Plec de prescripcions tècniques particulars que regeix la contractació basada relativa a SERVEIS DE DESPLEGAMENT DEL MODEL DE CIBERSEGURETAT DE SALUT A LES ENTITATS PROVEÏDORES D'ATENCIÓ SOCIOSANITÀRIA I DE SALUT MENTAL, estructurada en 4 lots

Lot 1: Avaluació de ciberseguretat de les entitats proveïdores d'atenció sociosanitària o intermèdia

Lot 2: Avaluació de ciberseguretat de les entitats proveïdores de salut mental

Lot 3: Enginyeria de Seguretat

Lot 4: Coordinació del desplegament del model de seguretat a les entitats proveïdores d'atenció sociosanitària i de salut mental

Exp. CO.05.2024

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

Índex

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

Financiado por la Unión Europea NextGenerationEU
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. 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

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

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.

1.1. Funcions de l'Agència de Ciberseguretat de Catalunya rellevants a efectes del la nova estratègia de contractació

Avui en dia l'Agència té les següents funcions:

- **Gerència** s'ocupa de la gestió financera i pressupostària de l'entitat, la contractació, la comunicació, la gestió de personal, la seguretat corporativa i la captació i gestió de fons que fomenta l'atracció de fons i gestions administratives ó la internacionalització de l'entitat.
- **Operacions** du a terme la prestació tècnica dels serveis de seguretat vinculats a les funcions de protecció, prevenció, detecció, resposta i recuperació de seguretat en la seva vessant més operativa (coneguda com SOC/CERT).
- **Desenvolupament d'Estratègia d'Àmbits** té les funcions de gestionar els destinataris de les actuacions i de desplegar els programes i iniciatives de seguretat a partir de les necessitats i particularitats de cadascun d'ells.
- **Producte** s'ocupa d'identificar les necessitats i proposar noves idees i estratègies per a l'elaboració de nous productes generats per l'Agència o millora dels existents, i coordina l'execució del cicle de vida dels productes, des de la seva concepció fins a la seva retirada, incloent el disseny, desenvolupament, desplegament i control de qualitat.
- **Centre de Competència i Innovació** en Ciberseguretat (CCI) s'ocupa de la coordinació, cohesió i capacitat de l'ecosistema de Ciberseguretat de Catalunya, recolza el coneixement, sensibilització i conscienciació, i la innovació com a palanca de transformació i creixement del sector.
- **Certificació** en matèria de Ciberseguretat per desplegar totes les eines i processos vinculats al procés de certificació en ciberseguretat de les entitats, garantint sempre la independència necessària per la correcta execució d'aquests processos.

1.2. Funcions del SOC/CERT

La següent figura mostra les 3 principals línies de treball que defineixen el SOC/CERT i reflecteix els diferents equips existents dins del SOC/CERT. Els serveis objecte de la present licitació es relacionaran amb la resta de funcions i amb els seus corresponents serveis de suport subjacents.

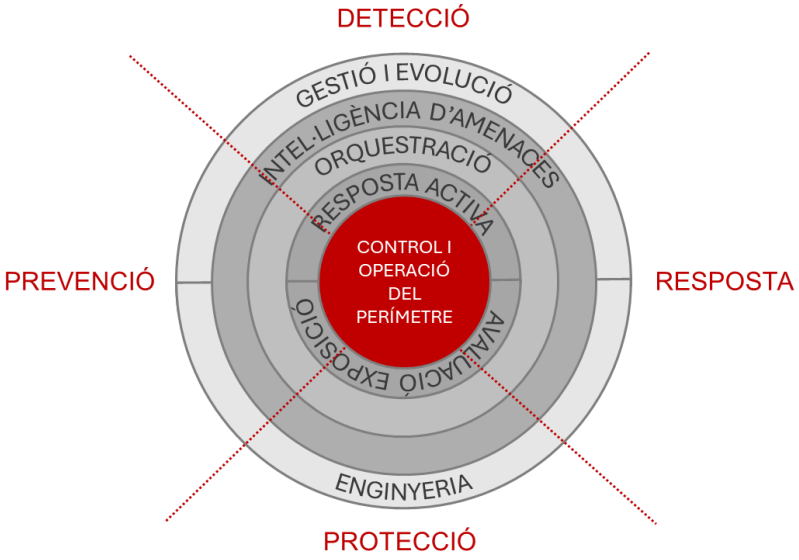
Funcions i subfuncions actuals del SOC/CERT

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

1.2.1. Model funcional agregat

L'estructura funcional dins del SOC/CERT, juntament amb els serveis de suport a l'operació de l'Agència de Ciberseguretat de Catalunya sobre la que es sustenta, pretenen satisfer els quatre eixos fonamentals de la seguretat de la informació enfront d'amenaces i incidents de seguretat (detecció, prevenció, protecció i resposta) i es distribueix en fins a 6 funcions diferenciades.

La distribució en funcions (amb els seus serveis de suport subjacents) té com a objectiu principal garantir la seguretat dels actius TIC de tot l'àmbit alhora que s'incrementa el nivell de maduresa actual de l'Àrea d'Operacions de Seguretat de l'Agència de Ciberseguretat de Catalunya.



Estructura funcional actual del SOC/CERT

La primera funció és la de **Control i Operació del Perímetre** (COP), que dona resposta a la operació de perímetres dels eixos de detecció, prevenció i resposta. Aquesta funció correspon a tasques relatives a la gestió del cicle de vida dels esdeveniments, vulnerabilitats, amenaces i atacs de ciberseguretat fins que aquests es considerin o categoritzin com a incidents (que consisteix entre d'altres en l'anàlisi i gestió proactiva de les alertes rebudes pels dispositius de seguretat desplegats) amb l'objectiu principal de prevenir, protegir i detectar possibles atacs a la seguretat que afectin els sistemes d'informació i a la protecció davant vulnerabilitats conegudes.

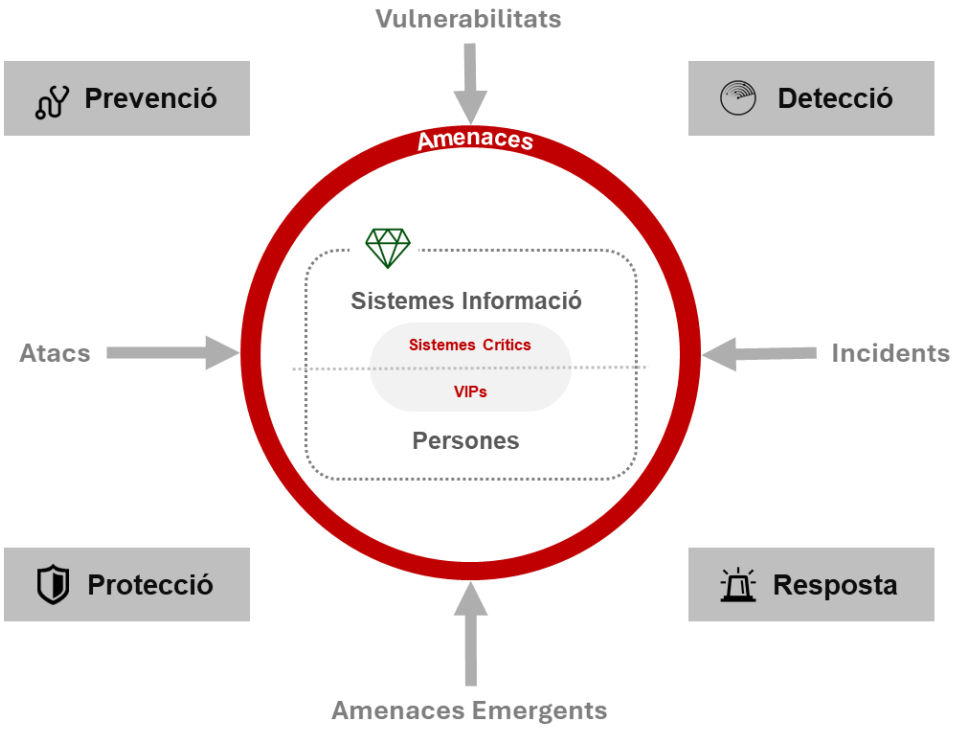
La funció de "**Avaluació d'Exposició**" (AVX) dona suport a la resta de funcions, avaluant i validant de manera proactiva els mecanismes i controls establerts respecte als quatre eixos de detecció, prevenció, protecció i resposta, per identificar punts de millora.

Tot i l'efectivitat dels controls i les tasques de prevenció desplegades, encara existeix la possibilitat de que una amenaça es materialitzi en un incident de ciberseguretat. Aleshores, la funció de **Resposta Activa** (RAC) s'activa de manera reactiva quan es detecta un incident de severitat elevada, per permetre reduir en temps i forma la seva afectació dins de l'àmbit i per garantir que el mateix tipus d'incident no torna a succeir en les mateixes circumstàncies. Addicionalment, aquesta mateixa funció de manera proactiva i transversal complementa a la d'AVX i realitza cerca d'amenaces '*huntings*' per identificar possibles incidents i altres punts de millora.

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

Al voltant de les funcions més operatives del SOC/CERT es desplega la funció d'Orquestració Operativa que permet garantir que tots els esforços dels diferents equips es centren en tot moment en els mateixos focus. Respecte a l'operació recurrent, l'orquestració també permet assegurar que per cada element a tractar (bé sigui una vulnerabilitat, un atac, un incident o una nova amenaça), es treballa sempre des d'un punt de vista construït sobre l'amenaça com a element central (*Threat-Centric*), el que permet assegurar tots els requeriments necessaris per una prevenció i una resposta efectiva i amb garanties.

De manera recurrent es porten a terme reunions operatives dins del SOC/CERT on totes les funcions i els seus serveis corresponents acorden les tasques a executar i els principals focus operatius, evolutius i incidentals sobre els que s'han de concentrar els recursos disponibles.



Plantejament "Threat-Centric"

Justament per sobre de l'Orquestració Operativa, es desplega la funció d'**Intel·ligència d'Amenaces** (IOP), que complementa l'activitat de les funcions anteriors, amb una visió orientada a l'anàlisi del context de la ciberseguretat de l'organització i l'àmbit d'actuació de l'Agència de Ciberseguretat.

A partir de la informació resultant de l'operativa de les diferents funcions prèviament citades i els seus serveis de suport, d'altres entitats de l'àmbit de la ciberseguretat i de fonts externes de coneixement, es realitza una correlació i anàlisi en profunditat per tal de determinar patrons d'actuació i potencials noves ciberamenaces. Aquestes tasques s'associen a totes les fases de la 'Cyber Kill Chain' del MITRE i també es realitza una tasca analítica de l'operativa resultant de la resta de funcions.

Aquesta correlació i anàlisi de la informació es realitza amb l'objectiu de definir una estratègia que sigui efectiva al llarg del temps mitjançant la retroalimentació dels resultats. Amb això es pretén evitar que aquestes ciberamenaces identificades es materialitzin en incidents de seguretat que puguin posar en perill qualsevol actiu dins de l'àmbit d'actuació de l'Agència de Ciberseguretat.

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

Addicionalment, de manera transversal, la funció de "**Enginyeria de seguretat**" (ENS) que principalment aporta i garanteix la disponibilitat de les solucions tecnològiques que donen resposta a les necessitats de tota l'Agència de Ciberseguretat de Catalunya.

Per últim, de manera transversal, la funció de "**Governança i Evolució de l'Operació**" permet evolucionar el SOC/CERT, garantir la gestió eficaç dels recursos i capacitats de les diferents funcions del SOC/CERT, i posar en valor tota l'activitat operativa portada a terme pels seus equips.

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

2. Descripció dels serveis objecte de la licitació.

2.1. Antecedents

Els estudis de tendències constaten que els atacs cibernètics a centres sanitaris poden provocar greus impactes en la qualitat assistencial als pacients, poden impedir l'accés als expedients mèdics i bloquejar el funcionament de tots sistemes informàtics, i per tant, provocar retards en els procediments i proves, i hospitalitzacions més llargues. En conseqüència, es constata un risc d'increment de les taxes de mortalitat.

En aquest context, l'Agència de Ciberseguretat va detectar més de mil milions d'atacs dirigits contra el sector sanitari a Catalunya durant el 2023, dels quals 308 van materialitzar-se en incidents. Alguns d'ells, com els succeïts a l'hospital Clínic o al Moises Broggi (Consorci Sanitari Integral) van suposar un greu impacte assistencial per la ciutadania, ja que van afectar de forma directa als principals hospitals i centres d'atenció primària del nucli de Barcelona.

Davant d'aquesta situació l'Agència de Ciberseguretat ha dissenyat i està desplegant un Model Integral de Ciberseguretat (en endavant, el Model), que té com a objectiu protegir els àmbits d'actuació públics més rellevants a Catalunya de les amenaces en ciberseguretat dirigides contra els seus sectors, i abordar les actuacions necessàries per a protegir-los dels ciberincidents que puguin impactar contra les diferents entitats que els conformen.

A tal efecte el Model preveu l'execució de les següents fases per al seu desplegament:

- **Diagnòstic:** identificació del grau actual d'exposició a les principals ciberamenaces que apliquen a l'àmbit.
- **Pla de seguretat:** determinació del pla de seguretat de cada entitat per tal de ser més resilient i reduir l'exposició a les amenaces més significatives, amb una orientació a assolir el compliment normatiu en l'Esquema Nacional de Seguretat i, quan correspongui, en altres normatives sectorials o específiques que siguin d'aplicació.
- **Integració operativa:** desplegament, a partir de les capacitats de protecció desplegades per les entitats, de les capacitats de prevenció, detecció i resposta, i dels processos i serveis associats a la integració amb l'Agència de Ciberseguretat de Catalunya.
- **Protecció:** activació i operació del serveis de monitorització i resposta 24x7 de l'Agència, i dels serveis i oficines necessàries per a la governança, comunicació, formació i evolució en la ciberseguretat.
- **Certificació:** procés de certificació mitjançant les auditories de la conformitat en l'Esquema Nacional de Seguretat.

Tota l'operació de la seguretat que contempla aquest Model gira al voltant del concepte "perímetre de ciberseguretat", entenent-se per perímetre el conjunt d'activitats i tecnologies desplegades i governades pel SOC/CERT, que contribueixen a la millora de la ciberseguretat dels sistemes d'informació, infraestructures transversals o de les persones.

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

2.2. Context dels serveis objecte de la licitació

Els serveis objecte de la present licitació tenen com a objectiu fonamental estendre el desplegament del Model de ciberseguretat de l'Agència a les principals entitats proveïdores d'atenció sociosanitària (o intermèdia) i de salut mental del sistema sanitari integral d'utilització pública de Catalunya (SISCAT) i per extensió als centres que conformen aquestes entitats regulades pel Decret 196/2010, de 14 de desembre, del sistema sanitari integral d'utilització pública de Catalunya.

La licitació s'estructura en els lots que s'enumeren tot seguit:

- Lot 1: **Avaluació de ciberseguretat de les entitats proveïdores d'atenció sociosanitària o intermèdia**
- Lot 2: **Avaluació de ciberseguretat de les entitats proveïdores de salut mental**
- Lot 3: **Enginyeria de Seguretat**
- Lot 4: **Coordinació del desplegament del model de seguretat a les entitats proveïdores d'atenció sociosanitària i de salut mental**

2.3. Lot 1: Avaluació de ciberseguretat de les entitats proveïdores d'atenció sociosanitària o intermèdia

2.3.1. Objecte i abast dels serveis

L'objecte dels serveis d'aquest lot és identificar els punts de millora que permetin incrementar la resiliència i reduir la superfície d'exposició de les entitats proveïdores d'atenció sociosanitària o intermèdia (en endavant entitats) envers les principals ciberamenaces que afecten al sector salut, tot vetllant per la implantació d'aquestes mesures i pel compliment de l'Esquema Nacional de Seguretat.

Objectiu del servei

Els objectius que s'espera assolir amb la prestació del servei són:

- Obtenir el coneixement del context de negoci, tecnològic i de funcions i serveis de ciberseguretat de les entitats.
- Identificar el grau d'exposició de les entitats a les principals ciberamenaces del sector.
- Elaborar i presentar un pla de seguretat que permeti augmentar de forma eficient la protecció i la resiliència de cada entitat davant les ciberamenaces i assolir l'adequació al perfil de compliment essencial de l'ENS.
- Establir el model de relació amb els serveis de l'Agència.
- Garantir l'assegurament de la qualitat dels productes generats i fer una correcta gestió i seguiment del servei.

Funcions i activitats

Les activitats i funcions que s'esperen del servei es classifiquen segons la seva fase dins del Model de Ciberseguretat de l'Agència.

- Com a part de la fase de diagnòstic, caldrà desenvolupar les següents activitats:

- Recopilació i tractament de la informació de context necessària per a poder executar la resta d'activitats i aquella sol·licitada expressament per l'Agència per arrencar d'altres serveis operatius.
- Compartició o registre de la informació de context recollida en els repositoris de dades que determini l'Agència per assegurar la disposició d'aquesta per la resta de funcions que puguin requerir-la.
- Preparació i planificació preliminar de l'anàlisi i proves tècniques, de manera coordinada amb altres possibles serveis de l'Agència involucrats i les pròpies entitats.
- Execució de proves tècniques de seguretat per la identificació de febleses de seguretat que permetin determinar de forma objectiva el nivell d'exposició a les principals ciberamenaces actives a l'àmbit, prenent com a base la informació d'intel·ligència d'amenaces proporcionada per l'Agència, i valorant les mesures de prevenció, protecció i detecció disponibles en les entitats.
- Anàlisi de l'arquitectura de seguretat de l'entitat, considerant els controls del NIST CSF i el model de perímetres de l'Agència.
- Diagnòstic de compliment dels controls del Perfil de Compliment Específic de Requeriments Essencials (PCE-RES).
- Generació de l'informe de diagnòstic de cada entitat, amb la visió consolidada del grau d'exposició a les amenaces.
- Presentació de resultats a cada entitat, elaborant el material de suport necessari en els formats acordats prèviament amb l'Agència.

- En la fase de Pla de Seguretat, s'inclouran les següents activitats:
  - Elaboració d'un pla de seguretat per a cada entitat que reculli iniciatives prioritzades, que permetin a cada entitat entendre i executar els projectes de millora i evolució identificats.
  - Presentació de resultats, en els formats acordats prèviament amb l'Agència.

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

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 es poden considerar productes que inclouen resums de l'activitat dels serveis periòdicament, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència.

Durant la prestació de servei l'empresa adjudicatària ha de generar i entregar de manera obligatòria els següents lliurables:

Document	Descripció	Periodicitat
Context de l'entitat	Documentació que reculli tota la informació de context recopilada de cada entitat durant la fase de diagnòstic.	Puntual
Documents de treball per valorar el nivell d'exposició a les amenaces	Formularis de treball, a partir de plantilla de l'Agència, que reflecteixin les proves i resultats obtinguts durant les diferents activitats del diagnòstic que permetin calcular el grau d'exposició a les ciberamenaces.	Puntual
Informes de diagnòstic	Informe detallat que exposi el grau d'exposició a les principals ciberamenaces de cada entitat, en base al resultat de l'auditoria tècnica i, l'avaluació de l'arquitectura de seguretat, així com la valoració preliminar del nivell d'adequació al perfil de compliment essencial de l'Esquema Nacional de Seguretat.	Puntual (fita de facturació)
Plans de seguretat	Informe per cada entitat que reculli el conjunt d'iniciatives i projectes necessaris i prioritzats per permetre'ls reduir la seva superfície d'exposició a les ciberamenaces, desplegar els models de perímetre de l'Agència i donar compliment a l'ENS. S'hi introduirà una estimació a alt nivell del cost de les iniciatives per donar visibilitat de les necessitats pressupostàries i de les capacitats associades a la implementació del pla que haurà d'executar cada entitat.	Puntual (fita de facturació)
Presentació de resultats	Presentació de resultats del diagnòstic i el pla de forma individual i agregada.	Puntual
Informes de seguiment	Informes de seguiment periòdics de l'estat de les tasques, incloent la planificació, avenços, possibles desviacions, i riscos observats durant el transcurs de totes les activitats	Setmanal

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

Mètriques del servei

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar en la prestació del servei. L'Agència es reserva el dret d'adaptar aquest llistat de mètriques de manera acordada amb l'adjudicatari.

Aspecte mesurat	Descripció
Entitats avaluades	Nombre d'entitats en què s'ha finalitzat el diagnòstic i pla de seguretat
Actius dins l'abast	Nombre d'actius dins l'abast de l'avaluació a l'exposició a les amenaces per entitat i de forma agregada
Dominis compromesos	Nombre de dominis compromesos com a resultat de les proves tècniques de forma individual, per entitat, i agregada
Sistemes de *backup* compromesos	Nombre de sistemes de còpies de seguretat compromesos com a resultat de les proves tècniques de forma individual, per entitat, i agregada
Tècniques provades	Tècniques MITRE ATT&CK provades aplicant la intel·ligència d'amenaces actualitzada a les directrius de *pentest* de l'Agència en cada exercici de proves tècniques de forma individual i globalment
Eines utilitzades	Nombre d'eines utilitzades aplicant les directrius de *pentest* de l'Agència en cada exercici de proves tècniques de manera individual i agregat
Vulnerabilitats avaluades	Nombre de vulnerabilitats i CVEs avaluades que s'han intentat explotar durant les proves tècniques, aplicant les directrius de *pentest* de l'Agència, en cada diagnòstic individual i globalment
Credencials exfiltrades	Nombre de credencials exfiltrades provades
Vulnerabilitats identificades	Nombre i tipologia de vulnerabilitats identificades durant cada exercici i de forma agregada
Deteccions realitzades	Nombre d'alertes detectades durant les proves tècniques per cada entitat i de forma agregada
Temps mínim per compromís	Mínim temps entre inici de les proves tècniques i compromís del domini de cada entitat i globalment
Entrevistes	Nombre de reunions de treball amb les entitats per arrencar les activitats i aconseguir informació per avaluar l'estat de ciberseguretat de les entitats.
Evidències revisades	Nombre de proves revisades per avaluar l'existència i eficàcia dels controls
Controls avaluats	Nombre de controls avaluats per cada entitat i de forma acumulada
Lliurables generats	Nombre de lliurables finals entregats (informe de diagnòstic, llibre de càlcul d'avaluació a l'exposició, presentacions de resultats, bitàcola *pentest*, pla de seguretat)
Seguiments realitzats	Nombre de reunions de seguiment internes dels equips i de punts de control amb l'Agència.
Enquesta de Satisfacció	Puntuacions de les enquestes de satisfacció de lliurables.

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

2.3.2. Característiques del servei

De tot el que s'ha exposat prèviament es pot observar com, a l'hora de presentar les seves ofertes i en l'execució del contracte han de tenir en compte els següents elements essencials:

- Les activitats es duran a terme seguint les directrius, eines i formats establerts per l'Agència.
- L'avaluació del grau d'exposició a les ciberamenaces haurà d'aportar una visió unificada. homogènia i íntegra, com a resultat dels exercicis de consultoria i de les proves tècniques. Serà imprescindible, per tant, que els membres de l'equip de diagnòstic de cada entitat cooperin i treballin des del primer moment en equip per elaborar i traslladar a l'Agència i posteriorment a l'entitat un relat únic.
- 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 de cada lot.
- L'empresa contractista ha d'estar localitzable en tot moment durant les proves d'intrusió per atendre possibles incidències derivades de la seva execució.

Planificació

- L'Agència juntament amb el Departament de Salut de la Generalitat de Catalunya i les pròpies entitats afectades determinaran la planificació i distribució mensual d'entitats a avaluar sempre respectant els límits temporals definits pel fons.
- L'execució de totes les tasques i emissió de resultats ha d'estar finalitzada abans del 30 de juny de 2026. Per poder complir amb aquesta data s'estima l'inici i execució de les tasques de diagnòstic a 5 entitats del LOT1 i a 5 entitats de LOT2 alhora cada mes. La periodicitat de les reunions de punt de control i l'entrega de lliurables serà acordada prèviament amb l'Agència.
- Caldrà detallar el pla de seguretat de cada entitat immediatament després de la finalització del servei de diagnòstic.

Volumetria

- El nombre d'entitats proveïdores d'atenció sociosanitària avaluar i elaborar el pla de tractament de seguretat serà aproximadament 49, segons s'especifica a la memòria justificativa.
- S'estima que un 60% de les entitats proveïdores d'atenció sociosanitària tenen més de 100 treballadors.

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

2.4. Lot 2: Avaluació de ciberseguretat de les entitats proveïdores de salut mental

2.4.1. Objecte i abast dels serveis

L'objecte dels serveis d'aquest lot és identificar els punts de millora què permetin incrementar la resiliència i reduir la superfície d'exposició de les entitats proveïdores d'atenció a la salut mental (en endavant entitats) envers les principals ciberamenaces que afecten al sector salut, tot vetllant per la implantació d'aquestes mesures i pel compliment de l'Esquema Nacional de Seguretat.

Objectiu del servei

Els objectius que s'espera assolir amb la prestació del servei són:

- Obtenir el coneixement del context de negoci, tecnològic i de funcions i serveis de ciberseguretat de les entitats.
- Identificar el grau d'exposició de les entitats a les principals ciberamenaces del sector.
- Elaborar i presentar un pla de seguretat que permeti augmentar de forma eficient la protecció i la resiliència de cada entitat davant les ciberamenaces i assolir l'adequació al perfil de compliment específic en requeriments essencials (PCE-RES) de l'ENS.
- Establir el model de relació amb els serveis de l'Agència.
- Garantir l'assegurament de la qualitat dels productes generats i fer una correcta gestió i seguiment del servei.

Funcions i activitats

Les activitats i funcions que s'esperen del servei es classifiquen segons la seva fase dins del Model de Ciberseguretat de l'Agència.

- Com a part de la fase de diagnòstic, caldrà desenvolupar les següents activitats:
    - Recopilació i tractament de la informació de context necessària per a poder executar la resta d'activitats i aquella sol·licitada expressament per l'Agència per arrencar d'altres serveis operatius.
    - Compartició o registre de la informació de context recollida en els repositoris de dades que determini l'Agència per assegurar la disposició d'aquesta per la resta de funcions que puguin requerir-la
    - Preparació i planificació preliminar de l'anàlisi i proves tècniques, de manera coordinada amb altres possibles serveis de l'Agència involucrats i les pròpies entitats.
    - Execució de proves tècniques de seguretat per la identificació de febleses de seguretat que permetin determinar de forma objectiva el nivell d'exposició a les principals ciberamenaces actives a l'àmbit, prenent com a base la informació d'intel·ligència d'amenaces proporcionada per l'Agència, i valorant les mesures de prevenció, protecció i detecció disponibles a les entitats.
    - Anàlisi de l'arquitectura de seguretat de l'entitat, considerant els controls del NIST CSF i el model de perímetres de l'Agència.

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

- Diagnòstic compliment dels controls del Perfil de Compliment Específic de Requeriments Essencials (PCE-RES).
- Generació de l'informe de diagnòstic de cada entitat, amb la visió consolidada del grau d'exposició a les amenaces.
- Presentació de resultats a cada entitat, elaborant el material de suport necessari en els formats acordats prèviament amb l'Agència.

- En la fase de Pla de Seguretat, s'inclouran les següents activitats:
  - Elaboració d'un pla de seguretat per a cada entitat que reculli iniciatives prioritzades, que permetin a cada entitat entendre i executar els projectes de millora i evolució identificats.
  - Presentació de resultats, en els formats acordats prèviament amb l'Agència.

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 es poden considerar productes que inclouen resums de l'activitat dels serveis periòdicament, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència.

Durant la prestació de servei l'empresa adjudicatària ha de generar i entregar de manera obligatòria els següents lliurables:

Document	Descripció	Periodicitat
Context de l'entitat	Documentació que reculli tota la informació de context recopilada de cada entitat durant la fase de diagnòstic	Puntual
Documents de treball per valorar el nivell d'exposició a les amenaces	Formularis de treball, a partir de plantilla de l'Agència, que reflecteixin les proves i resultats obtinguts durant les diferents activitats del diagnòstic que permetin calcular el grau d'exposició a les ciberamenaces.	Puntual
Informes de diagnòstic	Informe detallat que exposi el grau d'exposició a les principals ciberamenaces de cada entitat, en base al resultat de l'auditoria tècnica i, l'avaluació de l'arquitectura de seguretat, així com la valoració preliminar del nivell d'adequació al perfil de compliment essencial de l'Esquema Nacional de Seguretat.	Puntual (fita facturació)

Document	Descripció	Periodicitat
Plans de seguretat	Informe per cada entitat que reculli el conjunt d'iniciatives i projectes necessaris i prioritzats per permetre'ls reduir la seva superfície d'exposició a les ciberamenaces, desplegar els models de perímetre de l'Agència i donar compliment a l'ENS. S'hi introduirà una estimació a alt nivell del cost de les iniciatives per donar visibilitat de les necessitats pressupostàries i de les capacitats associades a la implementació del pla que haurà d'executar cada entitat.	Puntual (fita facturació)
Presentació de resultats	Presentació de resultats del diagnòstic i el pla de forma individual i agregada.	Puntual
Informes de seguiment	Informes de seguiment periòdics de l'estat de les tasques, incloent la planificació, avenços, possibles desviacions, i riscos observats durant el transcurs de totes les activitats	Setmanal

Mètriques del servei

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar en la prestació del servei. L'Agència es reserva el dret d'adaptar aquest llistat de mètriques de manera acordada amb l'adjudicatari.

Aspecte mesurat	Descripció
Entitats avaluades	Nombre d'entitats en què s'ha finalitzat el diagnòstic i pla de seguretat
Actius dins l'abast	Nombre d'actius dins l'abast de l'avaluació a l'exposició a les amenaces per entitat i de forma agregada
Dominis compromesos	Nombre de dominis compromesos com a resultat de les proves tècniques de forma individual, per entitat, i agregada
Sistemes de backup compromesos	Nombre de sistemes de *backups* compromesos com a resultat de les proves tècniques de forma individual, per entitat, i agregada
Tècniques provades	Tècniques MITRE ATT&CK provades aplicant la intel·ligència d'amenaces actualitzada a les directrius de *pentest* de l'Agència en cada exercici de proves tècniques de forma individual i globalment
Eines utilitzades	Nombre d'eines utilitzades aplicant les directrius de *pentest* de l'Agència en cada exercici de proves tècniques de manera individual i agregat
Vulnerabilitats avaluades	Nombre de vulnerabilitats i CVEs avaluades que s'han intentat explotar durant les proves tècniques, aplicant les directrius de *pentest* de l'Agència, en cada diagnòstic individual i globalment

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

Aspecte mesurat	Descripció
Credencials exfiltrades	Nombre de credencials exfiltrades provades
Vulnerabilitats identificades	Nombre i tipologia de vulnerabilitats identificades durant cada exercici i de forma agregada
Deteccions realitzades	Nombre d'alertes detectades durant les proves tècniques per cada entitat i de forma agregada
Temps mínim per compromís	Mínim temps entre inici de les proves tècniques i compromís del domini de cada entitat i globalment
Entrevistes	Nombre de reunions de treball amb les entitats per arrencar les activitats i aconseguir informació per avaluar l'estat de ciberseguretat de les entitats.
Evidències revisades	Nombre de proves revisades per avaluar l'existència i eficàcia dels controls
Controls avaluats	Nombre de controls avaluats per cada entitat i de forma acumulada
Lliurables generats	Nombre de lliurables finals entregats (informe de diagnòstic, llibre de càlcul d'avaluació a l'exposició, presentacions de resultats, bitàcola *pentest*, pla de seguretat)
Seguiments realitzats	Nombre de reunions de seguiment internes dels equips i de punts de control amb l'Agència.
Enquesta de Satisfacció	Puntuacions de les enquestes de satisfacció de lliurables.

2.4.2. Característiques del servei

De tot el que s'ha exposat prèviament es pot observar com, a l'hora de presentar les seves ofertes, els licitadors i en l'execució del contracte han de tenir en compte els següents elements essencials:

- Les activitats es duran a terme seguint les directrius, eines i formats establerts per l'Agència.
- L'avaluació del grau d'exposició a les ciberamenaces haurà d'aportar una visió unificada. homogènia i íntegra, com a resultat dels exercicis de consultoria i de les proves tècniques. Serà imprescindible, per tant, que els membres de l'equip de diagnòstic de cada entitat cooperin i treballin des del primer moment en equip per elaborar i traslladar a l'Agència i posteriorment a l'entitat un relat únic.
- 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 de cada lot.

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

Planificació

- L'Agència juntament amb el Departament de Salut de la Generalitat de Catalunya i les pròpies entitats afectades determinaran la planificació i la distribució mensual d'entitats a avaluar respectant sempre els límits temporals definits pel fons.
- L'execució de totes les tasques i emissió de resultats ha d'estar finalitzada abans del 30 de juny de 2026. Per poder complir amb aquesta data s'estima l'inici i execució de les tasques de diagnòstic a 5 entitats del LOT1 i a 5 entitats de LOT2 alhora cada mes.
- La periodicitat de les reunions de punt de control i l'entrega de lliurables serà acordada prèviament amb l'Agència.
- Caldrà detallar el pla de seguretat de cada entitat immediatament després de la finalització del servei de diagnòstic.
- L'empresa contractista ha d'estar localitzable en tot moment durant les proves d'intrusió per atendre possibles incidències derivades de la seva execució.

Volumetria

- El nombre d'entitats d'atenció a la salut mental a avaluar i elaborar el pla de tractament de seguretat serà aproximadament de 44, segons s'especifica a la memòria justificativa.
- S'estima que un 45% de les entitats d'atenció a la salut mental tenen més de 100 treballadors, segons s'especifica a la memòria justificativa.

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

2.5. Lot 3: Enginyeria de seguretat

2.5.1. Objecte i abast del servei

L'objecte del servei se centra en fer efectiva la integració operativa de les eines de ciberseguretat de les entitats proveïdores d'atenció sociosanitària i de salut mental que implementen les diferents funcionalitats del model de perímetre de persones i sistemes d'informació de l'Agència en el SIEM corporatiu.

El procés d'integració operativa ha de garantir la correcta generació d'alertes de seguretat en base a casos d'ús per identificar esdeveniments potencialment sospitosos o maliciosos perquè altres serveis del SOC/CERT de l'Agència puguin gestionar-les segons els seus procediments. S'entén per alerta de seguretat, els avisos o registres d'esdeveniments de seguretat generats per les eines de les entitats susceptibles de ser monitorades.

L'Agència disposa de diferents modelitzacions per desplegar les capacitats de Prevenció, Protecció, Detecció i Resposta d'amenaces, que es denominen perímetres de seguretat. Els models de perímetre de l'Agència conceptualitzen un conjunt de funcionalitats i tecnologies que contribueixen a millorar la ciberseguretat de les persones, els sistemes d'informació i les infraestructures transversals.

Objectius del servei

Els objectius que s'espera assolir amb la prestació del servei són:

- Augmentar el grau de desplegament dels perímetres de ciberseguretat en els les entitats proveïdores d'atenció sociosanitària i de salut mental.
- Millorar les capacitats de detecció de l'Agència dins l'àmbit, arran de la integració de diferents solucions de seguretat dels centres amb el SIEM.
- Desplegar i enfortir les capacitats d'intel·ligència de l'Agència mitjançant l'aplicació/implementació de casos d'ús.
- Industrialitzar els processos més repetitius amb l'objectiu d'aconseguir major eficiència operativa.

Funcions i activitats

El servei contempla la gestió complerta d'integració operativa de les eines de seguretat de les entitats proveïdores dins l'abast i definides dins dels models de perímetre de l'Agència juntament amb el posterior manteniment de les mateixes. Les activitats que s'esperen del servei són:

- Recopilació i validació de l'inventari d'eines de les entitats proveïdores que implementen les funcionalitats dels models de perímetre de l'Agència, fent les reunions necessàries amb SOC Salut i, si cal, els responsables tècnics dels centres que formen part d'aquestes entitats.
- Planificació, coordinació i seguiment de les integracions objectiu de la licitació.

- Realització de les diferents sessions tècniques amb les entitats, per desplegar els canals necessaris per obtenir les alertes o registres de seguretat necessaris per la integració operativa de les eines de seguretat analitzades anteriorment i ser rebudes e integrades en l'eina SIEM de l'Agència de Ciberseguretat de Catalunya.
- Manteniment de les integracions realitzades i solucionar els problemes que puguin sorgir si es produeixen pèrdues de registres per tal de recuperar l'estat operatiu de les integracions i el correcte funcionament dels Casos d'Ús.
- Parametrització de les solucions de seguretat que pertoqui per la inclusió del actius concrets a integrar.
- Vetllat per l'optimització del procés de desplegament de perímetre, aplicant sempre que es pugui la industrialització/automatització de tasques.
- Elaboració de la documentació de suport necessària perquè centres les entitats proveïdores puguin portar a terme les tasques tècniques requerides per la seva part.
- Normalització de les alertes i registres de seguretat al model d'informació utilitzat pels diferents equips i l'adaptació al model de dades utilitzat per l'Agència.
- Adaptació dels Casos d'Ús ja existents de l'eina SIEM perquè apliquin a les noves fonts d'informació integrades de les diferents entitats proveïdores. En el cas que per la tipologia de l'eina a integrar operativament no es disposi de Casos d'Ús, s'inclourà la definició i prova de nous casos amb el consens de la resta de funcions del SOC/CERT de l'Agència. També es funció del servei crear nous Casos d'Ús a petició dels altres serveis del SOC. Els Casos d'Ús han de ser testejats i s'ha de verificar el correcte funcionament dels mateixos abans de ser posats en producció.
- En cas d'existir processos automatitzats per la gestió dels casos d'ús, l'adaptació dels *Playbooks* de l'eina XSOAR per a que es pugui orquestrar, automatitzar i respondre davant les amenaces que es presentin d'acord als fluxos ja establerts i definits en els propis *Playbooks* i s'apliquin les mesures corresponents en les noves eines de seguretat.
- Industrialització o automatització dels processos més repetitius i que consumeixin més temps.
- Coordinació i suport a l'equip *core* d'Enginyeria de l'Agència.
- Gestió del coneixement sobre els processos propis del servei, per garantir l'execució efectiva de les tasques, independentment de les persones involucrades. Aquest punt inclou:
    - Documentar tots els procediments rellevants per la integració i el manteniment de noves solucions de seguretat.
    - Mantenir actualitzats els inventaris oficials del SOC/CERT de l'Agència, incloent totes les eines integrades de les entitats proveïdores, els centres als quals pertanyen, el mètode utilitzat i la relació de casos d'ús aplicables.
    - Gestionar el traspàs de coneixements entre els possibles membres de l'equip, així com assegurar que la documentació generada és útil per la resta d'equips que executen una funció similar o qualsevol altre tasca anàloga.

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

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 es poden considerar productes que inclouen resums de l'activitat dels serveis periòdicament, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència.

Durant la prestació de servei l'empresa adjudicatària ha de generar i entregar de manera obligatòria els següents lliurables:

Document	Descripció	Periodicitat
Procediments d'integració	Procediments tecnològics que incloguin els passos a seguir per assegurar la correcta integració de solucions de seguretat amb el SIEM de l'Agència.	Ad hoc
Mètriques i indicadors de servei	Recull d'indicadors que permetin mesurar el rendiment del servei	Setmanal
Inventari d'eines integrades	Inventari detallat de solucions de seguretat integrades conforme les necessitats de l'Agència	Setmanal

Entre els diferents lliurables a definir pel servei, s'haurà de ser capaç de calcular i facilitar a als equips encarregats de la construcció d'indicadors del SOC totes aquelles mètriques requerides. Aquestes mètriques s'han de realitzar mitjançant les eines que es disposen a la pròpia l'Agència.

Mètriques del servei

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar per part del licitador. L'Agència es reserva el dret de modificar aquest llistat de mètriques de manera acordada amb l'adjudicatari.

Aspecte mesurat	Descripció
Entitats integrades	Número d'entitats amb totes les solucions de seguretat integrades
Eines integrades	Número de solucions de seguretat integrades a l'eina SIEM
Casos d'ús adaptats	Número de casos adaptats per a que apliquin a les noves eines de seguretat integrades.
***Playbooks* adaptats**	Número de *playbooks* adaptats a les noves eines de seguretat integrades.
Control estat de tasques provinents de l'eina de *ticketing*	Disposar d'un control actualitzat de *tickets* pendents, en curs i realitzats
Número d'incidències	Nombre total d'incidències registrades a l'eina de *ticketing*
MTBF (Mean time between failures)	Temps mitjà entre el moment en què un servei o component es restaura completament i la següent vegada que es produeix un error en el mateix servei o component

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

Aspecte mesurat	Descripció
MTTR (Mean time to repair)	Temps mitjà entre el moment en què es produeix una incidència i la seva resolució
Número de processos industrialitzats	Número de processos industrialitzats que facilitin tasques al servei
Enquestes de Satisfacció	Puntuacions de les enquestes de satisfacció de lliurables.

A més de les llistades, s'hauran de poder obtenir de manera transversal per al servei i l'avaluació dels acords de nivell de servei.

2.5.2. Característiques del servei

De tot el que s'ha exposat prèviament es pot observar com, a l'hora de presentar les seves ofertes, els licitadors i en l'execució del contracte han de tenir en compte els següents elements essencials:

- Les activitats es duran a terme seguint les directrius, eines i formats establerts per l'Agència.
- 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 de cada lot.

Planificació

- L'Agència juntament amb el Departament de Salut de la Generalitat de Catalunya i les pròpies entitats proveïdores afectades determinaran la distribució mensual d'entitats que s'incorporaran a la planificació.
- La planificació dels serveis d'integració operativa dependrà del nombre de fonts a integrar per a cada entitat identificats durant la fase de diagnòstic. No obstant, totes les integracions hauran d'estar finalitzades abans del 30 de juny de 2026. Per poder complir amb aquesta data s'estima què l'execució de les tasques d'integració es puguin iniciar a un mínim de 10 entitats proveïdores alhora cada mes durant la vigència del contracte.
- 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 proveïdores d'atenció sociosanitària i de salut mental que caldrà integrar en el perímetre de l'Agència serà un mínim de 93, segons s'especifica a la memòria justificativa.
- S'estima que un 60% de les entitats proveïdores d'atenció sociosanitària tenen més de 100 treballadors. En el cas d'entitats proveïdores de salut mental, la previsió disminueix a un 45%.

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

2.6. Lot 4: Coordinació del desplegament del model de seguretat a les entitats proveïdores d'atenció sociosanitària i de salut mental

2.6.1. Objecte i abast del servei

L'objecte dels serveis d'aquest lot és donar suport a l'Agència en la coordinació i seguiment del desplegament del model de ciberseguretat a les entitats proveïdores d'atenció sociosanitària i de salut mental, per minimitzar la seva exposició envers les principals ciberamenaces que afecten al sector salut.

Objectius del servei

Els objectius que s'espera assolir amb la prestació del servei són:

- Donar suport a l'Agència en la planificació, organització i coordinació del desplegament del model a les entitats proveïdores d'atenció sociosanitària i de salut mental.
- Assegurar la disposició d'indicadors fiables i de qualitat per al seguiment del desplegament del model.
- Establir el model de relació amb els serveis de l'Agència.
- Garantir el compliment de les planificacions establertes i l'assegurament de la qualitat dels productes generats i fer una correcta supervisió del desplegament.
- Participar activament en la industrialització i evolució del servei.

Funcions i activitats

Les activitats i funcions que s'esperen del servei dins del desplegament del Model de Ciberseguretat de l'Agència són:

- Planificació i organització del desplegament del model a les entitats proveïdores d'atenció sociosanitària i de salut mental, en coordinació amb el Departament de Salut, l'Agència i les pròpies entitats.
- Coordinació de les activitats de les fases de diagnòstic, pla de seguretat i posada en servei, assegurant el compliment de les fites, directrius i planificacions acordades amb l'Agència i les pròpies entitats.
- Supervisió que les activitats que conformen les fases de diagnòstic, pla de seguretat i posada en servei, per garantir que es duen a terme seguint les directrius, eines i formats establerts per l'Agència, i aportant una visió unificada, íntegra i homogènia al voltant del grau d'exposició a les ciberamenaces.
- Participació en la presentació de resultats a les entitats proveïdores.
- Generació de resultats agregats que permetin disposar d'una visió global de l'estat de seguretat de totes les entitats proveïdores d'atenció sociosanitària i de salut mental, amb la visió consolidada del grau d'exposició a les amenaces i donar suport en la seva presentació.

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

- Assegurament de la disposició d'indicadors fiables i de qualitat, per a la presa de decisions i el seguiment del Model, així com del trasllat dels resultats i del coneixement adquirit als serveis de l'Agència, per a garantir la seva operativa diària.
- Participació activa en la industrialització i evolució del servei.

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 es poden considerar productes que inclouen resums de l'activitat dels serveis periòdicament, detall dels incidents/problemes més importants del període, seguiments de resolució de problemes, enquestes de satisfacció de lliurables, plans d'acció o planificacions, riscos operatius, mètriques i indicadors, entre d'altres. També, s'haurà de considerar la petició sota demanda de lliurables concrets per part de l'Agència.

Durant la prestació de servei l'empresa adjudicatària ha de generar i entregar de manera obligatòria els següents lliurables:

Document	Descripció	Periodicitat
Planificació del desplegament	Planificació del desplegament acordada amb l'Agència, el departament de Salut i les entitats	Mensual
Informe de seguiment consolidat del desplegament	Informes de seguiment global de l'estat del desplegament amb grau d'avenç, possibles desviacions, i riscos observats	Setmanal
Dashboard de seguiment	Indicadors de seguiment de les fases del desplegament i d'integració de fonts i entitats en PowerBi de l'Agència	Setmanal
Informe executiu del grau d'exposició a ciberamenaces de les entitats proveïdores d'atenció sociosanitària	Resultats agregats que permetin disposar d'una visió global de l'estat de seguretat de les entitats proveïdores d'atenció sociosanitària	Mensual
Informe executiu del grau d'exposició a ciberamenaces de les entitats proveïdores de salut mental	Resultats agregats que permetin disposar d'una visió global de l'estat de seguretat de les entitats proveïdores de salut mental	Mensual
Visió agregada dels plans	Matriu d'iniciatives	Puntual

Entre els diferents lliurables a definir pel servei, s'haurà de ser capaç de calcular i facilitar a als equips encarregats de la construcció d'indicadors del SOC totes aquelles mètriques requerides. Aquestes mètriques s'han de realitzar mitjançant les eines que es disposen a la pròpia l'Agència.

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

Mètriques del servei

A continuació es defineixen una sèrie orientativa i no definitiva de mètriques a millorar i completar per part del licitador. L'Agència es reserva el dret de modificar aquest llistat de mètriques de manera acordada amb l'adjudicatari.

Aspecte mesurat	Descripció
Entitats planificades	Nombre d'entitats amb *kickofff* acordat
Entitats avaluades i integrades	Nombre d'entitats en què s'ha finalitzat el diagnòstic, el pla de seguretat i la integració amb els serveis de monitorització i resposta de l'Agència.
Lliurables generats	Nombre de lliurables finals entregats (planificacions, informes executius, etc.)
Millores implementades	Nombre de millores implementades per a la industrialització i/o evolució del servei
Seguiments realitzats	Nombre de reunions de seguiment internes dels equips i de punts de control amb l'Agència.
Enquesta de Satisfacció	Puntuacions de les enquestes de satisfacció de lliurables.

A més de les llistades, s'hauran de poder obtenir de manera transversal per al servei i l'avaluació dels acords de nivell de servei.

2.6.2. Característiques del servei

De tot el que s'ha exposat prèviament es pot observar com, a l'hora de presentar les seves ofertes, els licitadors han de tenir en compte els següents elements essencials:

- Les activitats es duran a terme seguint les directrius, eines i formats establerts per l'Agència.
- 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 de cada lot.

Planificació

- L'Agència juntament amb el Departament de Salut de la Generalitat de Catalunya i les pròpies entitats proveïdores afectades determinaran la distribució mensual d'entitats que s'incorporaran a la planificació respectant sempre els límits temporals definits pel fons.
- Aquesta planificació tindrà en compte que la data límit per completar el desplegament de les fases del Model incloses en aquesta licitació (Diagnòstic, Pla de Seguretat i Integració de fonts) per a totes les entitats dins de l'abast dels diferents lots és del 30 de juny de 2026.
- 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 proveïdores d'atenció sociosanitària i de salut mental que caldrà integrar en el perímetre de l'Agència serà un mínim de 93, segons s'especifica a la memòria justificativa.
- S'estima que un 60% de les entitats proveïdores d'atenció sociosanitària tenen més de 100 treballadors. En el cas de les entitats proveïdores de salut mental, la previsió disminueix a un 45%.

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

El servei s'haurà de prestar d'acord amb els horaris de prestació dels serveis de l'Agència,

LOT 1: Avaluació de ciberseguretat de les entitats proveïdores d'atenció sociosanitària o intermèdia

Servei	Horari
Avaluació de la seguretat	8x5 (Dilluns a Divendres)

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.

LOT 2: Avaluació de ciberseguretat de les entitats proveïdores de salut mental

Servei	Horari
Avaluació de la seguretat	8x5 (Dilluns a Divendres)

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.

LOT 3: Enginyeria de Seguretat

Servei	Horari
Enginyeria de Seguretat	8x5 (Dilluns a Divendres)

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.

LOT 4: Coordinació del desplegament del model de seguretat a les entitats proveïdores d'atenció d'atenció sociosanitària i de salut mental

Servei	Horari
Suport a la coordinació	8x5 (Dilluns a Divendres)

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.

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

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 usuaris 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 dels serveis.

Es considera una obligació essencial per a l'empresa licitadora del lot 1 i lot 2, la presencialitat durant un període mínim aproximat d'una setmana a les instal·lacions de les entitats proveïdores d'atenció sociosanitària i de salut mental dins l'abast, per a la realització de les proves tècniques i reunions de consultoria necessàries, i la dedicació d'una altra setmana destinada a l'execució de proves tècniques en remot per analitzar els diferents vectors d'entrada que s'acordin a l'inici del projecte.

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 usuaris.

Per cadascun dels lots, l'adjudicatari disposarà d'una figura que assumirà les tasques de **"Cap de Servei**", que serà el principal responsable del servei. Aquest responsable, en base al model de relació de l'Agència, es coordinarà amb els responsables del servei per part de l'Agència, per tal de garantir la correcta execució de les capes de gestió, administració i servei. A aquest efecte, ha de assumir les següents responsabilitats:

- Coordinació amb la resta d'àrees i equips de l'Agència.
- Generació, implementació i càlcul de les mètriques i els indicadors del servei.
- Gestió de la capacitat del servei i la seva disponibilitat.
- Lideratge dels aspectes de ciberseguretat recollits en l'àmbit d'actuació del servei en els diferents comitès de seguiment/crisis o problemes endegats per l'Agència o CTTI.
- Gestió i control de la informació com procediments i instruccions operatives.
- Definició, millora i manteniment de procediments i instruccions operatives.
- Generació d'informes referents a incidències de servei, actes, informes executius, informes de resultats o informes de situació, entre d'altres, assegurant sempre la qualitat tècnica i executiva dels informes.
- Integració de l'operativa amb tercers: equips externs i interns o el propi negoci per exemple.
- Suport a la resolució de conflictes i incidències operatives.
- Pla de transformació i detecció d'oportunitats de millora.
- Consolidar i aportar a l'Agència les informacions objectives i subjectives que permetin a la Direcció la presa de decisions operatives, tàctiques i estratègiques relacionades amb el contracte.
- Assegurament de la qualitat del servei prestat i dels lliurables generats (*Quality Assurance*).
- Gestió de riscos operatius del servei.

D'altra banda, en el cas del **lot 4, s'haurà d'incorporar addicionalment** les figures de:

- **Coordinador de suport d'àmbit Salut:** que portarà a terme les següents activitats, tant en l'àmbit de les entitats proveïdores d'atenció sociosanitària com de salut mental:
    - Fer seguiment i coordinació per facilitar la correcta execució de les diferents activitats de dins de les respectives fases en el desplegament del Model.
        - Generar una proposta de distribució de les entitats per al període previst de desplegament.
        - Coordinar aquesta proposta amb els diferents actors que hi participen a nivell de proveïdors i entitats
        - Contactar amb les diferents entitats per coordinar la planificació de les reunions què siguin necessàries.
        - Avaluar la conveniència de que les reunions inicials siguin presencials o en remot, i individuals o agregades.

- Planificar i convocar les reunions corresponents per a la realització de les tasques amb la resta de participants i proveïdors.
    - Fer el seguiment de la correcta execució en temps i forma de les diferents fases del desplegament segons el calendari previst
    - Participar en els *kickoffs* i la presentació de resultats a les entitats, de les diferents fases de desplegament del Model.
    - Assegurar el traspàs d'informació a la resta d'equips de l'agència o proveïdors, tant en el desplegament del Model, entre les diferents fases, com al finalitzar amb l'equip que es farà càrrec dels serveis recurrents
    - Recollir el *feedback* de les entitats i traslladar-los als responsables de Programa.
    - Assegurar la disposició d'indicadors fiables i de qualitat, per la presa de decisions i seguiment del Model.
    - Donar suport als responsables de Programa en la presentació de resultats
    - Alertar de situacions de risc que es puguin generar amb les entitats o proveïdors als responsable de programa.
    - Gestionar incidències / conflictes amb els àmbits i/o terceres parts.
    - Participar activament en la industrialització i evolució del servei.
    - Identificar i proposar millores (output, evolució dels serveis, model de relació...).

- **Coordinador d'avaluació d'exposició (*pentest*):** que portarà a terme les següents activitats, tant en l'àmbit de les entitats proveïdores d'atenció sociosanitària com de salut mental:
    - Col·laborar en el disseny de les proves en coordinació amb els serveis i els responsables del servei de l'Agència.
    - Participar en els *kickoffs* i la presentació de resultats a les entitats.
    - Coordinar l'execució de les proves de *pentest* a les entitats proveïdores, garantint la correcta aplicació de la metodologia i les directrius definides per l'Agència i validant la qualitat dels lliurables produïts.
    - Realitzar reunions de seguiment i punts de control amb els equips de diagnòstic.
    - Elaborar informes executius agregats de les anàlisis tècniques realitzades de l'àmbit.
    - Supervisar que es realitzin les notificacions i avisos acordats durant l'execució de les proves de seguretat.
    - Gestionar incidències / conflictes amb els àmbits i/o terceres parts.
    - Garantir que es traslladen els resultats i el coneixement adquirit als corresponents equips d'àmbit del SOC/CERT, necessaris per la seva operativa diària.
    - Participar activament en la industrialització i evolució del servei.
    - Cooperar per l'elaboració i generació d'un relat únic al voltant de l'exposició a l'amenaça de les entitats proveïdores d'atenció sociosanitària i de salut mental.

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

- **Coordinador de Suport d'àmbit d'Operacions:** que portarà a terme les següents activitats, tant en l'àmbit de les entitats proveïdores d'atenció sociosanitària com de salut mental:
    - Participar en els *kickoffs* i la presentació de resultats a les entitats.
    - Fer seguiment de la correcta execució de les diferents activitats d'operacions, dins de les respectives fases en el desplegament del Model.
    - Coordinar i vetllar per la qualitat i alineament de les tasques de consultoria corresponent a les fases de diagnòstic i pla de seguretat del Model.
    - Fer seguiment continu del nivell de servei prestat (qualitat, temps resposta, alineació amb expectatives...).
    - Identificar i proposar millores (output, evolució dels serveis, model de relació...).
    - Coordinar amb els responsables interns de les diferents funcions del SOC/CERT, l'execució ordenada d'activitats i resolució de conflictes.
    - Garantir que es traslladen els resultats i el coneixement adquirit als corresponents equips d'àmbit del SOC/CERT, necessaris per la seva operativa diària.
    - Donar suport en el model relacional amb els àmbits.
    - Assegurar la disposició d'indicadors fiables i de qualitat, per la presa de decisions i seguiment de l'activitat operativa vinculada als àmbits.
    - Donar suport als responsables de Programa en la presentació de resultats generats per l'activitat dels serveis del SOC/CERT.
    - Cooperar per l'elaboració i generació d'un relat únic al voltant de l'exposició a l'amenaça de les entitats dins del seu abast.

Els Coordinadors d'Avaluació a l'Exposició i Suport a l'àmbit s'integraran a l'equip de responsables de servei de l'Agència com a suport a la coordinació i gestió dels serveis.

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.

3.3.1. Perfils

A continuació, es detallen els perfils professionals que des de l'Agència s'identifiquen per la disposició dels rols adients per la prestació dels serveis desitjats, deixant a la banda dels licitadors la proposta de desplegament, composició de l'equip, adequació de perfils i dedicació global dels mateixos.

Tots els perfils relacionats en aquest apartat i en l'apartat anterior han d'estar adscrits al contracte . L'empresa adjudicatària ha d'adscriure els perfils necessaris per a la correcta execució del contracte.

Addicionalment, per a cada perfil es llisten els requeriments mínims que haurien de complir les persones que assumeixin aquests rols.

LOT 1: Avaluació de ciberseguretat de les entitats proveïdores d'atenció sociosanitària o intermèdia

PERFIL	REQUISITS
Consultor Sènior	• Excel·lents habilitats de comunicació, tant orals com escrites, en entorns i audiències diverses, principalment en àmbits no versats en gestió TIC, seguretat de la informació i ciberseguretat. • Coneixement avançat de models de gestió de seguretat de la informació (ISO, NIST i similars). • Coneixement de l'entorn normatiu i regulatori que aplica a la ciberseguretat. • Coneixement de l'entorn tecnològic (desenvolupament, gestió de serveis TIC, xarxes, gestió de proveïdors,...) • Coneixement de sistemes de seguretat tant tradicionals com emergents. • 3 anys d'experiència mínims en serveis de consultoria de ciberseguretat.
Expert de seguretat (Pentester)	• Coneixements en metodologies i eines per a la realització d'anàlisis de vulnerabilitats i proves d'intrusió d'intrusió / '*pentesting*' (p.ex.: OSSTM, OWASP). • Coneixements que permetin aplicar tècniques d'evasió sobre els sistemes de seguretat implantats. • Coneixements sobre vulnerabilitats i debilitats tècniques més freqüents, així com la seva explotació, incloent-hi problemes de seguretat física, errors de disseny en protocols, programari maliciós, errors d'implementació, debilitats de configuració, errors o indiferència dels usuaris, entre d'altres, així com solucionar-los o definir accions mitigadores, o de contenció. • Capacitats per la descripció dels resultats obtinguts en les proves de *pentesting* de manera entenedora i permetent conèixer les seves implicacions i possibles recomanacions de mitigació. • 3 anys d'experiència mínims en l'execució de proves d'intrusió

Els perfils han de ser els necessaris per a la correcta execució del contracte. L'empresa s'obliga a adscriure al contracte amb els requisits mínims abans descrits els perfils necessaris per a la correcta execució del contracte.

LOT 2: Avaluació de ciberseguretat de les entitats proveïdores de salut mental

PERFIL	REQUISITS
Consultor Sènior	• Excel·lents habilitats de comunicació, tant orals com escrites, en entorns i audiències diverses, principalment en àmbits no versats en gestió TIC, seguretat de la informació i ciberseguretat. • Coneixement avançat de models de gestió de seguretat de la informació (ISO, NIST i similars). • Coneixement de l'entorn normatiu i regulatori que aplica a la ciberseguretat. • Coneixement de l'entorn tecnològic (desenvolupament, gestió de serveis TIC, xarxes, gestió de proveïdors,...) • Coneixement de sistemes de seguretat tant tradicionals com emergents. • 3 anys d'experiència mínims en serveis de consultoria de ciberseguretat.
Expert de seguretat (Pentester)	• Coneixements en metodologies i eines per a la realització d'anàlisis de vulnerabilitats i proves d'intrusió / '*pentesting'* (p.ex.: OSSTM, OWASP). • Coneixements que permetin aplicar tècniques d'evasió sobre els sistemes de seguretat implantats. • Coneixements sobre vulnerabilitats i debilitats tècniques més freqüents, així com la seva explotació, incloent-hi problemes de seguretat física, errors de disseny en protocols, programari maliciós, errors d'implementació, debilitats de configuració, errors o indiferència dels usuaris, entre d'altres, així com solucionar-los o definir accions mitigadores, o de contenció. • Capacitats per la descripció dels resultats obtinguts en les proves de *pentesting* de manera entenedora i permetent conèixer les seves implicacions i possibles recomanacions de mitigació. • 3 anys d'experiència mínims en l'execució de proves d'intrusió

Els perfils han de ser els necessaris per a la correcta execució del contracte. L'empresa s'obliga a adscriure al contracte amb els requisits mínims abans descrits els perfils necessaris per a la correcta execució del contracte.

LOT 3: Enginyeria de Seguretat

PERFIL	REQUISITS

Enginyer de Seguretat	• Expert en administració de solucions de seguretat i automatització de processos.
	• Capacitat d'abstracció i síntesis per tal d'obtenir resultats concisos.
	• Capacitat organitzativa i resolutiva.
	• Coneixement tècnics d'amenaces i vectors d'atacs
	• Coneixement de sistemes de seguretat tant tradicionals com emergents.
	  ○ Eines de perímetre de seguretat (NAC, IPS, firewalls, filtres de correu, entre d'altres).
	  ○ Eines d'anàlisi de seguretat (correlació d'informació, explotació d'informació no estructurada o en temps real, per exemple).
	• Capacitat d'integració d'elements de seguretat amb eines de tercers com Remedy, eines cloud, entre d'altres, mitjançant la programació d'API's.
	• Capacitat de programació en Phyton, Perl i altres llenguatges d'scripting per tal de realitzar programaris a mida.
	• Coneixements tècnics de xarxes, programari, protocols de comunicació, etc.
	• Coneixements de configuració segura de sistemes.
	• Coneixement d'eines d'anàlisi de seguretat (anàlisis heurística, traces, correlació d'informació, explotació d'informació no estructurada o en tremps real, per exemple).
	• 5 anys d'experiència en integració de solucions de seguretat.

Els perfils han de ser els necessaris per a la correcta execució del contracte. L'empresa s'obliga a adscriure al contracte amb els requisits mínims abans descrits els perfils necessaris per a la correcta execució del contracte.

LOT 4: Coordinació del desplegament del model de seguretat a les entitats proveïdores d'atenció sociosanitària i de salut mental

PERFIL	REQUISITS
Coordinador de suport d'àmbit de Salut	• Excel·lents habilitats de comunicació, tant orals com escrites, en entorns i audiències diverses, principalment en àmbits no versats en gestió TIC, seguretat de la informació i ciberseguretat. • Capacitats de lideratge, gestió i direcció organitzativa. • Capacitat de gestió d'equips i resolució de conflictes. • Destresa comunicativa i organitzativa. • Coneixements adequats en Ciberseguretat a nivell normatiu, regulatori, tècnic i de metodologies i models de gestió de seguretat de la informació, per poder dur a terme les tasques encomanades. • 5 anys d'experiència mínima en gestió de projectes i consultoria de ciberseguretat.

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

PERFIL	REQUISITS
Coordinador d'Avaluació a l'exposició	• Capacitats de lideratge, gestió i direcció organitzativa. • Capacitat de gestió d'equips i resolució de conflictes. • Destresa comunicativa. • Coneixements en metodologies i eines per a la realització d'anàlisis de vulnerabilitats i proves d'intrusió / '*pentesting*' (p.ex.: OSSTM, OWASP). • Coneixements que permetin aplicar tècniques d'evasió sobre els sistemes de seguretat implantats. • Coneixements sobre vulnerabilitats i debilitats tècniques més freqüents, així com la seva explotació, incloent-hi problemes de seguretat física, errors de disseny en protocols, programari maliciós, errors d'implementació, debilitats de configuració, errors o indiferència dels usuaris, entre d'altres, així com solucionar-los o definir accions mitigadores, o de contenció. • 5 anys d'experiència mínima en gestió i execució de proves d'intrusió.
Coordinador de suport d'àmbit d'operacions	• Capacitats de lideratge, gestió i direcció organitzativa. • Capacitat de gestió d'equips i resolució de conflictes. • Excel·lents habilitats de comunicació, tant orals com escrites, en entorns i audiències diverses, principalment en àmbits no versats en gestió TIC, seguretat de la informació i ciberseguretat. • Coneixement avançat de models de gestió de seguretat de la informació (ISO, NIST i similars). • Coneixement de l'entorn normatiu i regulatori que aplica a la ciberseguretat. • Coneixement de sistemes de seguretat tant tradicionals com emergents. • 5 anys d'experiència mínima en gestió de projectes i consultoria de ciberseguretat.

Els perfils han de ser els necessaris per a la correcta execució del contracte. L'empresa s'obliga a adscriure al contracte amb els requisits mínims abans descrits els perfils necessaris per a la correcta execució del contracte.

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 mateix.

3.3.2. Hores de dedicació

LOT 1: Avaluació de ciberseguretat de les entitats proveïdores d'atenció sociosanitària o intermèdia

El licitador haurà de proposar el dimensionament de l'equip de treball òptim i conforme amb els requeriments de solvència, per assolir la integració dels centres sociosanitaris dins l'abast abans del 30 de juny del 2026.

LOT 2: Avaluació de ciberseguretat de les entitats proveïdores de salut mental

El licitador haurà de proposar el dimensionament de l'equip de treball òptim i conforme amb els requeriments de solvència, per assolir la integració de les entitats proveïdores de salut mental dins l'abast abans del 30 de juny del 2026.

LOT 3: Enginyeria de Seguretat

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest lot és de **4.800 hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals[1] pels perfils indicats:

Perfil	Hores anuals mínimes estimades
Enginyers de Seguretat	**4.800 hores**

LOT 4: Coordinació del desplegament del model de seguretat a les entitats proveïdores d'atenció sociosanitària i de salut mental

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats en aquest lot és de **5.280 hores anuals**. Dins d'aquestes hores, s'estima el següent número d'hores mínimes anuals[2] pels perfils indicats:

Perfil	Hores anuals mínimes estimades
Coordinador d'avaluació d'exposició	**1.760 hores**
Coordinador de suport d'àmbit d'operacions	**1.760 hores**
Coordinador de suport d'àmbit de salut	**1.760 hores**

Tal com s'informa en la memòria justificativa, aquesta ha estat una estimació per al càlcul del pressupost del lot.

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

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

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

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.

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 contractista 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 el contractista 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.

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

- 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, el contractista 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. En el cas del lot 3, 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.

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

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.

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 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.

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

3.9. Control de Gestió

L'empresa adjudicatària, 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 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

L'empresa adjudicatària 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.

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 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 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:

3.14.1. 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.

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.

3.14.2. 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, 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.

3.14.6. 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, 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.

3.11. 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.

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.

3.12. 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 contracte, 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, 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.

Financiado por la Unión Europea NextGenerationEU
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.

3.13. 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.

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