tecnologies de la informació. • Coneixements de seguretat de la informació i gestió de riscos de seguretat, demostrable per mitjà de certificacions o experiència d'almenys 4 anys en aquestes competències. • Coneixement dels requisits de l'ENS, demostrable per mitjà de cursos o seminaris sobre aquestes competències, de qualitat i abast suficients, que comprenguin un mínim de 20 hores de formació. • Coneixements de la legislació aplicable quan l'auditoria pugui requerir l'avaluació de la conformitat de mesures derivades del compliment d'altres normatives, com les de protecció de dades o l'Esquema Nacional d'Interoperabilitat, entre d'altres. • Coneixements de les guies de seguretat CCN-STIC i Instruccions Tècniques de Seguretat aplicables a cada cas.	• Responsable de tot el procés d'auditoria i de l'equip d'auditoria involucrat, participant activament en l'execució de la mateixa com auditor en cap. • Elabora el pla d'auditoria, de forma prèvia a l'inici d'aquesta, que haurà d'establir amb claredat la responsabilitat i assignació de funcions a cada integrant de l'equip auditor. • Analitza i entén els objectius I abast de l'auditoria, així com les normes i regulacions aplicables, i detecta la necessitat de requerir de perfils experts especialistes quan les característiques de l'auditoria requereixin de coneixements específics. • Lidera i executa l'auditoria de conformitat. • Assegura l'exactitud de totes les troballes observades i la conclusió final de l'auditoria. • Elabora els informes d'auditoria, així com qualsevol altra documentació relacionada amb el procés, com la recomanació a certificar, i documenta amb exactitud les evidències recopilades. • Preserva les evidències d'auditoria seguint els repositori i eines de l'Agència. • Manté una comunicació efectiva tant amb l'equip d'auditoria com amb l'entitat auditada, assegurant que es transmeti la informació adequada en cada etapa del procés. • Identifica millores en els processos del servei.
Auditor	• Formació en auditories de sistemes d'informació, a través de certificacions reconegudes a nivell nacional o internacional, o cursos, seminaris o activitats formatives	• Actua sota la responsabilitat de l'auditor en cap de l'auditoria assignada. • Avalua i verifica el grau de compliment de les mesures de seguretat en les entitats

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Perfil	Requisits	Funcions
	reglades o impartides per entitats reconegudes. • Experiència verificable, d'almenys 1 any, en la realització regular d'auditories, avaluacions o inspeccions de seguretat en tecnologies de la informació. • Coneixements de seguretat de la informació i gestió de riscos de seguretat, demostrable per mitjà de certificacions o experiència d'almenys 1 any en aquestes competències. • Coneixement dels requisits de l'ENS, demostrable per mitjà de cursos o seminaris sobre aquestes competències, de qualitat i abast suficients, que comprenguin un mínim de 20 hores de formació. • Coneixements de les guies de seguretat CCN-STIC i Instruccions Tècniques de Seguretat aplicables a cada cas.	auditades que li assigni l'Auditor Expert en l'ENS • Realitza proves i verificacions tècniques per validar la correcta configuració i funcionament dels sistemes i tecnologies utilitzades. • Dona suport a l'Auditor Expert en l'ENS en l'elaboració dels informes d'auditoria, així com qualsevol altra documentació relacionada amb el procés d'auditoria.

Els perfils Auditor Expert en l'ENS hauran de complir amb els requeriments establerts per als OAT i per a les Entitats de Certificació segons la guia "*CCN-STIC 122. Procedimiento de Reconocimiento y Requisitos del Órgano de Auditoría Técnica del ENS*".

En cas que es detecti la necessitat, durant el procés d'una auditoria, de disposar d'habilitats i coneixements especialitzats o assessorament tècnic, quant l'entorn tecnològic i normatiu ho requereixi (p.e. entorns *cloud*, *blockchain*, intel·ligència artificial, aplicació de normativa molt específica) es podria requerir addicionalment d'un tècnic especialitzat en la matèria per donar suport durant l'auditoria en qüestió. Aquest perfil tècnic podria actuar en qualitat d'algun dels altres rols, sempre que reuneixi els requisits necessaris i que l'Agència així ho consideri.

