# Plec de prescripcions tècniques particulars que regeix la contractació basada relativa a **Serveis de generació de contingut formatiu en ciberseguretat i suport per la capacitació en l'àmbit sanitari.**

**Estructurada en 2 lots**

**Lot 1: Contingut específic de formació en ciberseguretat i suport per la capacitació de plantilles d'hospitals**

**Lot 2: Contingut bàsic i específic de formació en ciberseguretat i suport per la capacitació de plantilles de serveis d'atenció primària, serveis d'assistència sociosanitària i serveis de salut mental**

**Exp. CB25AMCOML3B003**

## Índex

# 1 Introducció

L'Agència de Ciberseguretat de Catalunya (en endavant, Agència), establerta sota el marc de la Llei 15/2017, del 25 de juliol, és l'entitat que lidera i coordina els esforços de la Generalitat de Catalunya en la protecció de la informació i les infraestructures del país davant les ciberamenaces. En un món digitalitzat i interconnectat, la seguretat de la informació s'ha convertit en una prioritat estratègica, i l'Agència subratlla el compromís de Catalunya amb la promoció d'un entorn digital segur i de confiança. Dins d'aquest context, els acords marc en matèria de ciberseguretat representen una eina essencial per a la implementació de solucions i serveis que reforcin la ciberseguretat de Catalunya, alineats amb l'Estratègia de Ciberseguretat 2019-2022 i la proposta per a la nova Estratègia 2023-2027.

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 assolits per l'Estratègia 2019-2022 han establert un sòlid punt de partida per a futures accions, incloent la consolidació de l'Agència com a entitat de referència. Aquests avenços han millorat la capacitat de resposta davant incidents i han promogut una major consciència i formació en ciberseguretat entre la ciutadania i les organitzacions, desenvolupant una cultura de ciberseguretat per assolir una ciutadania digital plena, conscient i capacitada per a l'ús de les TIC.

L'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. La resiliència d'una organització davant les amenaces digitals comença amb la formació dels seus empleats en ciberseguretat, ja que un equip conscient i preparat és la primera línia de defensa contra qualsevol atac.

En el marc de l'activitat gestionada per l'Agència, cal destacar que dels 2.200 sistemes d'informació, més de 220.000 usuaris i un perímetre de 24 departaments i organismes rellevants, s'ha anat ampliant el seu perímetre de protecció amb nous àmbits: el món local, el sanitari i l'universitari. Durant 2024, l'Agència ha implementat una iniciativa en l'àmbit de Salut per avaluar i assegurar el grau de preparació davant un incident de seguretat als 68 hospitals integrats al SISCAT (Sistema Sanitari Integral d'Utilització Pública de Catalunya).

El nivell d'activitat de gestió durant el 2024 ha estat de 3.372 ciberincidents, la gran majoria de caràcter lleu, relacionats amb fuites de credencials o accessos il·legítims al correu electrònic. Això significa un augment del 26% respecte als incidents atesos el 2023, que van ser 2.665.

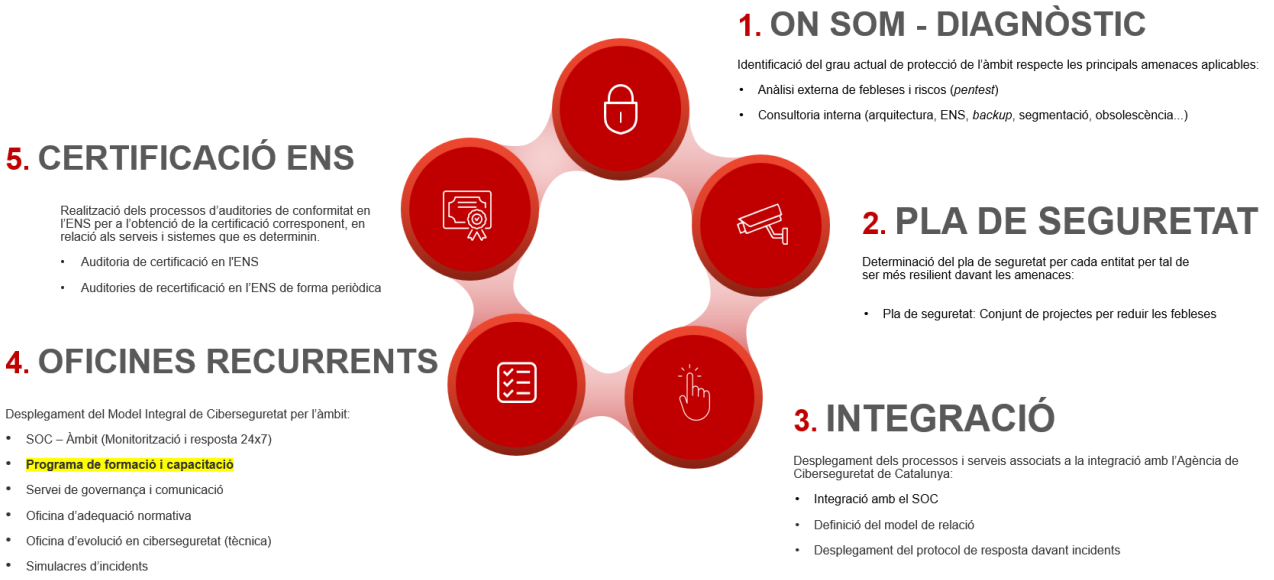
Les xifres fan paleses la necessitat de dotar-se de noves eines i de seguir ampliant el perímetre d'actuació en el sector sanitari, on als serveis hospitalaris gestionats actualment s'afegiran, en els propers mesos, els serveis d'atenció primària i els serveis sociosanitaris de Catalunya. En aquest

sentit, i alineat amb la nova Estratègia, l'Agència ampliarà més el perímetre d'actuació i, per tant, incrementa el nivell de protecció, resiliència i prevenció de més àmbits.

L'abast també s'ha vist en la necessitat d'incrementar-lo incorporant en la mesura del possible els centres per a l'atenció primària -seixanta entitats proveïdores principals- i els centres d'internament (l'atenció sociosanitària -unes noranta entitats- i l'atenció d'internament de salut mental -sobre la seixantena d'entitats-).

D'altra banda l'Agència vol culminar aquestes actuacions amb l'adequació i auditoria del compliment de l'Esquema Nacional de Seguretat (ENS) a les entitats del SISCAT.

## **Model** de ciberseguretat




*Il·lustració 1 Model de ciberseguretat en 5 fases pel projecte d'integració d'entitats del SISCAT amb l'Agència*

### 1.1 Funcions de l'Agència rellevants a efectes del l'estratègia de contractació

Avui en dia l'Agència s'estructura en:

- **Àrea de Gerència** s'ocupa de la gestió econòmico-financera, l'assessoria jurídica i contractació, la gestió de les persones i, la tecnologia i organització (on hi ha el servei Seguretat Corporativa i la unitat de Mitjans tècnics).
- **Àrea d'Operacions** realitza 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. Inclou serveis d'Operació de Seguretat d'Àmbits, Intel·ligència i resposta, Detecció i prevenció d'amenaces i Gestió i evolució operativa.
- **Àrea 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. L'Àmbit de Salut ha començat a tenir un paper rellevant amb el desplegament del model de ciberseguretat a 68 hospitals integrats al SISCAT, pel qual s'ha definit, l'aprovisionament i l'execució de projectes relacionats amb serveis i productes de ciberseguretat.

- **Àrea d'Innovació i 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. La promoció de la Innovació i l'Analítica i Ciència de Dades són palanques que ha incorporat recentment per aquesta funció de l'àrea.
- **Àrea de Capacitació i Promoció Ecosistema** s'ocupa de la comunicació de l'entitat, desenvolupar serveis públics a la ciutadania, ajuda a la transformació i creixement del sector de ciberseguretat, detecta i capta fons públics i capacita el talent professionals a través de la unitat de cultura o al projecte de Ciberacadèmia.
- **Àrea de Certificacions** 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.

# 2 Descripció dels serveis objecte de la contractació basada

## 2.1 Context dels serveis objecte de la licitació

El servei objecte de licitació en aquest plec està contextualitzat en l'expedient CB25AMCOML3B003 que regeix l'Acord Marc AM.04.2024. Concretament s'emmarca en l'anomenat Lot 3.

La present licitació es divideix en dos lots:

Lot 1 – Contingut específic de formació en ciberseguretat formatiu i suport a la capacitació de plantilles d'hospitals

El lot inclou l'activitat necessària per continuar la tasca iniciada i l'ampliació en contingut de ciberseguretat i en el suport a la formació d'empleats i empleades d'hospitals. La creació i adaptació de continguts adreçats als diferents grups d'empleats, la dinamització de les plataformes formatives (pròpia de l'entitat o proporcionada per l'Agència), el disseny i l'organització d'activitats formatives específiques en ciberseguretat per a diferents categories o nivells professionals d'hospitals (específicament els professionals dedicats a sistemes d'informació), la coordinació dels diferents actors participants per actualitzar el pla de formació i conscienciació de l'entitat i ajustar-lo al model de seguretat integral desplegat per l'Agència.

Lot 2 – Contingut bàsic i específic de formatiu en ciberseguretat i suport per la capacitació de plantilles de serveis d'atenció primària, serveis d'assistència sociosanitària i serveis de salut mental

El lot inclou l'activitat necessària per iniciar la formació d'empleats a serveis d'atenció primària. La creació i adaptació de continguts adreçats als diferents grups d'empleats i empleades, la dinamització de les plataformes formatives (pròpia de l'entitat o proporcionada per l'Agència).

El lot també inclou l'activitat necessària per crear un contingut formatiu en ciberseguretat adaptat a serveis sociosanitaris i de salut mental i iniciar el suport a la formació d'empleats i empleades als serveis sociosanitaris de Catalunya.

En un inici preveu desplegar el contingut creat a una plataforma autoformativa (pròpia de l'entitat o proporcionada per l'Agència) amb ajustos personalitzats, i, posteriorment, arrancar la dinamització de les edicions necessàries del curs per a tots els empleats i empleades i difusió de materials de conscienciació en ciberseguretat.

El disseny i l'organització d'activitats formatives específiques en ciberseguretat per a diferents categories o nivells professionals de serveis d'atenció primària, serveis sociosanitaris i de salut mental.

I l'establiment de la coordinació dels diferents actors participants per crear, i mantenir actualitzat, el pla de formació i conscienciació de l'entitat en qüestió segons l'evolució del model de seguretat integral previst per l'Agència.

## 2.2 Lot 1: Contingut formatiu i suport a la capacitació de plantilles d'hospitals

### 2.2.1 Objecte i abast dels serveis

L'objecte de la present licitació és la contractació de serveis de suport a la formació i capacitació en ciberseguretat per a plantilles de l'àmbit sanitari de la xarxa d'hospitals, ICS (hospitals de referència de l'empresa pública del sistema sanitari català) i d'organismes públics independents que presten

serveis especialitzats (Institut de Diagnòstic per la Imatge, Institut Català d'Oncologia, Banc de Sang i Teixits i Sistema d'Emergències Mèdiques).

Els serveis que inclouran són la creació de continguts específics en ciberseguretat per a als professionals de l'àmbit sanitari (personal assistencial sanitari, personal de suport, personal no assistencial, personal de recerca, personal de gestió i especialistes en sistemes d'informació), el disseny d'activitats formatives adaptades a les necessitats, la dinamització dels cursos i activitats formatives en diferents plataformes, i la coordinació dels diferents actors implicats per a la seva realització.

En concret els objectius que es persegueixen i que es volen assolir amb la contractació d'aquest servei són:

- Creació de continguts específics de ciberseguretat per a grups professionals.
- Coordinació amb les diferents persones responsables de formació i gestores del projecte en les entitats destinatàries.
- Gestió de les diferents activitats dinamitzadores per desenvolupar les activitats formatives dissenyades dins el calendari previst i en les diferents plataformes de formació.
- Alineació de continguts de ciberseguretat avançada per a professionals tècnics IT de les entitats amb els serveis de la Ciberacadèmia de l'Agència.

#### 2.2.1.1 Antecedents de les activitats formatives en ciberseguretat

Dins del marc de treball dels hospitals del SISCAT (on s'inclouen hospitals de Catalunya, el SEM, l'ICS i entitats de plataformes de servei com l'ICO, BST i IDI) s'han realitzat actuacions formatives bàsiques durant els anys 2023, 2024 i 2025 adreçades a totes les plantilles sense distingir les que tenen un caràcter assistencial sanitari de les que simplement fan gestió o suport amb caràcter no assistencial. Aquestes activitats formatives s'han ofert a través de plataformes en línia on destaca el campus de ciberseguretat proporcionat pel Departament de Salut o les pròpies plataformes en què compta cada entitat destinatària. L'abast total de l'actuació es situa al voltant de les 150.000 persones que pertanyen a **68 entitats hospitalàries o entitats transversals del SISCAT**.

Per a personal especialista en TIC i d'equips dels sistemes d'informació s'han impartit periòdicament seminaris per Internet específics (en entorns síncrons i amb possibilitat de recuperar materials gravats) on s'amplien les capacitats i els coneixements del personal tècnic que administra els serveis IT dels hospitals.

Amb aquest focus el nombre de persones formades durant 2024 i 2025 ha superat les 40.000.

El Pla de formació fins l'actualitat ha tingut l'objectiu de **conscienciar i sensibilitzar a tots els professionals** (treballadors de totes les categories) **del Sistema Sanitari Integral d'Utilització Pública de Catalunya** (SISCAT), mitjançant l'explicació dels impactes dels ciberatacs i la importància de la ciberseguretat, tant des del punt de vista personal com des del punt de vista de l'organització.

| | |
|---|---|
| **Formació bàsica de professionals sanitaris** | Difusió d'accions formatives que permeten **sensibilitzar els i les professionals sanitàries** per adquirir coneixements i hàbits bàsics en matèria de ciberseguretat. |
| **Capacitació de tècnics IT i no IT** | Difusió d'accions formatives que permeten capacitar tècnicament a les **persones amb responsabilitats tècniques** per aprofundir en aspectes de ciberseguretat. |

| | |
|---|---|
| **Conscienciació d'alts càrrecs** | conscienciar i transmetre la importància del rol que exerceixen els càrrecs directius a dins de l'entitat. |

A partir de diferents elements d'aplicació que es combinen en una metodologia que s'ajusta a l'aprenentatge en el lloc de treball i amb un format asíncron modular, amb un curt temps de dedicació, perquè cada persona pugui fer formació en línia al seu ritme.

Els materials que conté la formació bàsica actualment, en format SCORM, disposa d'aquest índex de continguts:

Mòdul 1H. Amenaces als sistemes d'informació sanitaris

Conceptes i temes tractats: atac de phishing, atac de ransomware, fuita de dades, metadades, seguretat física i protecció de dispositius, prevenció d'IoT i electromedicina.

Mòdul 2H. Bones pràctiques en les TIC

Conceptes i temes tractats: eines col·laboratives, autenticació i gestió de credencials, certificats digitals i xifrat, notificació d'incidents.

Mòdul 3H. Protecció de dades personals

Conceptes i temes tractats: RGPD, polítiques de protecció de dades, història clínica.

Plataformes formatives usades per a cursos virtuals

Les activitats formatives, fins ara, es desenvolupen en plataformes de referència pels alumnes participants, pròpies de l'entitat o cedida pel Departament de Salut o l'ICS. Aquestes fonamentalment són:

1. Campus de ciberseguretat del Departament de Salut https://formacio.salut.gencat.cat/ amb usuari i credencials gestionades de Moodle per a responsables de formació de cada hospital participant.
2. Plataforma pròpia de cada hospital. Entorns LMS Moodle o Canva que poden executar el curs en format SCORM que facilita el servei de formació de l'Agència.
3. L'ICS usa la plataforma TALICS, un LMS basat en *Cornerstone OnDemand***,** per gestionar la formació del personal sanitari. Permet la recollida d'informació dels professionals dels diferents centres on treballen els professionals de l'ICS.

Aquest material es complementa amb:

- Diferents Quiz (un exercici per mòdul) per a revisar que els alumnes han comprès els continguts dels mòduls.
- Infografies sobre casos d'ús: bones pràctiques al lloc de treball, gestió de credencials, notificació d'incidents, teletreball, IoMT...
- Vídeos interactius i materials infogràfics amb H5P o Genially: per aprendre a gestionar un cas de correu de phishing o com protegir dispositius d'electromedicina.
- Vídeos a Youtube que posen context sobre riscos i tendències en ciberseguretat del sector salut.
- Vídeos divulgatius sobre com es xifren les dades, com protegir l'enviament de la informació sensible, com protegir-se de l'enginyeria social...
- Podcasts sobre històries reals d'*smishing* i *vishing.*

### 2.2.1.2 Evolució del servei de formació

Tot seguit es descriuen les principals activitats i funcionalitats que s'esperen per l'evolució del servei actual:

- Funcionament optimitzat d'Oficina tècnica de formació.
- Redacció i gestió del nou contingut específic de capacitació de ciberseguretat en base a criteris de competència digital.
- Gestió dels nivells d'itineraris formatius que permetin orientar i enrolar els usuaris participants cap a l'activitat formativa de la Ciberacadèmia de l'Agència.

Es parteix d'una diversitat de plantilles d'entitats hospitalàries que es poden classificar per aquests grups d'activitat:

A. **Personal assistencial sanitari**
   Metges/esses especialistes medicina interna
   Cirurgia i altres especialitats mèdiques
   Pediatria
   Infermers/es
   Auxiliars d'infermeria
   Tècnics sanitaris (radiologia, laboratori, anatomia patològica)
   Farmacèutics hospitalaris
B. **Personal de suport**
   Tècnics d'emergències sanitàries
   Treballadors socials sanitaris
   Psicòlegs clínics
   Fisioterapeutes
   Terapeutes ocupacionals
   Logopedes
   Camillers
C. **Personal no assistencial**
   Personal d'admissions i gestió de pacients
   Administració i documentació clínica
   Serveis generals (neteja, manteniment)
   Servei de cuina
   Seguretat i vigilància
D. **Gestió**
   Direcció
   Servei tècnic no IT (compres, finances, recursos humans)
E. **Especialistes en TIC i sistemes d'informació**
   Desenvolupadors d'aplicacions
   Gestors de xarxes i usuaris
F. **Personal de recerca**
   Enginyers biomèdics
   Investigadors clínics

#### 2.2.1.3 Competències digitals que es volen completar

Aquestes són les competències a nivell general que s'han d'assolit en coneixement i skills:

- Ser conscient de la naturalesa canviant dels riscos i amenaces en entorns digitals, i tenir en compte la seguretat dels dispositius digitals i el contingut (a les aplicacions que usem en els dispositius de treball, en les comunicacions diàries, en la navegació a Internet, en la compartició de dades al núvol...).

- Avaluar i gestionar els riscos de privadesa i protegir les dades personals i la privadesa en entorns digitals. Utilitzar i compartir les dades personals pròpies i d'altres de manera segura, ètica i responsable.
- Utilitzar les tecnologies digitals de forma que donin suport al benestar i la inclusió. Minimitzar els riscos i les amenaces per al benestar físic, mental i social d'un mateix i dels altres en utilitzar les tecnologies digitals.
- Saber protegir-se d'atacs que esdevenen a la xarxa, incorporar mesures de protecció o alertar de les situacions que resolen els serveis de suport.
- Entendre l'alineament amb les polítiques de seguretat que es defineixen per al compliment normatiu.

#### 2.2.1.4 Producció de contingut de ciberseguretat específic

Els continguts de ciberseguretat que s'han de preparar per als diferents col·lectius han d'evolucionar a partir del nivell bàsic que han rebut de manera transversal per un contingut nou en un nivell intermig o avançat que s'adapti a la realitat del grup professional i alineades amb el marc de competències digitals DigComp 3.0, apartat 4 *Cybersecurity and Safety competence*[1].

A tall d'exemple d'estructura, per a formació en línia, aquestes són línies de desenvolupament de nous mòduls formatius i els temes clau que haurà de resoldre el licitant:

A. Contingut formatiu per personal assistencial sanitari

| | | |
|---|---|---|
| Intermig<br><br>Mòdul 4PAS i Mòdul 5PAS | **Ciberhigiene clínica i protecció de dades** | Contrasenyes robustes i MFA; phishing clínic i enginyeria social; principi de mínima informació; ús segur de dispositius portàtils; traçabilitat d'accés a la Història clínica |
| | **Seguretat de sistemes clínics (Història clínica, PACS, LIS)** | Perfils i rols d'accés; integritat de dades de laboratori; seguretat d'imatge mèdica (PACS/RIS); còpies de seguretat i restauració |
| Avançat<br><br>Mòdul 6PAS i Mòdul 7PAS | **Dispositius mèdics i IoMT: riscos i controls** | Inventari i segmentació de dispositius; gestió de pegats; comunicacions xifrades; procediments en cas de fallada/compromís |
| | **Resposta a incidents clínics** | Detecció i contenció; continuïtat assistencial (en casos de *ransomware*); recuperació de dades; comunicació interna/externa; notificació de bretxes |

B. Contingut formatiu per personal de suport

| | | |
|---|---|---|
| Intermig<br><br>Mòdul 4PSU i Mòdul 5PSU | **Conscienciació i enginyeria social en circuits assistencials** | Phishing/smishing/vishing; verificació d'identitat del pacient; bones pràctiques de compartició mínima; report de sospites |
| | **Mobilitat segura i privacitat en l'atenció** | Ús segur de mòbils/tauletes; accés remot a Història clínica; protecció de dades en espais compartits; comunicació xifrada amb equips clínics |
| Avançat<br><br>Mòdul 6PSU i Mòdul 7PSU | **Dispositius portables i telemetria (rehabilitació/monitoratge)** | Riscos d'IoT sanitari; parellament i autenticació; protecció de dades sensibles; protocols de desinfecció i custòdia física |
| | **Gestió d'incidents fora d'unitat (ambulàncies, domicili, sala d'espera)** | Procediments de contenció; cadena de custòdia d'equipament; comunicació amb TI; registre i aprenentatge post-incident |

C. Contingut formatiu per personal no assistencial

[1] *JRC Publications Repository - DigComp 3.0: European Digital Competence Framework 27/11/2025*

| | | |
|---|---|---|
| Intermig<br><br>Mòdul 4PNA i Mòdul 5PNA | **Protecció de dades personals en fluxos d'admissions i arxiu** | Validació d'identitat; confidencialitat al mostrador; gestió de documents físics/digitals; controls d'accés |
| | **Oficina segura: correu, fitxers i impressió** | Phishing i adjunts; macros i codi maliciós; impressió amb validació prèvia; gestió de comparticions i permisos |
| Avançat<br><br>Mòdul 6PNA i Mòdul 7PNA | **Governança i compliment (RGPD i polítiques de seguretat internes)** | Bases legals; minimització i retenció; Avaluacions d'impacte sobre protecció de dades; protocols de notificació de bretxes |
| | **Seguretat física i control d'accés** | Gestió d'acreditacions; prevenció de *tailgating*[2]; protecció d'àrees crítiques; coordinació amb vigilància |

D. Contingut formatiu per personal de gestió

| | | |
|---|---|---|
| Intermig<br>Mòdul 4PG i Mòdul 5PG | **Cultura de ciberseguretat i lideratge** | Factors humans; polítiques i comunicació interna; programes de sensibilització; indicadors i KPIs |
| | **Gestió de riscos i continuïtat de negoci en salut** | BIA (impacte en pacients/servei); plans de contingència; RTO/RPO; simulacres |
| Avançat<br><br>Mòdul 6PG i Mòdul 7PG | **Contractació segura i cadena de subministrament** | Due diligence de proveïdors; clàusules de seguretat/privacitat; avaluacions de tercers; monitoratge de SLA; Atacs de BEC i cadena de subministrament |
| | **Crisi i resposta davant ransomware** | Decisions operatives; comunicació amb parts interessades; negociació/no negociació; recuperació i lliçons apreses |

E. Contingut formatiu per especialistes en TIC i sistemes d'informació

| | | |
|---|---|---|
| Intermig HOS<br><br>Mòdul 4EIT i Mòdul 5EIT | **Seguretat d'endpoint i xarxa hospitalària** | Segmentació (VLAN/ACL); NAC i inventari; gestió de pegats; duresa de configuracions (hardening) |
| | **Identitats i accessos (IAM/PAM) en entorns clínics** | RBAC (control d'accés basat en rols) per rols clínics / administratius; MFA; delegació segura; revisió periòdica de permisos |
| Avançat HOS<br><br>Mòdul 6EIT i Mòdul 7EIT | **Seguretat de dispositius mèdics i IoMT** | Arquitectures i passarel·les; microsegmentació; gestió de vulnerabilitats de fabricant i de dia zero; proves i validació |
| | **Resposta a incidents i detecció (SIEM/SOAR)** | Casos d'ús específics hospitalaris; playbooks; anàlisi forense bàsica; comunicació amb assistència i gestió |

En paral·lel s'adaptarà el contingut en coordinació amb Lot 2 d'aquesta licitació per mòduls similars per atenció primària:

| | | |
|---|---|---|
| Intermig AP | **Endpoints i inventari en CAP** | Inventari HW/SW; pegats i hardening; antivirus/EDR; polítiques d'USB i impressió; còpies de seguretat |
| Mòdul 4EIT i Mòdul 5EIT | **Identitats i accessos (IAM) de baixa complexitat** | RBAC per rols del CAP; MFA; alta/baixa d'usuaris i revisió periòdica; accessos temporals |
| Avançat AP | **Xarxa de CAP i serveis de teleassistència** | Segmentació bàsica; Wi-Fi d'invitats vs clínic; VPN; QoS i seguretat de videotrucades; protecció de gateways |
| Mòdul 6EIT i Mòdul 7EIT | **Detecció i resposta (IR) de primer nivell** | Playbooks per phishing/ransomware; registre centralitzat (SIEM lleuger); comunicació amb assistència; post-incident i millora |

[2] Acció d'entrar de manera clandestina en una àrea restringida aprofitant que hi entra algú altre que hi té accés autoritzat, sovint esquitllant-se darrere de la persona amb accés o barrejant-se en un grup de gent.

I també es coordinarà per a professional d'atenció en assistència intermèdia, sociosanitària i salut mental:

| | | |
|---|---|---|
| Intermig SSM<br><br>Mòdul 4EIT i Mòdul 5EIT | **Endpoints i inventari en serveis sociosanitaris i salut mental** | Inventari HW/SW; pegats i hardening; antivirus/EDR; polítiques d'USB i impressió; còpies de seguretat |
| | **Identitats i accessos (IAM) bàsic** | RBAC per rols en el centre; MFA; alta/baixa d'usuaris i revisió periòdica; accessos temporals |
| Avançat SSM<br><br>Mòdul 6EIT i Mòdul 7EIT | **Xarxa i serveis de teleassistència** | Segmentació; Wi-Fi d'invitats vs clínic; VPN; seguretat de videotrucades; protecció de gateways |
| | **Detecció i resposta (IR) de primer nivell** | Playbooks per phishing/ransomware; registre centralitzat; comunicació amb assistència; post-incident i millora |

F. Contingut formatiu per personal de recerca

| | | |
|---|---|---|
| Intermig<br><br>Mòdul 4PR i Mòdul 5PR | **Gestió i integritat de dades de recerca** | Pseudonimització / anònims; traçabilitat; qualitat de dades; accés compartit segur |
| | **Compartició i transferència segura (consorcis/repositoris)** | Acords de dades; controls d'accés; xifrat i canals segurs; registre de descàrregues |
| Avançat<br><br>Mòdul 6PR i Mòdul 7PR | **Compliment legal/ètic en dades personals de salut (RGPD)** | Bases legals per recerca; Avaluacions d'impacte sobre protecció de dades; gestió de consentiment; publicació/responsabilitat |
| | **Seguretat d'equipament i laboratoris connectats** | Inventari IoT biomèdic; calibració / pegats; segmentació de xarxa; plans de contingència |

- Com que molts professionals que es volen formar desconeixen els tecnicismes de la ciberseguretat s'ha d'adaptar el llenguatge (sobretot pels professionals assistencials i de suport) i els casos d'ús escollits com exemples il·lustratius per fer més efectiva la formació.
- Redactar continguts efectius i personalitzats per a cada segment del públic objectiu, adaptant-se a les seves necessitats específiques i nivells de comprensió en matèria de ciberseguretat.
- Els continguts dedicats a gerents i càrrecs directius han de posar especial èmfasi en aspectes com l'impacte econòmic dels ciberatacs i els beneficis de les inversions en ciberseguretat, entre altres.
- Els continguts dels mòduls dedicats a especialistes en TIC i sistemes d'informació han de ser coordinats amb l'adjudicatari del Lot 2. També cal connectar els usuaris d'aquesta formació amb els diferents itineraris formatius previstos per a aquests perfils tècnics en l'activitat formativa en nivells 3 i 4 de la Ciberacadèmia de l'Agència.
- En els elements fabricats amb formats com infografies, presentacions de webinars/seminaris, vídeos divulgadors/interactius i els materials de comunicació cal emprar guions i recursos que siguin adaptables en els diferents contextos professionals previstos (grups A, B, C, D, E i F).
- Tenir present altres àrees de l'Agència (per exemple la de comunicació i àrees SOC i CERT) per assegurar que el contingut sigui tècnicament precís i rellevant.

### 2.2.1.5 Disseny i producció d'elements formatius

Algunes propietats a considerar en la qualitat dels lliurables a elaborar:

**Estil comunicatiu:** utilitzar llenguatge clar i accessible, en català normatiu, evitar tecnicismes o explicar-los amb exemples, incorporar storytelling i situacions reals per fer els conceptes comprensibles.

**Disseny visual**: crear interfícies netes amb navegació intuïtiva, colors que destaquin alertes, tipografia llegible i els recursos multimèdia seran vídeos breus, elements interactius, animacions o infografies. S'han de tenir present les característiques d'usabilitat i accessibilitat, segons les directrius de la Generalitat de Catalunya i les WCAG 2.1. Han de preveure: alternatives textuals, controls operables des de teclat, control de reproducció, contrastos gràfics (nivell AA), estructura semàntica clara, compatibilitat amb tecnologies d'assistència com els lectors de pantalla...

**Elements produïts**: prioritzar el microlearning amb mòduls poca extensió, incloure casos pràctics, simulacions interactives i gamificació per mantenir l'interès, garantint accessibilitat en tots els dispositius.

**Estratègia pedagògica**: establir una progressió gradual dels conceptes, oferir feedback immediat en activitats i adaptar exemples al context de l'usuari per personalitzar l'aprenentatge. Generar glossaris i índexs de recursos de consum no obligatori per a obtenir més informació de la ciberseguretat o ampliar conceptes.

**Confiança en els continguts**: basar-se en fonts fiables (prioritzant els de l'Agència i la Fundació TICSalut), actualitzar periòdicament els continguts i assegurar la protecció de dades dels usuaris dins la plataforma.

Aquests elements comunicatius inclosos a les plataformes LMS amb orientació formativa es coordinarà la seva producció amb la Unitat de Comunicació de l'Agència, qui pot demanar usar dissenys amb noves tendències de mercat.

Cal tenir present en el calendari d'actuació que aquest servei és crític pel desenvolupament del projecte avançar la creació de continguts el màxim possible per no condicionar les activitats dels altres serveis: dinamització de cursos i les actuacions del servei de gestió d'itineraris, tecnopedagoc, assessorament...

Les característiques dels elements que han de desenvolupar-se per a construir els nous mòduls formatius:

- Diferents Quiz (preferentment un exercici per mòdul) per a revisar que els alumnes que han fet el mòdul en comprenen el seu contingut.
- Infografies sobre els casos d'ús rellevants d'actualitat que s'expliquen: per exemple, bones pràctiques pel lloc de treball, evitar els enganys digitals, ús correcte de la IA corporativa...
- Vídeos interactius amb format creat per H5P, iSpring Suite, Articulate, Loom, Panopto o Genially que siguin integrables als diferents LMS. Aquests han de permetre fer una part pràctica i aplicable l'aprenentatge de ciberseguretat en cursos en línia, per exemple amb exercicis on l'usuari pugui comprendre les conseqüències en les diferents possibilitats de decisió.
- Vídeos breus a Youtube que posin context sobre els tipus de riscos i tendències actuals en les amenaces de ciberseguretat del sector salut.
- Vídeos divulgatius com a tutorials per a explicar com es poden usar les d'eines i procediments de seguretat que han d'usar especialistes en TIC per integrar-se a l'Agència i sistemes d'informació o per a protocols de resposta en cas d'incidents ...

- Presentacions, documents guies que siguin suport per a seminaris o presentacions en sessions formatives síncrones que es puguin desenvolupar (s'ha de preveure la difusió a la comunitat de professionals de la gravació de les ponències presentades). El licitant haurà fer una proposta de directori de possibles temes a desenvolupar en ciberseguretat, recollint la informació de sondejos i enquestes a interlocutors de les diferents entitats hospitalàries i altres entitats.

### 2.2.2 Característiques del servei

De tot el que s'ha exposat prèviament es pot observar com, el servei de conscienciació i formació en l'àmbit de Salut té els elements essencials següents:

El serveix requereix d'una capacitat d'anàlisi exhaustiva per identificar les característiques específiques de ciberseguretat de les diferents categories professionals dins de l'àmbit sanitari, incloent personal assistencial sanitari, de suport, no assistencial, de gestió (on s'inclouen càrrecs directius), especialistes en TIC i sistemes d'informació i personal de recerca. Així mateix, també requereix de capacitat per recopilar i analitzar quines preferències de consum de continguts digitals i hàbits d'ús de dispositius en la seva feina d'aquests col·lectius, amb l'objectiu d'assegurar que el procés formatiu sigui adequat i tingui impacte per a cada segment.

Aquest anàlisi es realitzarà mitjançant enquestes o a través de les conclusions d'un grup de treball amb diversos actors dels centres sanitaris, permetent definir les prioritats de les temàtiques emergents i les estratègies a seguir per maximitzar la seva aplicabilitat en el lloc de treball.

Les característiques que definiran el servei formatiu seran:

1. La sensibilització i consells en ciberseguretat seran personalitzades segons el perfil dels professionals. Per als diferents grups descrits anteriorment, es proporcionaran consells pràctics sobre ciberseguretat adaptats als seus rols.

   Per exemple, els rols gerencials i càrrecs directius han de rebre activitats formatives específiques que explicitin aspectes de l'impacte econòmic dels ciberatacs, aspectes d'adequació a les noves normatives (ENS i NIS2), els beneficis d'invertir en la ciberseguretat, la importància de incrementar la confiança en la cadena de subministrament, entre altres.

2. Les pàgines de presentació dels diferents cursos per perfil professional tindran informació sobre com es pot desenvolupar el curs (durada de temps a dedicar i període de disponibilitat), reconeixement que s'acreditarà al final de curs (certificat personal per alumne), informació sobre el sistema per obtenir APTE del curs (realització de qüestionaris o quiz), sistema de suport per resoldre dubtes previst (tot i ser preferentment un sistema autoformatiu pot haver l'opció d'elaborar apartats de preguntes i respostes freqüents sobre com funciona la plataforma), com contactar amb el responsable del curs per qualsevol altre gestió.

3. Definició i edició de particularitats per a cada curs d'entitat. En el curs de diferents mòduls s'ha de preveure que es pugui posar algunes referències documentals pròpies de l'entitat (eines col·laboratives que apliquen, sistema de notificació d'incidents, polítiques de protecció de dades...) que enfoquin els temes tractats en l'entitat que es desenvolupa la formació.

4. La dinamització, amb un perfil de docent editor a les plataformes formatives, s'ocuparà de la personalització, definició de la temporalitat i ajust de les edicions en aquestes plataformes (amb les corresponents actualitzacions i notificacions automatitzades si es requereixen) de les entitats. Ha de preveure una sistemàtica d'enrolament dels usuaris que es volen incloure

a les diferents edicions formatives, confirmar el correcte desenvolupament de cada activitat, fer activitats de seguiment per maximitzar l'eficàcia de les edicions i resoldre qualsevol incidència que pugui impedir la compleció dels cursos oberts.

Eventualment convé executar rols d'administrador a la plataforma formativa emprada per a gestionar permisos en els nous cursos o per poder extreure dades d'indicadors de l'assoliment dels alumnes matriculats i elaborar informes amb els resultats.

5. Seguiment i coordinació amb els actors claus de l'entitat que coneixen el projecte: a banda de les persones que coneixen els recursos humans i de formació de l'entitat cal coordinar activitats amb els responsables de seguretat que lideren el projecte d'integració de l'Agència dins l'entitat. Per això serà important un contacte periòdic amb reunió o amb comunicacions per correu electrònic per situar l'evolució del procés formatiu.

6. Seguiment i coordinació amb els responsables del projecte dins de l'Agència. No només fer seguiment i coordinació amb el responsable de la Unitat de Cultura en ciberseguretat, qui ha de conèixer en tot moment el detall del calendari i l'esforç previst en les diferents activitats formatives, sinó també els responsables de desplegament de l'auditoria de certificació ENS o de les diferents oficines recurrents de l'Agència que intervenen amb l'entitat.

7. Preparació de documentació sobre l'execució de la formació. Cada entitat compta amb un pla de formació en ciberseguretat, que representa el pla de treball sobre totes les activitats formatives en ciberseguretat realitzades en el passat (vinculades a Informes de cursos realitzats) i les previstes pel futur (continguts i públic objectiu previstos) per l'entitat. A nivell orientatiu hi constaran les sessions en plataforma virtual i els objectius previstos per aquestes per cada any. També s'haurà de documentar les activitats de sensibilització i conscienciació previstos. L'estructura dels diferents documents existents de l'entitat quedaran indexats en aquest pla de formació en ciberseguretat.

   Aquesta documentació és clau per a obtenir evidències del procés formatiu i tenir indicadors dels resultats de la formació realitzada. Per això es recullen indicadors i mètriques per mesurar l'impacte de forma mensual que gestiona la unitat de Govern de la Dada de l'Agència per representar la situació sobre els objectius marcats per a cada entitat.

   L'informe de formació de cada edició que haurà de lliurar a l'entitat participant per recollir:

   -Resultats de la formació
   - Nombre de persones que van ser inscrites en cada edició.
   - Nombre de persones que van superar el curs (APTES).
   - Mitjana de resultats dels mòduls.
   - Visualització dels continguts complementaris.
   - Nombre d'hores que la plataforma ha estat oberta.

   -Resultats de l'enquesta de satisfacció
   - Si ha faltat incloure o modificar algun aspecte més a la formació (millores a fer).
   - Si s'han assolit els objectius.
   - Aplicabilitat a les tasques diàries.
   - Valoració global de l'activitat formativa.

   -Llistat de persones que han superat en APTE cada curs: quins usuaris es van inscriure a la plataforma del curs en ser convocats i quin nombre d'aquests l'han superat.

8. En el cas d'organització de seminaris web o altres formacions presencials (tipus taller síncron o presencials) per a determinats col·lectius, si és el cas, cal seguir un procediment de convocatòria (coordinat amb la unitat de comunicació), de preparació dels contingut i tria de ponents previstos amb plataforma de videoconferència (preferentment ZOOM de l'Agència, que cal gestionar i dinamitzar durant l'activitat formativa) i de recollida de resultat i satisfacció. Els ponents que participen d'aquests seminaris s'escolliran, en funció de la temàtica, dels referents de l'Agència però convé tenir ponents presentadors o dinamitzadors de l'activitat, si escau, amb una expertesa suficient del tema que es tracti.

9. Les activitats de serveis de gestió d'itineraris, tecnopedagoc, altres assessoraments que es desenvolupin pel licitant seguiran les directrius de la Unitat de la Ciberacadèmia de l'Agència per a connectar les oportunitats ofertes en els itineraris de perfils disponibles amb l'estimulació de la demanda en l'àmbit sanitari, tan per upskilling o reskilling de professionals.

10. Les tasques de l'Oficina tècnica de formació de l'Agència es coordinaran amb altres proveïdors que fan activitat formativa a altres àmbits on treballa l'Agència i es seguiran les recomanacions i normes d'estandardització del procés, sobre la gestió de calendari de les activitats formatives i el recursos comuns a disposar, que és responsabilitat de la Unitat de Cultura en ciberseguretat de l'Agència. És clau sistematitzar al màxim, automatitzant les tasques que permetin alliberar els esforços pels àmbits de major valor afegit.

**Calendari d'execució**

A grans trets s'espera d'aquest contracte aquesta distribució temporal que haurà de ser ajustada i planificada amb els recursos assignats pel licitador i el tipus de categoria professional destinatària:

- Fase actualització del contingut bàsic existent (primer mes)
- Establiment de canal i coordinació amb responsables d'entitats destinatàries (1 mes)
- Elaboració del nou contingut específic (considerant la coordinació amb Lot 2 per a especialistes en TIC i sistemes d'informació) i pilotatge per a les diferents categories professionals (6 mesos per a principals lliurables)
- Desplegament de cursos i dinamització de les diferents edicions de cursos (des de la disponibilitat de mòduls específics fins a final de projecte).

De forma recurrent a aquestes fases: coordinació i seguiment amb els diferents promotors de la formació, actuacions del tecnopedagoc en objectius acordats amb servei de Ciberacadèmia, recollida d'indicadors i coordinació amb altres àrees de l'Agència (activitats de conscienciació i comunicació i certificació de les entitats).

**Altres consideracions sobre els materials nous que s'elaborin.**

Qualsevol suport gràfic o material utilitzat durant els materials formatius haurà d'incloure el logotip de l'Agència, el SISCAT i el de la Generalitat de Catalunya com a obligatori i ha de preveure la personalització de l'entitat hospitalària o centre sanitari.

A més, per garantir l'èxit d'aquest servei i justificar la facturació mensual, l'adjudicatari haurà de recollir i organitzar com a mínim aquests documents per a cada carpeta d'entitat:

- Pla de formació en ciberseguretat actualitzat per entitat.
- Informe d'avaluació dels alumnes inscrits i satisfacció del servei de cada edició realitzada: un document que detalli el resum d'impacte, els resultats de l'acció formativa, el temps emprat, la valoració de l'alumnat i les observacions per la millora de continguts i context de fer el curs.
- Recull d'indicadors i mètriques agregat per mesurar l'impacte de forma mensual sobre els objectius previstos per entitat.

## 2.3 Lot 2: Contingut bàsic i específic de formació en ciberseguretat i suport per la capacitació de plantilles de serveis d'atenció primària, serveis d'assistència sociosanitària i serveis de salut mental

### 2.3.1 Objecte i abast dels serveis

L'objecte de la present licitació és la contractació de serveis de suport a la formació i capacitació en ciberseguretat per a plantilles de l'àmbit sanitari de l'ICS (CAPs i EAPs serveis d'atenció primària pública del sistema sanitari català), dels consorcis sanitaris d'atenció primària i entitats de base associativa o fundacions que presten serveis d'atenció primària.

I també els serveis d'atenció intermèdia i salut mental, com són els centres d'atenció sociosanitària (residències i centres vinculats a hospitals), els vinculats a l'ICS (unitats d'atenció intermèdia i salut mental CSMA i CSMIJ pròpies en hospitals), dels consorcis sanitaris o empreses públiques locals o comarcals, centres específics i entitats del tercer sector o fundacions privades hospitalàries que gestionen centres sociosanitaris.

Els serveis que inclouran són la creació de continguts en ciberseguretat adaptat pels centres d'atenció primària per a als professionals de l'àmbit sanitari (professions sanitàries: metges i metgesses de família, pediatria, especialistes de medicina comunitària, infermers i infermeres; altres professionals de suport: treballadors socials sanitaris, psicòlegs clínics, fisioterapeutes; no assistencials: personal de recepció i administració i documentació clínica, personal de gestió i especialistes en sistemes d'informació), el disseny d'activitats formatives bàsiques i específiques adaptades a les necessitats, la dinamització dels cursos i activitats formatives en diferents plataformes.

I també la creació de contingut adaptat pels centres sociosanitaris i de salut mental per a als professionals de l'àmbit sanitari (professions sanitàries: infermers i infermeres, metges i metgesses en psicofarmacologia, psiquiatres; altres professionals de suport: treballadors socials sanitaris, psicòlegs clínics, psicoterapeutes i fisioterapeutes, terapeutes ocupacionals, educadors socials; no assistencials: personal d'admissions i gestió de pacients, administració i documentació clínica, seguretat i vigilància, personal de gestió i especialistes en sistemes d'informació), el disseny d'activitats formatives bàsiques i específiques adaptades a les necessitats, la dinamització dels cursos i activitats formatives en diferents plataformes

La coordinació dels diferents actors implicats en aquest contextos per a la seva realització.

En concret els objectius que es persegueixen i que es volen assolir amb la contractació d'aquest servei són:

- Adaptació de contingut bàsic de ciberseguretat de les diferents plantilles de les entitats.
- Creació de contingut específic de ciberseguretat per a grups professionals.
- Coordinació amb les diferents persones responsables de formació i gestores del projecte en les entitats destinatàries.
- Gestió de les diferents activitats dinamitzadores per desenvolupar les activitats formatives dissenyades dins el calendari previst i en les diferents plataformes de formació.
- Alineació de continguts de ciberseguretat avançada per a professionals tècnics IT de les entitats amb els serveis de la Ciberacadèmia de l'Agència.

Els destinataris de les formacions seran les plantilles d'**unes 60 entitats proveïdores de serveis d'atenció primària**, prop del 50% sota el paraigua d'entitats hospitalàries i la resta depenen de consorcis amb ajuntaments o consells comarcals.

Cada una d'aquestes plantilles de serveis d'atenció primària es poden classificar per aquests grups d'activitat:

**Personal assistencial sanitari**
Metges/esses de família
Pediatria
Especialistes de medicina comunitària
Infermers/es
Auxiliars d'infermeria
**Personal de suport**
Treballadors socials sanitaris
Psicòlegs clínics
Fisioterapeutes
**Personal no assistencial**
Personal de recepció i gestió de cites
Administració i documentació clínica
Serveis generals (neteja, manteniment)
Seguretat i vigilància
**Gestió**
Direcció
Servei tècnic no IT (compres, finances, recursos humans)
**Especialistes en TIC i sistemes d'informació**

També s'adreçarà a les plantilles de serveis d'atenció intermèdia, sociosanitaris o salut mental. Representen al voltant de 65.000 persones que pertanyen a **88 entitats sociosanitàries i 62 entitats proveïdores de serveis de salut mental**. Aquestes plantilles es poden classificar per aquests grups d'activitat:

**Personal assistencial sanitari**
Metges/esses especialistes medicina interna
Metges/esses en geriatria
Psiquiatres
Metges/esses especialistes en psicofarmacologia
Infermers/es
Auxiliars d'infermeria
**Personal de suport**
Treballadors socials sanitaris
Psicòlegs clínics
Psicoterapeutes
Fisioterapeutes
Terapeutes ocupacionals
Educadors socials
Auxiliars de geriatria
Personal d'atenció directa (assistents de cura o acompanyament)
Camillers
**Personal no assistencial**
Personal de recepció i gestió de cites
Personal d'admissions i gestió de pacients
Administració i documentació clínica
Serveis generals (neteja, manteniment)
Servei de cuina
Seguretat i vigilància
**Gestió**

Direcció
Servei tècnic no IT (compres, finances, recursos humans)
Coordinació de serveis
**Especialistes en TIC i sistemes d'informació**

Tot seguit es descriuen les principals activitats i funcionalitats que s'esperen pel servei que es crea en aquestes entitats:

- Funcionament coordinat i difusió d'esquema de treball de l'Oficina tècnica de formació.
- Adaptació de contingut bàsic i, elaboració i gestió del contingut específic de capacitació de ciberseguretat.
- Gestió dels nivells d'itineraris formatius que permetin orientar i enrolar els usuaris participants cap a l'activitat formativa de la Ciberacadèmia de l'Agència.

Adaptació a la plataforma per a cursos virtuals:

Les activitats formatives es desenvoluparan en les plataformes de referència pels alumnes participants, pròpies de l'entitat de serveis a qui ens adrecem o les plataformes cedides pel Departament de Salut o l'ICS. Segons les preferències dels serveis de primària o serveis d'atenció intermèdia, sociosanitaris i salut mental que ens adrecem s'haurà d'adaptar el contingut per a:

a. La plataforma TALICS, amb *Cornerstone OnDemand***,** per gestionar la formació del personal sanitari de les primàries i de serveis d'atenció intermèdies on treballen professionals de l'ICS (CAPS, ).
b. Campus de ciberseguretat del Departament de Salut https://formacio.salut.gencat.cat/ amb usuari i credencials gestionades de Moodle per a responsables de formació de cada entitat o servei d'assistència primària o servei d'assistència sociosanitària o salut mental, de consorcis o empreses públiques.
c. Plataforma pròpia de cada entitat o fundació, sempre que siguin entorns LMS Moodle o Canva gestionats per ells mateixos i que permeti l'execució del curs en format SCORM.

#### 2.3.1.1 Activitats formatives bàsiques en ciberseguretat

Els continguts de les activitats formatives bàsiques de ciberseguretat que s'han d'adaptar per als diferents col·lectius s'inspiraran al nivell bàsic comú que ha estat disponible per a hospitals i alineades amb el marc de competències digitals DigComp 3.0, apartat 4 *Cybersecurity and Safety competence*. Aquest continguts adaptats cercaran una simplificació i ajustament per als serveis d'atenció primària, serveis sociosanitaris i serveis de salut mental als que han rebut de manera transversal tots els professionals d'àmbit hospitalari, extraient nous exemples de casos d'ús que apliquin i actualitzats al temps present.

Així es definiran els mòduls bàsics:

Mòdul 1C. Amenaces als sistemes d'informació sanitaris

Conceptes i temes tractats: atac de phishing, atac de ransomware, fuita de dades, metadades, seguretat física i protecció de dispositius, prevenció d'IoT i electromedicina

Mòdul 2C. Bones pràctiques en les TIC

Conceptes i temes tractats: eines col·laboratives, autenticació i gestió de credencials, certificats digitals i xifrat, notificació d'incidents.

Mòdul 3C. Protecció de dades personals

Conceptes i temes tractats: RGPD, polítiques de protecció de dades, història clínica.

### 2.3.1.2 Competències digitals que es volen desenvolupar

- Ser conscient de la naturalesa canviant dels riscos i amenaces en entorns digitals, i tenir en compte la seguretat dels dispositius digitals i el contingut (a les aplicacions que usem en els dispositius de treball, en les comunicacions diàries, en la navegació a Internet, en la compartició de dades al núvol...).
- Avaluar i gestionar els riscos de privadesa i protegir les dades personals i la privadesa en entorns digitals. Utilitzar i compartir les dades personals pròpies i d'altres de manera segura, ètica i responsable.
- Utilitzar les tecnologies digitals de forma que donin suport al benestar i la inclusió. Minimitzar els riscos i les amenaces per al benestar físic, mental i social d'un mateix i dels altres en utilitzar les tecnologies digitals.
- Saber protegir-se d'atacs que esdevenen a la xarxa, incorporar mesures de protecció o alertar de les situacions que resolen els serveis de suport.
- Entendre l'alineament amb les polítiques de seguretat que es defineixen per al compliment normatiu.

### 2.3.1.3 Producció de contingut de formació específic

El nou contingut que cal desenvolupar tindrà mòduls en un nivell intermig i en un avançat que s'adaptaran a la realitat de cada grup professional destinatari.

A tall d'exemples d'estructures aquestes són línies de desenvolupament de nous mòduls formatius i els temes clau que ha de resoldre el licitant:

- Mòduls per a serveis d'atenció primària:

A. Personal assistencial sanitari

| | | |
|---|---|---|
| Intermig<br><br>Mòdul 4PAS i Mòdul 5PAS | **Ciberhigiene a la consulta del CAP** | Contrasenyes i MFA; reconeixement de phishing/smishing; ús segur de correu i missatgeria clínica; bones pràctiques amb dispositius mòbils (BYOD) |
| | **Privacitat i seguretat en la història clínica** | Principi de mínima informació; rols/perfils d'accés; confidencialitat en espais compartits; impressió/escaneig segur de documents clínics |
| Avançat<br><br>Mòdul 6PAS i Mòdul 7PAS | **Teleassistència i telemonitoratge segurs** | Privacitat en vídeoconsulta; configuració i entorns domèstics segurs del pacient; xifrat i canals; registre i custòdia de fitxers multimèdia |
| | **Resposta a incidents i continuïtat assistencial** | Procediments davant ransomware/phishing; comunicació interna; derivació/contingència; notificació i aprenentatge de l'incident |

B. Personal de suport

| | | |
|---|---|---|
| Intermig<br><br>Mòdul 4PSU i Mòdul 5PSU | **Conscienciació i enginyeria social en assistència de gent gran** | Identificació de trucs d'engany; verificació d'identitat; compartició mínima de dades; com reportar sospites |
| | **Mobilitat segura i documents sensibles** | Custòdia física de informes; ús de tauletes/mòbils en sessions; esborrat segur i comparticions temporals; impressió segura |
| Avançat | **Telerehabilitació/telepsicologia segura** | Plataformes conformes; consentiments i informació al pacient; entorns privats; gestió de fitxers de sessió i còpies de seguretat |

| | | |
|---|---|---|
| Mòdul 6PSU i Mòdul 7PSU | **Gestió d'incidents fora de consulta** | Protocols de contenció; cadena de custòdia d'equipament; comunicació amb TI; registre i tancament de l'incident |

C. Personal no assistencial

| | | |
|---|---|---|
| Intermig | **Recepció segura i gestió de cites** | Validació d'identitat; confidencialitat al mostrador; prevenció de filtracions verbals/visuals; gestió de cues i documents |
| Mòdul 4PNA i Mòdul 5PNA | **Oficina segura (correu, fitxers, impressió)** | Detecció de phishing; macros i codi maliciós; comparticions i permisos; impressió amb validació prèvia |
| Avançat | **Governança i compliment bàsic** | Registres d'accés; retenció/minimització; gestió de peticions de drets; preparació per autoavaluacions (DSPT/IG equivalents) |
| Mòdul 6PNA i Mòdul 7PNA | **Seguretat física i control d'accés** | Acreditacions; prevenció de *tailgating*; zones restringides; coordinació amb vigilància i manteniment |

D. Gestió

| | | |
|---|---|---|
| Intermig Mòdul 4PG i Mòdul 5PG | **Cultura de ciberseguretat i factor humà** | Lideratge en sensibilització; polítiques de seguretat i comunicació; incentius i formació; indicadors bàsics de progrés |
| | **Gestió de riscos i continuïtat** | Avaluació de riscos; dependències crítiques (Història clínica, cites, telefonia); plans de contingència CAP; simulacres |
| Avançat Mòdul 6PG i Mòdul 7PG | **Proveïdors i cadena de subministrament** | Identificar riscos (due diligence); clàusules de seguretat/privacitat; riscos de tercers; seguiment de SLA i compliance; Atacs de BEC i cadena de subministrament |
| | **Gestió de crisis** | Presa de decisions (en cas de ransomware); comunicació amb parts interessades; recuperació; lliçons apreses i millora contínua |

E. Especialistes en TIC i sistemes d'informació

Es coordinaran els continguts de mòduls que es proveiran des del Lot 1 d'aquesta licitació.

- Mòduls per a serveis d'atenció sociosanitària i salut mental:

A. Personal assistencial sanitari

| | | |
|---|---|---|
| Intermig | **Ciberhigiene clínica** | Contrasenyes robustes i MFA; reconeixement de phishing; ús segur de correu i missatgeria; bones pràctiques amb dispositius mòbils |
| Mòdul 4PAS i Mòdul 5PAS | **Privacitat i seguretat en Història clínica** | Principi de mínima informació; rols/perfils d'accés; confidencialitat en espais compartits; impressió/escaneig segur de documents clínics |
| Avançat | **Teleassistència i telepsiquiatria segures** | Privacitat en vídeoconsulta; configuració segura; xifrat de comunicacions; custòdia de fitxers multimèdia |
| Mòdul 6PAS i Mòdul 7PAS | **Resposta a incidents clínics** | Procediments davant ransomware/phishing; comunicació interna; derivació/contingència; notificació i aprenentatge de l'incident |

B. Personal de suport

| | | |
|---|---|---|
| Intermig | **Conscienciació i enginyeria social en assistència de gent gran** | Identificació de trucs d'engany; verificació d'identitat; compartició mínima; report de sospites |

| | | |
|---|---|---|
| Mòdul 4PSU i Mòdul 5PSU | **Mobilitat segura i custòdia de documents** | Ús segur de mòbils/tauletes; esborrat segur; comparticions temporals; impressió segura |
| Avançat<br>Mòdul 6PSU i Mòdul 7PSU | **Telerehabilitació i telepsicologia segura** | Plataformes conformes; consentiments; entorns privats; gestió de fitxers de sessió |
| | **Gestió d'incidents fora d'unitat** | Protocols de contenció; cadena de custòdia; comunicació amb TI; registre i tancament |

C. Personal no assistencial

| | | |
|---|---|---|
| Intermig<br>Mòdul 4PNA i Mòdul 5PNA | **Recepció segura i gestió de cites** | Validació d'identitat; confidencialitat al mostrador; prevenció de filtracions; gestió de cues |
| | **Oficina segura (correu, fitxers, impressió)** | Detecció de phishing/adjunts; macros i codi maliciós; comparticions i permisos; impressió amb validació prèvia |
| Avançat<br>Mòdul 6PNA i Mòdul 7PNA | **Governança i compliment bàsic** | Registres d'accés; retenció/minimització; gestió de drets; autoavaluacions |
| | **Seguretat física i control d'accés** | Acreditacions; prevenció de *tailgating*; zones restringides; coordinació amb vigilància |

D. Gestió

| | | |
|---|---|---|
| Intermig<br>Mòdul 4PG i Mòdul 5PG | **Cultura de ciberseguretat i factor humà** | Lideratge en sensibilització; polítiques de seguretat i comunicació; incentius i formació; indicadors bàsics |
| | **Gestió de riscos i continuïtat** | Avaluació de riscos; dependències crítiques; plans de contingència; simulacres |
| Avançat<br>Mòdul 6PG i Mòdul 7PG | **Proveïdors i cadena de subministrament** | Identificar riscos (due diligence); clàusules de seguretat; riscos de tercers; seguiment de SLA; Atacs de BEC i cadena de subministrament |
| | **Gestió de crisis** | Presa de decisions (en cas de ransomware); comunicació amb parts interessades; recuperació; lliçons apreses |

E. Especialistes en TIC i sistemes d'informació

Es coordinaran els continguts de mòduls que es proveiran des del Lot 1 d'aquesta licitació.

Les dues estructures de continguts, tot i ser molt semblants, cal considerar aquests atributs en preparar-los:

- Com que els professionals que es volen formar desconeixen els tecnicismes de la ciberseguretat s'ha d'adaptar el llenguatge (sobretot pels professionals assistencials i de suport) i els casos d'ús escollits com exemples il·lustratius per fer més efectiva la formació.
- Redactar continguts efectius i personalitzats per a cada segment del públic objectiu, adaptant-se a les seves necessitats específiques i nivells de comprensió en matèria de ciberseguretat.
- Els continguts dedicats a gerents i càrrecs directius han de posar especial èmfasi en aspectes com l'impacte econòmic dels ciberatacs i els beneficis de les inversions en ciberseguretat, entre altres.

- En els elements fabricats amb formats com infografies, presentacions de webinars/seminaris, vídeos divulgadors/interactius i els materials de comunicació cal emprar guions i recursos que siguin adaptables en els diferents contextos professionals previstos (grups A, B, C i D) i els que calgui coordinar amb el Lot 1 respecte a Especialistes en TIC (grup E).
- Tenir present altres àrees de l'Agència (com és el cas de la unitat de comunicació i l'àrea del SOC i CERT) per assegurar que el contingut sigui tècnicament precís i rellevant.

#### 2.3.1.4 Disseny i producció d'elements formatius

Algunes propietats a considerar en la qualitat dels lliurables a elaborar:

**Estil comunicatiu:** utilitzar llenguatge clar i accessible, en català normatiu, evitar tecnicismes o explicar-los amb exemples, incorporar storytelling i situacions reals per fer els conceptes comprensibles.

**Disseny visual**: crear interfícies netes amb navegació intuïtiva, colors que destaquin alertes, tipografia llegible i els recursos multimèdia seran vídeos breus, elements interactius, animacions o infografies. S'han de tenir present les característiques d'usabilitat i accessibilitat, segons les directrius de la Generalitat de Catalunya i les WCAG 2.1. Han de preveure: alternatives textuals, controls operables des de teclat, control de reproducció, contrastos gràfics (nivell AA), estructura semàntica clara, compatibilitat amb tecnologies d'assistència com els lectors de pantalla...

**Elements produïts**: prioritzar el microlearning amb mòduls poca extensió, incloure casos pràctics, simulacions interactives i gamificació per mantenir l'interès, garantint accessibilitat en tots els dispositius.

**Estratègia pedagògica**: establir una progressió gradual dels conceptes, oferir feedback immediat en activitats i adaptar exemples al context de l'usuari per personalitzar l'aprenentatge. Generar glossaris i índexs de recursos de consum no obligatori per a obtenir més informació de la ciberseguretat o ampliar conceptes.

**Confiança en els continguts**: basar-se en fonts fiables (prioritzant els de l'Agència i la Fundació TIC Salut), actualitzar periòdicament els continguts i assegurar la protecció de dades dels usuaris dins la plataforma.

Aquests elements comunicatius inclosos a les plataformes LMS amb orientació formativa es coordinarà la seva producció amb la Unitat de Comunicació de l'Agència, qui pot demanar usar dissenys amb noves tendències de mercat. Cal tenir present en el calendari d'actuació que aquest servei és crític pel desenvolupament del projecte avançar la creació de continguts el màxim possible per no condicionar les activitats dels altres serveis: dinamització de cursos i actuacions del servei de gestió d'itineraris, tecnopedagoc, assessorament...

Les característiques dels elements que han de desenvolupar-se per a construir els mòduls formatius:

- Diferents Quiz (preferentment un exercici per mòdul) per a revisar que els alumnes que han fet el mòdul en comprenen el seu contingut.

- Vídeos interactius creades amb les aplicacions H5P.com, iSpring Suite, Articulate, Loom, Panopto o Genially que siguin integrables als diferents LMS utilitzats. Aquests vídeos han de permetre fer pràctic i aplicable l'aprenentatge de ciberseguretat en els cursos en línia, per exemple amb exercicis on l'usuari pugui comprendre les conseqüències en les diferents possibilitats de decisió (amb un acurat sistema de retroaccions).

- Infografies sobre els casos d'ús rellevants que s'expliquen: per exemple, bones pràctiques pel lloc de treball, evitar els enganys digitals, ús correcte de la IA corporativa...
- Vídeos breus a Youtube que posin context sobre els tipus de riscos i tendències actuals en les amenaces de ciberseguretat del sector salut.
- Vídeos divulgatius com a tutorials per a explicar els protocols de seguretat previstos, per exemple de resposta a incidents ...
- Presentacions i documents guies que siguin suport per a seminaris o presentacions en sessions formatives síncrones que es puguin desenvolupar.

### 2.3.2 Característiques del servei

El serveix requereix d'una capacitat d'anàlisi exhaustiva per identificar les necessitats específiques de ciberseguretat dels diferents grups professionals dins de l'àmbit sanitari, incloent personal assistencial sanitari, de suport, no assistencial, de gestió (on s'inclouen càrrecs directius) i especialistes en TIC i sistemes d'informació. Així mateix, també requereix de capacitat per recopilar i analitzar les dades sobre les preferències de comunicació i hàbits de consum de mitjans d'aquests col·lectius, amb l'objectiu d'assegurar que el contingut sigui adequat i impactant per a cada segment.

Aquest anàlisi es realitzarà mitjançant enquestes als diferents tipus de serveis assistencials, de primària, sociosanitaris o salut mental, permetent definir les prioritats de les temàtiques emergents i les estratègies a seguir per maximitzar la seva aplicabilitat en el lloc de treball.

Les característiques que definiran el servei formatiu seran:

1. La sensibilització i consells en ciberseguretat seran personalitzades segons el perfil dels professionals. Per als diferents grups descrits anteriorment, es proporcionaran consells pràctics sobre ciberseguretat adaptats als seus rols.

   Per exemple, els rols de personal de suport de serveis de primària, sociosanitaris o salut mental han de rebre activitats formatives específiques que explicitin aspectes de l'impacte de la ciberseguretat o mesures de seguretat previstes en els usuaris a qui s'atén, majoritàriament usuaris amb edat avançada, exposats als enganys digitals, i que té una forta component de bretxa digital, entre altres. (Doble factor d'autenticació)

2. Les pàgines de presentació dels diferents cursos per perfil professional tindran informació sobre com es pot desenvolupar el curs (durada de temps a dedicar i període de disponibilitat), reconeixement que s'acreditarà al final de curs (certificat personal per alumne), informació sobre el sistema per obtenir APTE del curs (realització de qüestionaris o quiz), sistema de suport per resoldre dubtes previst (tot i ser preferentment un sistema autoformatiu pot haver l'opció d'elaborar apartats de preguntes i respostes freqüents sobre com funciona la plataforma), com contactar amb el responsable del curs per qualsevol altre gestió.

3. Definició i edició de particularitats per a cada curs d'entitat. En el curs de diferents mòduls s'ha de preveure que es pugui posar algunes referències documentals pròpies de l'entitat (eines col·laboratives que apliquen, sistema de notificació d'incidents, polítiques de protecció de dades...) que enfoquin els temes tractats en l'entitat que es desenvolupa la formació.

4. La dinamització, amb un perfil de docent editor a les plataformes formatives, s'ocuparà de la personalització, definició de la temporalitat i ajust de les edicions en aquestes plataformes (amb les corresponents actualitzacions i notificacions automatitzades si es requereixen) de les entitats. Ha de preveure una sistemàtica d'enrolament dels usuaris que es volen incloure a les diferents edicions formatives, confirmar el correcte desenvolupament de cada activitat, fer activitats de seguiment per maximitzar l'eficàcia de les edicions i resoldre qualsevol incidència que pugui impedir la compleció dels cursos oberts.

   Eventualment convé executar rols d'administrador a la plataforma formativa emprada per a gestionar permisos en els nous cursos o per poder extreure dades d'indicadors de l'assoliment dels alumnes matriculats i elaborar informes amb els resultats.

5. Seguiment i coordinació amb els actors claus de l'entitat que coneixen el projecte: a banda de les persones que gestionen els recursos humans i plans de formació de l'entitat cal coordinar les activitats amb els responsables de seguretat que lideren el projecte d'integració de l'Agència dins l'entitat. Per això serà important un contacte periòdic amb reunió o amb comunicacions per correu electrònic per situar l'evolució del procés formatiu.

6. Seguiment i coordinació amb els responsables del projecte dins de l'Agència. No només fer seguiment i coordinació amb el responsable de la Unitat de Cultura en ciberseguretat, qui ha de conèixer en tot moment el detall del calendari i l'esforç previst en les diferents activitats formatives, sinó també els responsables de desplegament de l'auditoria de certificació ENS o de les diferents oficines recurrents de l'Agència que intervenen amb l'entitat.

7. Preparació de documentació sobre l'execució de la formació. Cada entitat compta amb un pla de formació en ciberseguretat, que representa el pla de treball sobre totes les activitats formatives en ciberseguretat realitzades en el passat (vinculades a Informes de cursos realitzats) i les previstes pel futur (continguts i públic objectiu previstos) per l'entitat. A nivell orientatiu hi constaran les sessions en plataforma virtual i els objectius previstos per aquestes per cada any. També s'haurà de documentar les activitats de sensibilització i conscienciació previstos. L'estructura dels diferents documents existents de l'entitat quedaran indexats en aquest pla de formació en ciberseguretat.

   Aquesta documentació és clau per a obtenir evidències del procés formatiu i tenir indicadors dels resultats de la formació realitzada. Per això es recullen indicadors i mètriques per mesurar l'impacte de forma mensual que gestiona la unitat de Govern de la Dada de l'Agència per representar la situació sobre els objectius marcats per a cada entitat.

   L'informe de formació de cada edició que haurà de lliurar a l'entitat participant per recollir:

   -Resultats de la formació
   - Nombre de persones que van ser inscrites en cada edició.
   - Nombre de persones que van superar el curs (APTES).
   - Mitjana de resultats dels mòduls.
   - Visualització dels continguts complementaris.
   - Nombre d'hores que la plataforma ha estat oberta.

   -Resultats de l'enquesta de satisfacció:
   - Si ha faltat incloure o modificar algun aspecte més a la formació (millores a fer).
   - Si s'han assolit els objectius.
   - Aplicabilitat a les tasques diàries.
   - Valoració global de l'activitat formativa.

-Llistat de persones que han superat en APTE cada curs: quins usuaris es van inscriure a la plataforma del curs en ser convocats i quin nombre d'aquests l'han superat.

8. En el cas d'organització de seminaris web o altres formacions presencials (tipus taller síncron o presencials) per a determinats col·lectius, si és el cas, cal coordinar-se amb el licitant del Lot 1 per ajudar en les entitats a seguir el procediment previst.

9. Les activitats de serveis de gestió d'itineraris, tecnopedagoc, altres assessoraments que es desenvolupin pel licitant seguiran les directrius de la unitat de la Ciberacadèmia de l'Agència per a connectar les oportunitats ofertes en els itineraris de perfils disponibles amb l'estimulació de la demanda en l'àmbit sanitari, tan per upskilling o reskilling de professionals.

10. Les tasques de l'Oficina tècnica de formació de l'Agència es coordinaran amb altres proveïdors que fan activitat formativa a altres àmbits on treballa l'Agència i es seguiran les recomanacions i normes d'estandardització del procés de formació, sobre la gestió de calendari de les activitats formatives i el recursos comuns a disposar, que és responsabilitat de la Unitat de Cultura en ciberseguretat de l'Agència. És clau seguir sistematitzar al màxim i fer automatització de tasques que alliberi els esforços pels àmbits de major valor afegit.

**Calendari d'execució**

A grans trets s'espera d'aquest contracte aquesta distribució temporal que haurà de ser ajustada i planificada amb els recursos assignats pel licitador i el tipus de categoria professional destinatària:

- Fase adequació i millora de contingut bàsic existent (primer mes)
- Establiment de canal i coordinació amb responsables d'entitats destinatàries (2 mesos)
- Elaboració del nou contingut específic i pilotatge per a les diferents categories professionals (5 mesos per a principals lliurables)
- Desplegament de cursos i dinamització de les diferents edicions de cursos (des de la disponibilitat de mòduls específics fins a final de projecte).

De forma recurrent a aquestes fases: coordinació i seguiment amb els diferents promotors de la formació, actuacions del tecnopedagoc en objectius acordats amb servei de Ciberacadèmia, recollida d'indicadors i coordinació amb altres àrees de l'Agència (activitats de conscienciació i comunicació i certificació de les entitats).

**Altres consideracions sobre els materials que s'elaborin.**

Qualsevol suport gràfic o material utilitzat durant els materials formatius haurà d'incloure el logotip de l'Agència, el SISCAT i el de la Generalitat de Catalunya com a obligatori i ha de preveure la personalització del servei de primària, servei intermedi, servei sociosanitari o servei de salut mental.

A més, per garantir l'èxit d'aquest servei i justificar la facturació mensual, l'adjudicatari haurà de recollir i organitzar com a mínim aquests documents per a cada carpeta d'entitat:

- Pla de formació en ciberseguretat actualitzat per entitat.
- Informe d'avaluació dels alumnes inscrits i satisfacció del servei de cada edició realitzada: un document que detalli el resum d'impacte, els resultats de l'acció formativa, el temps emprat, la valoració de l'alumnat i les observacions per la millora de continguts i context de fer el curs.
- Recull d'indicadors i mètriques agregat per mesurar l'impacte de forma mensual sobre els objectius previstos per entitat, amb subgrups de serveis de d'atenció primària, atenció intermèdia o sociosanitària i atenció de salut mental.

# 3 Condicions d'execució del servei

## 3.1 Horaris

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

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

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

## 3.2 Localització física

Inicialment, els equips prestataris dels serveis estaran ubicats físicament a les oficines de l'adjudicatari o en alguna altra que ambdues parts acordin, atenent sempre a la seguretat de la informació gestionada pel servei. Tot i això, l'Agència considera que els recursos haurien de desplaçar-se a les instal·lacions de l'Agència de Ciberseguretat a l'Hospitalet de Llobregat només dos dies per setmana.

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

Addicionalment, les campanyes hauran d'abastar tots els centres sanitaris de Catalunya, incloent hospitals, centres sociosanitaris i d'atenció primària, podent esser necessari el desplaçament fins a la ubicació del centre sanitari en qüestió, desplaçament que anirà a càrrec de l'empresa adjudicatària.

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

## 3.3 Equip de treball

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos de l'adjudicatari del contracte basat 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 la ciberseguretat i de l'entorn del sistema sanitari integral d'utilització pública de Catalunya (SISCAT).
- Altres coneixements de l'ofici formatiu en plataformes en línia, sistemes síncrons o asíncrons necessaris per al bon desenvolupament dels serveis.

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

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

#### 3.3.1 Descripció de serveis i volums previstos a Lot 1 i Lot 2

L'adjudicatari haurà de disposar d'un servei que assumeixi les tasques:

**A. Gestió i coordinació DCP de les activitats de formació**

A aquest efecte, ha de assumir les següents responsabilitats:

- Desenvolupador del pla de formació previst per a cada entitat, coordina l'evolució dels recursos formatius i estableix la relació amb els diferents promotors i destinataris dins les entitats del sector sanitari on destinen les diferents activitats formatives. Aquest pla de formació s'actualitza amb diàleg permanent amb els responsables del projecte d'integració d'entitats del SISCAT amb l'Agència.
- Seguir l'estandardització de l'Oficina tècnica de formació de l'Agència i fer de hub de gestió de totes les necessitats expressades dins l'Agència (àrees d'Operacions, Capacitació i Promoció Ecosistema, i Certificacions) i les entitats involucrades en aquest projecte d'integració d'entitats del SISCAT amb l'Agència. Interlocució contínua amb l'Oficina de seguiment del projecte de salut de l'Agència.
- Realitzar funcions de direcció, planificació, supervisió i coordinació dels diferents equips definits en el Lot per realitzar els serveis.
- Vetllar per la correcta coordinació dels serveis del contracte tot garantint-ne l'assoliment dels objectius.
- Garantir que l'equip dels serveis objecte del contracte siguin els més adequats i vetllar per l'eficiència per l'assoliment dels objectius.
- Seguiment en l'elaboració de lliurables previstos i estructura per a ser accessibles en tot moment del projecte.

**B. Redacció i gestió de continguts**

Amb les següents responsabilitats:

- Gestió de plataformes de formació digitals previstes en cada entitat i adequació de continguts als diferents programes d'actuació segons categoria professional. Actualització de continguts segons el model de ciberseguretat que proposa l'Agència a les diferents entitats i pels diferents professionals.
- Redactar i desenvolupar els continguts redaccionals i audiovisuals que seran utilitzats en diferents formats de comunicació, com els elements necessaris dins els cursos en línia o en la realització de webinars, vídeos formatius i sessions presencials.

- Coordinar amb els serveis de comunicació corporativa de l'Agència per assegurar que els continguts escrits i visuals estan integrats de manera efectiva i segueixen el llibre d'estil i la normativa d'accessibilitat de l'Agència.
- Revisar i actualitzar contínuament els continguts per reflectir les tendències i necessitats en matèria de ciberseguretat.
- Coordinar amb altres àrees de l'Agència per a garantir que els continguts redactats siguin tècnicament correctes i pertinents per als diferents segments del públic objectiu.
- Recopilar i analitzar el feedback dels alumnes per comprendre millor la recepció dels cursos i ajustar les necessitats pedagògiques segons els perfils professionals a qui ens adrecem.
- Administrar l'arxiu de continguts elaborats i assegurar-ne l'accessibilitat i coherència.
- Vetllar perquè tots els continguts comunicatius compleixin.

**C. Dinamització de les activitats formatives**

Amb les següents responsabilitats:

- Assegurar que tots els cursos elaborats es troben disponibles i són revisats per a responsables de formació de l'Entitat sanitària destinatària. Que inclouen els logotips obligatoris de l'Agència, la Generalitat i del centre sanitari corresponent.
- Preparació amb els responsables de les entitats de les diferents edicions de cursos, gestió de calendari previst en cada entitat i enrolament d'usuaris les diferents edicions si és necessari.
- Suport a resoldre problemes d'inscripció o correcta realització dels cursos que puguin sorgir pel tipus de plataforma formativa emprada.
- Proposar millores al servei de redacció en base a la resposta de les diferents edicions elaborades per les entitats.
- Mantenir contacte i seguiment per a la correcta realització de les edicions formatives amb una voluntat d'optimitzar el recurs i els objectius formatius en tots els usuaris previstos. Completar recomanacions i requeriments als responsables de les formacions en les entitats per a complir estàndards de qualitat del servei (recordatoris d'avanç en els mòduls, comunicacions paral·leles...).
- Comunicació permanent per assegurar l'avenç de l'activitat a les entitats i recollida periòdica d'indicadors previstos en el projecte.
- Trasllat de principals elements i problemes a resoldre a través de la coordinació del servei o a través de diferents responsables del projecte de salut de l'Agència (interlocutor de l'Oficina de seguiment del projecte de salut).
- Suport a l'organització de webinars o activitats presencials en diferents tasques de convocatòria, seguiment dels continguts previstos o dinamització/lideratge en la comunicació requerida davant els usuaris (en xats o en videoconferència).
- Elaboració i actualització de lliurables previstos per a cada entitat: pla de formació en ciberseguretat per entitat i informe de formació de cada edició.

**D. Serveis de gestió d'itineraris, tecnopedagoc, assessorament...**

Amb les següents responsabilitats:

- Coordinació amb els diferents referents del projecte de cada entitat per a determinar els usuaris amb un pla de carrera que els aplica el coneixement més avançat de temàtiques de ciberseguretat. En aquesta coordinació d'identifiquen bones pràctiques i activitats històricament desenvolupades.
- Proposar activitats síncrones o materials a elaborar (organització de seminaris web o altres formacions presencials) per a col·lectius específics amb l'objectiu de resoldre metodologies d'integració amb l'Agència i planificar possibles admissions al servei de la Ciberacadèmia.

- Desenvolupar l'activitat amb el suport de la dinamització i redacció de continguts, amb el rol de conductor i gestor de les intervencions amb diferents nivells d'expertesa dins les entitats sanitaris, a l'Agència o per tercers.

- Coordinar amb la unitat de la Ciberacadèmia de l'Agència per a entendre les oportunitats en els itineraris de perfils disponibles que garanteixi que l'àmbit sanitari, tan per upskilling o reskilling de professionals, participa i connecta amb el servei.

Els licitadors hauran d'incloure en la seva proposta l'organigrama i esquemes d'equips per tal de donar resposta als serveis descrits en aquest plec.

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

L'estimació aproximada d'hores efectives necessàries per l'execució dels serveis demanats, per una durada de 24 mesos, en aquest plec és de 9.420 hores pel Lot 1 i de 15.475 hores pel Lot 2.

Dins d'aquest volum estimatiu d'hores, es desprèn aquesta distribució d'hores mínimes per la totalitat del contracte i dels perfils necessaris en els serveis indicats i per a cada Lot:

**Lot 1**

| Perfil / servei | Hores mínimes estimades |
|---|---|
| Gestió i coordinació DCP activitats de formació | 2.245 hores (22-24%) |
| Redacció i gestió de contingut capacitador | 3.200 hores (33-35%) |
| Servei de dinamització d'activitats | 2.750 hores (29-31%) |
| Serveis de gestió d'itineraris, tecnopedagoc, assessorament... | 1.225 hores (12-13%) |

**Lot 2**

| Perfil / servei | Hores mínimes estimades |
|---|---|
| Gestió i coordinació DCP activitats de formació | 3.200 hores (20-22%) |
| Redacció i gestió de contingut capacitador | 5.000 hores (30-32%) |
| Servei de dinamització d'activitats | 6.300 hores (39-41%) |
| Serveis de gestió d'itineraris, tecnopedagoc, assessorament... | 965 hores (5-6%) |

La distribució d'esforç expressada s'ha d'entendre com a mínims aproximats, podent els licitadors ampliar-los i millorar-los a les seves ofertes.

La distribució de consum d'aquestes hores no serà homogènia durant tots els mesos de contracte i s'elaborarà proposta segons perfil de demanda estimat. En aquest sentit és convenient que els serveis de redacció i adaptació/personalització de continguts s'avantposin als altres serveis i es reservi capacitat per a manteniment o ajustament segons resposta de les activitats formatives realitzades.

### 3.3.2 Perfils

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

| PERFIL | REQUISITS |
|---|---|
| Gestió i coordinació DCP activitats de formació | – Titulacions:<br>Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en l'àrea de gestió de projecte i, a poder ser, de l'àmbit formatiu en ciberseguretat.<br><br>– Experiència:<br>5 anys en aspectes pedagògics, elaboració de metodologia de formació i adequació a continguts tècnics a entorns concrets d'especificitat (segons nivell d'usuari i sectors).<br>Valorable l'experiència en projectes en el sector sanitari.<br><br>– Coneixements:<br>Coneixement acreditat d'un nivell de suficiència C2 o nivell superior de la llengua catalana.<br>Acreditar un domini avançat de la llengua per a les imprescindibles tasques de revisió i acceptació de producte acabat<br>Administrador d'entorns virtuals d'aprenentatge (tipus Moodle o Canvas), d'eines de seguiment de projectes (gestió d'equips i control de recursos, com d'elaboració de quadres d'indicadors d'execució i seguiment).<br>Idiomes: anglès<br><br>– Aptituds:<br>Iniciativa, proactivitat, autonomia i motivació.<br>Capacitat de treballar i liderar un equip.<br>Destresa comunicativa oral i escrita. |
| Redacció i gestió de contingut capacitador | – Titulacions:<br>Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en l'àrea de formació en tecnologia o de comunicació digital<br>Coneixement acreditat d'un nivell de suficiència C2 o nivell superior de la llengua catalana.<br><br>– Experiència:<br>2 anys en tasques educatives, de l'àmbit formatiu en ciberseguretat, creació i redacció de contingut pedagògic i adequació a continguts tècnics a entorns concrets d'especificitat (segons nivell d'usuari i sectors).<br>1 any en relació la creació de contingut en eines de vídeo interactiu<br>Valorable l'experiència en projectes en el sector sanitari.<br><br>– Coneixements:<br>Dinamitzador/administrador d'entorns virtuals d'aprenentatge (tipus Moodle, Canva, Cornerstone o similars).<br>Usuari avançat en eines de creació de continguts audiovisuals.<br>Usuari avançat en eines de creació d'anotacions interactives (preguntes incrustades) i de gamificació del tipus Kami, Nearpod, Edpuzzle, Genially (escape rooms digitals) i de seguiment del progrés dels participants, (o amb funcionalitats similars).<br>Usuari avançat en eines d'enriquiment en continguts audiovisuals com H5P.com, iSpring Suite, Articulate, Loom o Panopto (o amb funcionalitats similars).<br>Idiomes: anglès.<br><br>– Aptituds:<br>Capacitat de treballar en equip.<br>Capacitat analítica i d'adaptació de casos d'ús.<br>Domini de la llengua, claredat en l'expressió, llenguatge culte. |

| | |
|---|---|
| | Capacitat de sistematitzar i adaptar continguts a diferents. |
| Dinamització d'activitats | – Titulacions:<br>Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en l'àrea de formació en ciberseguretat.<br><br>– Experiència:<br>2 anys en activitats de conscienciació o formació en ciberseguretat, desenvolupament de plans de formació en plataforma digital i adequació a continguts tècnics a entorns concrets d'especificitat (segons nivell d'usuari i sectors).<br>2 anys d'experiència en la dinamització d'entorns virtuals d'aprenentatge (tipus Moodle, Canva, Cornerstone o similars).<br><br>Valorable l'experiència en projectes en el sector sanitari.<br><br>– Coneixements:<br>Dinamitzador/administrador d'entorns virtuals d'aprenentatge (tipus Moodle, Canva, Cornerstone o similars).<br>Coneixement acreditat d'un nivell de suficiència C2 o nivell superior de la llengua catalana.<br>màster oficial de formació de professorat per ESO i Batxillerat, FP i Ensenyament d'Idiomes<br>Noves tecnologies, amenaces i atacs cibernètics, protecció de dades.<br>Coneixement avançat de la plataforma de seminaris ZOOM o similars.<br>Idiomes: anglès.<br><br>– Aptituds:<br>Capacitat de treballar en equip.<br>Capacitat analítica.<br>Domini de la llengua, claredat en l'expressió en informes i comunicacions de plataforma, llenguatge culte.<br>Resolució de problemes i donar suport a usuaris. |
| Gestió d'itineraris, tecnopedagoc, assessorament a alumnes | – Titulacions:<br>Titulació universitària o formació equivalent (incloent, però no només, Formació Professional) en l'àrea de formació en ciberseguretat<br><br>– Experiència:<br>3 anys en projectes pedagògics, elaboració de metodologia de formació i adequació de continguts tècnics a entorns concrets d'especificitat (segons nivell d'usuari i sectors).<br>2 anys en aspectes pedagògics, elaboració de metodologia de formació ciberseguretat i adequació a continguts tècnics a entorns o sectors concrets d'especificitat (segons nivell d'usuari i sectors).<br>1 any en la creació de webinars o vídeotutorials formatius.<br>2 anys d'experiència en el sector de la ciberseguretat, en participació directe o autoria en:<br>-materials educatius en capacitació avançada en ciberseguretat.<br>-plans de creació de capacitació en matèria de recursos humans en ciberseguretat<br>-desenvolupament de polítiques educatives, formatives i de sensibilització en ciberseguretat.<br>Valorable l'experiència en projectes en el sector sanitari.<br><br>– Coneixements:<br>Domini de la llengua, claredat en l'expressió, llenguatge culte i dots de comunicació verbal.<br>Coneixement acreditat d'un nivell de suficiència C1 o nivell superior de la llengua catalana.<br><br>– Aptituds:<br>Iniciativa, proactivitat, autonomia i motivació.<br>Capacitat de treballar en equip.<br>Destresa comunicativa oral i escrita<br>Resolució de problemes<br>Pensament creatiu / lateral<br>Capacitat d'anàlisi i síntesi |

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

### 3.4 Canvi de recurs

L'Agència tindrà dret a exigir justificadament a l'adjudicatari del contracte basat 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 basat. 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.

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

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

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

### 3.6 Eines i equipament per a la prestació de serveis

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

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

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l'Agència.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides l'Agència.
- Telefonia fixa a les instal·lacions del servei.

- Telefonia mòbil per donar cobertura als serveis de guàrdia.
- Accés a Internet a través de la xarxa d'àrea local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.

L'Agència no proveirà:

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

En conseqüència, els adjudicataris hauran de:

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

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

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

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

### 3.7 Gestió del coneixement

Amb l'objectiu de garantir que l'Agència disposi del coneixement necessari per a la correcta execució de les seves funcions i, especialment, l'impuls de la transformació fonamentada en el coneixement col·laboratiu, la coordinació de l'ecosistema de ciberseguretat i la voluntat per la innovació continua, es requereix que l'empresa adjudicatària registri tot el coneixement que disposi i es generi en la contractació basada que derivi del present Acord Marc.

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 basat, tant l'empresa adjudicatària com el personal de l'empresa adjudicatària s'haurà de sotmetre a les polítiques i regulacions internes que estableix el servei de Seguretat Corporativa en matèria de seguretat de la informació:

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes pel servei de 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.
- Acceptar les normes i polítiques que estableix el servei 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 la unitat 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, RGPD, LOPDGDD, NIS2, LSSI, etc.).

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

### 3.9 Control de Gestió

L'empresa adjudicatària del contracte basat, 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 els informes 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.

D'altra banda, la producció i impressió dels materials necessaris per a la realització del servei anirà a càrrec de l'empresa adjudicatària.

### 3.11 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 licitador, que inclouran:

- Estacions de treball amb el programari adequat per realitzar les tasques descrites.
- Comunicacions d'accés a les aplicacions informàtiques.
- Telefonia fixa a les instal·lacions del servei.
- Accés a Internet a través de la xarxa d'àrea local.
- Espai suficient per allotjar en condicions de treball òptimes:
    - El personal necessari de l'adjudicatari per realitzar el servei 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.

### 3.12 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 basat.

### 3.13 Seguretat

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

#### 3.13.1 Deure de confidencialitat

Tot el personal de l'empresa adjudicatària així com els possibles subcontractistes han de mantenir absoluta confidencialitat i estricte secret sobre la informació coneguda arrel de l'execució dels serveis contractats. Aquesta obligació de confidencialitat s'haurà de mantenir durant 10 anys, o el que s'especifiqui en el contracte basat, 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.

#### 3.13.2 Dades de caràcter personal

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

#### 3.13.3 Compliment del marc legal de ciberseguretat i del marc normatiu intern

L'empresa adjudicatària del contracte basat 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 basat 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 podrà requerir a l'empresa adjudicatària del contracte basat el lliurament de la documentació acreditativa de la conformitat amb l'ENS. L'empresa adjudicatària del contracte basat haurà de designar, segons estableix l'ENS, un punt de contacte per a la seguretat (POC) que canalitzarà i supervisarà el compliment dels requisits

de seguretat de la informació i la gestió dels incidents que es puguin produir durant l'execució del contracte.

A més de l'ENS i la normativa i guies tècniques que el desenvolupen, l'empresa adjudicatària del contracte basat 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. 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 basat haurà de desenvolupar els procediments que siguin necessaris per a poder aplicar el marc normatiu.

#### 3.13.4 Capacitat tècnica

Per a poder executar el contracte i oferir garanties de la seva capacitat tècnica, l'empresa adjudicatària del contracte basat 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 basat 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.

#### 3.13.5 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 basat 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 Centro Criptológico Nacional o bé complir amb els criteris que estableixi el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional o, en el seu defecte, acreditar que el producte o servei disposa de requeriments equivalents.

### 3.13.6 Interconnexions

Segons preveu l'ENS, en el cas que sigui necessari realitzar interconnexions entre sistemes de l'empresa adjudicatària del contracte basat 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 basat 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 basat 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.

### 3.13.7 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 basat 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.

### 3.13.8 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 basat 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 basat 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.

### 3.13.9 Accés a la informació

L'empresa adjudicatària del contracte basat 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 estabiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat a aquesta informació, establint els controls de seguretat mínims.

## 3.14 Assegurament i control de la qualitat i la millora contínua

L'empresa ha de vetllar per l'excel·lència i millora contínua dels processos, components tècnics i serveis sota el seu abast.

Per tal de garantir que s'aborda la qualitat i la millora, l'adjudicatari haurà d'elaborar, mantenir i

executar un "Pla de Qualitat i Millora Contínua" que inclogui, entre d'altres:

- Anàlisi i avaluació de les dades obtingudes de la mesura del servei, tant de producció i activitat com de gestió de l'incidental i operació.
- Plans de millora del servei orientats a millorar el compliment dels objectius del servei i del negoci.
- Accions per l'assegurament i control de la qualitat (revisions, proves, etc.), amb major rigor, intensitat i profunditat segons la criticitat del projecte/servei/component.
- Accions per reduir el nombre d'incidències, problemes freqüents i el suport.
- Accions per millorar la qualitat percebuda i la satisfacció dels usuaris.
- Accions preventives per la mitigació de riscos, tenint en compte la seva probabilitat i el seu impacte.
- Accions dirigides a millorar la gestió del coneixement i incrementar la usabilitat dels serveis.
- Accions per maximitzar l'eficiència i la sostenibilitat del servei.

## 3.15 Seguiment del servei

Les empreses adjudicatària haurà de presentar un informe de seguiment. 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 basat, amb indicació de les activitats realitzades i les previstes realitzar, les volumetries globals d'activitat i els indicadors de compliment especificats als. Acords de Nivell de Servei (ANS) de cada basat.
- Un informe de dedicació del basat a les diferents funcions requerides, per tal de poder avaluar la distribució dels esforços.
- Un informe d'accions de millora de l'activitat del propi basat, 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 basat o el que es determini per part del responsable del contracte de l'Agència de Ciberseguretat.

Si existeix cap especificitat en aquest sentit, es recollirà al basat corresponent.

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

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

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

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

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

### 3.16 Integració amb altres equips

L'adjudicatari del contracte basat 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.


ciberseguretat.gencat.cat