3.3.2. Estimació per perfil

L'Agència ha realitzat una estimació inicial per a cada tipus d'auditoria, basant-se en les jornades mínimes establertes pel CCN tal com s'indica a la guia "*CCN-STIC CCN-CERT IC-01/19 – ENS. Criterios Generales de Auditoría y Certificación*" i, en el cas de les auditories del Perfil de Compliment Específic, s'ha realitzat en base a l'experiència prèvia de l'Agència en la realització d'aquest tipus d'auditories. Tot i així, com ja s'ha indicat anteriorment, cada auditoria s'avaluarà de forma independent per fer l'estimació d'esforços adient un cop conegut el context i l'abast de la mateixa i, per tant, la volumetria i l'esforç final podria variar respecte el que s'indica a continuació.

Tipus d'auditoria	Perfils (*)	Jornades mínimes estimades	Volum inicial estimatiu
Perfil de Compliment Específic de Requisits Essencials	Auditor Expert en l'ENS	2	15
Categoria Bàsica	Auditor Expert en l'ENS	3	2
Categoria Mitjana	Auditor Expert en l'ENS	4	4
Categoria Alta	Auditor Expert en l'ENS	5	1

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

(*) Depenent de les característiques de l'auditoria, l'Agència podria sol·licitar algun dels perfils addicionals descrits a l'apartat 3.3.1 Perfils.

Cal recordar que el volum d'auditories de la taula, així com la distribució de les mateixes és una estimació inicial i podria veure's modificat.

S'estima la dedicació del perfil del **Cap de Servei** en un 10% de les hores totals del servei.

Tal com s'informa en la memòria justificativa, aquesta ha estat una estimació per al càlcul del pressupost del contracte. Tant el nombre d'auditories com la distribució entre els diferents tipus d'auditoria és estimat i en qualsevol cas es podran fer auditories fins a la finalització del pressupost base de licitació.

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.

3.6. Eines i equipament per a la prestació de serveis

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Les principals eines requerides 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.
- 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 4G/5G.
- Cap altre recurs no especificat explícitament.

En conseqüència, els adjudicatari haurà 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.
- L'adjudicatari 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.

3.8. Seguretat Corporativa

Un cop adjudicat el contracte, l'empresa i els mitjans personals adscrits al contracte 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 pels adscrits al contracte en les oficines de l'Agència.
- 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, entre altres.).

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 dels mitjans adscrits al contracte. 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 per l'adjudicatari referent al servei prestat per l'adjduicatari 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. 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 licitació.

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

3.11. Formació

Es realitzarà, 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.

3.12. Contingència

Les empreses adjudicatàries 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 del contractista, 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.

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:

3.14.1. Deure de confidencialitat

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.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

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.

Deure de confidencialitat a l'OAT de l'Agència de Ciberseguretat

Com a requeriment establert per als Òrgans d'Auditoria Tècnica per part del CCN, serà imprescindible que el personal de l'empresa adjudicatària que participi en activitats del contracte, així com la mateixa empresa, signin un acord específic de confidencialitat i absència de conflicte d'interès amb les activitats desenvolupades i la informació tractada a l'OAT de l'Agència.

3.14.2. 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.

3.14.3. 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.

3.14.4. 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.

3.14.5. 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), 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.

3.14.6. 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.

3.14.7. 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.

3.14.8. 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.

3.14.9. 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.) 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.

3.15. **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), amb major rigor, intensitat i profunditat segons la criticitat del projecte/servei/component.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

- 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.

3.16. Seguiment del servei

Les empreses adjudicatària haurà de presentar un informe de seguiment en l'execució del 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, 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)
- Un informe de dedicació de les diferents funcions requerides, per tal de poder avaluar la distribució dels esforços.
- Un informe d'accions de millora de l'activitat del 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.). 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.

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

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.

3.17. 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), 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.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD